

AI FOR CYBER SECURITY

ASSIGNMENT-2

Name: V.Y.Koushik

Reg.No:21BCE9368

Explore the first 10 tools in Kali Linux

1. Information Gathering

For information gathering, a tool named dnsenum is used. It is a command-line tool used for DNS (Domain Name System) enumeration and information gathering. It is typically used by security professionals, network administrators, and ethical hackers to gather information about a target domain's DNS configuration.

For this, I have used www.wcofun.org website.



```
manasa13@Kali:~$ dnsenum --help
-d, --delay <value> The maximum value of seconds to wait between whois queries, the value is defined randomly, default: 3s.
-w, --whois Perform the whois queries on c class network ranges.
**Warning**: this can generate very large netranges and it will take lot of time to perform reverse lookups.
REVERSE LOOKUP OPTIONS:
-e, --exclude <regex> Exclude PTR records that match the regex expression from reverse lookup results, useful on invalid hostnames.
OUTPUT OPTIONS:
-o, --output <file> Output in XML format. Can be imported in MagicTree (www.growwell.com)
manasa13@Kali:~$ dnsenum www.wcofun.org
dnsenum VERSION:1.2.6
www.wcofun.org

Host's addresses:
www.wcofun.org.      248  IN  A      104.26.3.85
www.wcofun.org.      248  IN  A      104.26.2.85
www.wcofun.org.      248  IN  A      172.67.71.150

Name Servers:
www.wcofun.org NS record query failed: NOERROR

manasa13@Kali:~$ dnsenum --dnsserver 8.8.8.8 www.wcofun.org
dnsenum VERSION:1.2.6
www.wcofun.org

Host's addresses:
www.wcofun.org.      300  IN  A      172.67.71.150
www.wcofun.org.      300  IN  A      104.26.3.85
www.wcofun.org.      300  IN  A      104.26.2.85

Name Servers:
www.wcofun.org NS record query failed: NOERROR

manasa13@Kali:~$
```

2. Vulnerability Analysis

For vulnerability analysis, nmap tool is used. Nmap (Network Mapper) is a widely used open-source tool for network discovery and vulnerability analysis. It's primarily used for network scanning, mapping, and fingerprinting, but it can also assist in vulnerability assessment.

```
File Actions Edit View Help
--data-length <num>: Append random data to sent packets
--ip-options <options>: Send packets with specified ip options
--ttl <val>: Set IP time-to-live field
--spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
--badsum: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT:
--oX/-oX/-o5/-o6 <file>: Output scan in normal, XML, s/crypt kiddie3,
and Greppable format, respectively, to the given filename.
--oX <filename>: Output in the three major formats at once
--v: Increase verbosity level (use -vv or more for greater effect)
--d: Increase debugging level (use -dd or more for greater effect)
--reason: Display the reason a port is in a particular state
--open: Only show open (or possibly open) ports
--packet-trace: Show all packets sent and received
--iflist: Print host interfaces and routes (for debugging)
--append-output: Append to rather than clobber specified output files
--resume <filename>: Resume an aborted scan
--noninteractive: Disable runtime interactions via keyboard
--stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
--xhtml: Reference stylesheet from Nmap.org for more portable XML
--no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
--G: Enable IPv6 scanning
--A: Enable OS detection, version detection, script scanning, and traceroute
--datadir <dirname>: Specify custom Nmap data file location
--send-eth/--send-ip: Send using raw ethernet frames or IP packets
--privileged: Assume that the user is fully privileged
--unprivileged: Assume the user lacks raw socket privileges
--V: Print version number
--h: Print this help summary page.
EXAMPLES:
nmap -v -A scanme.nmap.org
nmap -v -sn 192.168.0.0/20 10.0.0.0/8
nmap -v -iR 10000 -ps 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
manasa13@kali:~$ nmap -v -A scanme.nmap.org
Starting Nmap 7.91 ( https://nmap.org ) at 2023-09-04 16:04 IST
Nmap scan report for scanme.nmap.org (104.20.3.85)
Host is up (0.0001s latency).
Other addresses for scanme.nmap.org (not scanned): 2606:4700:20::681a:355 2606:4700:20::681a:255 2606:4700:20::ac43:47a0 194.26.2.85 172.67.71.168
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
8080/tcp   open  http-proxy
443/tcp    open  https-alt
Nmap done: 1 IP address (1 host up) scanned in 4.87 seconds
manasa13@kali:~$
```

3. Web Application Analysis

For Web Application Analysis, a tool named wpscan is used. WPScan is a popular open-source security scanner specifically designed for WordPress websites. It is used for identifying vulnerabilities, misconfigurations, and security issues in WordPress installations. It can be a valuable tool for security professionals, website administrators, and penetration testers to assess the security posture of WordPress sites.

4. Database Assessment

For Database Assessment, sqlmap tool is used. sqlmap is a popular open-source tool used for automated penetration testing and database assessment. Its primary purpose is to detect and exploit SQL injection vulnerabilities in web applications and their underlying databases. SQL injection is a common attack vector where malicious SQL statements are inserted into input fields of a web application to manipulate the database or gain unauthorized access to sensitive data.

