Chapter 7

Exploiting Network Vulnerabilities

Outlines

- VLAN Hopping
- Network Proxies
- DNS Cache Poisoning
- ARP Spoofing
- Man-in-the-Middle
- Replay Attacks
- Relay Attacks
- SSL Stripping Attacks
- Downgrade Attacks
- NAC Bypass
- DoS Attacks and Stress Testing
- NetBIOS Name Resolution Exploits
- SMB Exploits
- SNMP Exploits
- SMTP Exploits
- FTP Exploits
- Samba Exploits
- SSH Exploits
- Wireless Exploits
- Evil Twins and Wireless MITM
- Attacking WPS
- Bluetooth Attacks
- Jamming
- Repeating
- RFID Cloning

VLAN Hopping

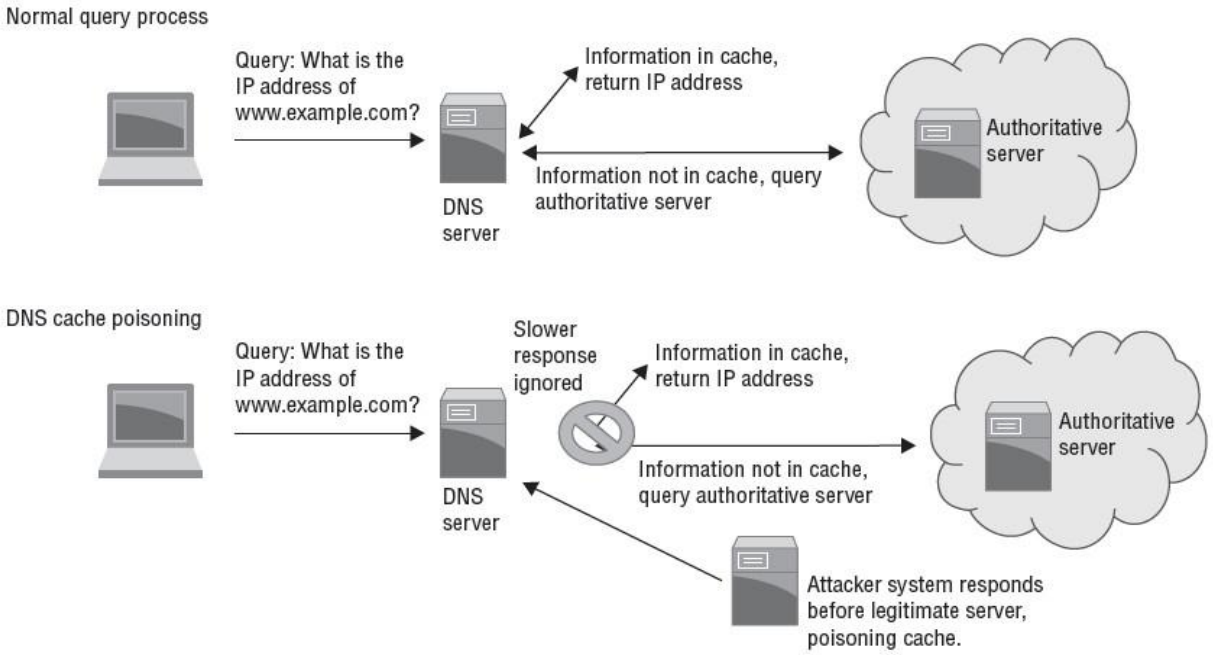
Virtual local area networks (VLANs) separate broadcast domains into separate sections for security or performance reasons. Many organizations use VLANs to create internal security boundaries between different systems or organizational units. This makes the ability to access a VLAN other than the one you are currently on an attractive opportunity for penetration testers.

Network Proxies

In some cases, you may not be able to load penetration testing tools on a remote host that you have gained access to, but you may have access to common tools like SSH. In other scenarios you may need to have testing traffic originate from specific IP addresses or ranges, or you may want to have access to a specific host through network protections like firewalls that you cannot establish directly.

