

Master of Cybersecurity Network scanning

Prepared by Dr. Nermin Hamza

Lecture 5

جامعة الجميع الذكية

تسعى لتكون الكيان الأول الذي يتبنى مبدأ المجتمع التعليمي
التعاوني ويقدم العلم مقابل العمل للخدمة وبناء المجتمعات

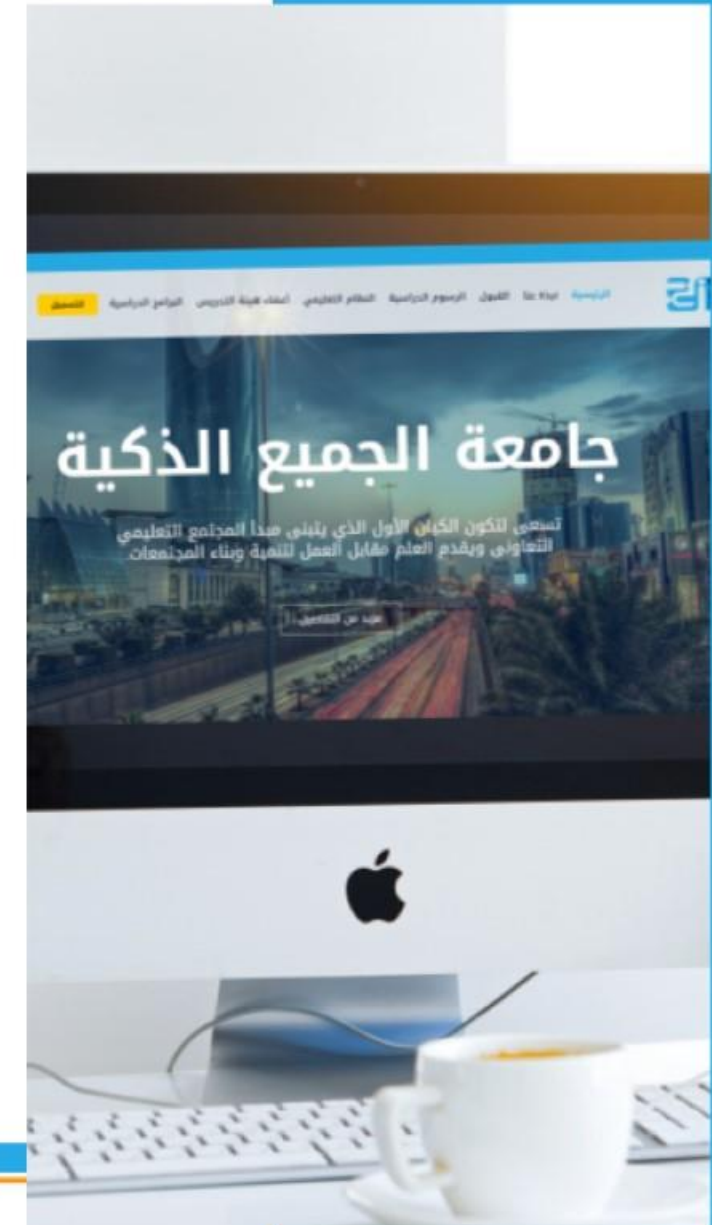
CYB740

Penetration test and Ethical hacking



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

- Password Cracking
 - Introduction
 - How can the passwords be stored?
 - Password Cracking Techniques
 - How to Defend against Password Cracking
- Network sniffing
 - Introduction
 - Types of Sniffing
 - Protocol Analyzer
 - Types of Sniffing Attacks
 - Wireshark



Chapter 05

Exploitation

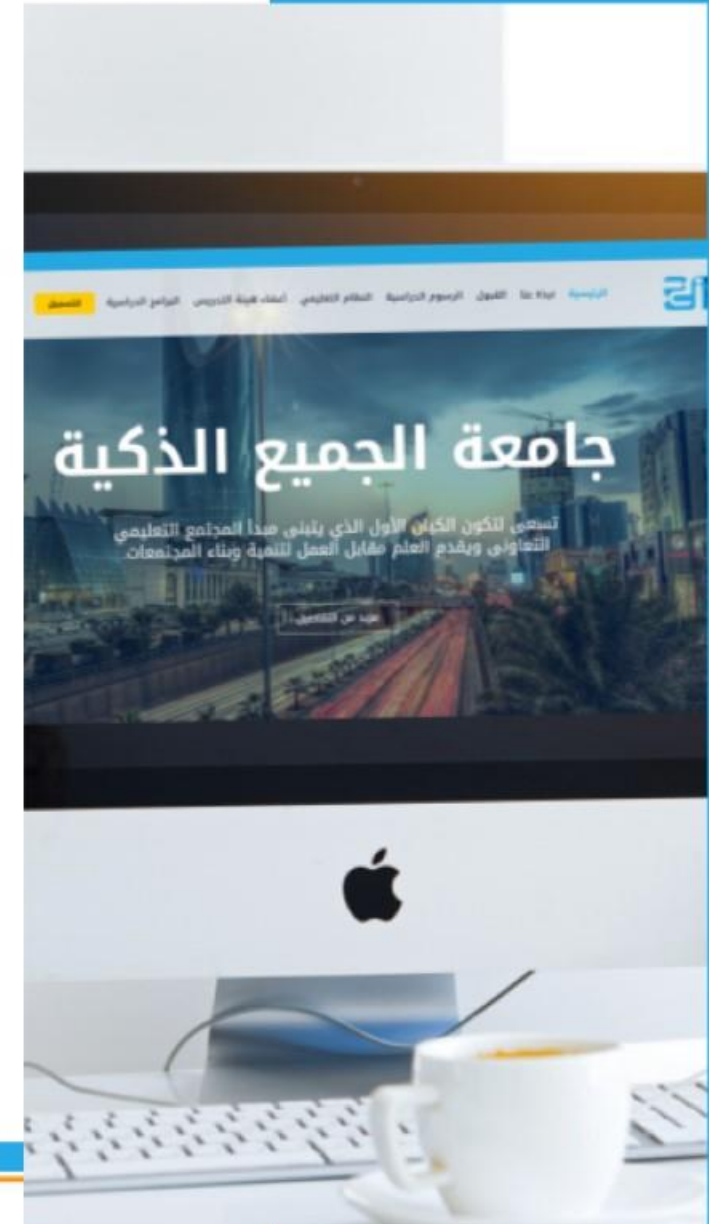
- Password Crack
- Sniffing



Chapter 05

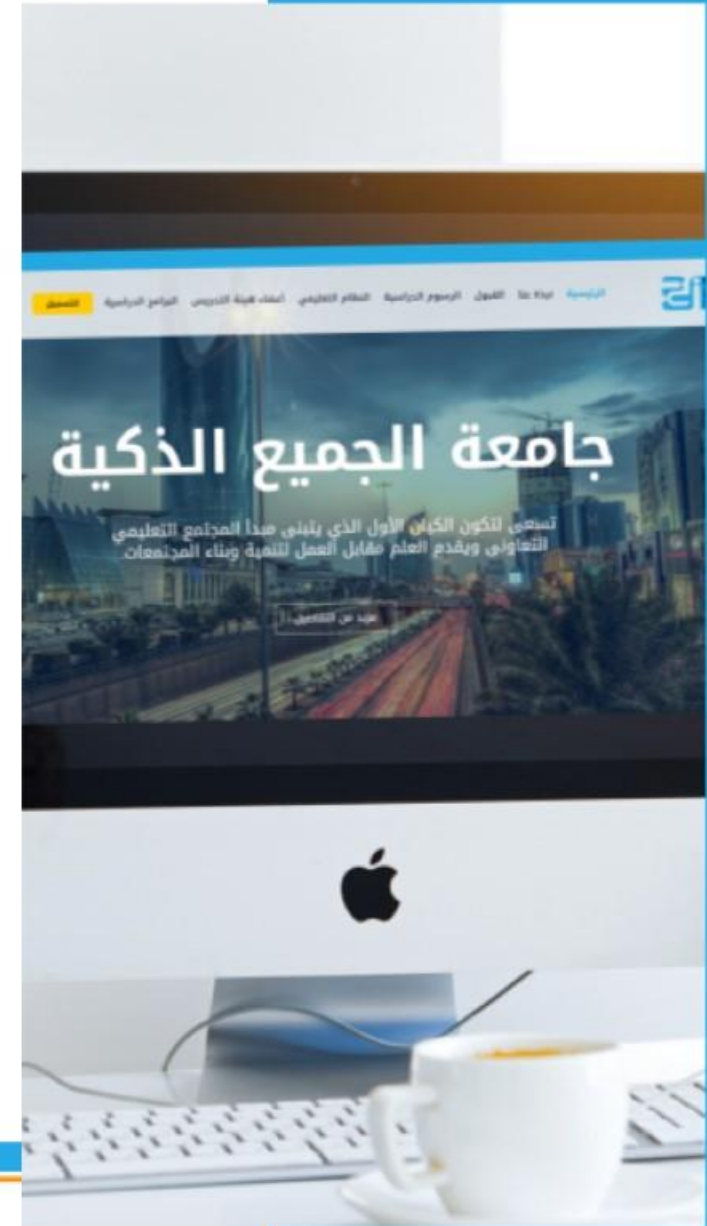
Password Cracking

- Why discussing passwords and password cracking.
- No matter what we do or how far we advance, it appears that passwords remain the most popular way to protect data and allow access to systems.
- With this in mind, let us take a brief detour to cover the basics of password cracking.

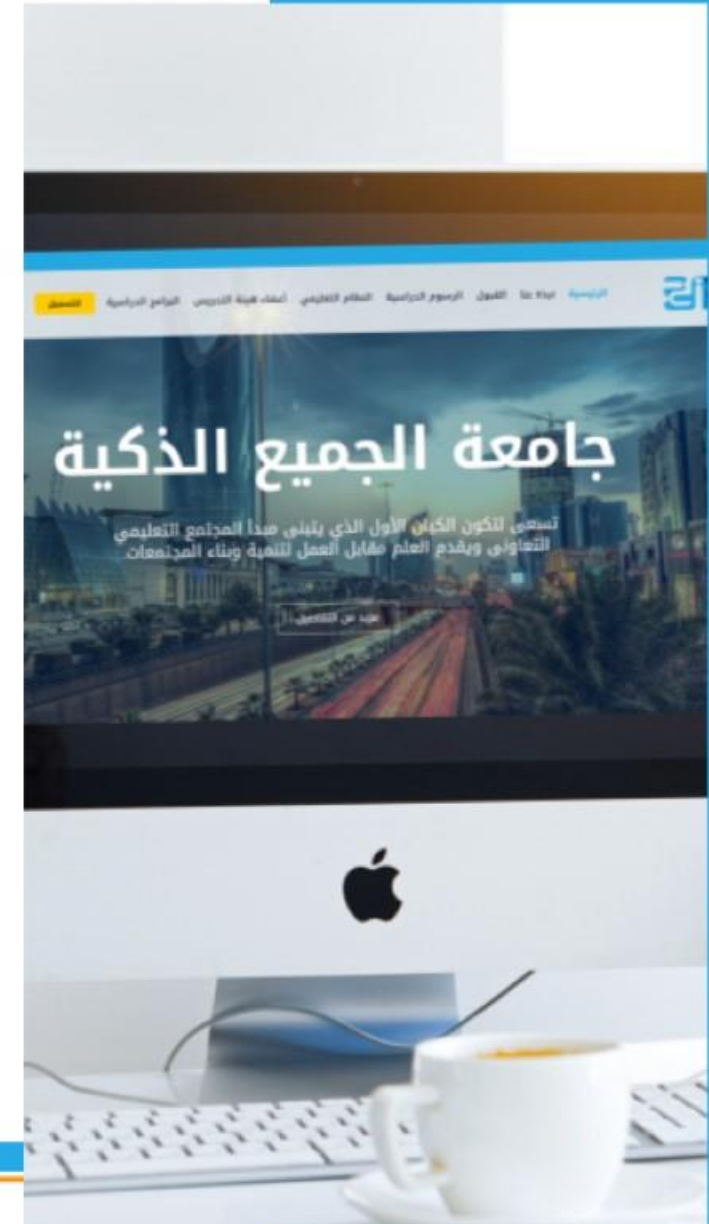


There are several reasons why a penetration tester would be interested in cracking passwords.

- First and foremost, this is a great technique for elevating and escalating privileges.
- Consider the following example: assume that you were able to compromise a target system but after logging in, you discover that you have no rights on that system.
- No matter what you do, you are unable to read and write in the target's files and folders and even worse, you are unable to install any new software.
- This is often the case when you get access to a low-privileged account belonging to the "user" or "guest" group.

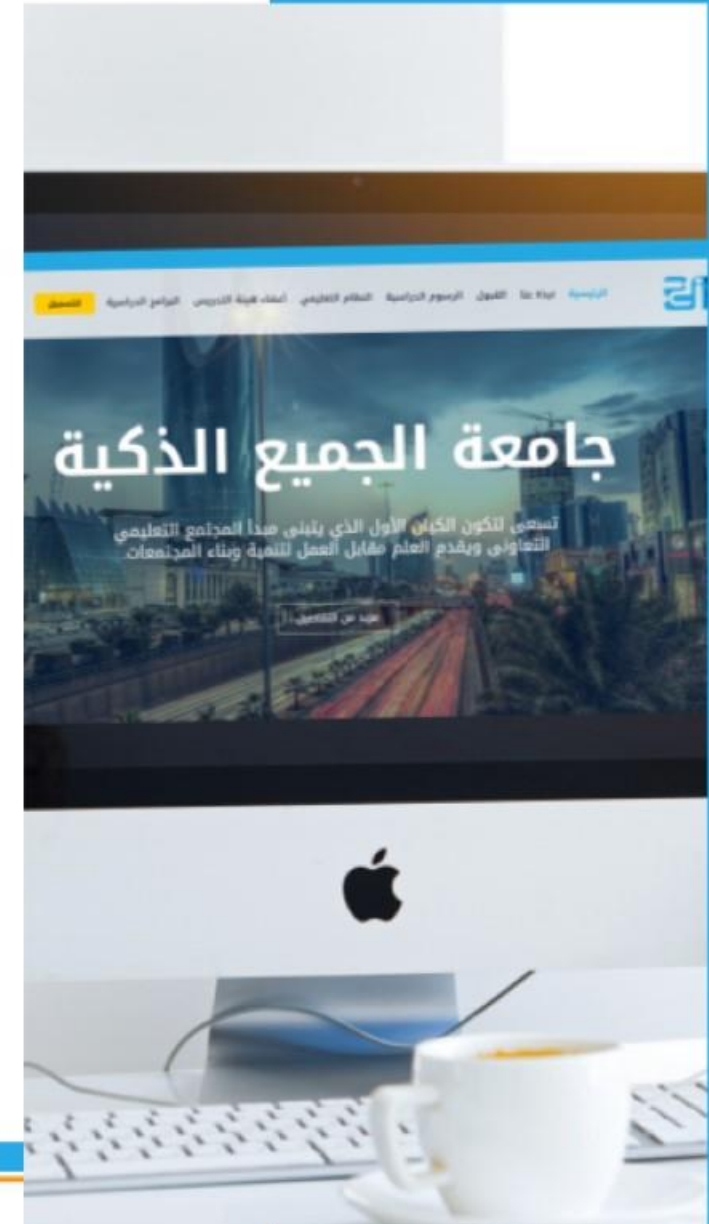


- Another reason for cracking passwords and escalating privileges is that many of the tools we run as penetration testers require administrative-level access in order to install and execute properly.
- As a final thought, on occasion, penetration testers may find themselves in a situation where they were able to crack the local administrator password (the local admin account on a machine) and have this password turn out to be the exact same password that the network administrator was using for the domain administrator account