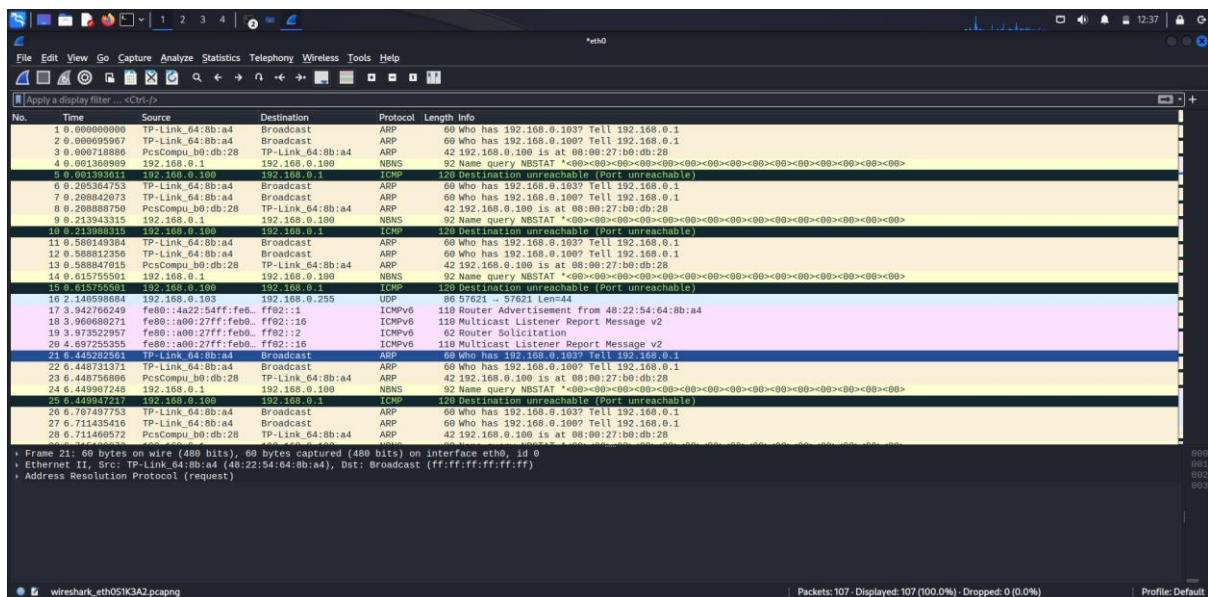
5. Password Attacks

For exploring password attacks, ncrack tool is used. Ncrack is a powerful open-source network authentication cracking tool. It is primarily used for performing password attacks, including brute force attacks and dictionary attacks, against various network services and protocols. Ncrack is designed for legitimate security testing and auditing purposes to assess the strength of passwords used for authentication on network services.

```
manasa13@Kali: ~  
File Actions Edit View Help  
cr (connection retries): caps number of service connection attempts  
to (time-out): maximum cracking <time> for service, regardless of success so far  
-T<0-5>: Set timing template (higher is faster)  
--connection-limit <number>: threshold for total concurrent connections  
--stealthy-linear: try credentials using only one connection against each specified host  
until you hit the same host again. Overrides all other timing options.  
AUTHENTICATION:  
-U <filename>: username file  
-P <filename>: password file  
--user <username_list>: comma-separated username list  
--pass <password_list>: comma-separated password list  
--passwords-first: Iterate password list for each username. Default is opposite.  
--pairwise: Choose usernames and passwords in pairs.  
OUTPUT:  
-oN/-oX <file>: Output scan in normal and XML format, respectively, to the given filename.  
-oA <basename>: Output in the two major formats at once  
-v: Increase verbosity level (use twice or more for greater effect)  
-d[level]: Set or increase debugging level (Up to 10 is meaningful)  
--nsock-trace <level>: Set nsock trace level (Valid range: 0 - 10)  
--log-errors: Log errors/warnings to the normal-format output file  
--append-output: Append to rather than clobber specified output files  
MISC:  
--resume <file>: Continue previously saved session  
--save <file>: Save restoration file with specific filename  
-f: quit cracking service after one found credential  
-6: Enable IPv6 cracking  
-sl or --list: only list hosts and services  
--datadir <dirname>: Specify custom Ncrack data file location  
--proxy <type>://proxy:port: Make connections via socks4, 4a, http.  
-V: Print version number  
-h: Print this help summary page.  
MODULES:  
SSH, RDP, FTP, Telnet, HTTP(S), Wordpress, POP3(S), IMAP, CVS, SMB, VNC, SIP, Redis, PostgreSQL, MQTT, MySQL, MSS  
QL, MongoDB, Cassandra, WinRM, OWA, DICOM  
EXAMPLES:  
ncrack -v --user root localhost:22  
ncrack -v -T5 https://192.168.0.1  
ncrack -v -iX ~/nmap.xml -g CL=5,to=1h  
SEE THE MAN PAGE (http://nmap.org/ncrack/man.html) FOR MORE OPTIONS AND EXAMPLES  
(manasa13@Kali)-[~]  
$ ncrack -p ssh 127.0.0.1  
  
Starting Ncrack 0.7 ( http://ncrack.org ) at 2023-09-06 01:19 IST  
  
Ncrack done: 1 service scanned in 3.00 seconds.  
  
Ncrack finished.  
(manasa13@Kali)-[~]  
$
```

6. Wireless Attacks

For exploring wireless attacks, wifite tool is used. Wifite is a popular wireless auditing tool available in Kali Linux. It's designed to automate various wireless attacks, including WEP and WPA/WPA2-PSK cracking, using a combination of well-known attack methods.



10. Post Exploitation

For exploring Post exploitation, Mimikatz tool is used. Mimikatz is a powerful post-exploitation tool that is widely known for its capability to extract plaintext passwords, hashes, and other authentication credentials from memory, as well as performing other post-exploitation tasks on Windows systems. It is used by security professionals, penetration testers, and sometimes malicious actors for legitimate and malicious purposes.

