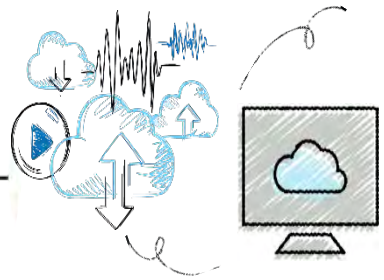
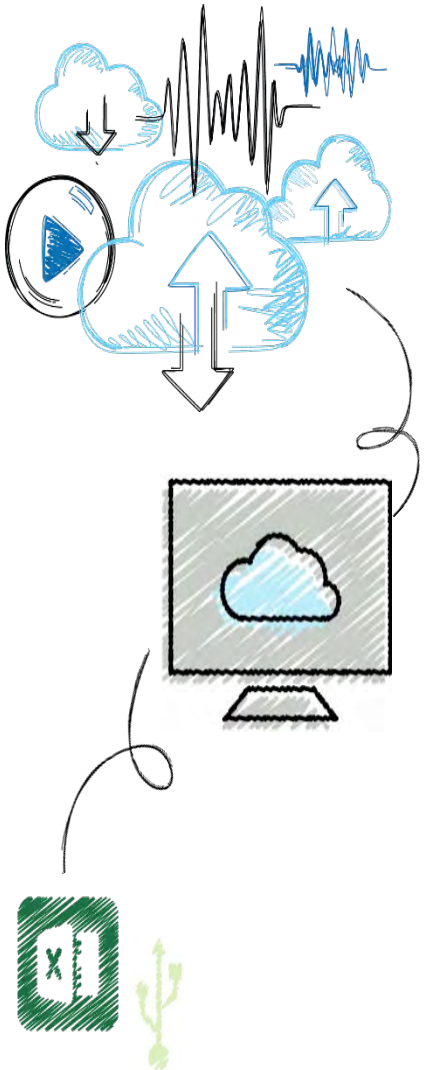
CompTIA Security+

Module 5

Networking and Server Attacks





Objectives

5.1 Describe the different types of networking-based attacks

5.2 Explain how servers are attacked

Networking-Based Attacks

- There are several attacks that target a network or a process that relies on a network
- These attacks can be grouped into:
  - Interception attacks
  - Poisoning attacks

Interception

- Some attacks are designed to intercept network communications
- Three of the most common interception attacks:
  - Man-in-the-middle attacks
  - Man-in-the-browser attacks
  - Reply attacks

Man-in-the-Middle (MITM) (1 of 2)

- Man-in-the-Middle attacks
  - Interception of legitimate communication and forging a fictitious response to the sender
  - Two computers are sending and receiving data with a computer between them
- A MITM could occur between two users
  - However, many MITM attacks are between a user and a server

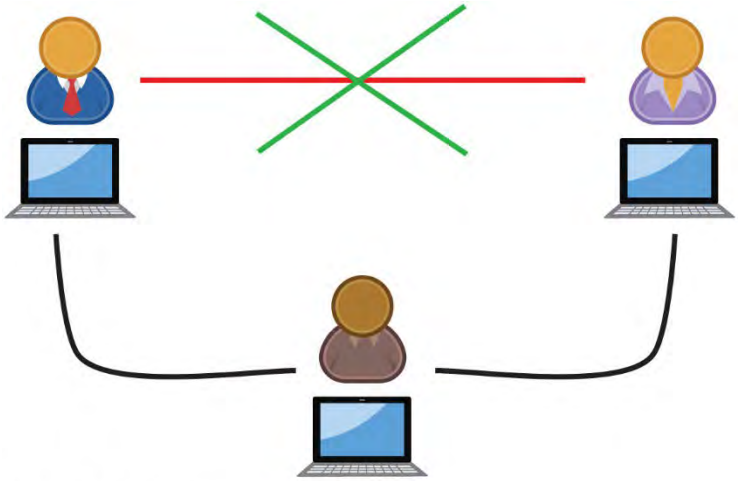


Figure 5-1 Conceptual MITM attack

Man-in-the-Middle (MITM) (2 of 2)

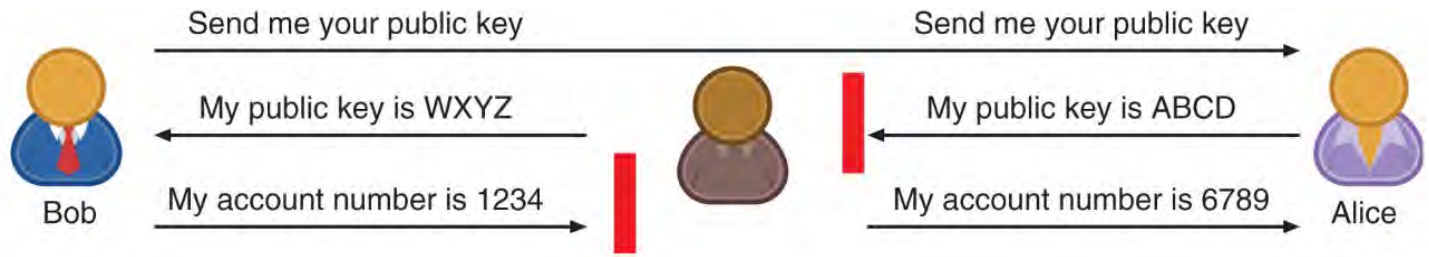


Figure 5-2 MITM attack intercepting public key

Man-in-the-Browser (MITB) (1 of 2)

- Man-in-the-browser (MITB) attack intercepts communication between parties to steal or manipulate the data
  - Occurs between a browser and the underlying computer
- A MITB attack usually begins with a Trojan infecting the computer and installing an “extension” into the browser configuration
  - When the browser is launched the extension is activated
  - Extension waits for a specific webpage in which a user enters information such as account number and password for a financial institution
  - When users click “Submit” the extension captures all the data from the fields on the form
    - May even modify some of the data

Man-in-the-Browser (MITB) (2 of 2)

- Advantages to a MITB attack:
  - Most MITB attacks are distributed through a Trojan browser extension making it difficult to recognize that malicious code has been installed
  - An infected MITB browser might remain dormant for months until triggered by the user visiting a targeted website
  - MITB software resides exclusively within the web browser, making it difficult for standard anti-malware software to detect it

Replay

- Replay attacks
  - Attacker makes copy of transmission before sending it to the original recipient
    - Uses copy at a later time
  - Example: capturing logon credentials
- Methods to prevent replay attacks
  - Both sides can negotiate and create a random key that is valid for a limited period or for a specific process
  - Use timestamps in all messages and reject any message that fall outside of a normal window of time

Poisoning

- Poisoning
  - The act of introducing a substance that harms or destroys
- Three types of attacks inject “poison” into a normal network process to facilitate an attack:
  - ARP poisoning
  - DNS poisoning
  - Privilege escalation

ARP Poisoning (1 of 2)