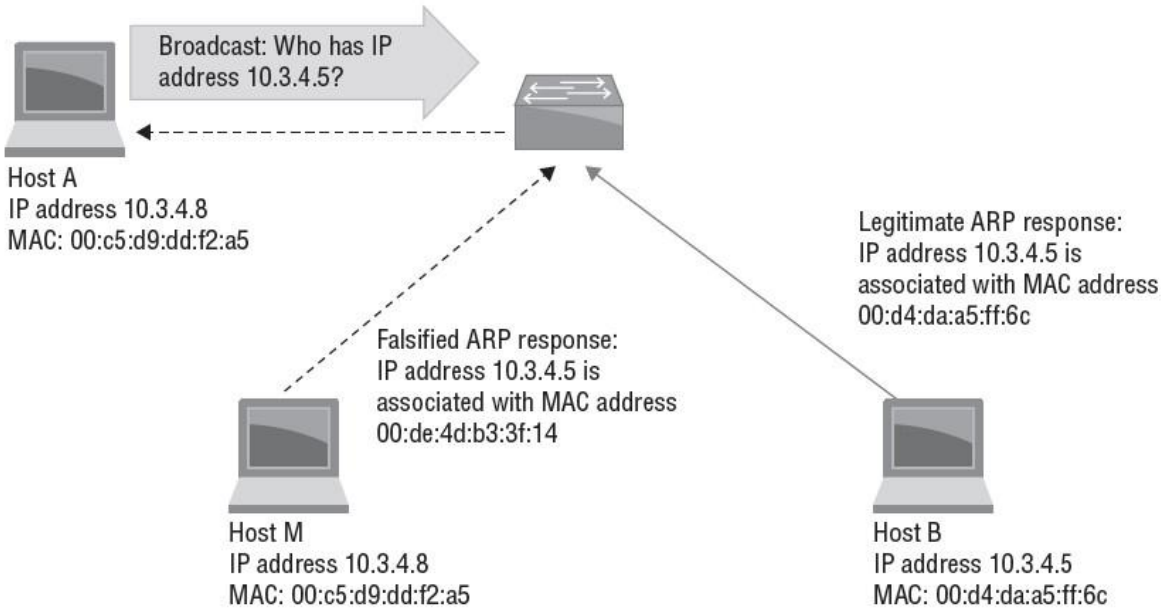
DNS Cache Poisoning

DNS spoofing, also known as DNS cache poisoning, can allow you to redirect traffic to a different host that you control.



ARP Spoofing

The Address Resolution Protocol (ARP) is used to map IP addresses to physical machine addresses (MAC, or Media Access Control, addresses). Because that is how most local networks are tracked for systems, falsifying responses to ARP queries about which address traffic should be sent to can allow attackers to conduct various attacks that rely on victims sending their traffic to the wrong system, including man-in-the-middle attacks. ARP spoofing occurs when an attacker sends falsified ARP messages on a local network, thus providing an incorrect MAC address to IP address pairing for the deceived system or systems. This information is written to the target machine's ARP cache, and the attacker can then either intercept or capture and forward traffic. If man-in-the-middle packet capture isn't your goal, the same technique can be used to hijack sessions or cause additional traffic to hit a target system, potentially causing a DoS condition



Man-in-the-Middle

Penetration testers often want to capture traffic that is sent to or from a target system, but without control of the network devices along the path, they cannot access that traffic in most cases on a modern switched network. That means they need to find a way to insert themselves into the middle of the traffic flow, either by persuading the systems involved to send traffic via another path or by compromising network equipment that is in the path of the target traffic, thus acting as a man in the middle.