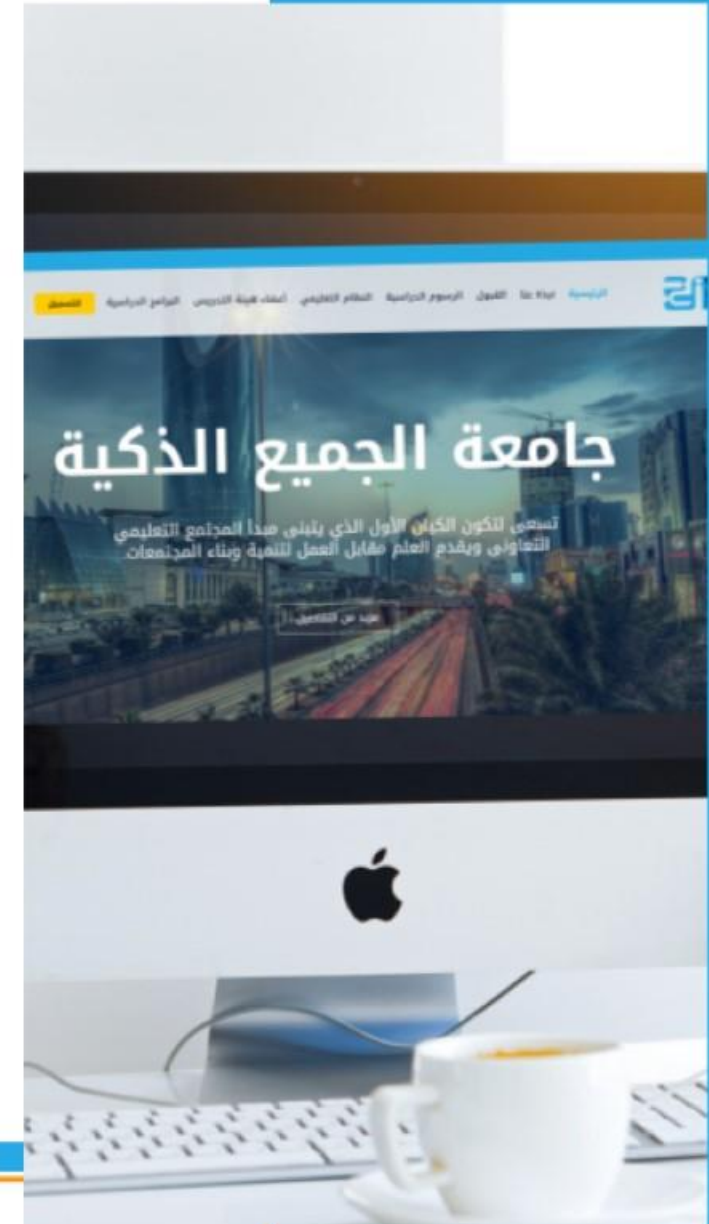


How can the passwords be stored?

- Most systems do not store your password as the plaintext value you enter, but rather they store an **encrypted version of the password**.
- This encrypted version is called a **hash**. For example, assume you pick a password “qwerty” (which is obviously a bad idea).
- When you log into your PC, you type your password “qwerty” to access the system. However, behind the scenes your computer is actually calculating, creating, passing, and checking an encrypted version of the password you entered.
- This encrypted version or hash of your password appears to be a random string of characters and numbers.



- Different systems use different hashing algorithms to create their password hashes. Most systems store their password hashes in a single location. This hash file usually contains the encrypted passwords for several users and system accounts.
- Unfortunately, gaining access to the password hashes is only half the battle because simply viewing or even memorizing a password hash (if such a thing were possible) is not enough to determine the plaintext.
- This is because technically it is not supposed to be possible to work backward from a hash to plaintext. By its definition, a hash, once encrypted, is never meant to be decrypted.



Chapter 05

Password Crack

- How Hash Passwords Are Stored in Windows SSAM?

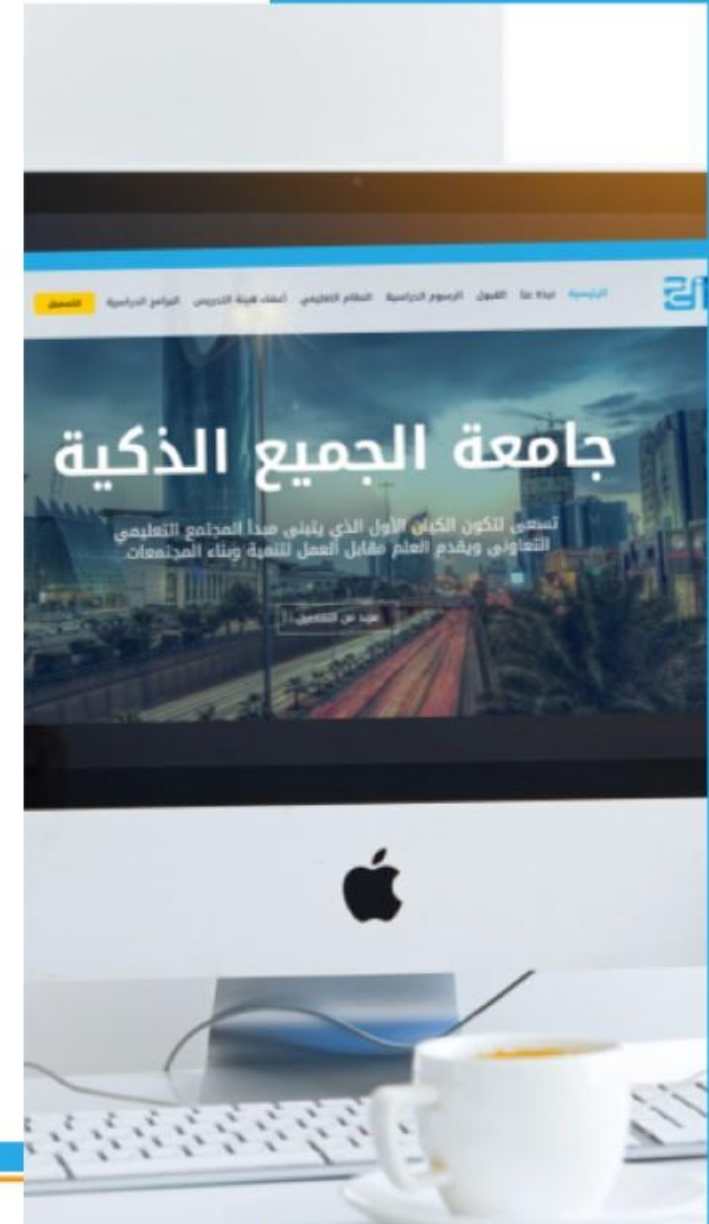
SAM File is located at `c:\windows\system32\config\SAM`

```
Administrator:500:NO PASSWORD*****:61880B9EE373475C8148A7108ACB3031:::  
Guest:501:NO PASSWORD*****:NO PASSWORD*****::  
Admin:1001:NO PASSWORD*****:BE40C450AB99713DF1EDC5B40C25AD47::  
Martin:1002:NO PASSWORD*****:BF4A502DA294ACBC175B394A080DEE79::  
Juggyboy:1003:NO PASSWORD*****:488CDCDD2225312793ED6967B28C1025::  
Jason:1004:NO PASSWORD*****:2D20D252A479F485CDF5E171D93985BF::  
Shiela:1005:NO PASSWORD*****:0CB6948805F797BF2A82807973B89537:::
```

User name User ID LM Hash NTLM Hash

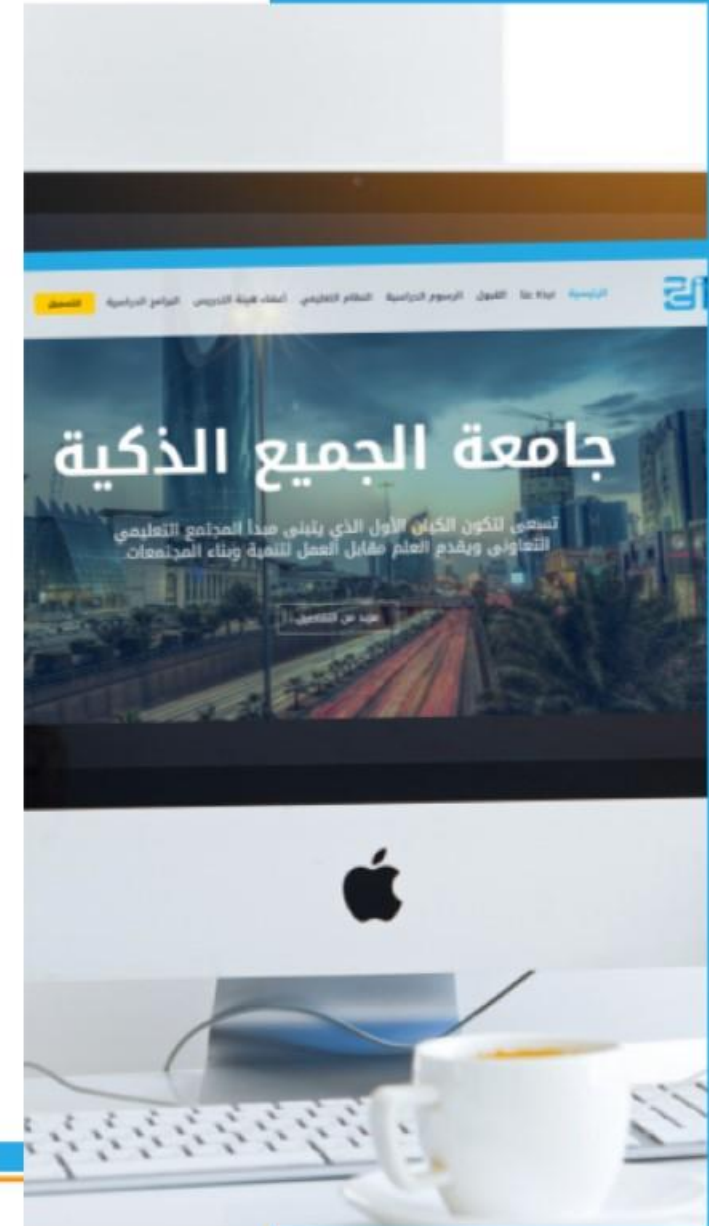


- In order to discover the plaintext version of a password, we need to circle through a series of steps.
 1. First we select a hashing algorithm
 2. second we pick a plaintext word
 3. third we encrypt the plaintext word with the hashing algorithm,
 4. and finally we compare the newly hashed word with the hash from our target.
- If the hashes match, we know the plaintext password because no two different plaintext words should produce the exact same hash.
- So, it will be slow process for a human, computers specialize in tasks like this.
- Given the computing power available today, completing the four-step process outlined above is trivial for a modern machine.



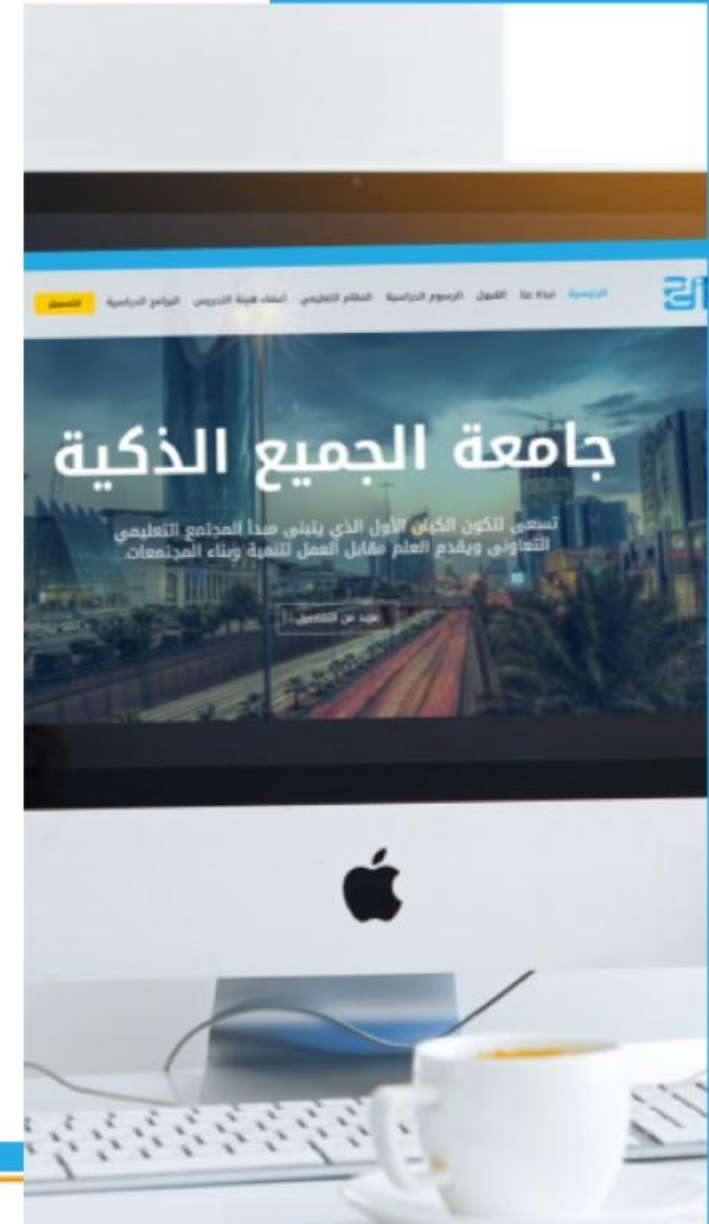
In its most basic form, password cracking consists of two parts:

1. Locate and download the target system's password hash file.
2. Use a tool to convert the hashed (encrypted) passwords into a plaintext password.