- Address Resolution Protocol (ARP)
  - If the IP address for a device is known but the MAC address is not, the sending computer sends an ARP packet to determine the MAC address
  - MAC addresses are stored in an ARP cache for future reference
  - All computers that “hear” the ARP reply also cache the data
- ARP poisoning
  - Relies upon MAC spoofing, which is imitating another computer by means of changing the MAC address

ARP Poisoning (2 of 2)

Attack	Description
Steal data	An attacker can substitute her own MAC address and steal data intended for another device
Prevent internet access	An attacker can substitute an invalid MAC address for the network gateway so that no users can access external networks
Man-in-the-middle	A man-in-the-middle device can be set to receive all communications by substituting that MAC address
Denial of Service attack	The valid IP address of the target can be substituted with an invalid MAC address, causing all traffic destined for the target to fail

DNS Poisoning (1 of 2)

- DNS poisoning
  - Domain Name System is the current basis for name resolution to IP address
  - DNS poisoning substitutes DNS addresses to redirect a computer to another device
- Two locations for DNS poisoning
  - Local host table
  - External DNS server

```
127.0.0.1       localhost
161.6.18.20     www.wku.edu          # Western Kentucky University
74.125.47.99    www.google.com       # My favorite search engine
216.77.188.41   www.att.net          # Internet service provider
```

Figure 5-3 Sample HOSTS file

Privilege Escalation

- Access rights
  - Privileges to access hardware and software resources that are granted to users
- Privilege escalation
  - Exploiting a software vulnerability to gain access to resources that the user normally would be restricted from accessing
- Two types of privilege escalation:
  - When a lower privilege user accesses functions restricted to higher privilege users (sometimes called **vertical privilege escalation**)
  - When a user with restricted privilege accesses different restricted functions of a similar user (**horizontal privilege escalation**)

Server Attacks

- A compromised server can provide threat actors with its privileged contents or provide an opening for attacking any of the devices that access that server
- Typical server attacks include:
  - Denial of service
  - Web server application attacks
  - Hijacking
  - Overflow attacks
  - Advertising attacks
  - Exploiting browser vulnerabilities

Denial of Service (DoS) (1 of 3)

- Denial of service (DoS)
  - A deliberate attempt to prevent authorized users from accessing a system by overwhelming it with requests
- Most DoS attacks today are **distributed denial of service (DDoS)**
  - Using hundreds or thousands of devices flooding the server with requests
- Smurf attack
  - An attacker broadcasts a network request to all computers on the network but changes the address from which the request came from (called **IP spoofing**)
  - Appears as if victim's computer is asking for response from all computers on the network
  - All computers send a response to the victim's computer so that it is overwhelmed

Denial of Service (DoS) (2 of 3)

- DNS amplification attack
  - Flood a victim by redirecting valid responses to it
  - Uses publicly accessible and open DNS servers to flood a system with DNS response traffic
- SYN flood attack
  - Takes advantage of procedures for initiating a session
- In a SYN flood attack against a web server:
  - The attacker sends SYN segments in IP packets to the server
  - Attacker modifies the source address of each packet to computer addresses that do not exist or cannot be reached

Denial of Service (DoS) (3 of 3)

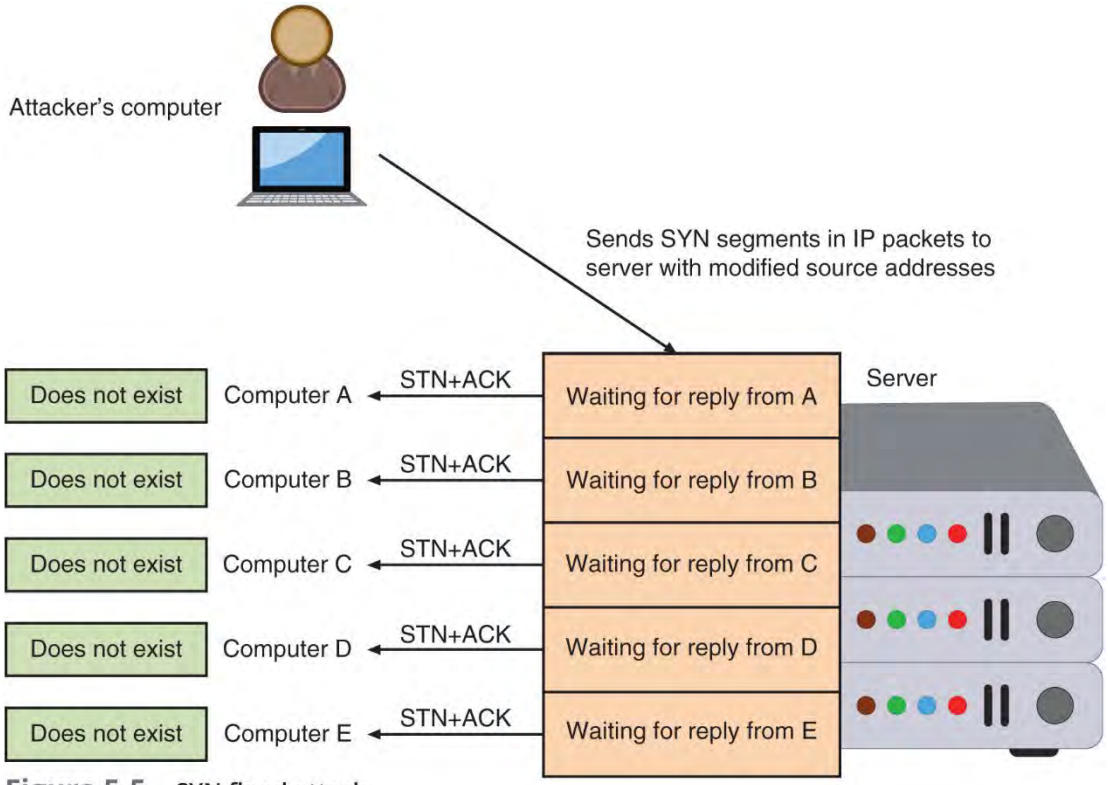


Figure 5-5 SYN flood attack

Web Server Application Attacks (1 of 2)

- Securing web applications is more difficult than protecting other systems
- **Zero-day attack** - an attack that exploits previously unknown vulnerabilities, victims have no time to prepare for or defend against the attack
- Traditional network security devices can block traditional network attacks, but cannot always block web application attacks
  - Many network security devices ignore the content of HTTP traffic
- Several different web application attacks target the input from users and are grouped into two categories:
  - Cross-site attacks
  - Injection attacks

Cross-Site Attacks (1 of 4)

- In a **cross-site scripting (XSS) attack**
  - The threat actor takes advantage of web applications that accept user input without validating it before presenting it back to the user
- When victim visits injected Web site:
  - Malicious instructions are sent to victim's browser
- Some XSS attacks are designed to steal information:
  - Retained by the browser when visiting specific sites
- An XSS attack requires a website meets two criteria:
  - Accepts user input without validating it
  - Uses input in a response