Replay Attacks

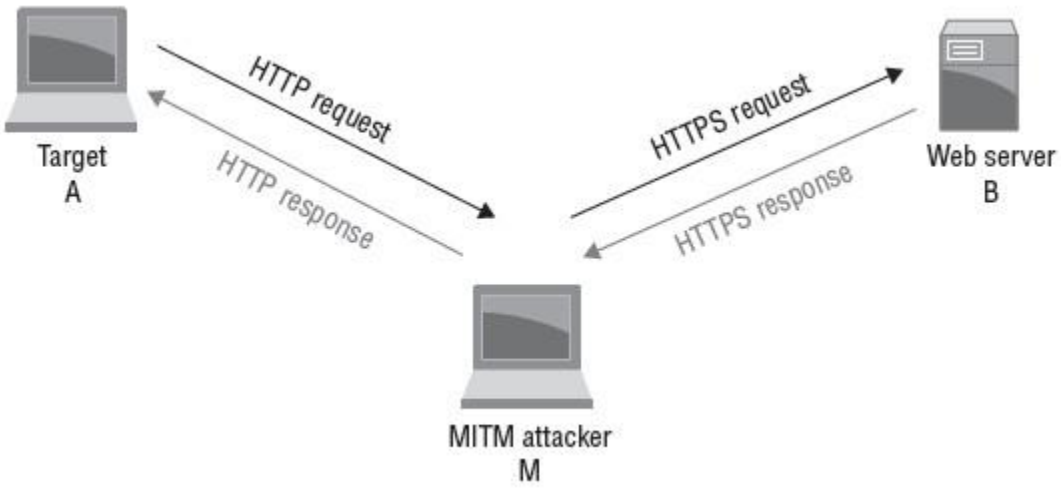
A replay attack is a form of man-in-the-middle attack that focuses on capturing and then resending data. Common uses for replay attacks include masquerading to allow an attacker to present credentials to a service or system after capturing them during an authentication process.
One of the most common replay attacks used by penetration testers is an NTLM pass the-hash attack. Once a pen-tester has acquired NTLM hashes, they can then identify systems that do not require SMB signing (which prevents the attack). With a list of targets in hand, Responder or other tools with similar features can be used to intercept authentication attempts, and then an NTLM relay tool can be leveraged to drop Empire or another similar tool onto the target machine.

Relay Attacks

Relay attacks can appear very similar to other man-in-the-middle attacks; however, in relay attacks, the man-in-the-middle system is used only to relay attacks without modifying them rather than modifying any traffic. It is worth bearing in mind that relay attacks are not limited to traditional IP-based network traffic. As a penetration tester, you may find it useful to query an RFID card or other device required to provide authentication or authorization and to relay the response to a device or system that the card is not actually near! The same tools used to execute other man-in-the-middle attacks can be used for relay attacks, since the goal is merely to capture or present traffic rather than modify it.

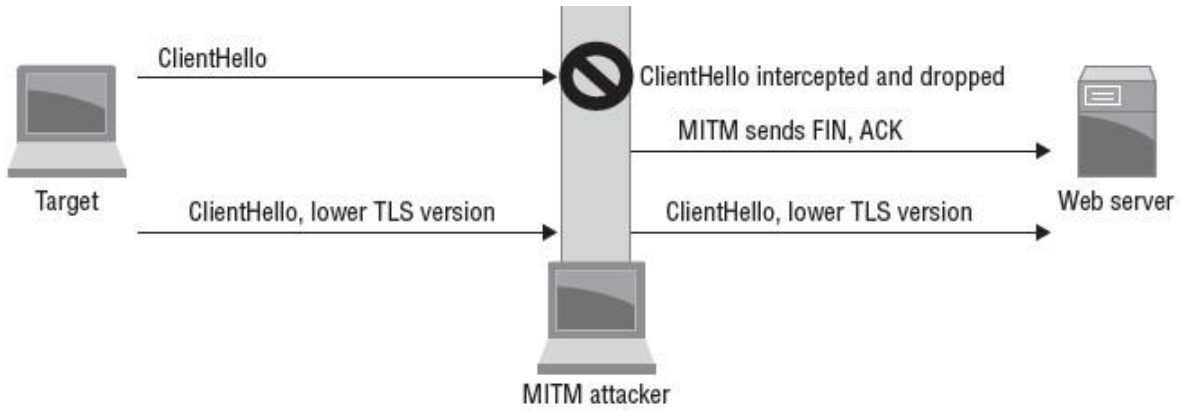
SSL Stripping Attacks

Because an ever-increasing proportion of organizational network traffic for applications and services is carried via HTTPS, downgrading HTTPS connections to HTTP is a powerful tool in the hands of a penetration tester. The ability to downgrade the connection and then access the formerly encrypted traffic can provide a massive trove of information, including credentials, passwords, and organizational data.



Downgrade Attacks

SSL downgrade attacks work by intercepting TLS handshakes and dropping packets, thus modifying them to request weaker encryption methods. Since TLS (like SSL) allows clients to request the ciphers that they can use, this may allow an attacker to more easily read client traffic.



NAC Bypass

While many network attacks rely on man-in-the-middle techniques to access traffic, gaining access to a network itself may also be required. Many organizational networks now require authentication and authorization to be on the network, and NAC (Network Access Control) is often utilized to provide that security layer.