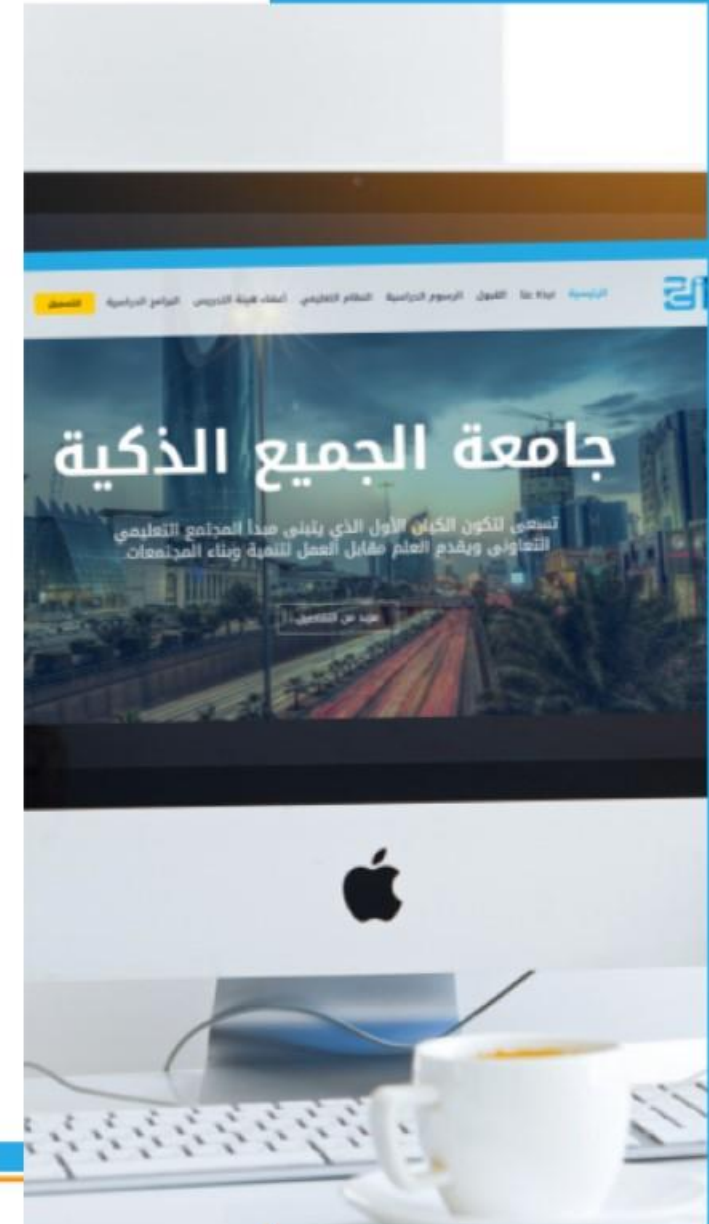
Password Cracking Techniques

- Password cracking techniques are used to recover password from computer systems
- Attackers use password cracking techniques to gain unauthorized access to the vulnerable system
- Most of the password cracking techniques are successful due to weak or easily guessable password



Password Cracking Techniques

- Dictionary attack
- Brute force attack
- Rule-based attack
- Rainbow table

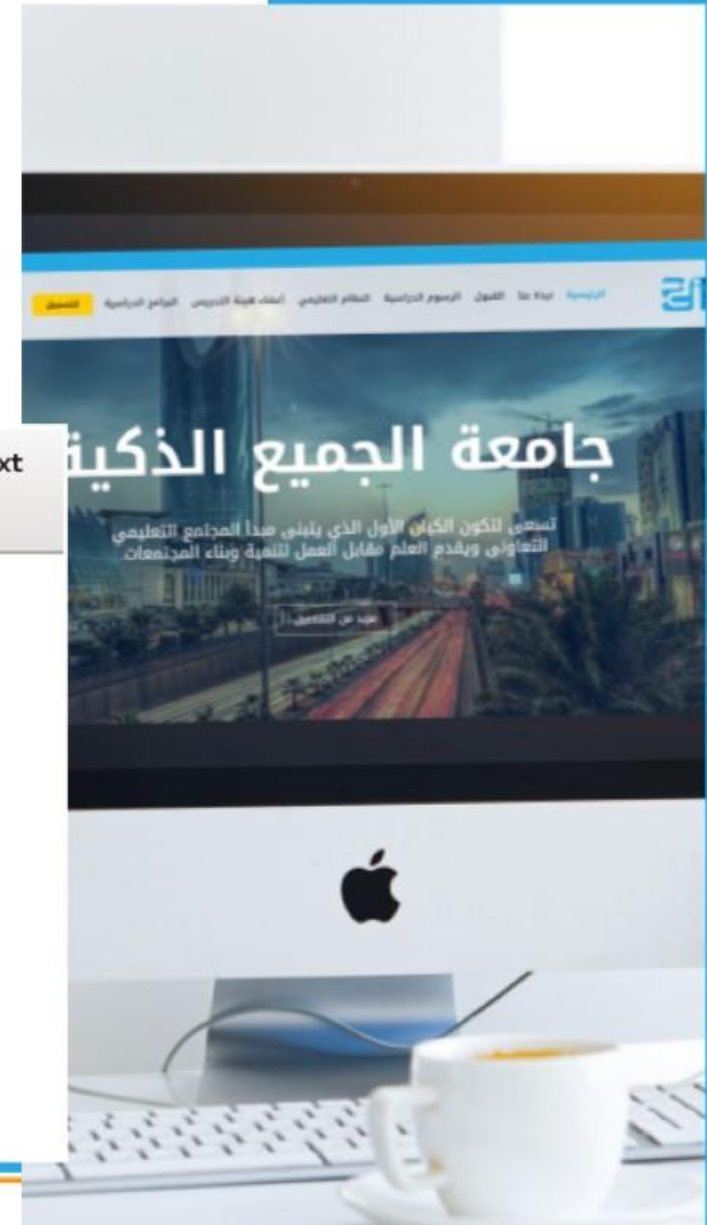


Dictionary Attack

- Dictionary Attack: is loaded into the cracing application that runs against user account

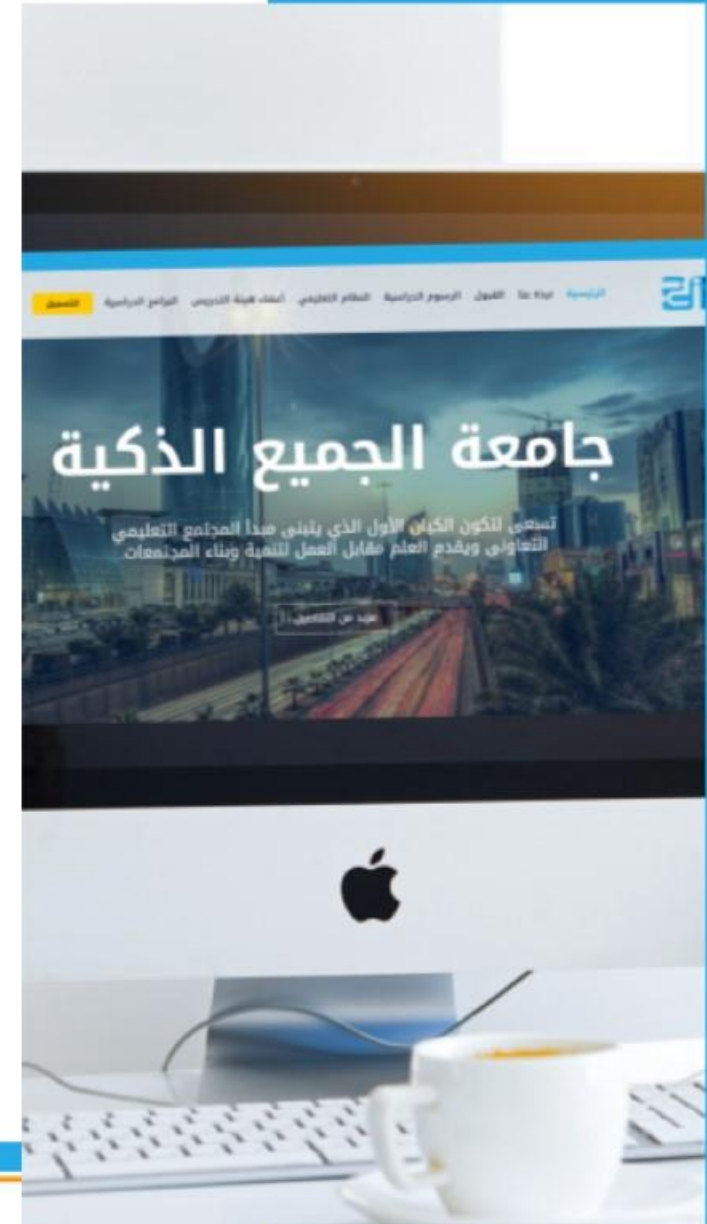
dict.txt

File	Edit	Search	Options	Help
Jackandjill				
Jackandjill0				
Jackandjill1				
Jackandjill2				
Jackandjill3				
Jackandjill4				
Jackandjill5				
Jackandjill6				
Jackandjill7				
Jackandjill8				
Jackandjill9				
Jackandjill10				
Jackandjill11				
Jackandjill12				
Jackandjill13				
Jackandjill14				



Brute Forcing Attack

- The program tries every combination of characters until the password is broken



Dictionary Attacks vs. Brute Force Attacks

Dictionary Attacks



Hackers generate a list of common passwords to try against vulnerable accounts



Take less time



Adaptable based on location

Brute Force Attacks



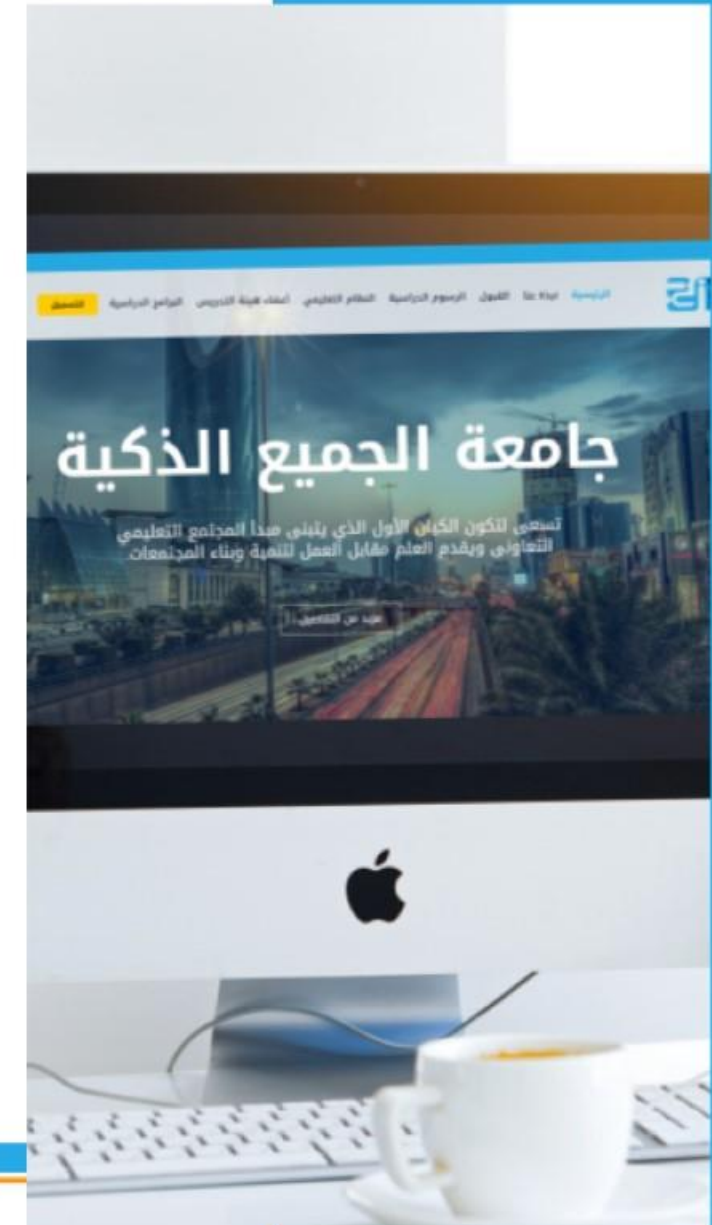
Hackers generate a list of complex passwords to try against vulnerable accounts



Take more time

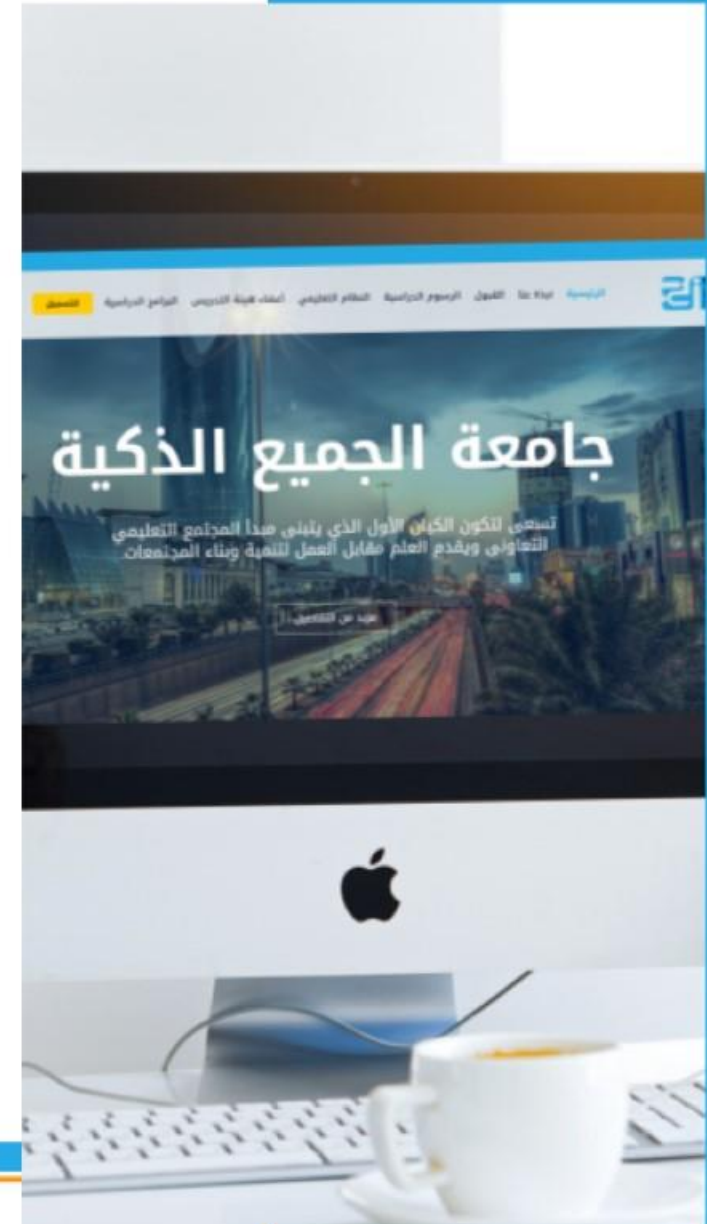


Require advanced password cracking software



Rule-Based Attack

- This attack is used when the attacker get some information about the password.



Rainbow Table

- Is precomputed table which contains word lists like dictionary files and brute force list and their hash values.
- Compare the hash of the passwords and compare it with the precomputed hash table.
- If a match is found then the password is cracked.
- It is easy to recover passwords by comparing captured password hashes to the precomputed tables.

