

Armitage + Metasploit for Penetration Testing: from Information Collecting to Post Exploitation



Xinwen Fu, Ph.D

Professor

Department of Computer Science
University of Massachusetts Lowell



Disclaimer

Most contents are from the Internet!



Outline



- Introduction to cyber attack cycle
- Introduction to Metasploit and Armitage
- Demos



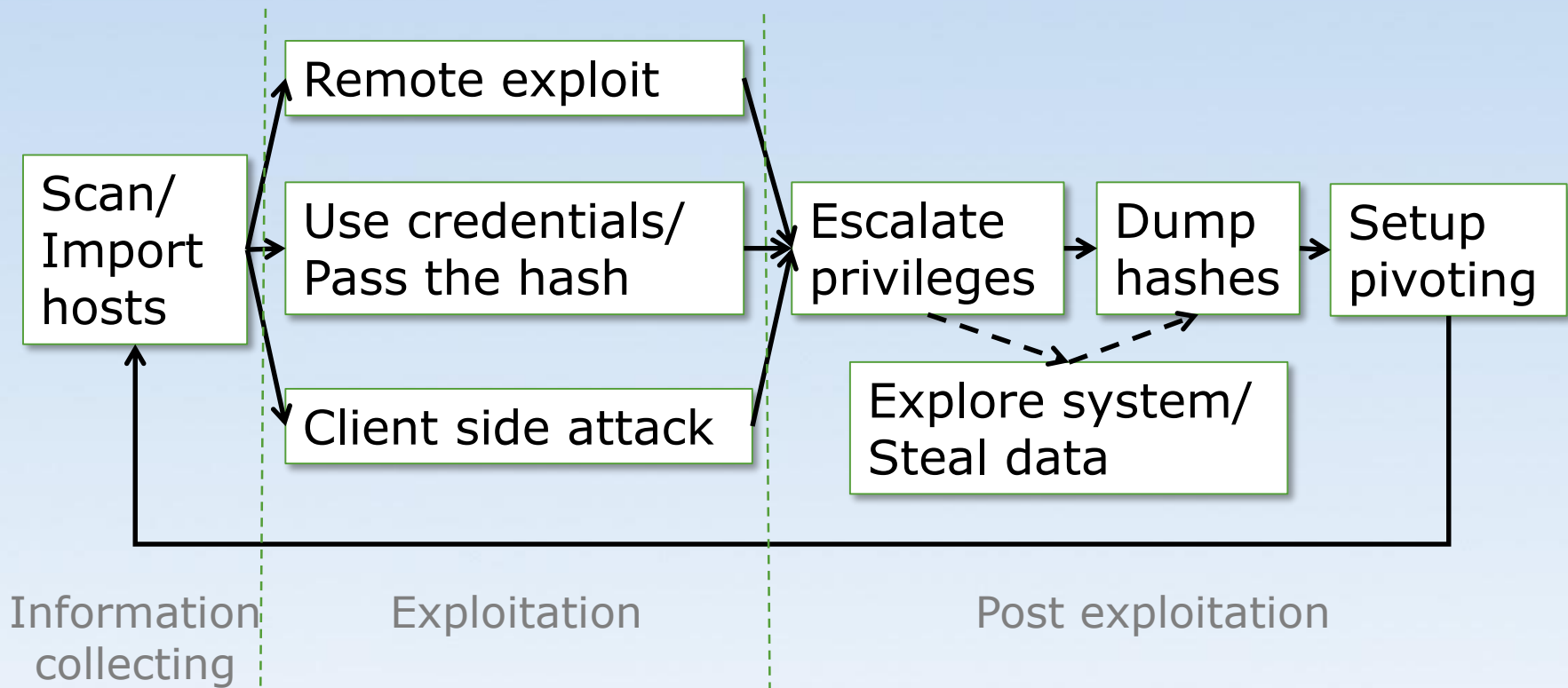
Cyberattacks

- Fighting cybercrimes is among FBI's top three priorities
- We shall think like an adversary and understand cyberattacks for the sake of defense
- Penetration testing requires cyberattack knowledge too



Cyberattack Cycle

- Penetration testing follows a similar cycle



<https://onehack.us/t/armitage-fast-easy-hacking/162550>

Cyberattack Cycle (Cont'd)



1. Launches scans and imports data from other scanners
2. Choose exploits and optionally check which exploits work
3. Perform post-exploitation
 - Escalate your privileges
 - Log keystrokes
 - Dump password hashes
 - Screen capture
 - Camera streaming
 - Browse the file system
 - Use command shells
 - Setup and use pivots: use compromised hosts as stepping stones to attack target network from inside



Remote Exploit

- The target is on the Internet or in a network
- The attacker is not on the target computer
- The attacker attacks the target remotely
 - from its own/local (maybe compromised) computer against a target