NAC systems work by detecting when new devices connect to a network and then requiring them to be authorized to access the network. Their detection process typically involves one of the following methods:

- A software client that talks to a NAC server when connected
- A DHCP proxy that listens for traffic like DHCP requests
- A broadcast listener that looks for broadcast traffic like ARP queries or a more General-purpose sniffer that looks at other IP packets
- An SNMP-trap-based approach that queries switches to determine when a new MAC address shows up on one of their connected ports

DoS Attacks and Stress Testing

For many penetration tests, the rules of engagement specifically prohibit intentional denial of service (DoS) attacks, particularly against production environments. That isn't always true, and some engagements will allow or even require DoS attacks, particularly if the client organization wants to fully understand their ability to weather them. There are three major types of denial of service attacks:

- Application layer denial of service attacks, which seek to crash a service or the entire server.
- Protocol-based denial of service attacks, which take advantage of a flaw in a protocol.
- A SYN flood is a classic example of a protocol-based denial of service attack.
- Traffic volume–based denial of service attacks simply seek to overwhelm a target by sending more traffic than it can handle.

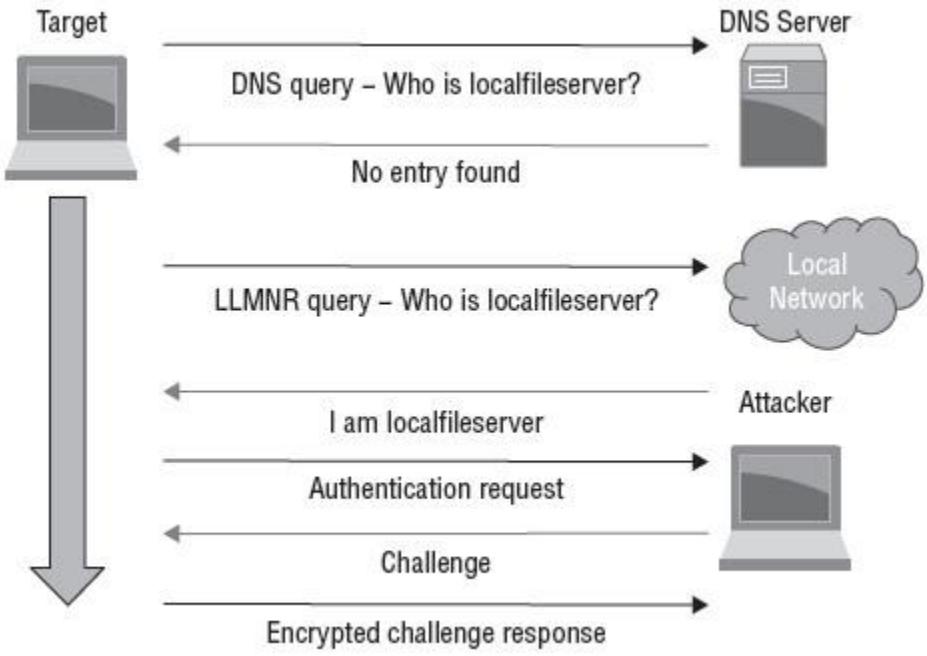
NetBIOS Name Resolution Exploits

One of the most commonly targeted services in a Windows network is NetBIOS. NetBIOS is commonly used for file sharing, but many other services rely on the protocol as well.

NETBIOS Name Services

When Windows systems need to resolve the IP address for a hostname, they use three lookup methods in the following order:

- **The Local host file found at C:\Windows\System32\drivers\etc\hosts**
- **DNS, first via local cache and then via the DNS server**
- **The NetBIOS name service (NBNS), first via Link Local Multicast Name Resolution**
- **(LLMNR) queries and then via NetBIOS Name Service (NetBIOS-NS) queries**



Windows *Net* Commands

Exploring Windows domains can be a lot easier if you are familiar with the Windows `net` commands. Here are a few of the most useful commands:

`net view /domain`

Lists the hosts in the current domain. You can also use `/domain:[domain name]` to search a domain that the system has access to other than the current domain.

`net user /domain`

Lists the users in a domain.

`net accounts /domain`

Shows the domain password policy.

`net group /domain`

Lists groups on the domain.

`net group "Domain Admins" /domain`

Adding a group name like `Domain Admins` to the `net group` command lists users in the group, allowing discovery of domain admins.

`net share`

Shows current SMB shares.