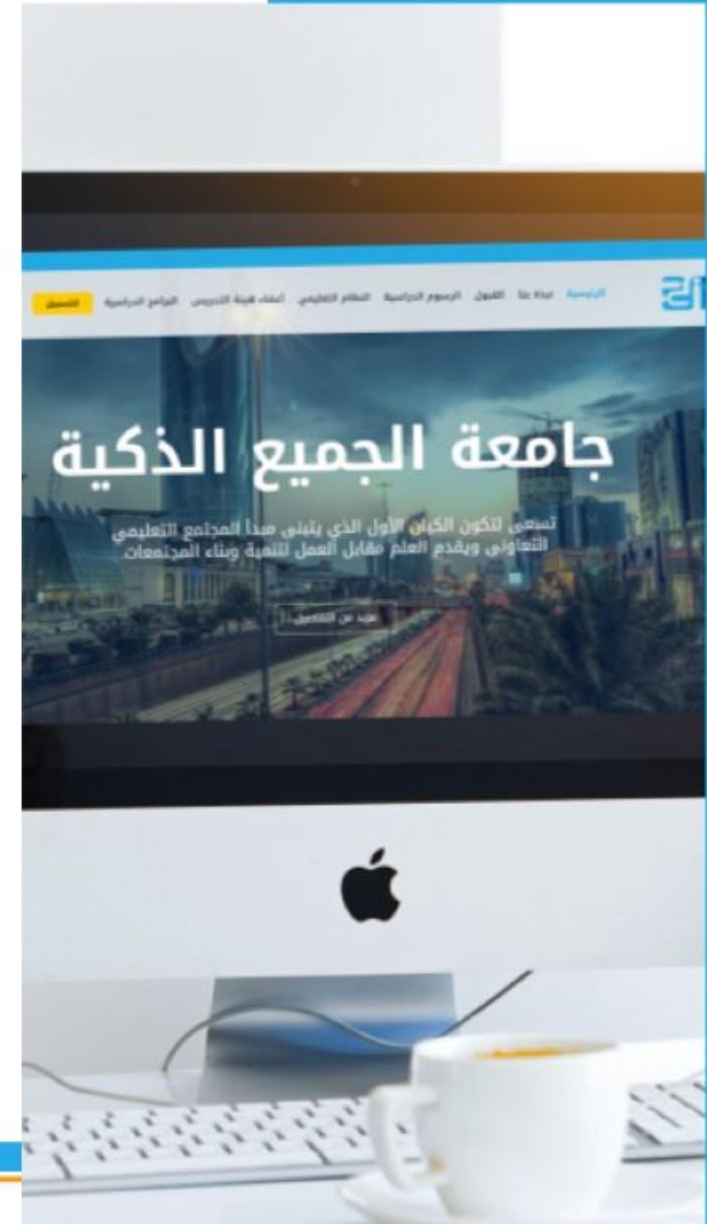
Precomputed Hashes	
1qazwed	4259cc34599c530b28a6a8f225d668590
hh021da	c744b1716cbf8d4dd0ff4ce31a177151
9da8dasf	3cd696a8571a843cda453a229d741843
sodifo8sf	c744b1716cbf8d4dd0ff4ce31a177151



Chapter 05

Password Cracking

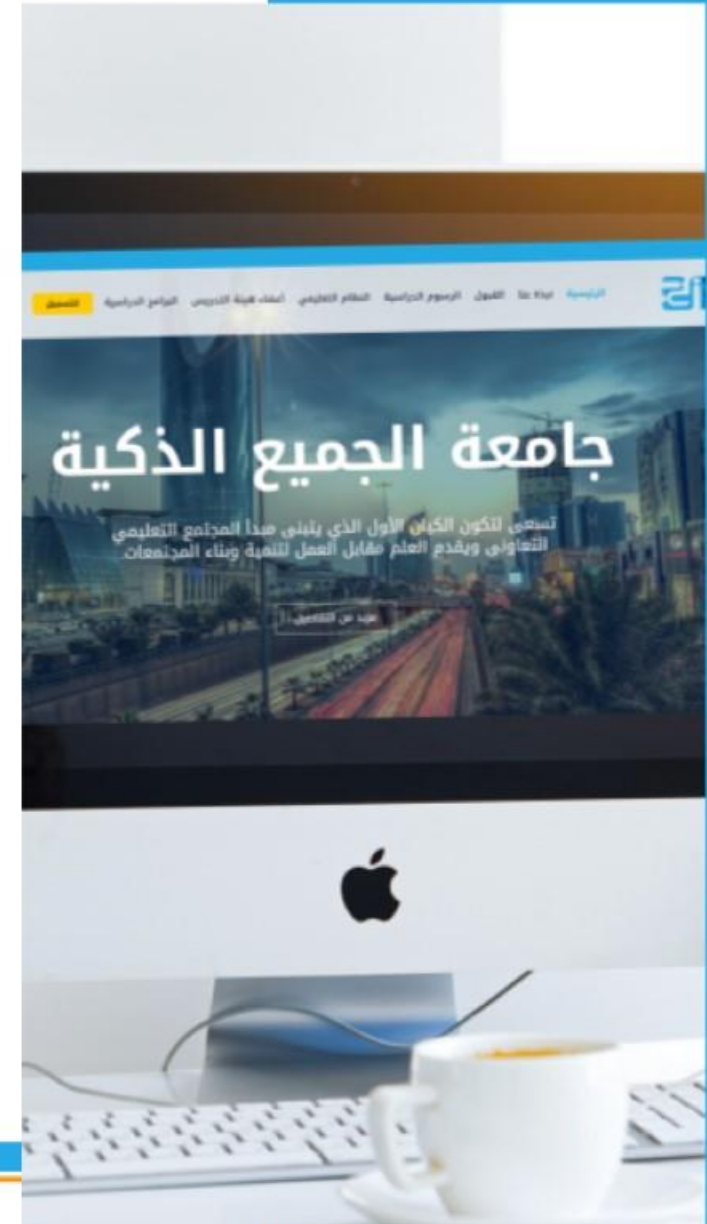
Password Cracking can be performed as either a local attack or a remote attack



Local attack

- Where to locate the password hash file?
- As mentioned earlier, most systems store the encrypted password hashes in a single location.
- In Windows-based systems, the hashes are stored in a special file called the security account manager (SAM) file

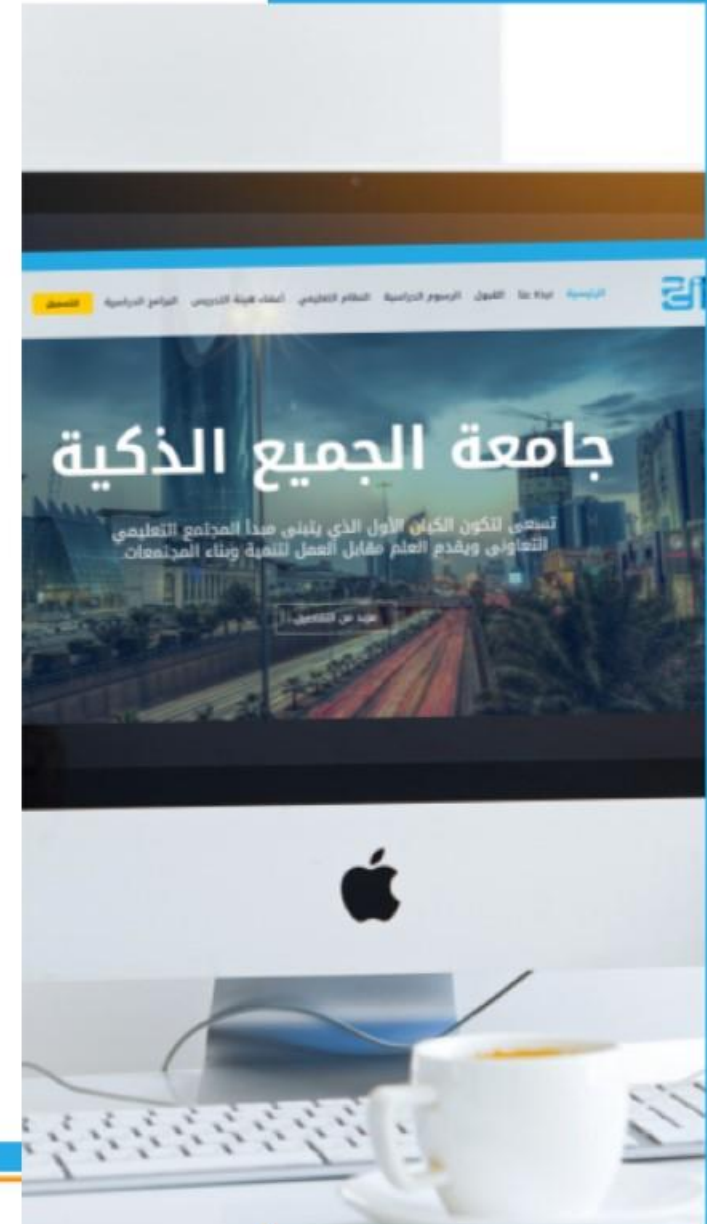
Windows 2000 and above, the SAM file is located in the C:\Windows\System32\Config\ directory



Chapter 05

Password Cracking

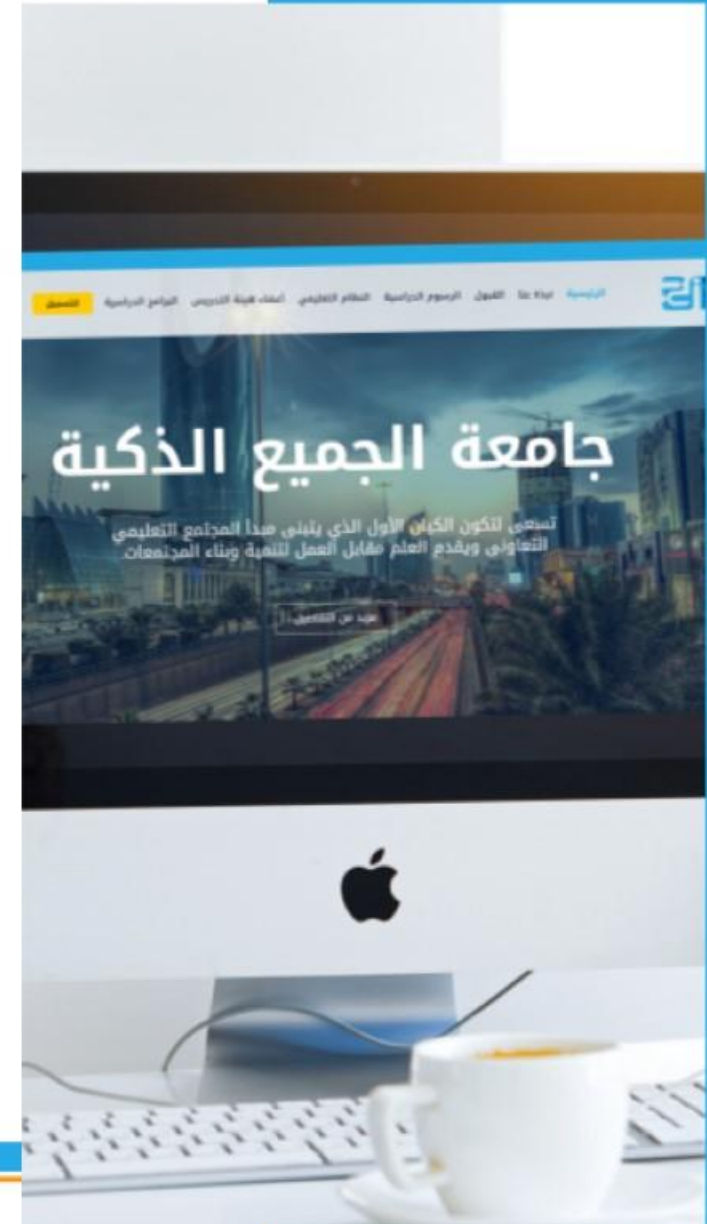
- The first protection is that the SAM file is actually locked when the OS boots up.
- This means that while the OS is running we do not have the ability to open or copy the SAM file.
- In addition to the lock, the entire SAM file is encrypted and not viewable.



Chapter 05

Password Cracking

- Fortunately, there is a way to bypass both these restrictions.
- Because we are discussing local attacks and because we have physical access to the system, the simplest way to bypass these protections is to boot to an alternate OS like Kali.
- By booting our target to an alternate OS, we are able to bypass the Windows SAM lock.
- This is possible because the Windows OS never starts, the lock never engages, and we are free to access the SAM file

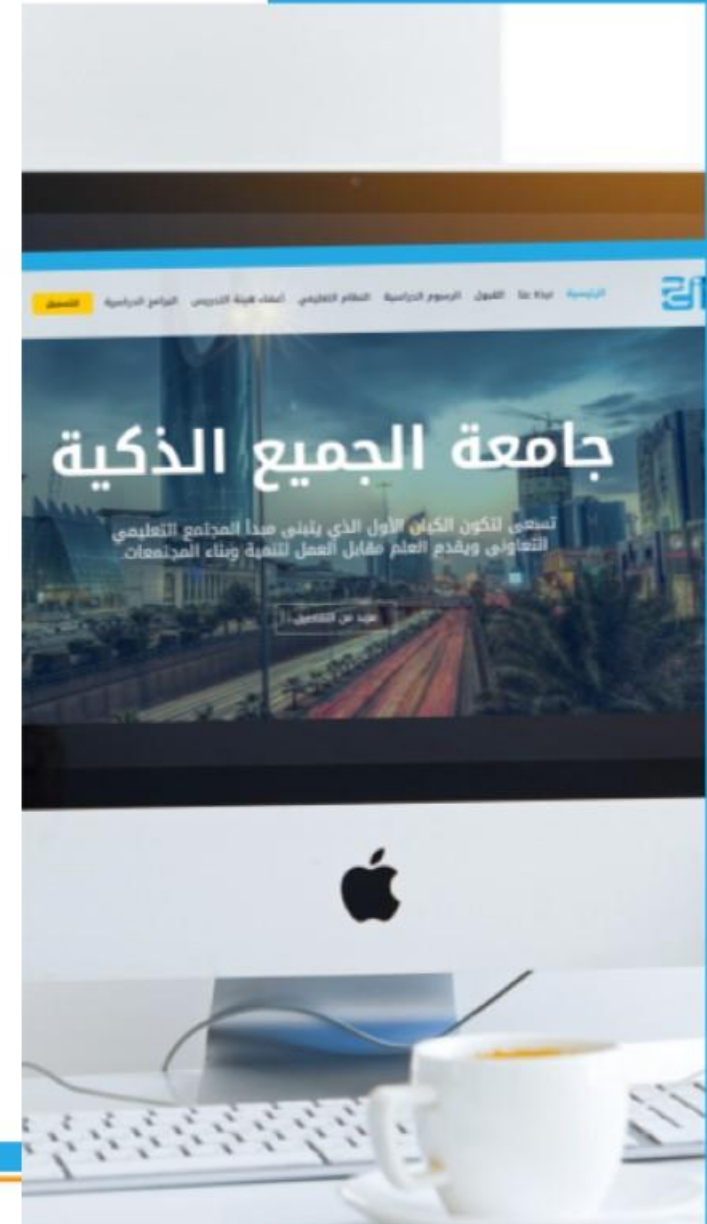


Chapter 05

Password Cracking

Steps to get SAM file form its location:

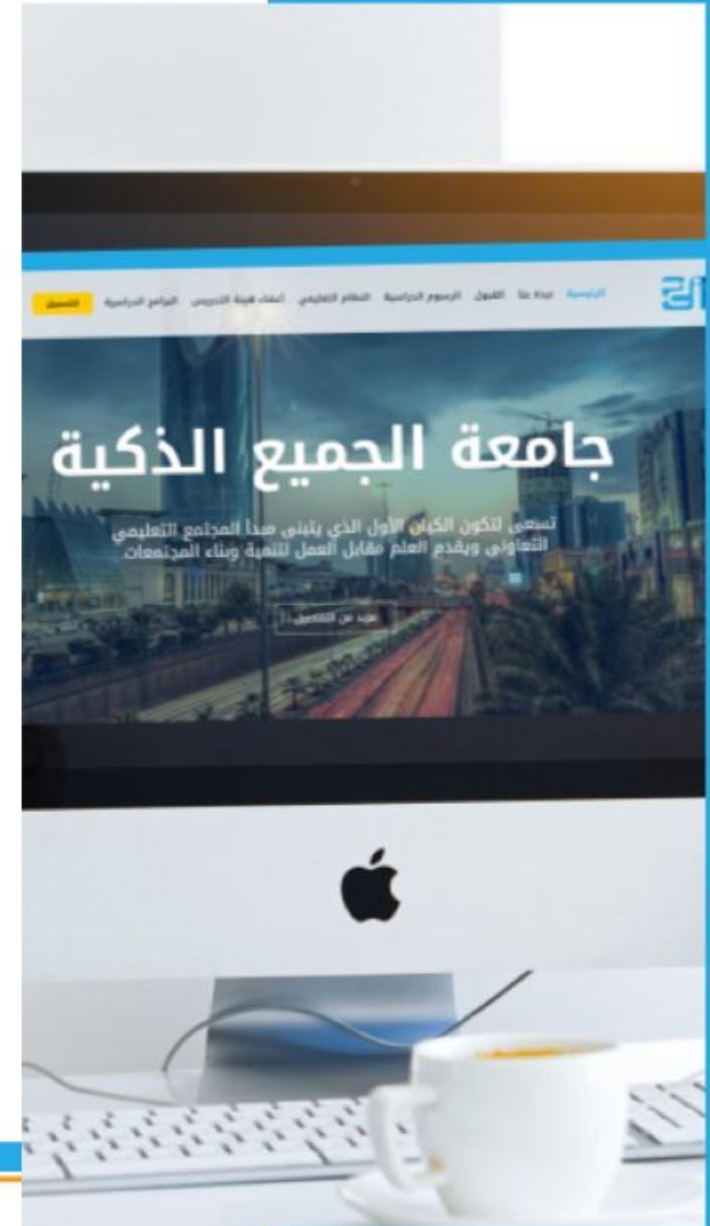
1. Shut down the target machine.
2. Boot the target to Backtack or an alternate OS via a live CD or USB drive.
3. Mount the local hard drive.
4. Use a tool to extract the hashes.
5. Use a tool to crack the passwords.



Chapter 05

Password Cracking

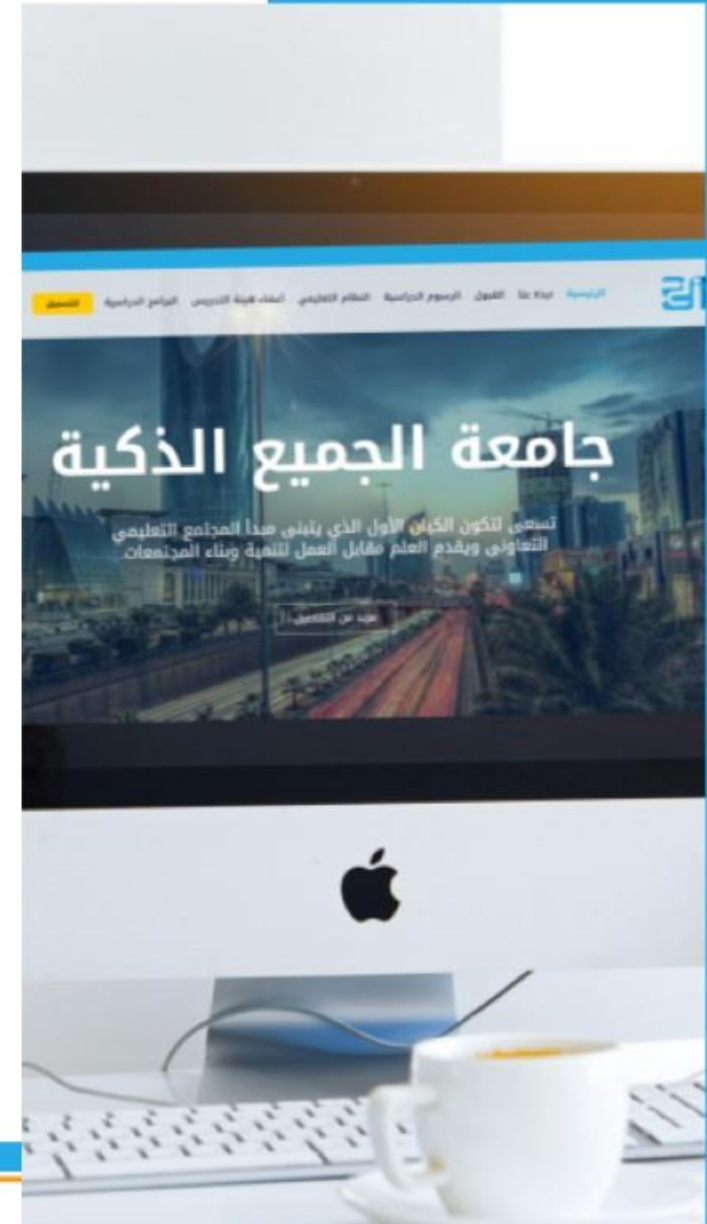
<https://www.youtube.com/watch?v=ZljJQ1W2ue4>



Chapter 05

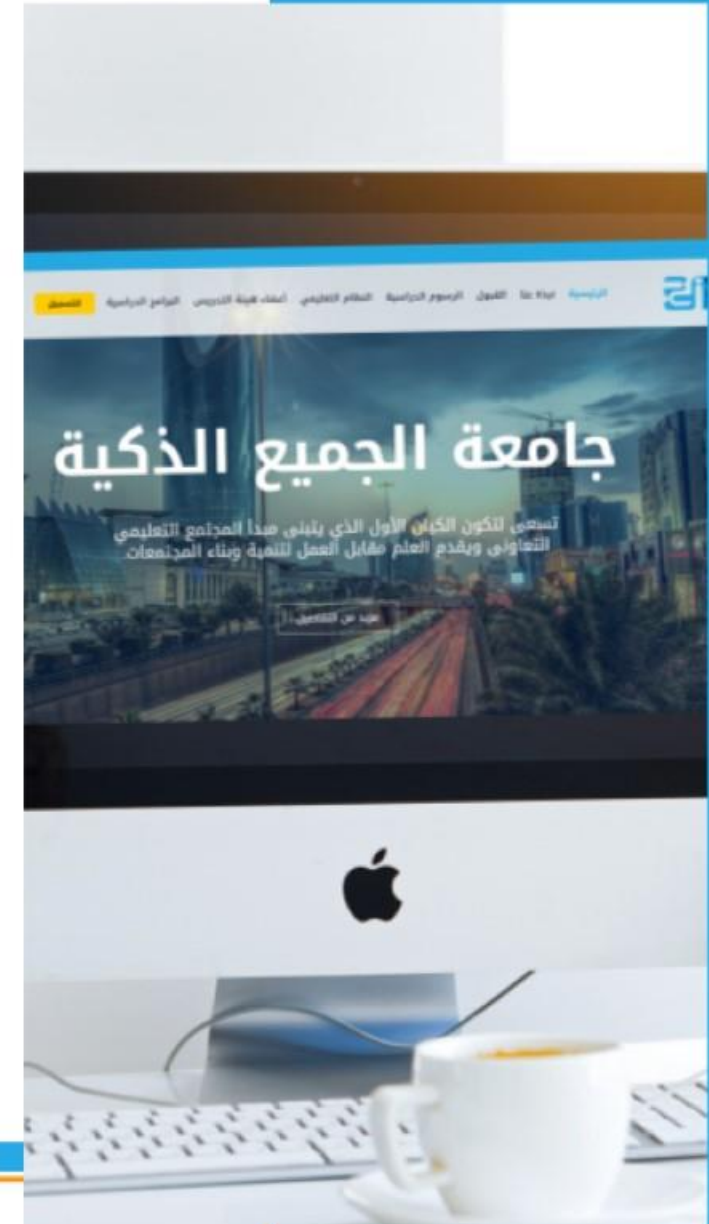
Password Cracking

- Unfortunately, the SAM file is still encrypted, so we need to use a tool to access the hashes. Fortunately, the required tool is built into Kali.



Remote attack

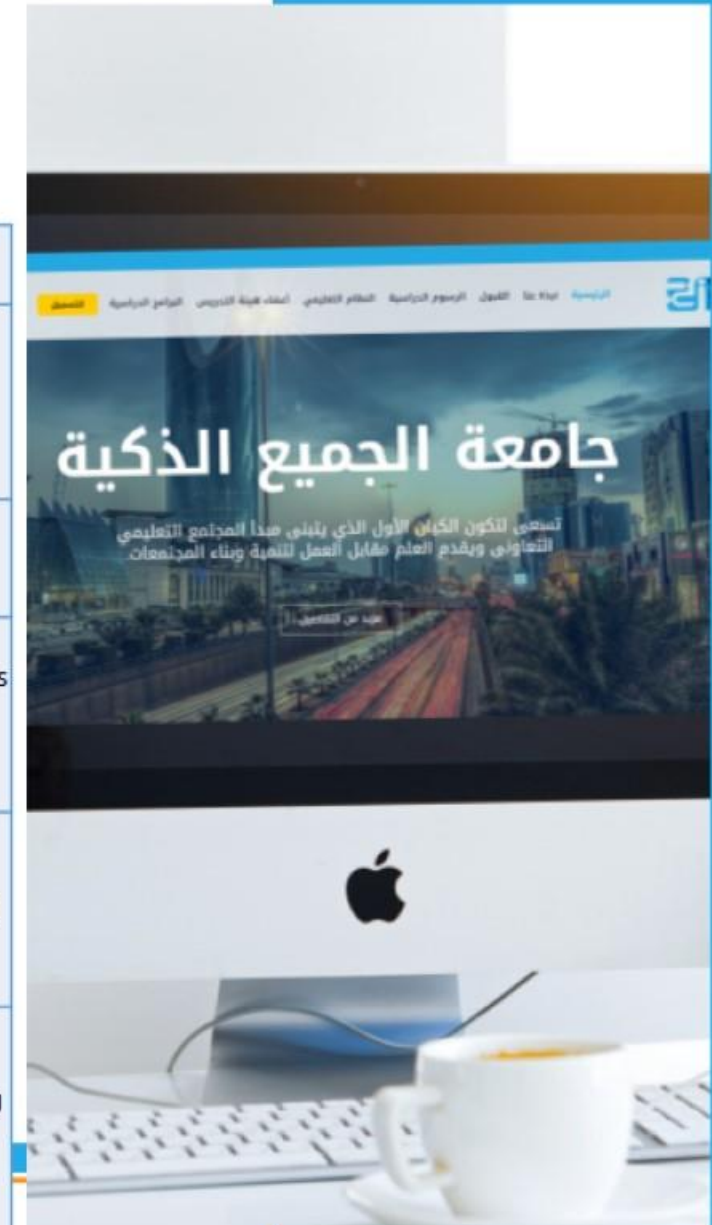
- Use password crack tools
 1. CrackStation
 2. Password Cracker
 3. Brutus Password Cracker
 4. AirCrack
 5. RainbowCrack
 6. THC Hydra
 7. Cain and Abel
 8. Medusa
 9. John The Ripper



Chapter 05

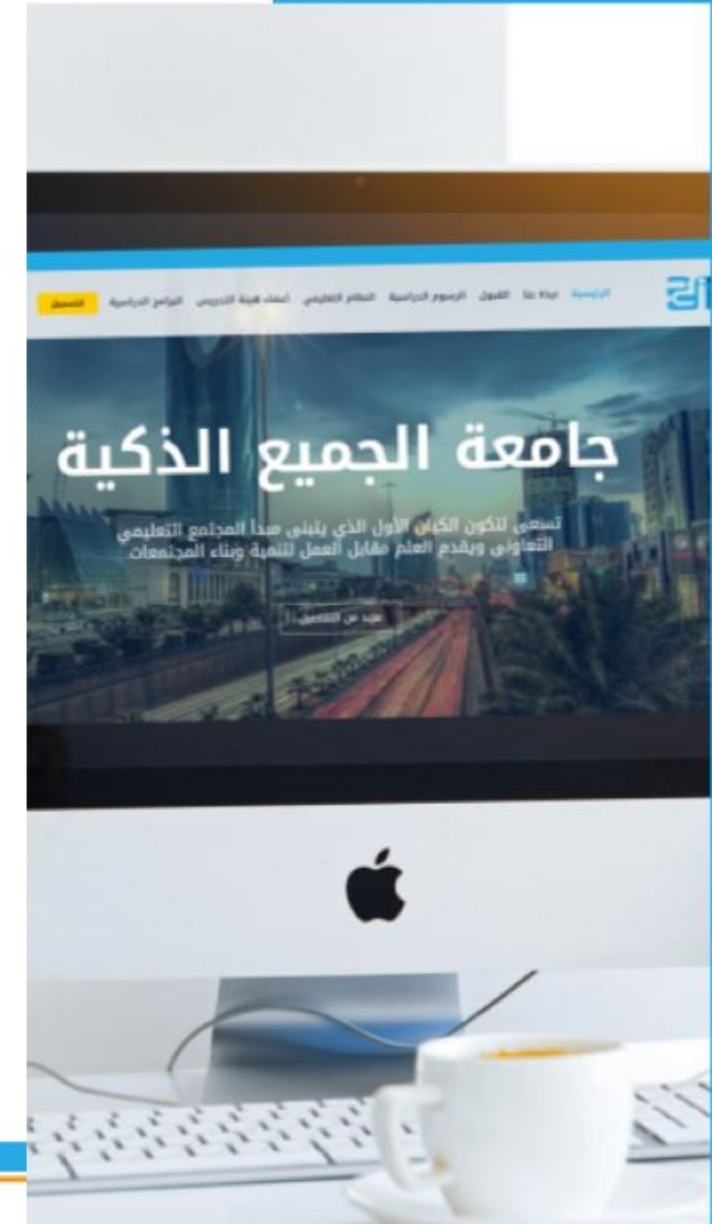
Password Crack

Password Cracking Tools	Platform	Supported Protocols	Features
CrackStation	Linux, macOS, and Windows	LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults	• Password Hash Cracking • Uses Look-up Table with +15 billion entries • Works only for 'nonsalted hashes'
Password Cracker	Windows	N/A	• View Hidden Passwords • Supports multiple languages
Brutus	Windows	FTP, HTTP, POP3, SMB, Telnet, NetBus, IMAP, NNTP, and other platforms	• Multistage authentication engine • Supports sixty simultaneous connections • Configurable brute force modes • Supports Socks Proxy
AirCrack	Windows, OS X, Linux, FreeBSD, NetBSD, OpenBSD, Solaris, and eComStation2	WPA and WEP passwords	• Uses FMS Attack • Supports WEP and WPA passwords • Monitoring, analyzing, and testing Wi-Fi connection
RainbowCrack	Windows and Linux	NTLM Tables, MD5 Tables, SHA2 Tables	• Optimized memory trade-off tool for table creation, conversion, and lookup. • Supports multi-core processing and GPU acceleration. • High-performance hash cracking.