Cross-Site Attacks (2 of 4)

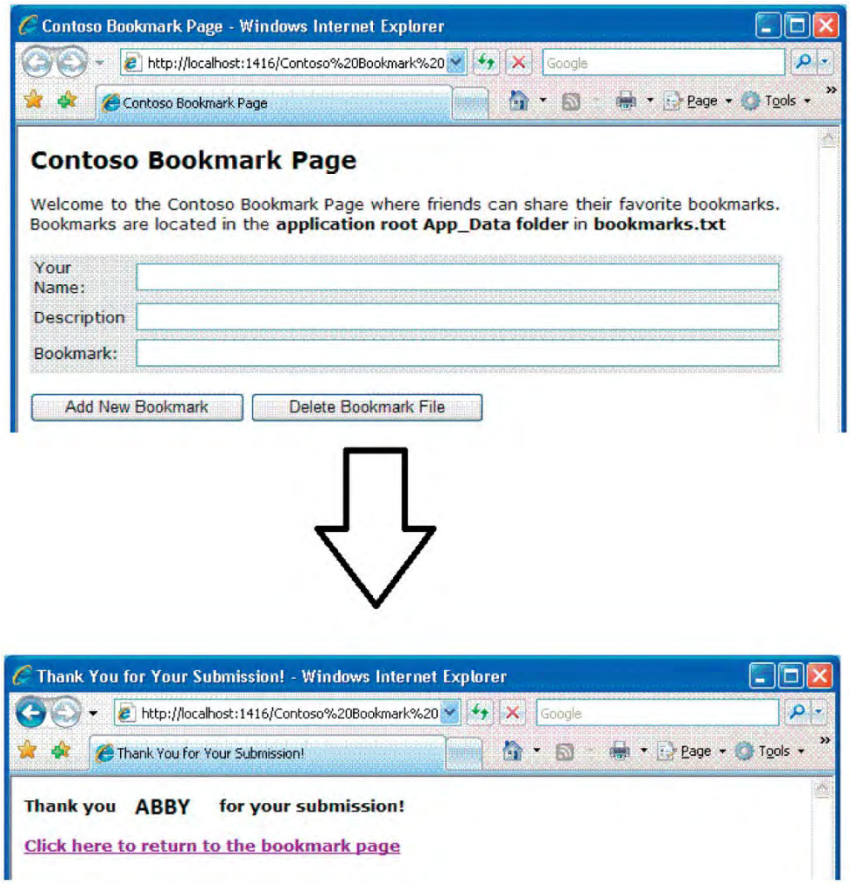


Figure 5-7 Bookmark page that accepts user input

Cross-Site Attacks (3 of 4)

- Cross-Site Request Forgery (XSRF)
  - This attack uses the user's web browser settings to impersonate that user
- If a user is currently authenticated on a website and is tricked into loading another webpage
  - The new page inherits the identity and privileges of the victim to perform an undesired function on the attacker's behalf

Cross-Site Attacks (4 of 4)

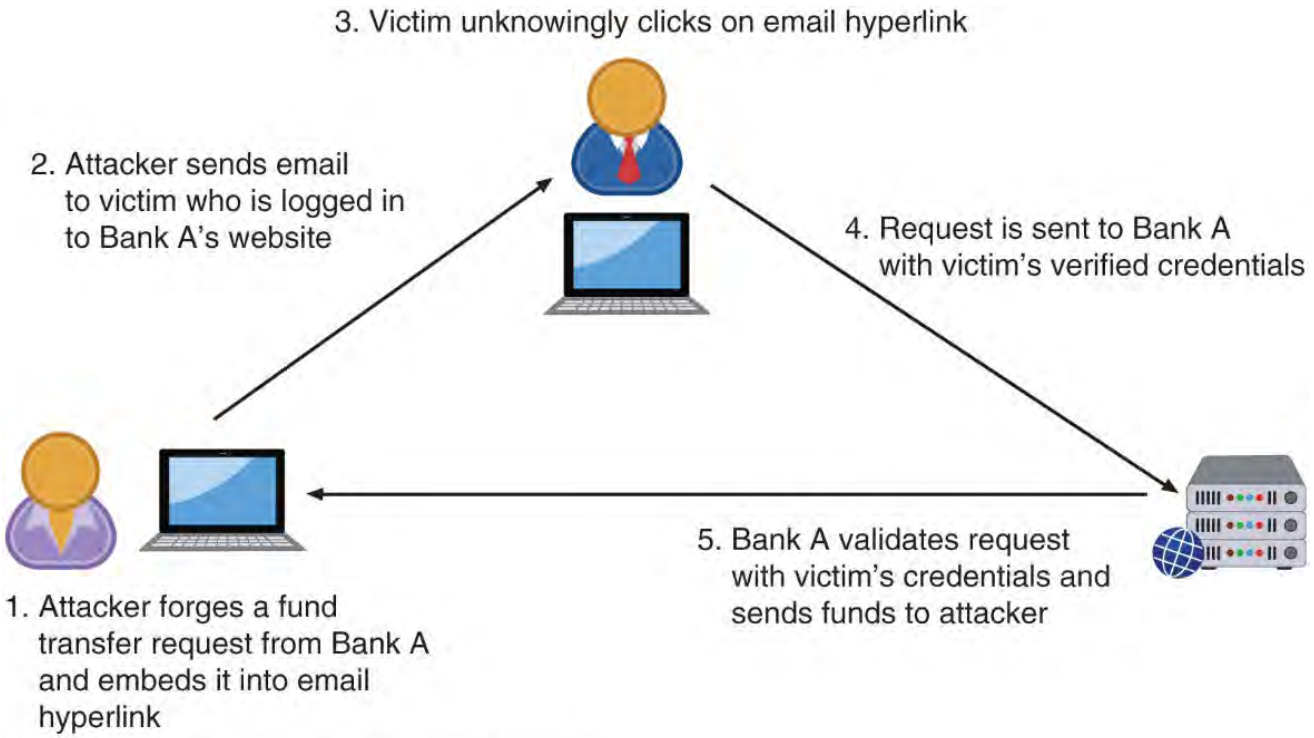


Figure 5-9 Cross-site request forgery

Injection Attacks (1 of 4)

- Injection attacks
  - Introduce new input to exploit a vulnerability
- One of the most common injection attacks, called SQL injection, inserts statements to manipulate a database server
- SQL (Structured Query Language)
  - Used to view and manipulate data stored in relational database
- Forgotten password example:
  - Attacker enters fictitious e-mail address that included a single quotation mark as part of the data
  - Response lets attacker know whether input is being validated
  - Attacker enters email field in SQL statement

Injection Attacks (2 of 4)

- Forgotten password example (continued):
  - Statement is processed by the database
  - Example statement:

    SELECT fieldlist FROM table WHERE field = ‘whatever’ or ‘a’=‘a’
  - Result: All user email addresses will be displayed

Injection Attacks (3 of 4)