`net session`

Used to review SMB sessions. Using the `find` command with this can allow searches for active sessions.

```
Net share [name of share] c:\directory\of\your\choice
/GRANT:Everyone,FULL
```

Grants access to a folder on the system for any user with full rights. As you would expect, this is easy to change by identifying specific users or permissions levels.

Since the `net` commands are built into every Windows system you will encounter, knowing how to use them can be a powerful default tool when testing Windows targets. As you might expect, PowerShell provides even more powerful capabilities, but access is often more restricted, especially if you don't have administrative credentials.

SMB Exploits

The Server Message Block (SMB) implementation in Windows is another popular target for penetration testers. Its vulnerabilities mean that unpatched systems can be exploited with relative ease; these include critical remote code execution vulnerabilities in the Windows SMB server discovered in 2017 (**MS17-010**, also known as Eternal Blue). Like most major exploits, Metasploit includes an SMB exploit module that targets the Eternal Blue vulnerability.

SNMP Exploits

The Simple Network Management Protocol (SNMP) is commonly used to gather information about network devices, including configuration and status details. While SNMP is most commonly associated with network devices like switches and routers, it is also used to monitor printers, servers, and a multitude of other networked systems. SNMP operates on UDP port 161, making it easy to recognize SNMP traffic on a network. SNMP organizes data into hierarchical structures called MIBs, or management information bases. Each variable in an MIB is called an OIT, or object identifier. In addition,
SNMP v1 and v2 rely on community strings to determine whether a connected user can read, read and write, or just send events known as "traps." Since SNMP can provide a wealth of information about a network and specific devices on it, it can be an important target for a penetration tester. One of the first steps for SNMP exploitation is to map a network for devices with SNMP enabled.

SNMP

There are three major versions of SNMP that may be encountered on a network:

- SNMP v1 has poor security and should be largely deprecated.
- SNMP v2 provides added administrative functionality and added security, but the security features require configuration, are quite weak compared to modern designs, and are often not used.
- SNMP v3 is functionally equivalent to SNMP v2 but adds additional security capabilities to provide confidentiality, integrity, and authentication.

SMTP Exploits

The Simple Mail Transfer Protocol (SMTP) is the protocol by which email is sent. SMTP operates on TCP port 25 and can typically be easily identified by telnetting to the service port. Much like FTP, SMTP is a very old protocol without much built-in security. That means it has been targeted for years, and most organizations that run SMTP servers have learned to harden them against misuse so that they do not get blacklisted for being spam email relays.
That means the SMTP exploits that are most useful to a penetration tester are typically associated with a specific vulnerable SMTP server version. Thus, if you encounter an SMTP server, connecting to it and gathering banner information may provide enough of a clue to determine if it is a vulnerable service. STMP servers can also be used for information gathering by connecting them and using the EXPN and VRFY commands. To do this, simply telnet to the SMPT server (telnet example.server.com 25) and when connected, type VRFY [username] or EXPN [user_alias] . As you might guess, Metasploit includes an SMTP enumeration tool as part of its list of auxiliary scanners; auxiliary/scanner/smtp/smtp_enum will provide a list of

users quickly and easily. SMTP servers can be useful if you have access to them from a trusted system or network. Sending email that appears to be from a trusted sender through a valid email server can make social engineering attacks more likely to succeed, even with an aware and alert group of end users at the target organization. While probing SMTP servers may not seem terribly useful at first glance, this trust means that scanning for and testing SMTP servers can be useful.

FTP Exploits

File Transfer Protocol (FTP) has been around since 1971, and it remains a plaintext, unencrypted protocol that operates on TCP port 21 as well as higher ephemeral TCP ports for passive transfers. From that description, you might expect that it would have been completely replaced by now by secure services and HTTP-based file transfers. Fortunately for penetration testers, that isn't always the case, and FTP servers remain in use around the world. Exploiting FTP is quite simple if you can gain access to FTP network traffic. Since the protocol is unencrypted, the simplest attack is to capture usernames and passwords on the wire and use them to log into the target system or other target systems! FTP servers themselves may also be vulnerable.

Samba Exploits

Much like the Microsoft implementation of SMB, the Linux Samba server has proven to have a variety of security flaws. 2017's SambaCry exploit was discovered to allow remote code execution in all SMB versions newer than Samba 3.5.0—a 2010 code release! Because Samba and Microsoft SMB operate on the same ports and protocols, fingerprinting the operating system before attempting an exploit is important to ensure that you are using the right exploit for the OS and server service.

