TASK – 4

Sniffing Attack using Wireshark

A sniffing attack, also known as network sniffing or packet sniffing, is a method used by attackers to intercept and log network traffic. This type of attack is often employed to capture sensitive information such as usernames, passwords, and other confidential data as it travels over a network.

To protect against sniffing attacks, it's essential to implement security measures such as encryption, secure network configurations, and monitoring systems to detect unusual network behavior. Additionally, raising awareness among users about the importance of using secure protocols and avoiding unsecured networks can help mitigate the risks associated with sniffing attacks.

Nmap is a utility for network exploration or security auditing. It supports ping scanning (determine which hosts are up), many port scanning techniques, version detection (determine service protocols and application versions listening behind ports), and TCP/IP fingerprinting (remote host OS or device identification). Nmap also offers flexible target and port specification, decoy/stealth scanning, sunRPC scanning, and more. Most Unix and Windows platforms are supported in both GUI and commandline modes. Several popular handheld devices are also supported, including the Sharp Zaurus and the iPAQ.

```
rsf > use exploits/multi/misfortune_cookie
rsf (Misfortune Cookie) > show options

Target options:

   Name       Current settings     Description
   ----       ----------------     -----------
   port       80                   Target port
   target                          Target address e.g. http://192.168.1.1


rsf (Misfortune Cookie) > set target 192.168.0.2
[+] {'target': '192.168.0.2'}
rsf (Misfortune Cookie) > check
[-] Target is not vulnerable
rsf (Misfortune Cookie) > back
rsf > use
creds     exploits  scanners
rsf > use scanners/
scanners/autopwn     scanners/dlink_scan
rsf > use scanners/autopwn
rsf (AutoPwn) > show options

Target options:

   Name       Current settings     Description
   ----       ----------------     -----------
   port       80                   Target port
   target                          Target IP address e.g. 192.168.1.1
```

```
rsf (AutoPwn) > set target 192.168.0.2
[+] {'target': '192.168.0.2'}
rsf (AutoPwn) > run
[*] Running module...
[-] exploits/fortinet/fortigate_os_backdoor is not vulnerable
[-] exploits/belkin/n150_path_traversal is not vulnerable
[-] exploits/belkin/g_n150_password_disclosure is not vulnerable
[-] exploits/belkin/n750_rce is not vulnerable
[-] exploits/belkin/g_plus_info_disclosure is not vulnerable
```

```
rsf (HTTP Basic Bruteforce) > show options

Target options:

   Name       Current settings     Description
   ----       ----------------     -----------
   port       80                   Target port
   target                          Target IP address or file with target:port (file:///)


Module options:

   Name          Current settings                                                  Description

   ----          ----------------                                                  -----------

   path          /                                                                 URL Path

   usernames     admin                                                             Username or file
with usernames (file:///)
   passwords     file:///usr/share/routersploit/routersploit/wordlists/passwords.txt     Password or file
with passwords (file:///)
   threads       8                                                                 Numbers of thread
s
   verbosity     yes                                                               Display authentic
ation attempts
```

Using tools like hping, scanrand, traceroute, the network mapping of targets can be determined. It is also useful for detecting defensive measures like IDS, IPS, UTM, and firewalls.

2.3.3 SNMP Scans

SNMP scanning is the process of using a Simple Network Management Protocol (SNMP) to collect valuable data about the state of devices on a network.

```
┌──(mearaj㉿kali)-[~]
└─$ snmp-check 23.227.38.74 -c public
snmp-check v1.9 - SNMP enumerator
Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)

[+] Try to connect to 23.227.38.74:161 using SNMPv1 and community 'public'

[!] 23.227.38.74:161 SNMP request timeout
```

SNMP is used to collect data related to network changes or to determine the status of network-connected devices. Collecting this data can help IT professionals keep their finger on the pulse of all their managed devices and applications.

2.3.4. Server Identification

Using tools like httprint, smtpscan, detected servers (HTTP, FTP, SMTP, POP, IMAP, etc) from previous scans are listed and classified by their brand/model/operation systems/version numbers.