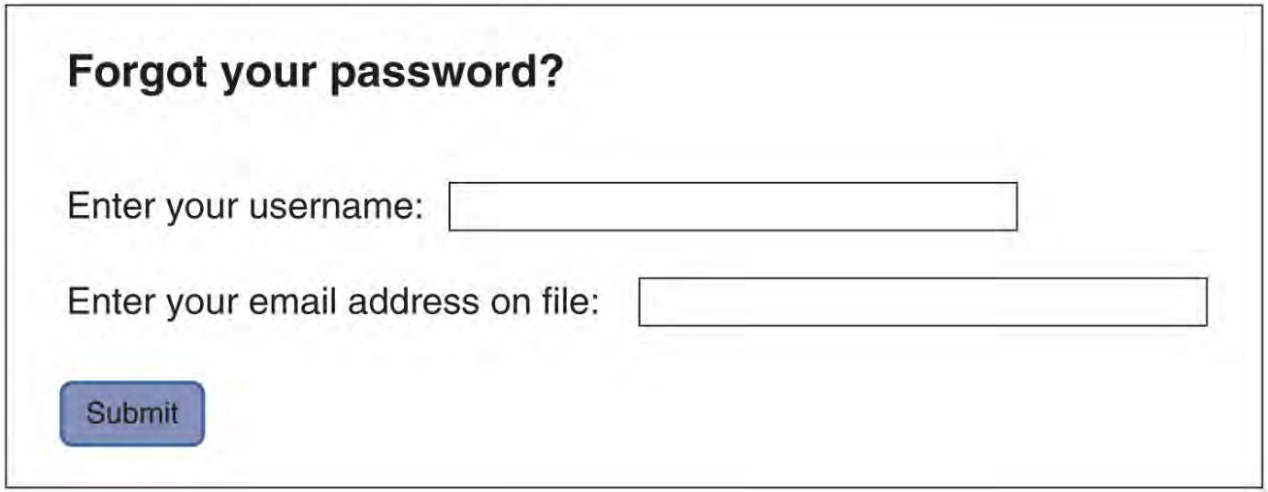


Figure 5-10 Request form for forgotten password

Injection Attacks (4 of 4)

SQL injection statement	Result
whatever’ AND email is NULL;--	Determine the names of different fields in the database
whatever’ AND 1=(SELECT COUNT(*)FROM tabname);-	Discover the name of the table
whatever’ OR full name LIKE Mia	Find specific users
whatever’; DROP TABLE members; --	Erase the database table
whatever’; UPDATE members SET email= ‘attacker-email@evil.net’ WHERE email = ‘Mia@good.com’;	Mail password to attacker’s email account

Hijacking

- Several server attacks are the result of threat actors “commandeering” a technology and then using it for an attack
- Common hijacking attacks include:
  - Session hijacking
  - URL hijacking
  - Domain hijacking
  - Clickjacking

Session Hijacking

- **Session Hijacking**
  - Attacker attempts to impersonate user by stealing or guessing session token
  - Session token is a random string assigned to an interaction between user and web application
- An attacker can attempt to obtain the session token:
  - By using XSS or other attacks to steal the session token cookie from the victim's computer
  - Eavesdropping on the transmission
  - Guessing the session token

URL Hijacking

- **URL hijacking** (also called **typo squatting**)
  - Users are directed to a fake look-alike site filled with ads for which the attacker receives money for traffic generated to the site
  - Attackers purchase the domain names of sties that are spelled similarly to actual sites
- Threat actors are also registering domain names that are one bit different (called **bitsquatting**)

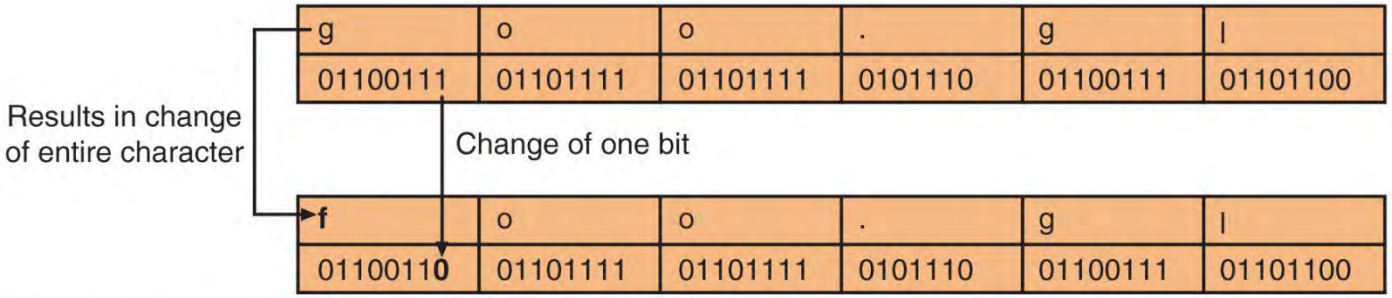


Figure 5-11 Character change by bit flipping

Domain Hijacking

- **Domain hijacking** occurs when a domain pointer that links a domain name to a specific web server is changed by a threat actor
- When a domain is hijacked
  - A threat actor gains access to the domain control panel and redirects the registered domain to a different physical web server

Clickjacking

- Clickjacking
  - Hijacking a mouse click
  - The user is tricked into clicking a link that is other than what it appears to be
- Clickjacking often relies upon threat actors who craft a zero-pixel IFrame
  - IFrame (short for inline frame) is an HTML element that allows for embedding another HTML document inside the main document
  - A zero-pixel IFrame is virtual invisible to the naked eye

Overflow Attacks

- Overflow attacks
  - Designed to “overflow” areas of memory with instructions from the attacker
- Types of overflow attacks:
  - Buffer overflow attacks
  - Integer overflow attacks

Buffer Overflow (1 of 2)

- Buffer overflow attacks
  - Occur when a process attempts to store data in RAM beyond the boundaries of a fixed-length storage buffer
  - Extra data overflows into adjacent memory locations
- An attacker can overflow the buffer with a new address pointing to the attacker's malware code

Buffer Overflow (2 of 2)