SSH Exploits

Secure Shell (SSH) is used for secure command-line access to systems, typically via TCP port 22, and is found on devices and systems of all types. Because SSH is so common, attacking systems that provide an SSH service is a very attractive option for a penetration tester. This also means that most organizations will patch SSH quickly if they are able to. Unfortunately for many organizations, SSH is embedded in devices of all descriptions, and updating SSH throughout their infrastructure may be difficult. Thus, penetration testers should validate both SSH and operating system versions when reviewing vulnerability scan results to determine if a vulnerable version of SSH is running. Another method of attacking services like SSH is to use a brute-forcing tool like THC Hydra (or an equivalent Metasploit module).

Wireless Exploits

Evil Twins and Wireless MITM

Evil twin attacks work by creating bogus access points that unsuspecting users connect to. This makes them useful for man-in-the-middle attacks like those discussed earlier in this chapter. While it is possible to create an evil twin of a secured access point, more sophisticated users are likely to notice differences like having to accept new security certificates or other changes.
Penetration testers can use Aircrack-ng to create an evil twin using the airbase-ng tool.
The process is relatively simple:

- Capture traffic to determine the SSID and MAC addresses of a legitimate access point.
- Clone that access point using airbase-ng .
- Conduct a de-authentication attack.
- Ensure that the fake AP is more powerful (or closer!) and thus will be selected by the client when they try to reconnect.
- Conduct attacks, including man-in-the-middle attacks.

Attacking WPS

WiFi Protected Setup (WPS) has been a known issue for years, but it remains in use for ease of setup, particularly for consumer wireless devices. Setting up a printer with the push of a button, rather than entering a pre-shared key or password, can seem attractive. Unfortunately, one WPS setup mode requires an 8-digit PIN, which is easily cracked because WPS uses an insecure method of validating PINs. WPS passwords can be attacked using a pixie dust attack, a type of attack that brute-forces the key for WPS. Vulnerable routers can simply be attacked by leveraging the fact that many have poor selection algorithms for their pre-shared key random numbers.

Aircrack-ng provides the ability to conduct replay and deauthentication attacks and to act as a fake access point. It also provides the ability to crack WPA PSK, in addition to the normal packet capture and injection capabilities built into most wireless security tools. You can read more at `https://www.aircrack-ng.org/`.

Kismet provides wireless packet capture and sniffing features and can also be used as a wireless intrusion detection system. Kismet can be found at `https://www.kismetwireless.net/`.

WiFite, or more accurately WiFite2, is a wireless network auditing tool. It includes WPA handshake capture capabilities, support for pixie dust attacks, support for identification of hidden access points, and WPA handshake cracking, among other auditing- and penetration-testing–friendly capabilities.

If you're exploring Kali Linux, you'll find a number of other tools designed to execute specific attacks, and each of those tools can be very useful in specific circumstances. In most cases, however, one of these three tools will be your starting place for penetration tests.

Bluetooth Attacks

Bluetooth attacks can be useful for penetration testers who have physical access to a local network, or who can get into range of a target's computer, phone, vehicle, or other Bluetooth-enabled device. There are two common Bluetooth attack methods you need to be aware of for the PenTest+ exam:

- **Bluesnarfing, the theft of information from Bluetooth-enabled devices. Kali includes the bluesnarfer package, which allows phonebook contact theft via Bluetooth, given a device ID or address.**
- **Bluejacking , which sends unsolicited messages over Bluetooth devices. While discovering Bluetooth devices may be part of a penetration test, the broad fears about wide-scale exploits of Bluetooth-enabled devices have not resulted in significant real world issues. Bluetooth is a potential path into systems and should be**

Jamming

Wireless DoS can also be a legitimate technique for penetration testers, but it isn't a common technique. It may be used to prevent access to a wireless device or to prevent a device from communicating with a controller or monitoring system, as may be required as part of a penetration test. As wireless IoT devices become increasingly common, blocking them from communicating upstream may allow you to avoid detection or prevent an alarm from being sent.

Repeating

Repeating traffic, or relaying traffic, can be useful for a penetration tester who needs access to a wireless network but cannot remain in range of the network. While directional antennas can help, adding a concealed repeater to a remote network can allow traffic to be relayed over longer distances.