How to Defend against Password Cracking

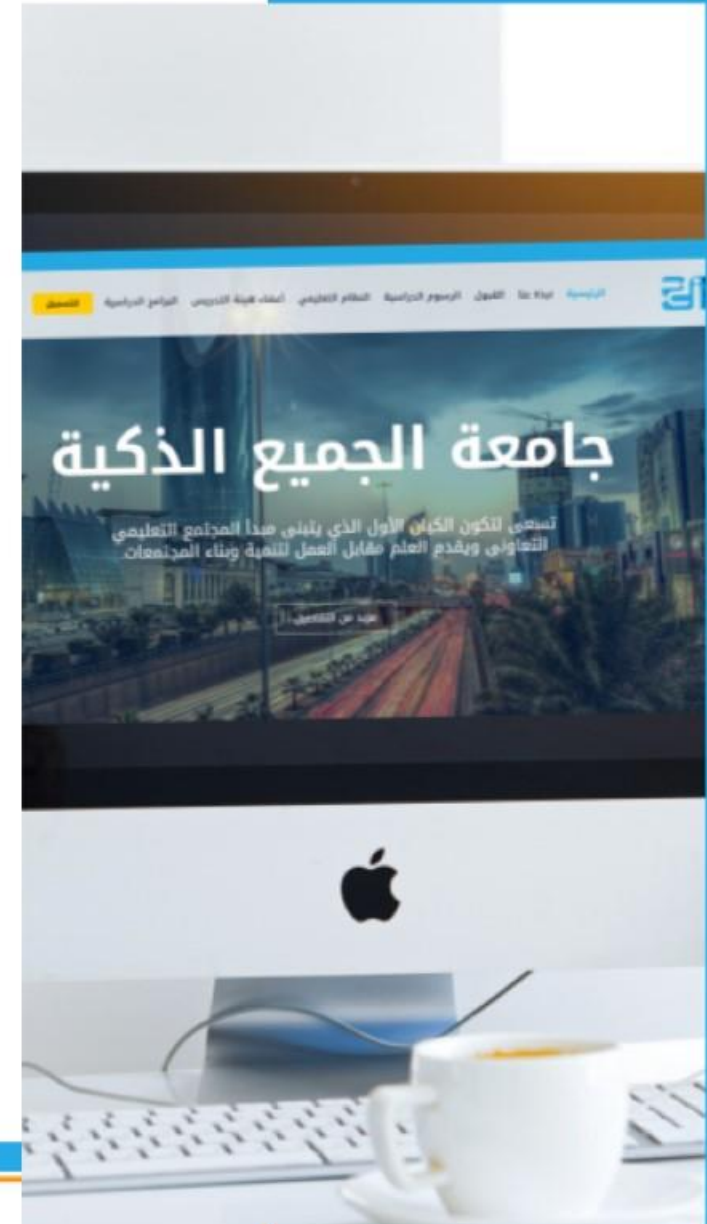
- Don't use the same password during password change
- Don't share passwords
- Don't use passwords that can be found in dictionary
- Set the password change policy to 30 days
- Don't use any system's default passwords



Chapter 05

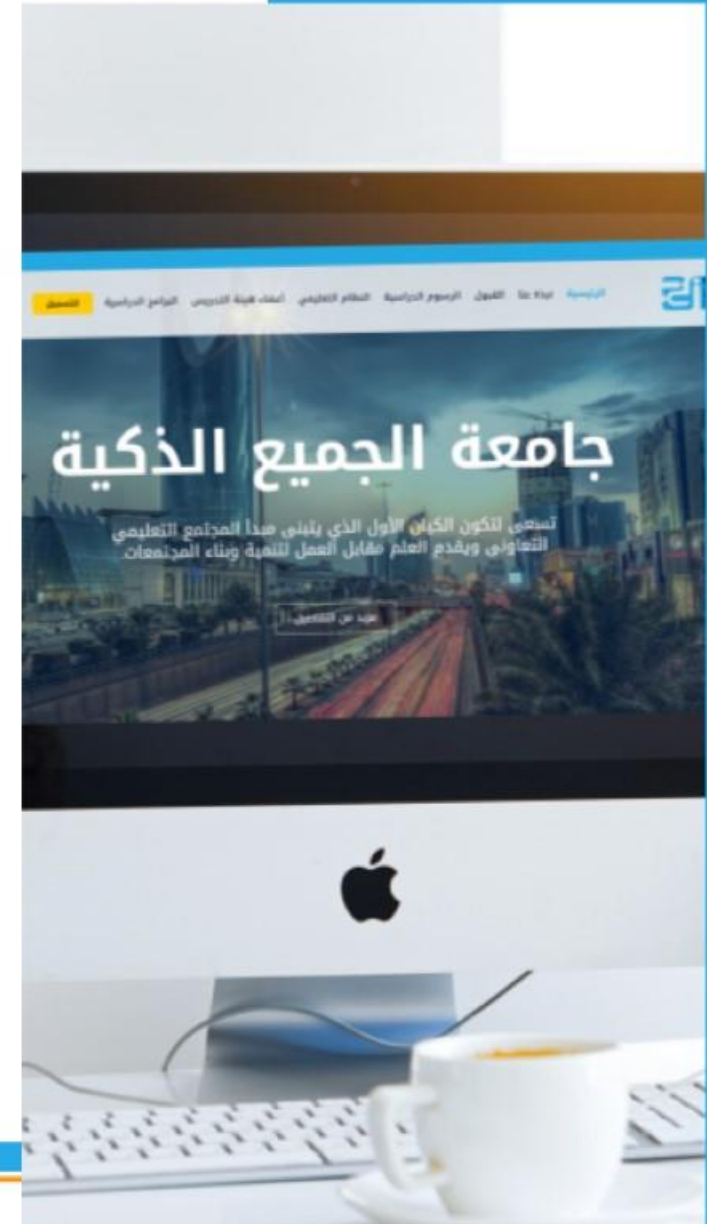
Password Crack

- Make passwords hard to guess by using 8-12 alphanumeric characters in combination of uppercase and lower letters , numbers and symbols
- Never use passwords such as date of birth or child's or pet's name

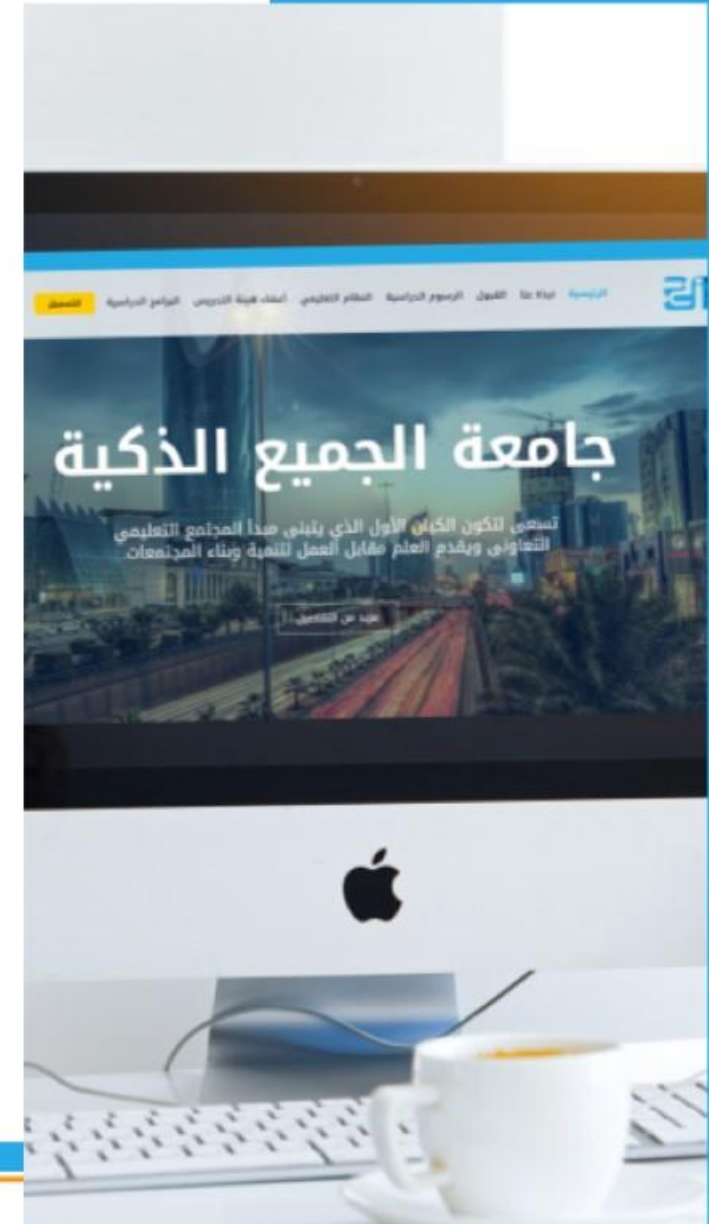


Chapter 05

Network Sniffing



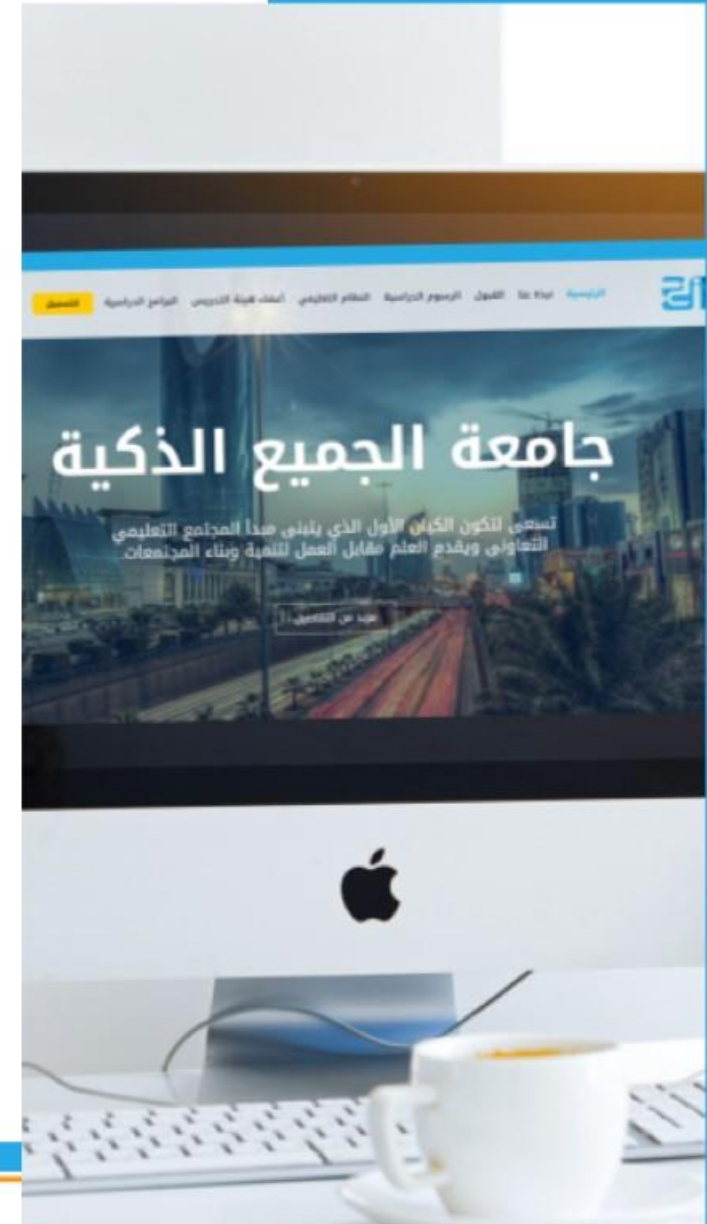
- Network sniffing, is a type of attack where an attacker captures the packets across a wire or across air (wireless connection).
- the process of monitoring and capturing all data packets passing through a given network using sniffing tools.
- The main goal is to capture unencrypted credentials across the network.
- Is sniffing always being attack ?



Types of Sniffing

Sniffing can be primarily divided into two main categories:

1. Active sniffing
2. Passive sniffing

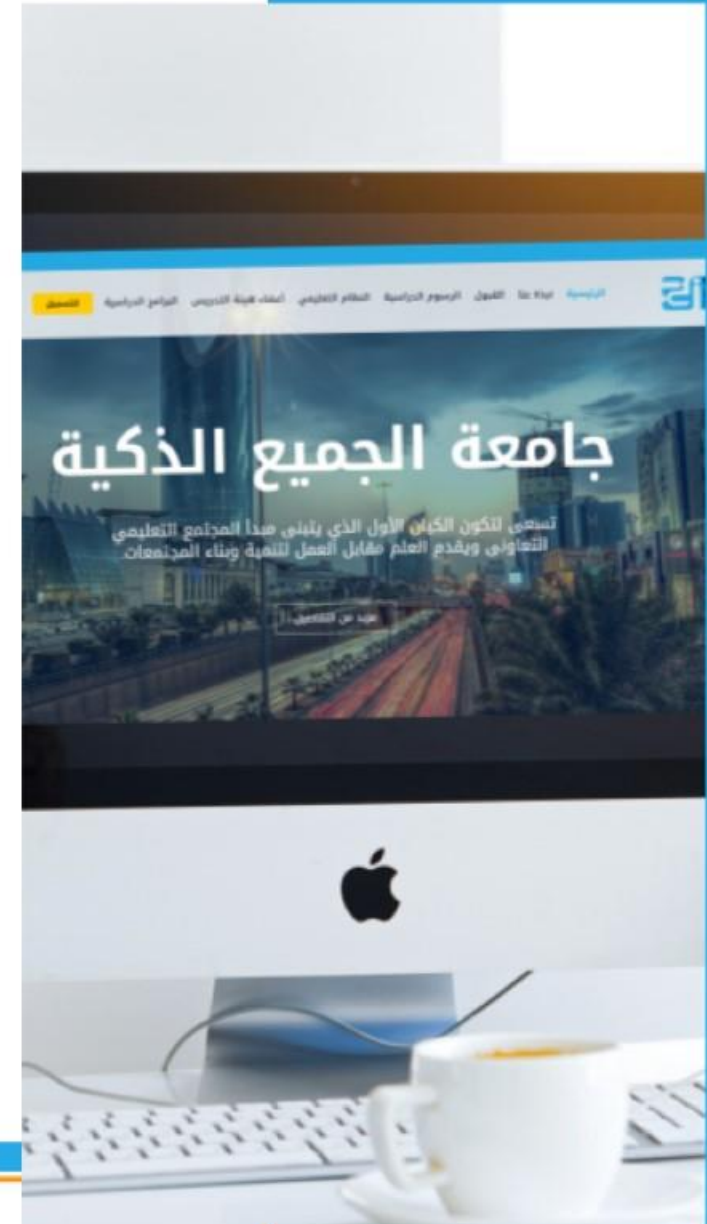


Active Sniffing

- is where we directly interact with our target machine, by sending packets and requests. ARP spoofing and MAC flooding are common examples.