Use credentials/Pass the hash



- Use potential credentials to try to log into the target
- Sometimes, the target accepts the credential hash
 - *Pass the hash* to login



Client Side Attack

- The user is tricked to run the malicious payload/malware
 - click a link,
 - open a document, or
 - somehow get to the malicious website
- The malware runs on the target computer, not deployed from a remote computer



Outline

- Introduction to cyber attack cycle
- Introduction to Metasploit and Armitage
- Demos



Metasploit

- Used for penetration testing to find security vulnerabilities
- Available within Kali Linux
- Can be used through command prompt or Web UI or other GUI interfaces



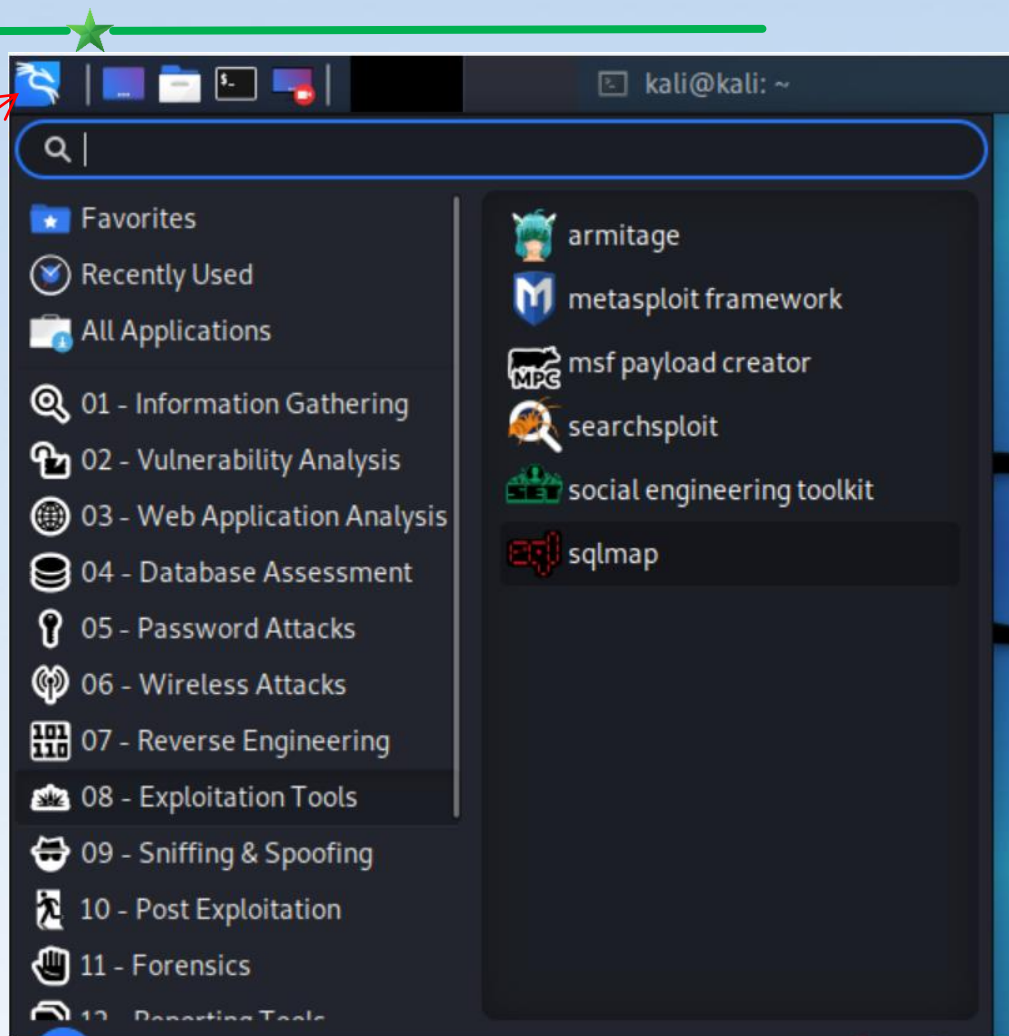
Armitage

- GUI front-end for the Metasploit framework
 - What you do in Armitage will be translated into Metasploit commands
 - What you can do in Armitage can also be done with Metasploit commands



Start Metasploit/Armitage in Kali

- Better work as root
- Metasploit
 - *Applications*
 - *Exploitation Tools*
 - *Metasploit framework*
- Armitage
 - *Applications*
 - *Exploitation Tools*
 - *Armitage*



Armitage Interface

The screenshot displays the Armitage application window. On the left, a sidebar lists modules: auxiliary, exploit, payload, and post. The main area shows two target hosts: 10.0.2.10 (Linux) and 10.0.2.7 (Windows). At the bottom, a console window shows a list of services for 10.0.2.10.