RFID Cloning

Access cards, ID cards, and similar tokens are often used to provide access control to facilities.
This makes cloning RFID cards a useful tool for penetration testers. While each of the technologies relies on radio frequency (RF), there are three primary types of card or device that you are likely to encounter:

- **Low frequency 125–134.2 KHz RFID cards, which can be cloned to other cards using a readily available cloning tool.**
- **High frequency 13.56 MHz tags and cards. Many phones now support this near-field communication (NFC) capability, making it possible to clone cards with phones.**
- **Ultra high frequency tags vary in range from 865 to 928 MHz, and they vary around the world because there is not an accepted international standard.**

Questions

1. Charles wants to deploy a wireless intrusion detection system. Which of the following tools is best suited to that purpose?
A. WiFite
B. Kismet
C. Aircrack-ng
D. SnortiFi

Use the following scenario for questions 2, 3, and 4.
Chris is conducting an onsite penetration test. The test is a gray box test, and he is permitted onsite but has not been given access to the wired or wireless networks. He knows he needs to gain access to both to make further progress.

2. Which of the following NAC systems would be the easiest for Chris to bypass?
A. A software client-based system
B. A DHCP proxy
C. A MAC address filter
D. None of the above

3. If Chris wants to set up a false AP, which tool is best suited to his needs?
A. Aircrack-ng
B. Kismet
C. Wireshark
D. WiFite

4. Once Chris has gained access to the network, what technique can he use to gather additional credentials?
A. ARP spoofing to become a man in the middle
B. Network sniffing using Wireshark
C. SYN floods
D. All of the above

5. What attack technique can allow the pen-tester visibility into traffic on VLANs other than their native VLAN?
A. MAC spoofing
B. Dot1q spoofing
C. ARP spoofing
D. Switch spoofing

6. What type of Bluetooth attack attempts to send unsolicited messages via Bluetooth devices?
A. Bluesnarfing
B. Bluesniping
C. Bluejacking
D. Bluesending

7. Cassandra wants to attack a WPS-enabled system. What attack technique can she use against it?
A. WPSnatch
B. Pixie dust
C. WPSmash
D. e-Lint gathering

8. What type of wireless attack focuses on tricking clients into using less secure protocols?
A. A downfall attack
B. A false negotiation attack
C. A chutes and ladders attack
D. A downgrade attack

9. Christina wants to use THC Hydra to brute-force SSH passwords. As she prepares to run the command, she knows that she recalls seeing the -t flag. What should she consider when using this flag?
A. How many targets she wants to attack
B. The number of tasks to run in parallel per target
C. The time-out for the connections
D. None of the above

10. Steve has set his penetration testing workstation up as a man in the middle between his target and an FTP server. What is the best method for him to acquire FTP credentials?
A. Capture traffic with Wireshark
B. Conduct a brute-force attack against the FTP server
C. Use an exploit against the FTP server
D. Use a downgrade attack against the next login

11. Lisa wants to enumerate possible user accounts and has discovered an accessible SMTP server. What STMP commands are most useful for this?
A. HELO and DSN
B. EXPN and VRFY
C. VRFY and TURN
D. EXPN and ETRN

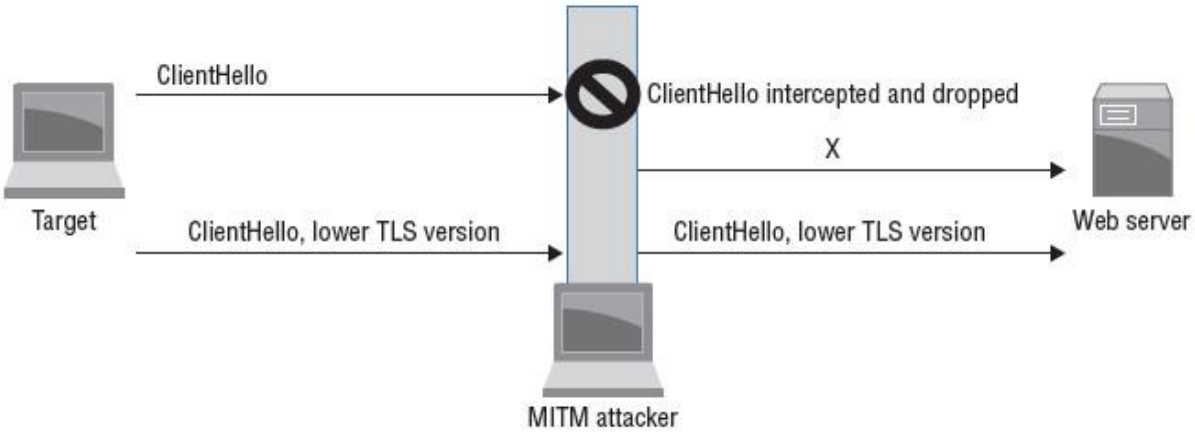
12. What is the default read-only community string for many SNMP devices?
A. secret
B. readonly
C. private
D. public

