Ethical hacking and Penetration Testing

Infrastructure attacks. Metasploit Framework

Author: Kutlymurat Mambetniyazov (@manfromkz)

Identifying the goals of lesson

- Understanding basic terms
- Practicing post-exploitation techniques and privilege escalation
- Practicing Metasploit Framework
- Practicing Merlin C2

What is post-exploitation?

- **Post-exploitation** is any action taken after gaining shell

- Examples:
  - escalating privileges
  - persistence
  - pivoting
  - dumping hashes, passwords
  - internal resources enumeration
  - etc.

What is privilege escalation?

- **Privilege escalation (privesc)** means users receive privileges they are not entitled to.

- For example, you've hacked web server and have www-data web shell. Gaining shell as another user (example, root or NT/SYSTEM) using current shell is privilege escalation.

Windows privesc

- Checklist - https://book.hacktricks.xyz/windows/checklist-windows-privilege-escalation

- Automated enumeration scripts:
  - winPEAS - https://github.com/carlospolop/PEASS-ng/tree/master/winPEAS
  - WES-NG - https://github.com/bitsadmin/wesng

- Useful resources:
  - LOLBAS - https://lolbas-project.github.io/

Windows privesc practice

- Room - https://tryhackme.com/room/windows10privesc

Linux privesc

- Checklist - https://book.hacktricks.xyz/linux-unix/linux-privilege-escalation-checklist

- Automated enumeration scripts:
  - linPEAS - https://github.com/carlospolop/PEASS-ng/tree/master/linPEAS
  - LES - https://github.com/mzet-/linux-exploit-suggester
  - LES2 - https://github.com/jondonas/linux-exploit-suggester-2

- Useful resources:
  - GTFOBins - https://gtfobins.github.io/

Linux privesc practice

- Room - https://tryhackme.com/room/linuxprivesc

Active Directory attacks

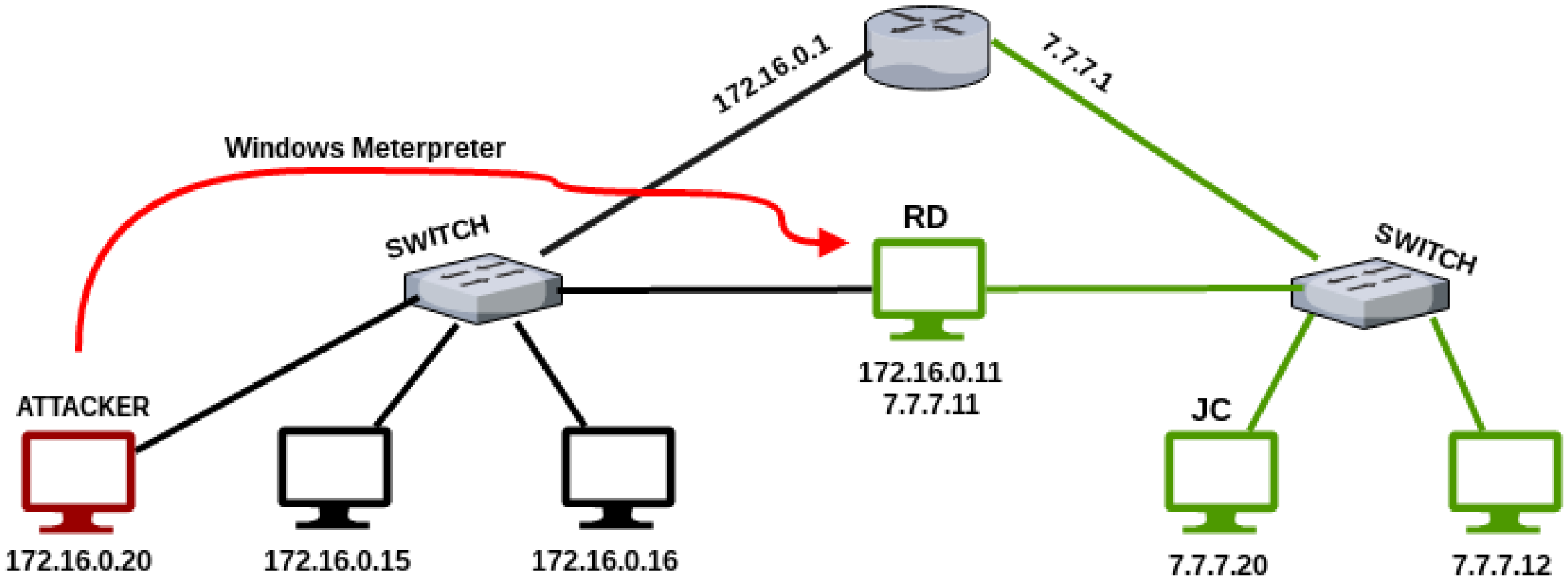
- Cheat sheet - https://zer1t0.gitlab.io/posts/attacking_ad