Modules

- auxiliary
- exploit
- payload
- post

Targets

- 10.0.2.10
- 10.0.2.7

Console

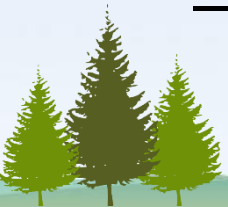
host	name	port	proto	info
10.0.2.10	ftp	21	tcp	vsftpd 2.3.4
10.0.2.10	ssh	22	tcp	OpenSSH 4.7p1 Debian 8ubuntu1 protoc...
10.0.2.10	telnet	23	tcp	Linux telnetd
10.0.2.10	smtp	25	tcp	Postfix smtpd
10.0.2.10	domain	53	tcp	ISC BIND 9.4.2
10.0.2.10	http	80	tcp	Apache/2.2.8 (Ubuntu) DAV/2 (Powered ...

Refresh Copy

Notes of Starting Armitage

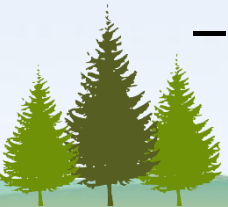


- Better work as root to use all functionalities and avoid confusion
 - E.g., start Armitage with *sudo* in a *terminal*:
sudo armitage&
- If Armitage cannot start, start Metasploit first, close it and then start Armitage
- After Armitage is started, configure to try all exploits
 - *Armitage* → *Set Exploit Rank* → **Poor**



Terms

- Nmap Scans
 - Armitage can launch nmap scans and import results into Metasploit
- MSF Scans
 - Armitage combines several Metasploit scans into a feature called MSF Scans
- Payload
 - Scripts/code adversary utilizes to compromise target system and interact with compromised system
- Exploit rank
 - How reliable the exploit is and impacts the target



Armitage for Demonstrating Cyberattack Cycle

1. Scanning
2. Exploitation
3. Post exploitation



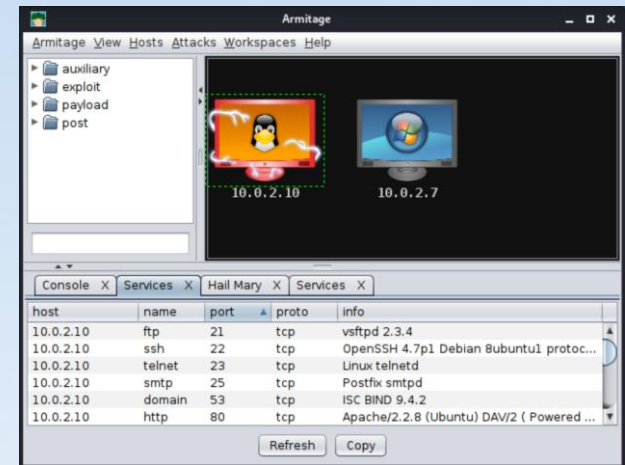
Example Target: Metasploitable

- Vulnerable computers on the Internet
 - Do not try!
 - Presenter takes no responsibility
- Metasploitable 2 virtual machine
 - A lot of vulnerabilities for exercise
 - Default username: msfadmin
Default password: msfadmin



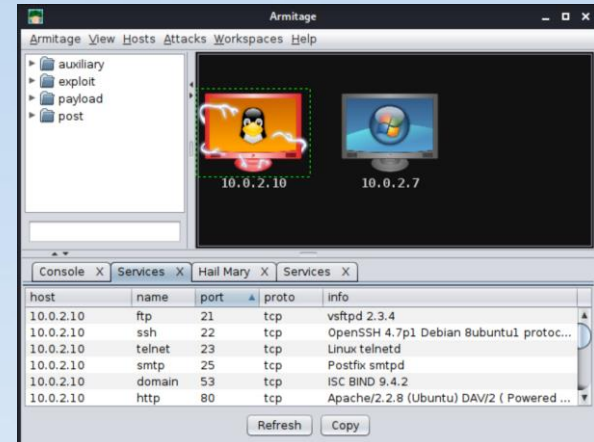
1. Armitage Scanning

- Hosts → MSF Scans
 - Enter a single IP: 10.0.2.16
 - Or enter scan range: or 10.0.2.0/25 or 10.0.2.1-254
- Hosts → Nmap Scan → Intense Scan
- Found IPs are listed as computer icons



2. Armitage Exploitation

- Select the IPs/hosts
- Deploy attack
 - Find the exploit in the tree
 - Or *Attacks* → *Find Attacks*
- Learning *which exploits to use* and *when* needs experience
- (Double) click on it to bring up the configuration
- Launch