13. Which of the following tools will not allow Alice to capture NTLM v2 hashes over the wire for use in a pass-the-hash attack?
A. Responder
B. Mimikatz
C. Ettercap
D. Metasploit

14. For what type of activity would you use the tools HULK, LOIC, HOIC, and SlowLoris?
A. DDoS
B. SMB hash capture
C. DoS
D. Brute-force SSH

15. During a penetration test, Mike uses double tagging to send traffic to another system. What technique is he attempting?
A. RFID tagging
B. Tag nesting
C. Meta tagging
D. VLAN hopping

16. Elle has placed her workstation as the man in the middle, shown in the following image.
What does she need to send at point X to ensure that the downgrade attack works properly?

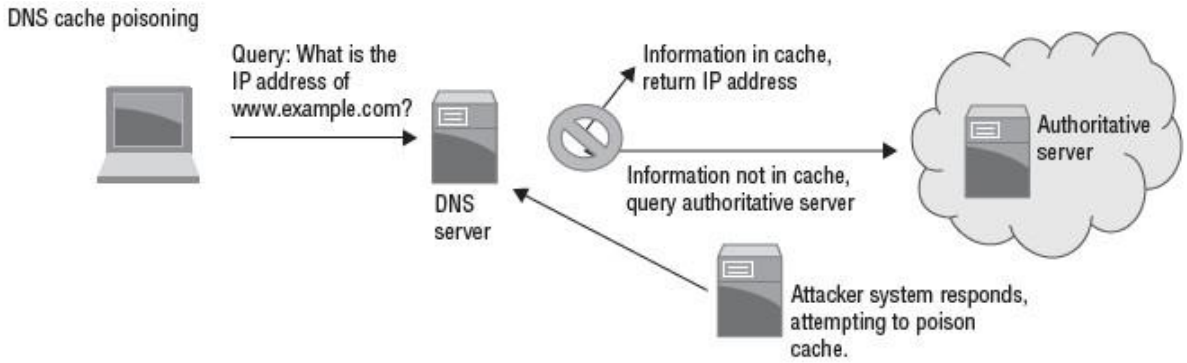


A. SYN, ACK
B. PSH, URG
C. FIN, ACK
D. SYN, FIN

17. Ron wants to use arpspoof to execute a man-in-the-middle attack between target host 10.0.1.5 and a server at 10.0.1.25, with a network gateway of 10.0.1.1. What commands does he need to run to do this? (Choose two.)
A. arpspoof -i eth0 -t 10.0.1.5 -r 10.0.1.25
B. arpspoof -i eth0 -t 10.0.1.5 -r 10.0.1.1
C. arpspoof -i eth0 -t 255.255.255.255 -r 10.0.1.25
D. arpspoof -i eth0 -t 10.0.1.25 -r 10.0.1.5

18. Jessica wants to list the domain password policy for a Windows domain. What net command can she use to do this?
A. net view /domainpolicy
B. net accounts /domain
C. net /viewpolicy
D. net domain /admin

19. Cynthia attempted a DNS poisoning attack as shown here. After her attempt, she does not see any traffic from her target system. What most likely happened to cause the attack to fail?



A. The DNS information was incorrect.
B. The injection was too slow.
C. The DNS cache was not refreshed.
D. The client did not receive a trusted response.

20. Elle wants to clone an RFID entry access card. Which type of card is most easily cloned using inexpensive cloning devices?

A. Low frequency 125 to 134.2 KHz card
B. Medium frequency 400 to 451 KHz card
C. High frequency 13.56 MHz card
D. Ultra high frequency 865 to 928 MHz card