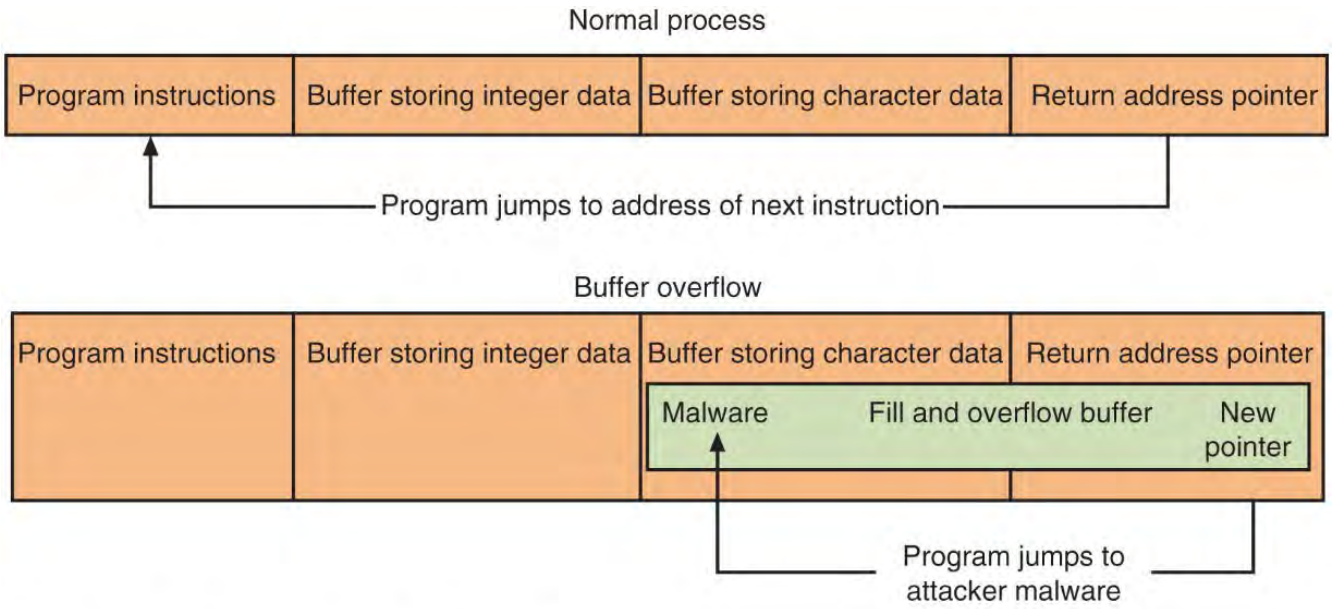


Figure 5-12 Buffer overflow attack

Integer Overflow

- An **integer overflow** is the condition that occurs when the result of an arithmetic operation exceeds the maximum size of the integer type used to store it
- In an **integer overflow attack**:
  - An attacker changes the value of a variable to something outside the range that the programmer had intended by using an integer overflow
- This type of attack could be used in the following situations:
  - An attacker could use an integer overflow attack to create a buffer overflow situation
  - A program that calculates the total cost of items purchased would use the number of units sold times the cost per unit. If an integer overflow were introduced, it could result in a negative value and a resulting negative total cost
  - A large positive value in a bank transfer could be wrapped around by an integer overflow attack to become a negative value
    - Could reverse flow of money

Advertising Attacks

- Several attacks attempt to use ads or manipulate the advertising system
- Two of the most common:
  - Malvertising
  - Ad fraud

Malvertising

- Threat actors use third-party advertising networks to distribute malware to unsuspecting users who visit a well-known site
  - Known as malvertising or a poisoned ad attack
- An ad that contains malware redirects visitors who receive it to the attacker's webpage that then downloads Trojans and ransomware onto the user's computer
- Preventing malvertising is difficult
  - Website operators are unaware of the types of ads that are being displayed
  - Users have a false sense of security going to a "mainstream" website
  - Turning off ads that support plug-ins such as Adobe Flash often disrupts the user's web experience

Ad Fraud

- Threat actors manipulate pre-roll ads to earn ad revenue that is directed back to them
- Attackers have created a “robo-browser” called Methbot
  - That spoofs all the necessary interacted needed to initiate, carry out, and complete ad auctions

Browser Vulnerabilities

- Web browser additions have introduced vulnerabilities in browsers that access servers
- These additions are:
  - Extensions
  - Plug-ins
  - Add-ons

Scripting Code

- Adding dynamic content
  - Web server downloads a “script” or series of instructions in the form of computer code that commands the browser to perform specific actions
- JavaScript is the most popular scripting code
  - JavaScript instructions are embedded inside HTML documents
- There are different defense mechanisms intended to prevent JavaScript programs from causing serious harm
- However, there are security concerns
  - A malicious JavaScript program could capture and remotely transmit user information without the user’s knowledge or authorization

Extensions

- Extensions expand the normal capabilities of a web browser
  - For a specific webpage
- Most extensions are written in JavaScript
  - So that the browser can support dynamic actions
- Extensions are browser dependent
  - An extension that works in Google Chrome will not function in Microsoft Edge

Plug-Ins (1 of 2)

- Plug-in
  - Adds new functionality to a web browser so users can play music, view videos, or display special graphical images
- A single plug-in can be used on different web browsers
- One common plug-in supports Java
  - Java can be used to create a separate program called a Java applet
- Most widely used plug-ins for web browsers:
  - Java, Adobe Flash player, Apple QuickTime, and Adobe Acrobat Reader

Plug-Ins (2 of 2)

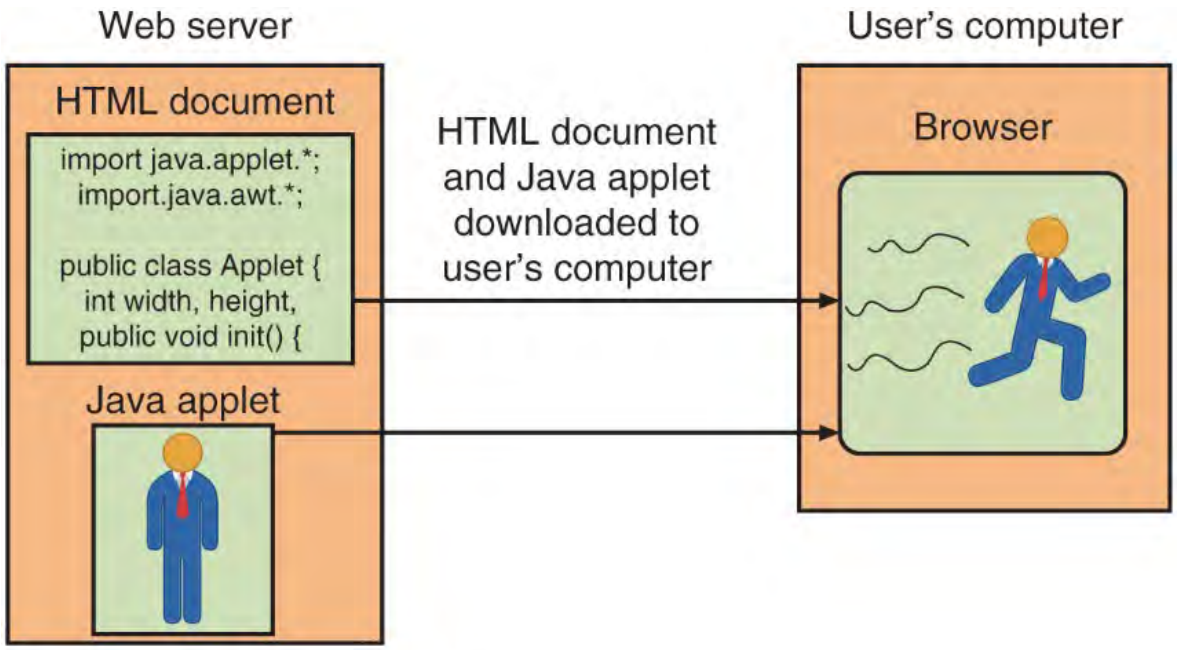


Figure 5-14 Java applet

Add-Ons (1 of 2)