Example Exploitation: Brute-Force Attacks

- The attacker enumerates possible passwords automatically to guess the password and gain access over a host or a service
 - Time consuming
 - Dictionary attack will help
- Potential services for brute-force attacks
 - FTP, SSH, mysql, http, Telnet, etc



Social Engineering

- Social engineering is a process of extracting sensitive information (e.g., usernames and passwords) by tricks
 - E.g. fake websites and phishing attacks
- Metasploit can perform *Phishing Campaign*



3. Armitage Post Exploitation



- Select the post exploitation module
- (Double) click on it
- Click on 'Launch'



Example Post Exploitation: Collect Credentials

- Once into a computer, collect sensitive information for the purpose of auditing (in penetration testing)
 - E.g., usernames and passwords
- ***Meterpreter*** is a Metasploit attack payload
 - provides an interactive shell to the attacker exploring the target machine and execute code
- For example, within meterpreter, *hashdump* can list all the usernames and the passwords
 - Then use John the ripper to crack password hashes



Example Post Exploitation: Maintaining Access

- If we don't maintain access, we will have to exploit it from the beginning in case the hacked system is closed or patched
 - The best way is to install a *backdoor*.
- Metasploit can plant persistent backdoors so that even if the system restarts, we can still get in



Meterpreter commands!!!

- help
- getuid
- getsystem
- webcam_list
 - Enable webcam within VM (Devices -> Webcams -> Click the camera name)
- webcam_snap
- webcam_stream
- screenshot
- record_mic
- keyscan_start
- keyscan_dump
- keyscan_stop
- shell
- Installing service
Persistence and opening a persistent backdoor



Screen Capture!!!



1. ps
2. migrate **PID** # e.g. explorer.exe
3. use espia # loading extension espia
4. screengrab



Reports

- Metasploit has in-built options that you can use to generate reports to summarize all your activities and findings



Outline



- Introduction to cyber attack cycle
- Introduction to Metasploit and Armitage
- **Demos**



Demo Setup

- Kali VM and Metasploitable 2 VM on VirtualBox
 - Networking: the two VMs shall be able to ping each other
 - E.g. Nat Network

Attacker



Kali

Target



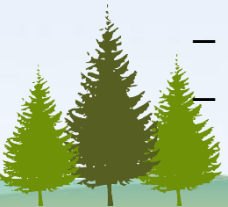
Metasploitable 2 VM

Video Demo



Steps

-
1. Start armitage: *sudo armitage&*
 - If “could not connect to database”, start Metasploit, exit it and start Armitage again
 2. Set to use what exploits: *Armitage → Set Exploit Rank → Poor*
 3. Post scanning: *Hosts → MSF Scans*
 4. Select a found IP and detect the OS running on that IP
 - *Hosts → Nmap Scan → Quick Scan (OS Detect)*
 5. Select a found IP and find attacks
 - *Attacks → Find Attacks*
 6. Select a found IP, choose an attack and deploy it
 - *Attack → IRC → unreal_ircd_3281_backdoor*
 - Check “Use a reverse connection”
 - *Shell 1 → Interact*
 7. Post exploitation
 - Search *hashdump* within modules and choose *post -> Linux -> gather -> hashdump*
 - Copy and paste the displayed hashes into a file, e.g. *hash-dump* (remove “[+]”)
 - John the ripper to crack the hashes: *john hash-dump*



unreal_ircd_3281_backdoor



UnrealIRCd 3.2.8.1 Backdoor Command Execution

Disclosed	Created
06/12/2010	05/30/2018

Description

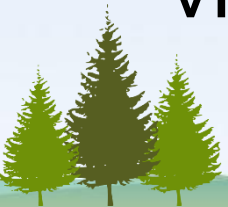
This module exploits a malicious backdoor that was added to the Unreal IRCd 3.2.8.1 download archive. This backdoor was present in the Unreal3.2.8.1.tar.gz archive between November 2009 and June 12th 2010.

https://www.rapid7.com/db/modules/exploit/unix/irc/unreal_ircd_3281_backdoor/



Summary

- Armitage + Metasploit for intuitive live demos to explain cyberattacks and penetration testing
- A few clicks and commands needed to perform information collecting, exploitation and post exploitation
- Armitage and Metasploit on a Kali Linux virtual machine.



References



- [1] [Metasploit tutorial](#), accessed on 1/4/22
- [2] [Tutorial on armitage](#), accessed on 1/4/22
- [3] Jamie Pegg, [Spy On Windows Machines Using Metasploit](#), Jun 21, 2019
- [4] Lester Obbayi, [How to attack Windows 10 machine with metasploit on Kali Linux](#), February 10, 2021
- [5] OTW, [Metasploit Basics, Part 15: Post- Exploitation Fun \(Web Cam, Microphone, Passwords and more\)](#), Oct 16, 2018



**THANK
YOU!**



Q&A