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-01 14:26 India Standard Time
Nmap scan report for shops.myshopify.com (23.227.38.74)
Host is up (0.024s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
8443/tcp open  https-alt
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host

OS detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.39 seconds
```

2.3.5. VPN Identification

Using ike-scan, the network was traced for VPN servers.

```
┌──(mearaj㉿kali)-[~]
└─$ searchsploit windows
```

Exploit Title	Path
(Gabriel's FTP Server) Open & Compact FTP Server 1.2 - 'POR	windows/dos/12698.py
(Gabriel's FTP Server) Open & Compact FTP Server 1.2 - Auth	windows/remote/27401.py
(Gabriel's FTP Server) Open & Compact FTP Server 1.2 - Full	windows/remote/13932.py
(Gabriel's FTP Server) Open & Compact FTP Server 1.2 - Univ	windows/dos/12741.py
(Gabriel's FTP Server) Open & Compact FTPd 1.2 - Buffer Ove	windows/remote/11742.rb
(Gabriel's FTP Server) Open & Compact FTPd 1.2 - Crash (PoC	windows/dos/11391.py
(Gabriel's FTP Server) Open & Compact FTPd 1.2 - Remote Ove	windows/remote/11420.py
.NET Framework - Tilde Character Denial of Service	windows/dos/19575.txt
.NET Remoting Services - Remote Command Execution	windows/remote/35280.txt
.NET Runtime Optimization Service - Local Privilege Escalat	windows/local/16940.c
0irc-client 1345 build20060823 - Denial of Service	windows/dos/3547.c
1 Click Audio Converter 2.3.6 - Activex Local Buffer Overfl	windows/local/37211.html
1 Click Extract Audio 2.3.6 - Activex Buffer Overflow	windows/local/37212.html
10-Strike Bandwidth Monitor 3.7 - Local Buffer Overflow (SE	windows/local/45085.py
10-Strike Bandwidth Monitor 3.9 - Buffer Overflow (SEH) (AS	windows/local/48570.py
10-Strike LANState 8.8 - Local Buffer Overflow (SEH)	windows/local/45086.py
10-Strike Network File Search Pro 2.3 - Local Buffer Overfl	windows/local/40903.py
10-Strike Network Inventory Explorer - 'srvInventoryWebServ	windows/local/48251.txt
10-Strike Network Inventory Explorer 8.54 - 'Add' Local Buf	windows/local/48253.py
10-Strike Network Inventory Explorer 8.54 - 'Registration K	windows_x86/local/44840.py
10-Strike Network Inventory Explorer 8.54 - Local Buffer Ov	windows/local/46283.py
10-Strike Network Inventory Explorer 8.54 - Local Buffer Ov	windows_x86/local/44838.py
10-Strike Network Inventory Explorer 8.65 - Buffer Overflow	windows/local/49134.py
10-Strike Network Inventory Explorer 9.03 - 'Read from File	windows/local/48264.py
10-Strike Network Inventory Explorer Pro 9.05 - Buffer Over	windows/local/49322.py
10-Strike Network Inventory Explorer Pro 9.31 - 'srvInvento	windows/local/50494.txt
10-Strike Network Inventory Explorer Pro 9.31 - Buffer Over	windows/local/50472.py
10-Strike Network Scanner 3.0 - Local Buffer Overflow (SEH)	windows_x86/local/44841.py
10Strike LANState 9.32 - 'Force Check' Buffer Overflow (SEH	windows/local/48277.py
123 FlashChat 7.8 - Multiple Vulnerabilities	windows/remote/14658.txt
1by1 1.67 - '.m3u' Local Stack Overflow (PoC)	windows/dos/8484.pl
1C: Arcadia Internet Store 1.0 - Arbitrary File Disclosure	windows/remote/20947.txt
1C: Arcadia Internet Store 1.0 - Denial of Service	windows/dos/20949.c
1C: Arcadia Internet Store 1.0 - Path Disclosure	windows/remote/20948.txt
1CLICK DVD Converter 2.1.7.1 - Multiple DLL Loading Arbitra	windows/remote/34848.c
1ClickUnzip 3.00 - '.zip' Heap Overflow	windows/dos/17363.pl
2345 Security Guard 3.7 - '2345BdPcSafe.sys' Denial of Serv	windows/dos/44615.cpp