- Add-ons
  - Add a greater degree of functionality to the web browser
- Add-ons can do the following:
  - Create additional web browser toolbars
  - Change browser menus
  - Be aware of other tabs open in the same browser
  - Process the content of every webpage that is loaded
- Due to the risks associated with extensions, plug-ins, and add-ons
  - Efforts are being made to minimize them
  - Some web browsers now block plug-ins
  - HTML5 standardizes sound and video formats so that plug-ins like Flash are no longer needed

Add-Ons (2 of 2)

Name	Description	Location	Browser support	Examples
Extension	Written in JavaScript and has wider access to privileges	Part of web browser	Only works with a specific browser	Download selective links on webpages, display specific fonts
Plug-in	Links to external programs	Outside of web browser	Compatible with many different browsers	Audio, video, PDF file display
Add-on	Adds functionality to browser itself	Part of the web browser	Only works with a specific browser	Dictionary and language packs

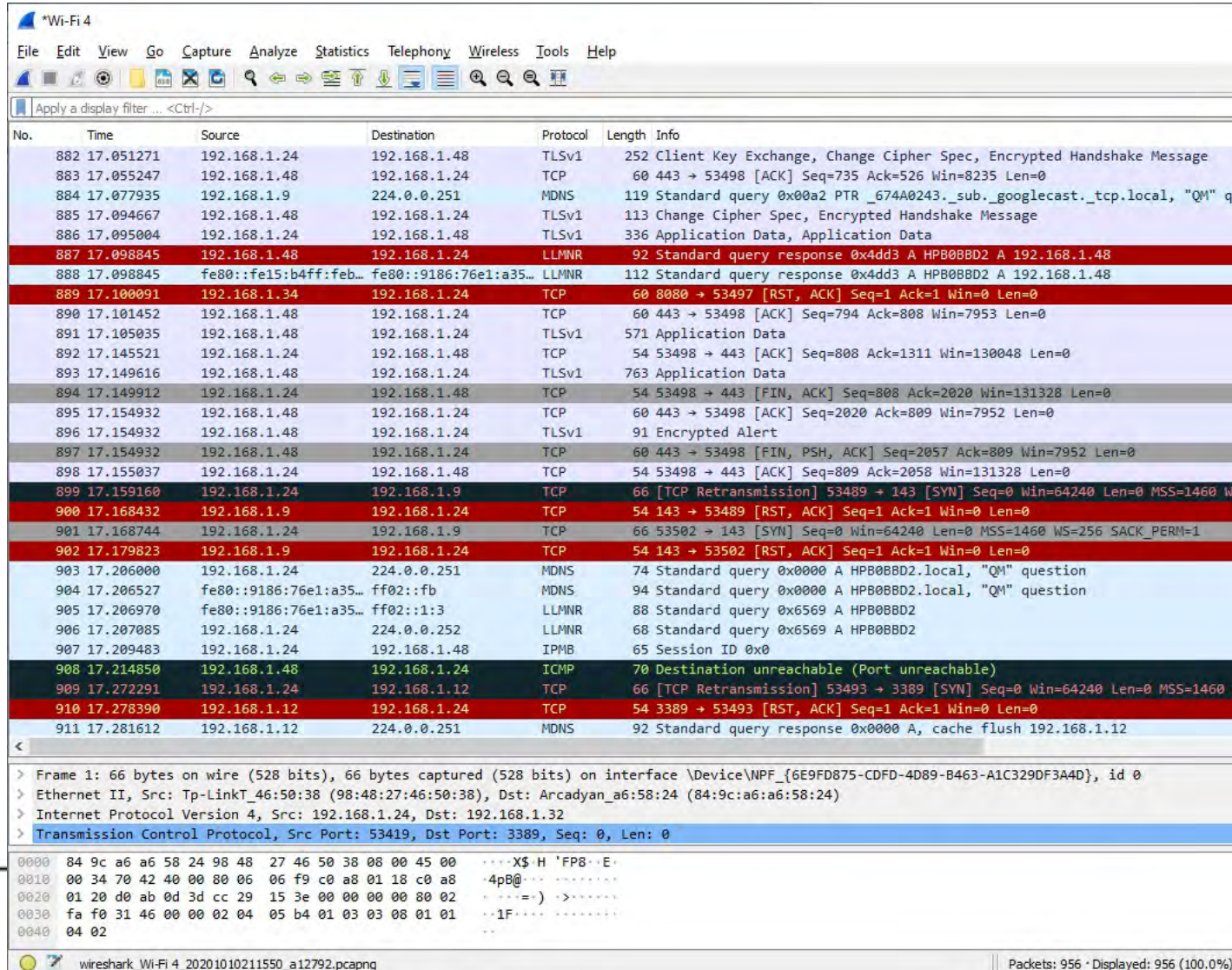
WireShark

- Download and Install WireShark

  -https://www.wireshark.org/#download

WireShark

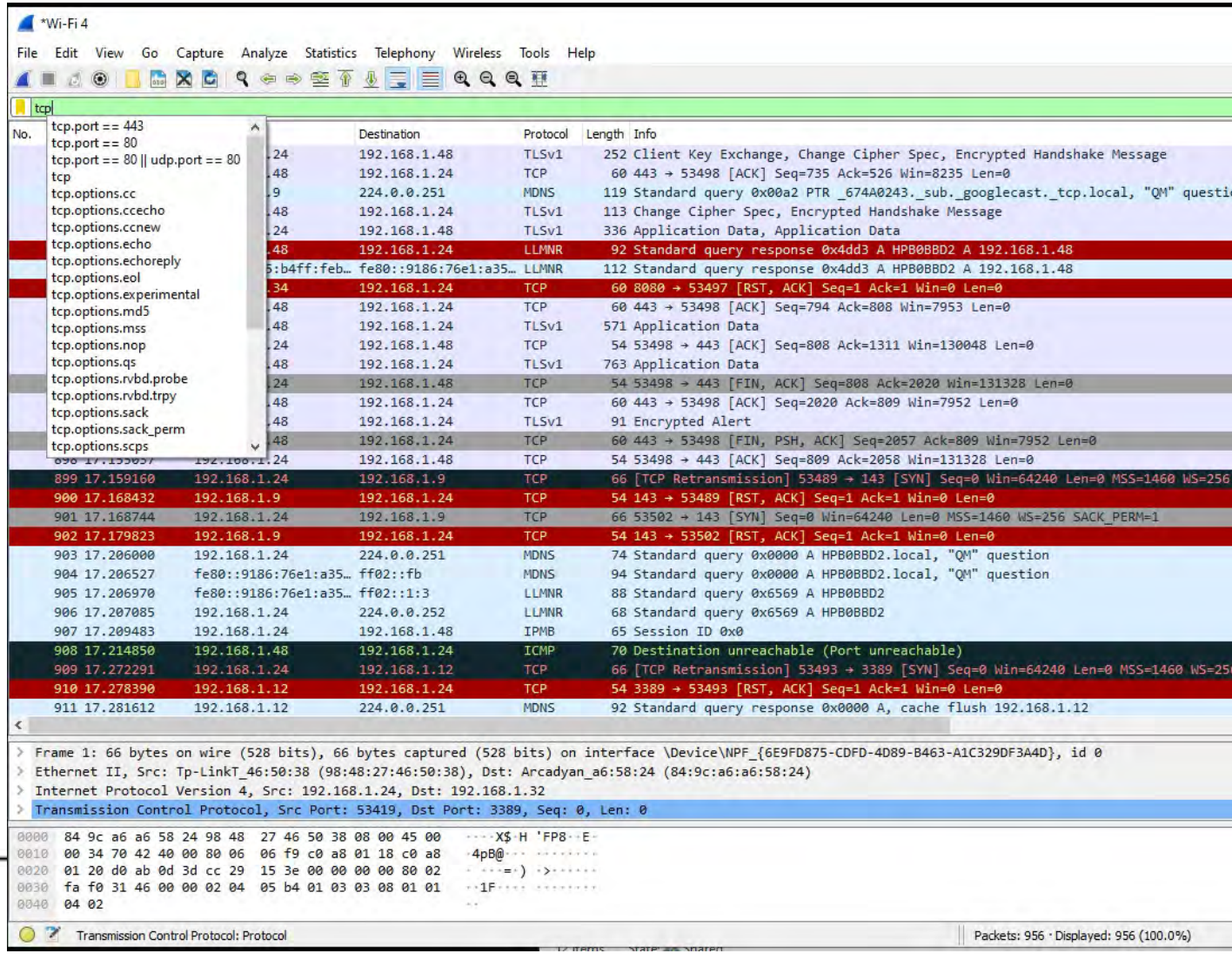
- Start/Open Capture



WireShark

- In the Filter Box

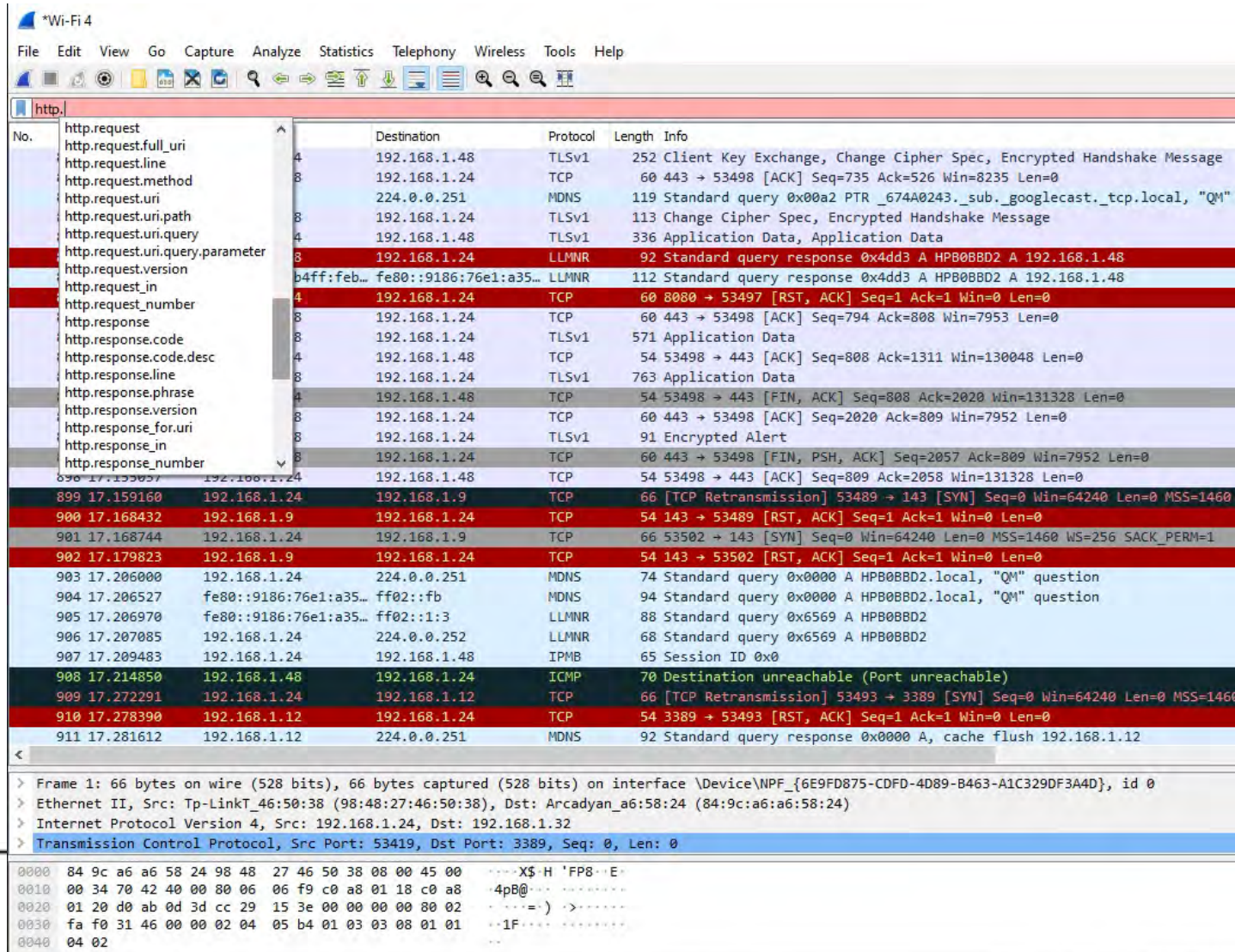
  Type “TCP”