Passive Sniffing

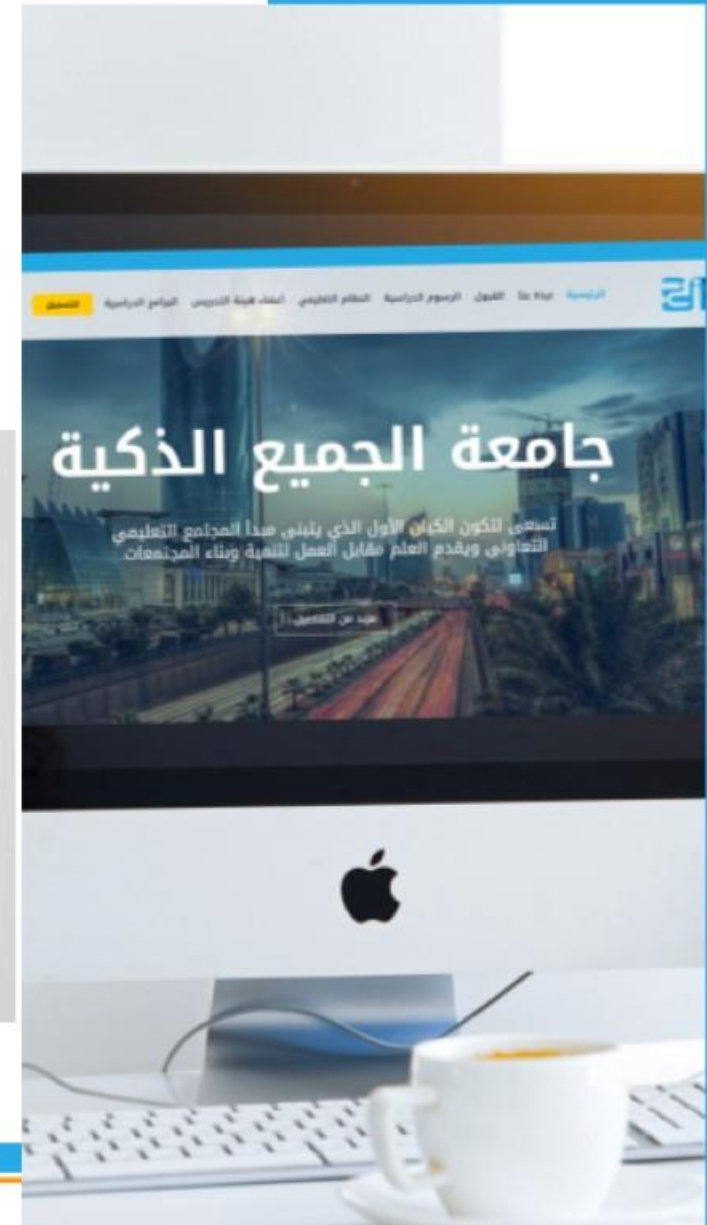
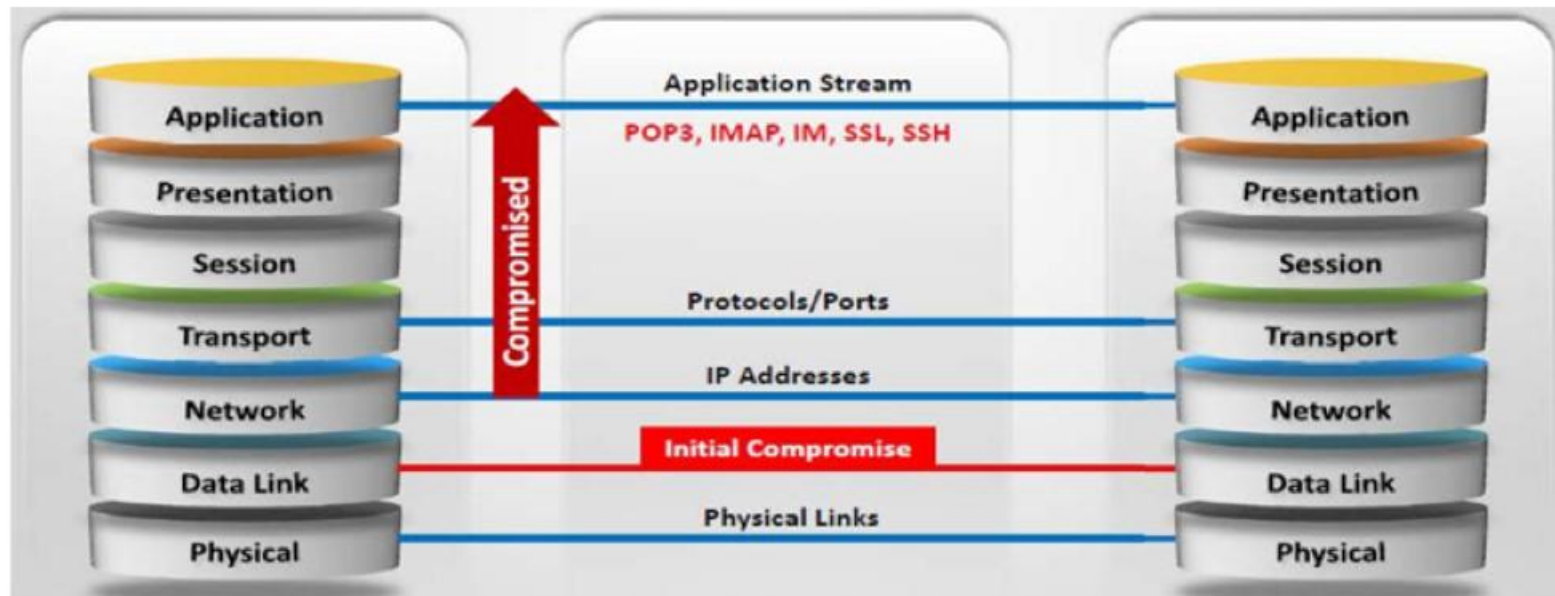
- In passive sniffing, the attacker does not interact with the target. They just sit on the network and capture the packets sent and received by the network.
- This happens in the case of hub-based networks or wireless networks.



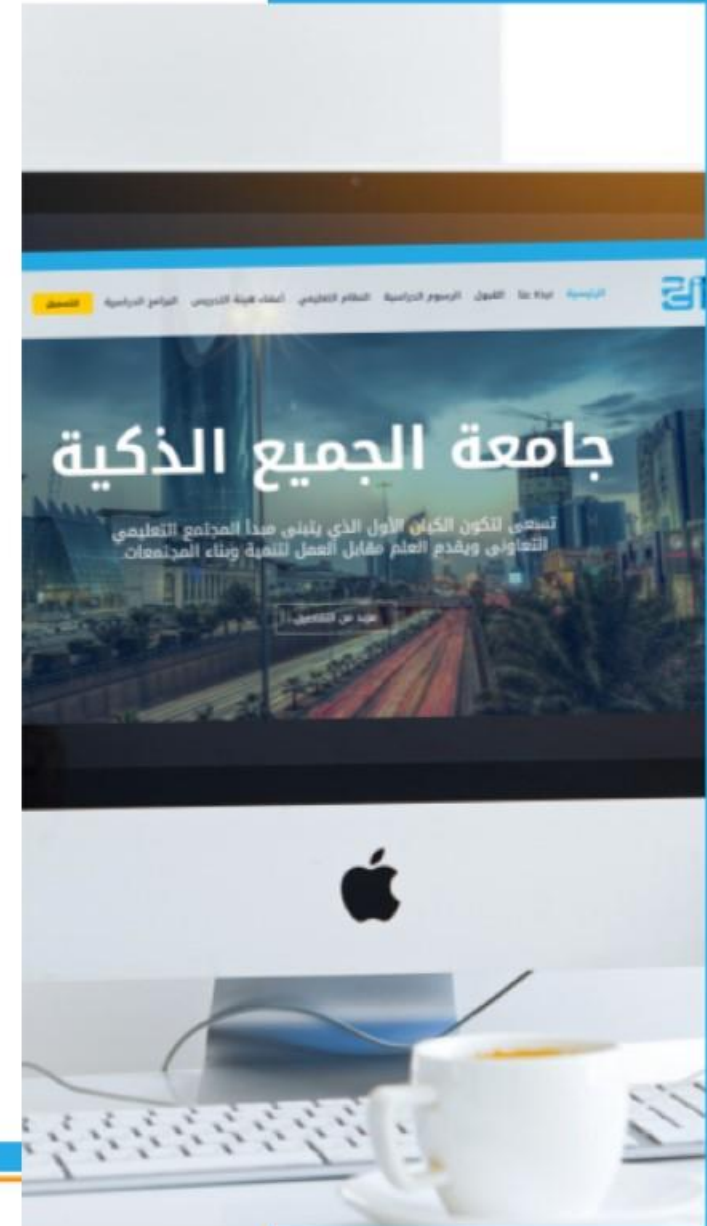
Chapter 05

Network Sniffing

- Sniffers operate at the Data Link Layer of the OSI model



- A **Protocol Analyzer Hardware/Software** is a measurement tool or device used to capture and monitor the data over communication channel.
- It captures the data on the communication channel and converts the data bits into meaningful protocol sequence.
- A protocol analyzer uses a combination of software and hardware to analyze and capture the data over the communication channel.
- Protocol analyzer is very powerful in debugging the device and bus failures in the embedded system.