- Useful tools:
  - Bloodhound
  - Rubeus
  - mimikatz
  - Impacket
  - etc.

What is pivoting?

- **Pivoting** is the unique technique of using an instance (also referred to as a ‘plant’ or ‘foothold’) to be able to move around inside a network.

- Popular tools:
  - Chisel - https://github.com/jpillora/chisel
  - SSH
  - Ncat
  - Metasploit
  - etc.


172.16.0.1
7.7.7.1
Windows Meterpreter
SWITCH
RD
SWITCH
ATTACKER
172.16.0.11
7.7.7.11
JC
172.16.0.20
172.16.0.15
172.16.0.16
7.7.7.20
7.7.7.12

Classic example with SSH

- Create socks proxy on 9000 port:
  - ssh -D localhost:9000 -f -N pentester@172.16.0.11
- Then use this proxy in web browser or Proxychains.
- Using proxy at 172.16.0.11, we can access resources in network 7.7.7.0

What is Proxychains?

- **ProxyChains** is a UNIX program, that hooks network-related libc functions in dynamically linked programs via a preloaded DLL and redirects the connections through SOCKS or HTTP proxies.

- Add proxy to /etc/proxychains.conf or place proxychains.conf near the tool, which needed to be proxified. Example:
  - socks5 127.0.0.1 9000

- Run:
  - proxychains nmap -p1-100 10.0.0.1

What is Metasploit Framework?

- **The Metasploit Framework** is a Ruby-based, modular penetration testing platform that enables you to write, test, and execute exploit code.

- he Metasploit Framework contains a suite of tools that you can use to test security vulnerabilities, enumerate networks, execute attacks, and evade detection.

What is persistence?

- **Persistence** is the step of creating backdoors on the system.

- Windows - https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Windows%20-%20Persistence.md
- Linux - https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Linux%20-%20Persistence.md

What is C2 framework?

- C2 frameworks — the abbreviation to the Command and Control (C&C) infrastructure — are how red teamers and pentesters can control compromised machines during security assessments.

- Examples:
  - Cobaltstrike
  - Covenant
  - Sillenttrinity
  - Metasploit
  - Merlin
  - Empire
  - etc.

Structure of C2 frameworks

- Agent – malicious binary installed on victim, that connects to the server and waits for instructions
- Server – remote server, that responds to agents and manages them
- Client – program (runned on attacker), that helps to conveniently control agents. In some cases, server = client

Covenant C2

- Github - https://github.com/cobbr/Covenant

- Covenant targets .NET Core, which is multi-platform. This allows Covenant to run natively on Linux, MacOS, and Windows platforms. Additionally, Covenant has docker support, allowing it to run within a container on any system that has docker installed.

Merlin C2

- Github - https://github.com/Ne0nd0g/merlin

- Merlin is a cross-platform post-exploitation Command & Control server and agent written in Go.

Any questions?

Homework for the next lesson

- Exploit any service of Metasploitable using Metasploit
- Perform at least two techniques of privilege escalation on rooms at Tryhackme (https://tryhackme.com/room/linuxprivesc or https://tryhackme.com/room/windows10privesc)

Feedback: did we achieved the goals of our lesson?

- Discussion 5-10 minutes

Useful links

- https://en.wikipedia.org/wiki/Privilege_escalation
- https://docs.rapid7.com/metasploit/msf-overview/
- https://github.com/haad/proxychains
- https://nullsweep.com/pivot-cheatsheet-for-pentesters/
- https://www.offensive-security.com/metasploit-unleashed/pivoting/
- https://pentest.blog/explore-hidden-networks-with-double-pivoting/
- https://pentestlab.blog/methodologies/red-teaming/persistence/
- https://resources.infosecinstitute.com/topic/red-team-c2-frameworks-for-pentesting/