WireShark

- In the Filter Box

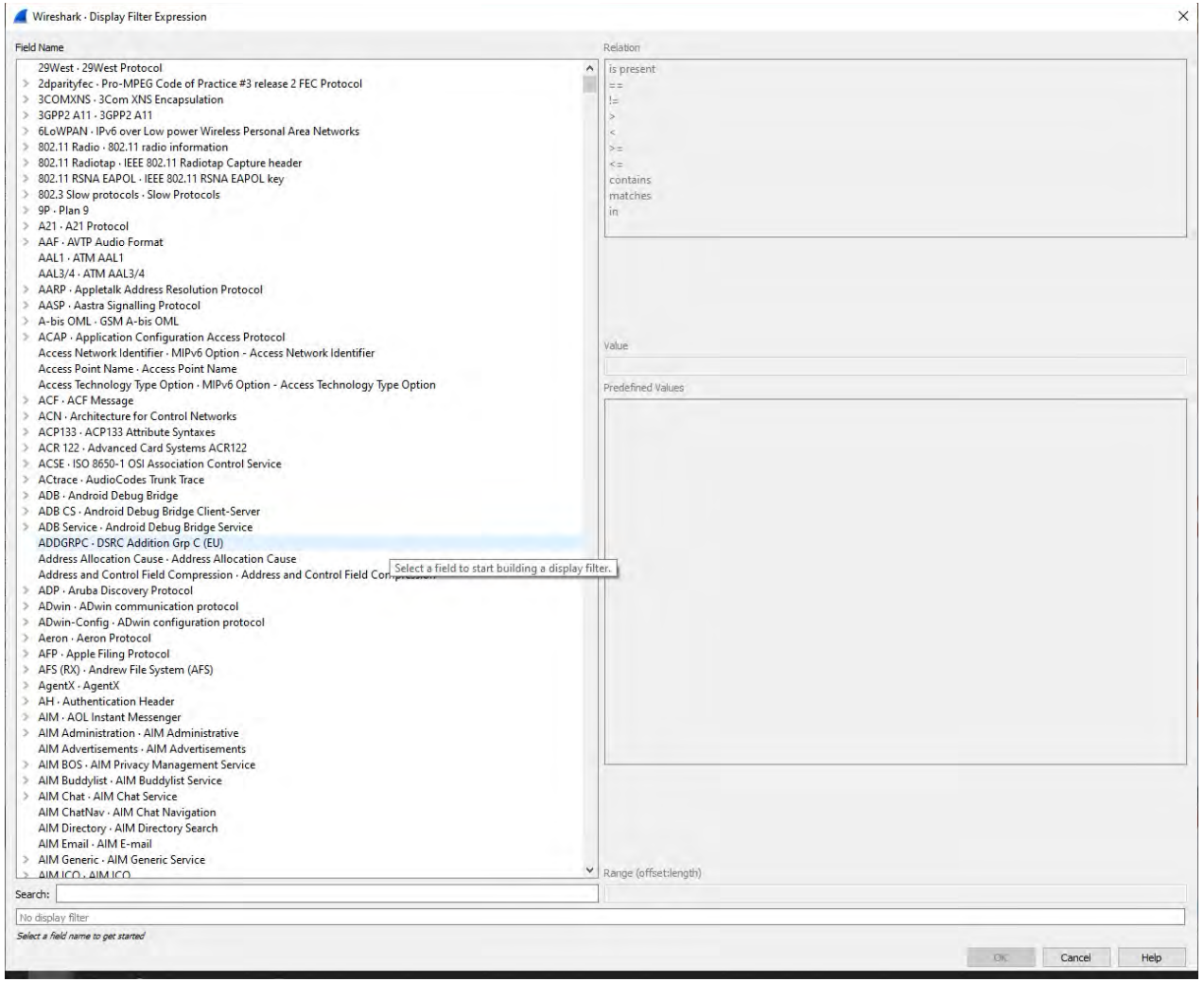
  Type “HTTP”



WireShark

On the Tool Bar

- Select
- “Analyze”
- Then
- “Display Filter Expression”



Review Questions

Which attack intercepts communications between a web browser and the underlying computer?

A. man-in-the-middle (MITM)

B. man-in-the-browser (MITB)

C. replay

D. ARP poisoning

Review Questions

Which attack intercepts communications between a web browser and the underlying computer?

A. man-in-the-middle (MITM)

B. **man-in-the-browser (MITB)**

C. replay

D. ARP poisoning

Review Questions

Lydia was asked to protect the system from a DNS poisoning attack. What are the locations she would need to protect?

A. Web server buffer and host DNS server

B. Reply referrer and domain buffer

C. Web browser and browser add-on

D. Hosts file and external DNS server

Review Questions

Lydia was asked to protect the system from a DNS poisoning attack. What are the locations she would need to protect?

A. Web server buffer and host DNS server

B. Reply referrer and domain buffer

C. Web browser and browser add-on

D. **Hosts file and external DNS server**

Review Questions

Nathan is concerned that attackers could be exploiting a vulnerability in software to gain access to resources that the user normally would be restricted from accessing. What type of attack is he worried about?

A. Privilege escalation

B. Session replay

C. Scaling exploit

D. Amplification

Review Questions

Nathan is concerned that attackers could be exploiting a vulnerability in software to gain access to resources that the user normally would be restricted from accessing. What type of attack is he worried about?

A. **Privilege escalation**

B. Session replay

C. Scaling exploit

D. Amplification

Review Questions

What is the difference between a DoS and a DDoS attack?

A. DoS attacks are faster than DDoS attacks

B. DoS attacks use fewer computers than DDoS attacks

C. DoS attacks do not use DNS servers as DDoS attacks do

D. DoS attacks user more memory than a DDoS attack

Review Questions

What is the difference between a DoS and a DDoS attack?

A. DoS attacks are faster than DDoS attacks

B. **DoS attacks use fewer computers than DDoS attacks**

C. DoS attacks do not use DNS servers as DDoS attacks do

D. DoS attacks user more memory than a DDoS attack

Review Questions

John was explaining about an attack that accepts user input without validating it and uses that input in a response. What type of attack was he describing?

A. SQL

B. XSS

C. XSRF

D. DDoS DNS

Review Questions

John was explaining about an attack that accepts user input without validating it and uses that input in a response. What type of attack was he describing?

A. SQL

B. **XSS**

C. XSRF

D. DDoS DNS

Review Questions

What is the basis of an SQL injection attack?

A. to expose SQL code so that it can be examined

B. to have the SQL server attack client web browsers

C. to insert SQL statements through unfiltered user input

D. to link SQL servers into a botnet

Review Questions

What is the basis of an SQL injection attack?

A. to expose SQL code so that it can be examined

B. to have the SQL server attack client web browsers

C. **to insert SQL statements through unfiltered user input**

D. to link SQL servers into a botnet

Review Questions

Why are extensions, plug-ins, and add-ons considered to be security risks?

A. They are written in Java, which is a weak language.

B. They have introduced vulnerabilities in browsers.

C. They use bitcode.

D. They cannot be uninstalled.

Review Questions

Why are extensions, plug-ins, and add-ons considered to be security risks?

A. They are written in Java, which is a weak language.

B. **They have introduced vulnerabilities in browsers.**

C. They use bitcode.

D. They cannot be uninstalled.

Review Questions

A replay attack _____.

A. can be prevented by patching the web browser

B. is considered to be a type of DoS attack

C. makes a copy of the transmission for use at a later time

D. replays the attack over and over to flood the server

Review Questions

A replay attack _____.

A. can be prevented by patching the web browser

B. is considered to be a type of DoS attack

C. **makes a copy of the transmission for use at a later time**

D. replays the attack over and over to flood the server

Coming Up Next…

CompTIA Security+

Module 6

Network Security Devices, Design, and Technology