Chapter 05

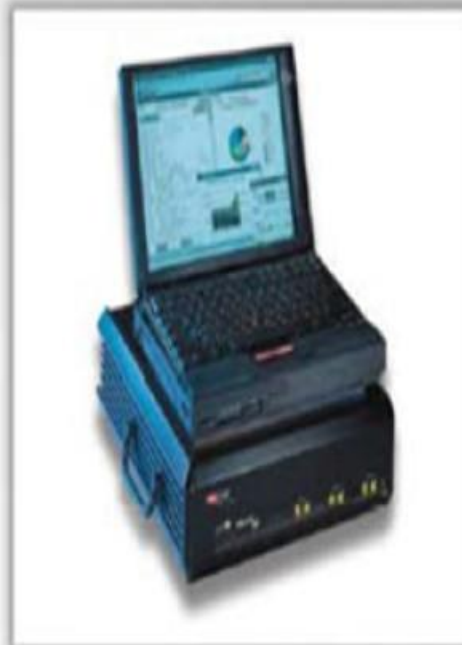
Network Sniffing



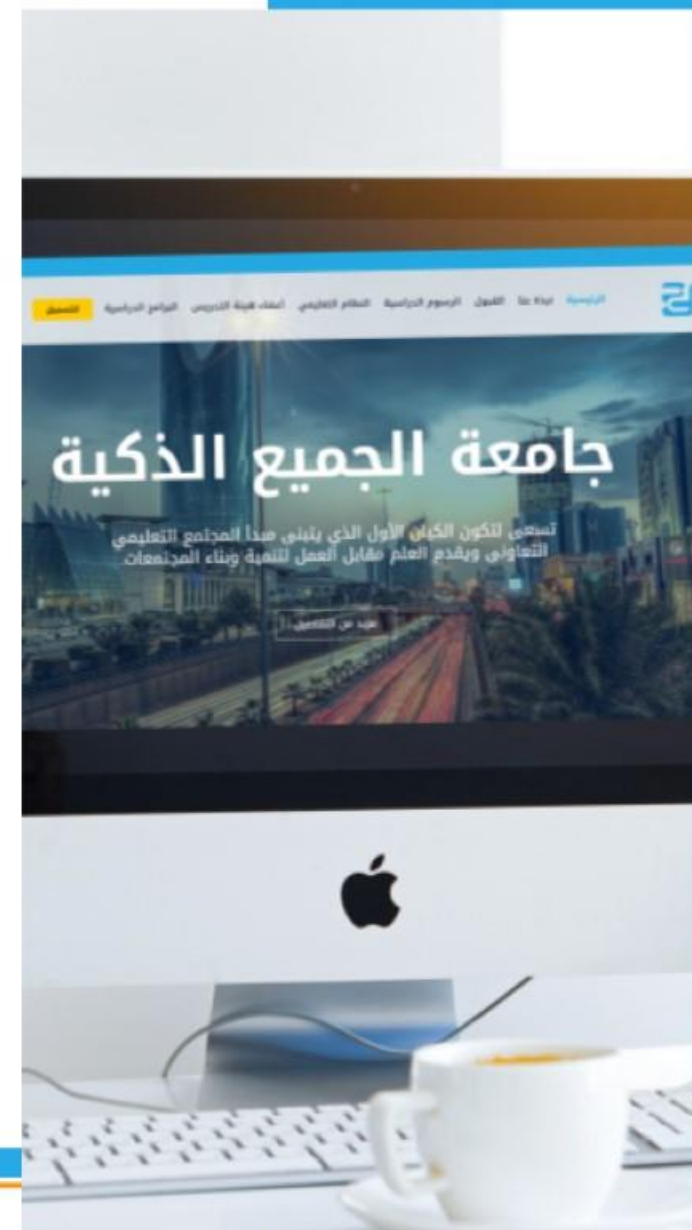
Keysight N2X N5540A



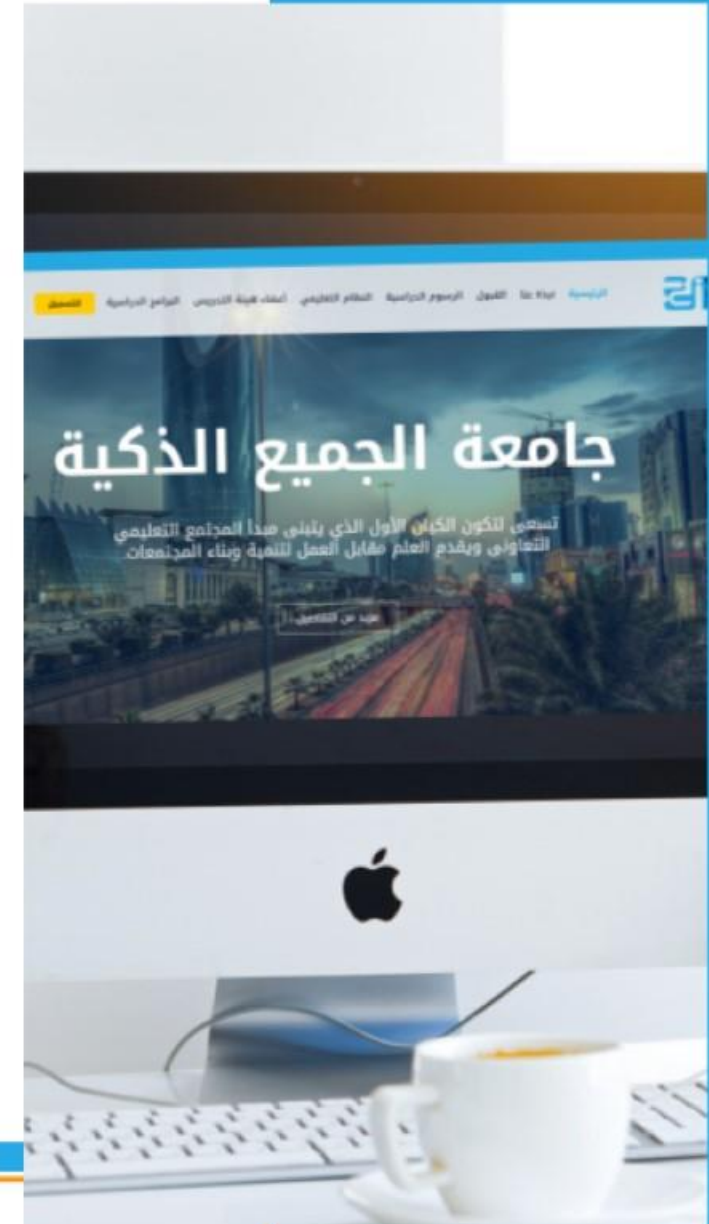
Keysight E2960B



RADCOM PrismLite Protocol Analyzer



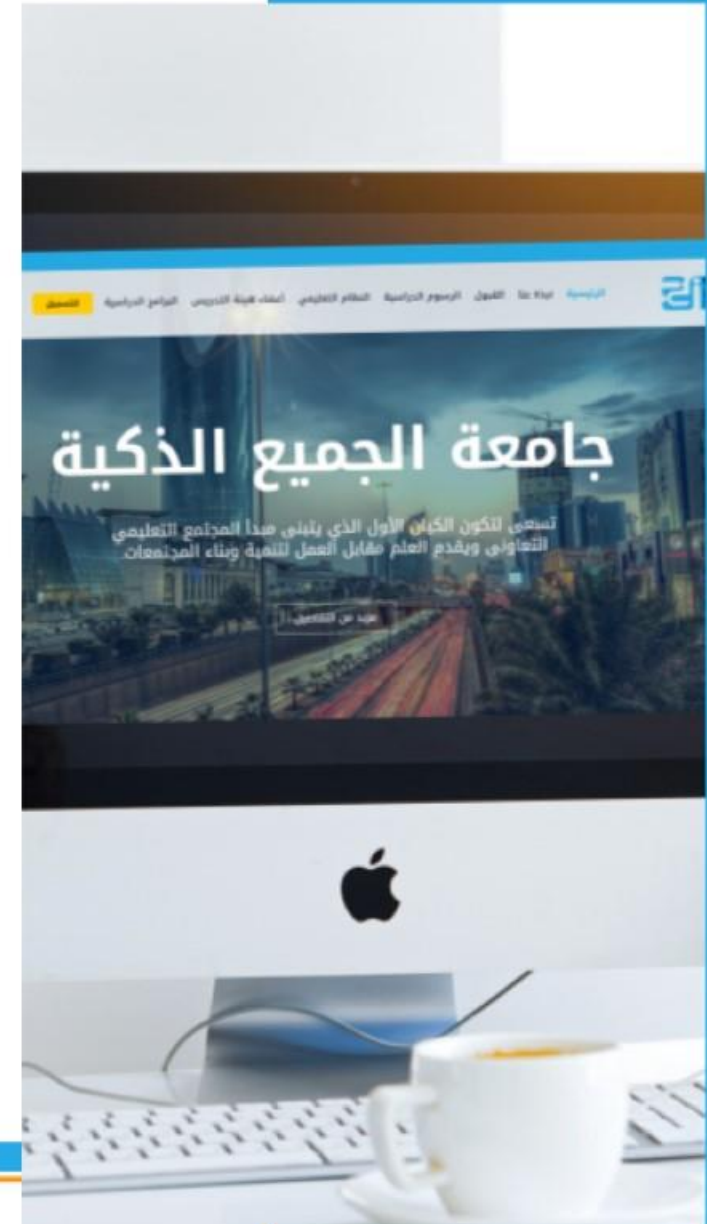
- Sniffing Attacks
 - ARP Spoofing attack
 - DHCP Spoofing attack



Chapter 05

Network Sniffing

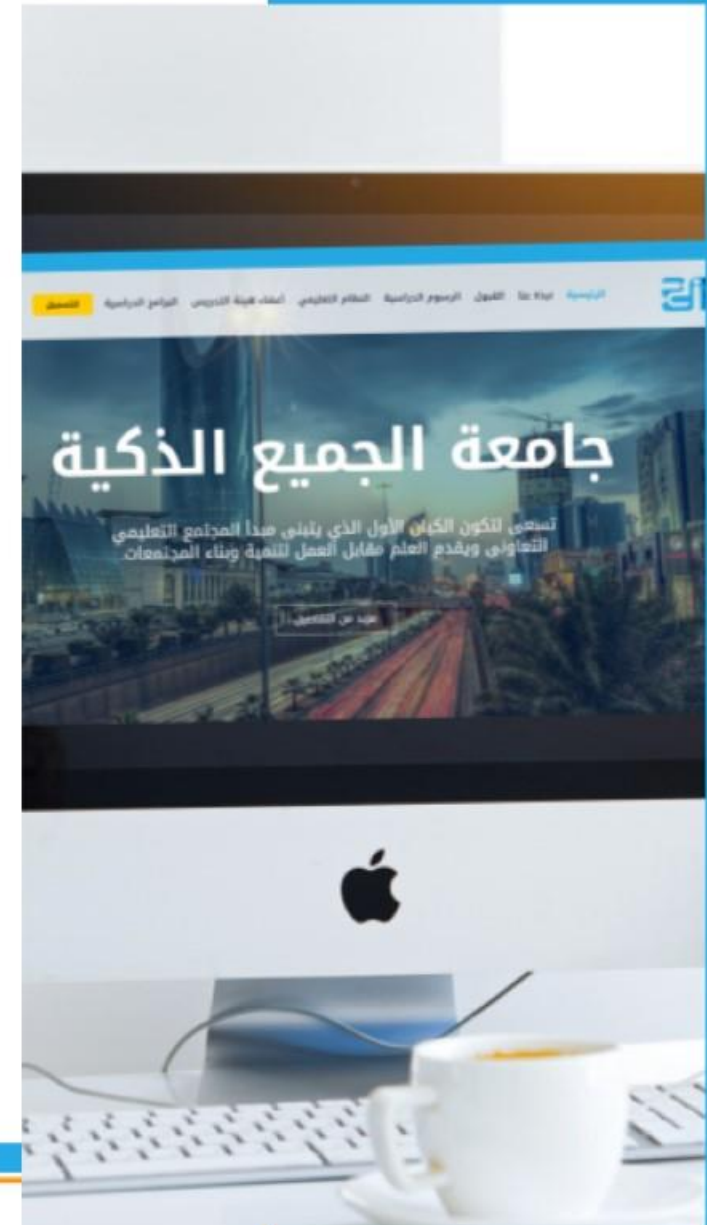
- **ARP spoofing attack**
 - ARP Table
 - ARP Spoofing (ARP Poisoning)



What is an ARP Table?

- An ARP table is the method for storing the info discovered through the protocol. It's used to record the discovered MAC and IP address pairs connected to a network.
- Each device that's connected to a network has its own ARP table, and it stores address pairs that the specific device has communicated with.

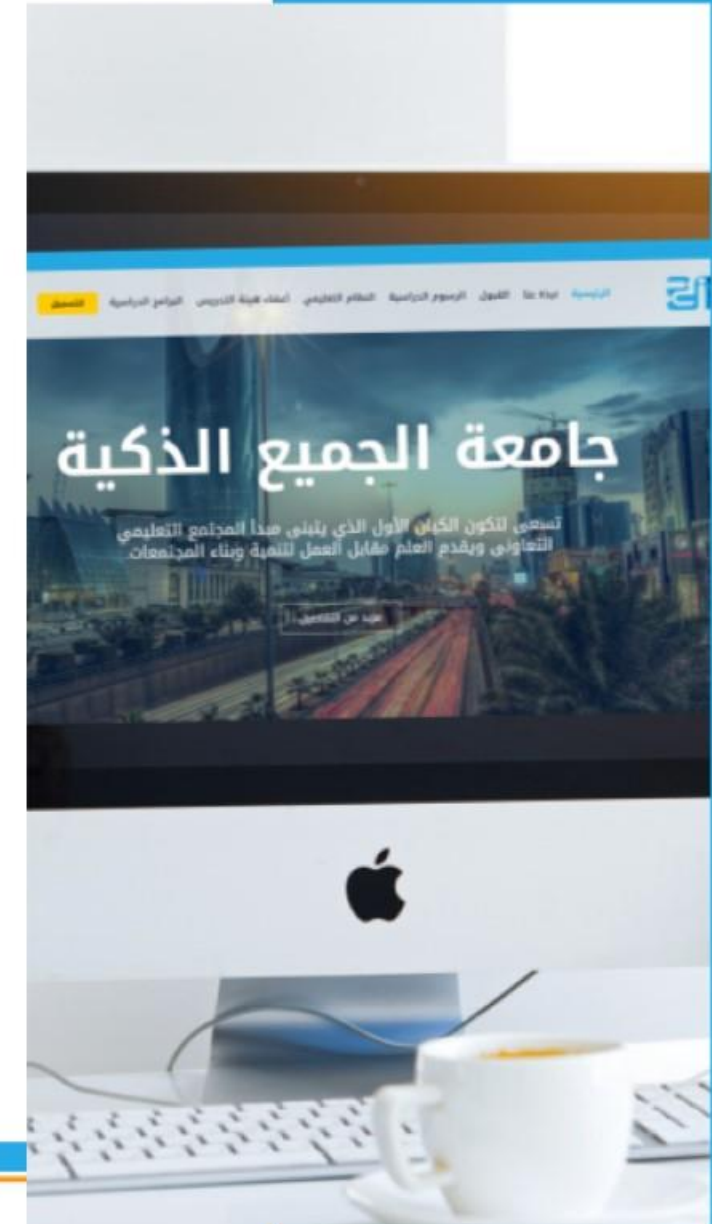
Neighbour	Linklayer Address	Expire (O)	Expire (I) Netif	Refs	Prbs
10.0.0.1	0:c:29:12:34:56	2m25s	2m25s	en0	1 none
10.0.0.41	0:c:29:65:43:21	39s	39s	en0	1 none
10.0.0.47	0:c:00:00:00:01	1m14s	1m14s	en0	1 none
10.0.0.53	ab:cd:ef:81:6:72	2m32s	2m32s	en0	1 none
10.0.0.58	fe:dc:ba:11:e2:6e	1m51s	1m51s	en0	1 none



Chapter 05

Network Sniffing

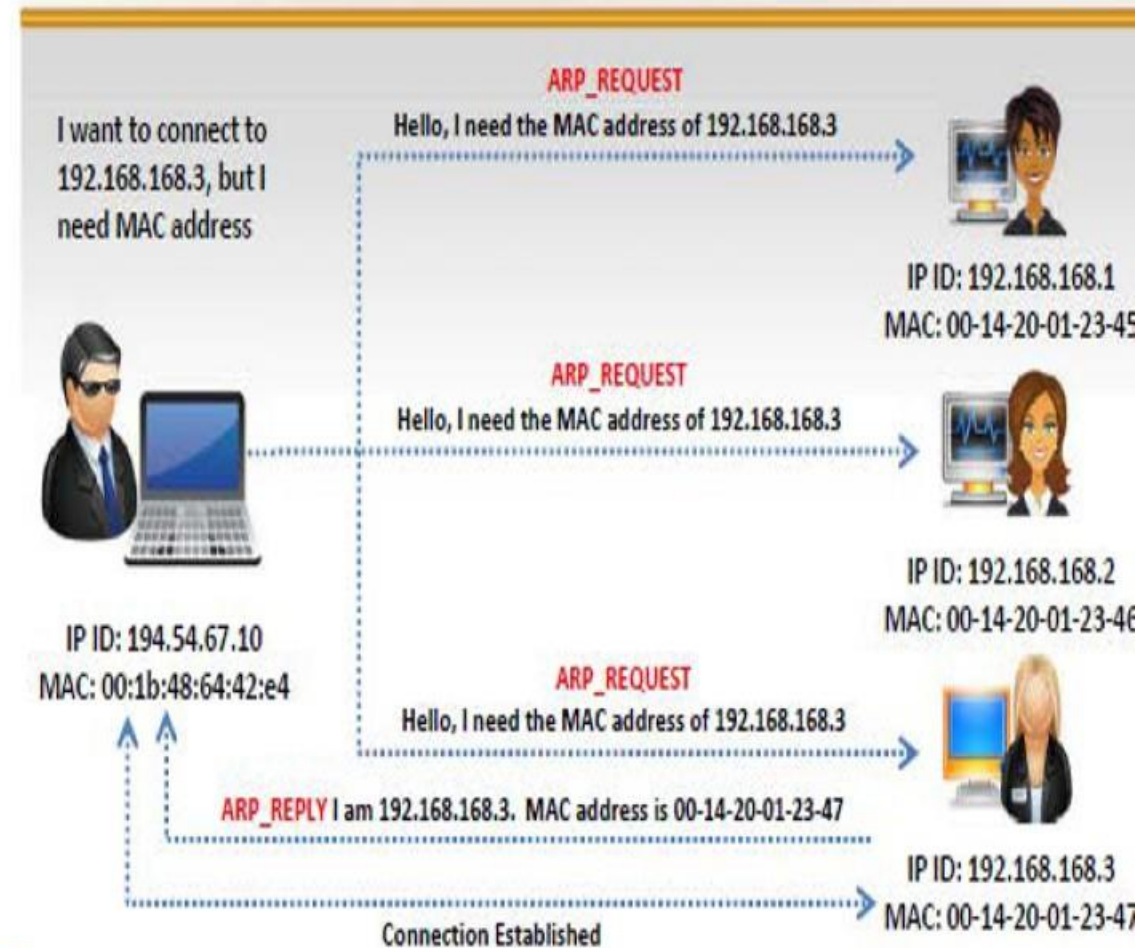
- ARP makes it so pairs of MAC and IP addresses don't need to be rediscovered every time data is sent. Once a MAC and IP address pair is learned, it's kept in the ARP table for a specified period of time.
- If there's no record on the table for a specific IP address, ARP will need to send out a broadcast message. This is to all devices in that specific subnet to determine what the receiver MAC address should be.
- All network devices broadcast ARP queries in the network to find out other machines mac addresses
- When one machine needs to communicate with another, it looks up its ARP table. If the MAC address is not found in the table, the ARP request is broadcasted over the network



Chapter 05

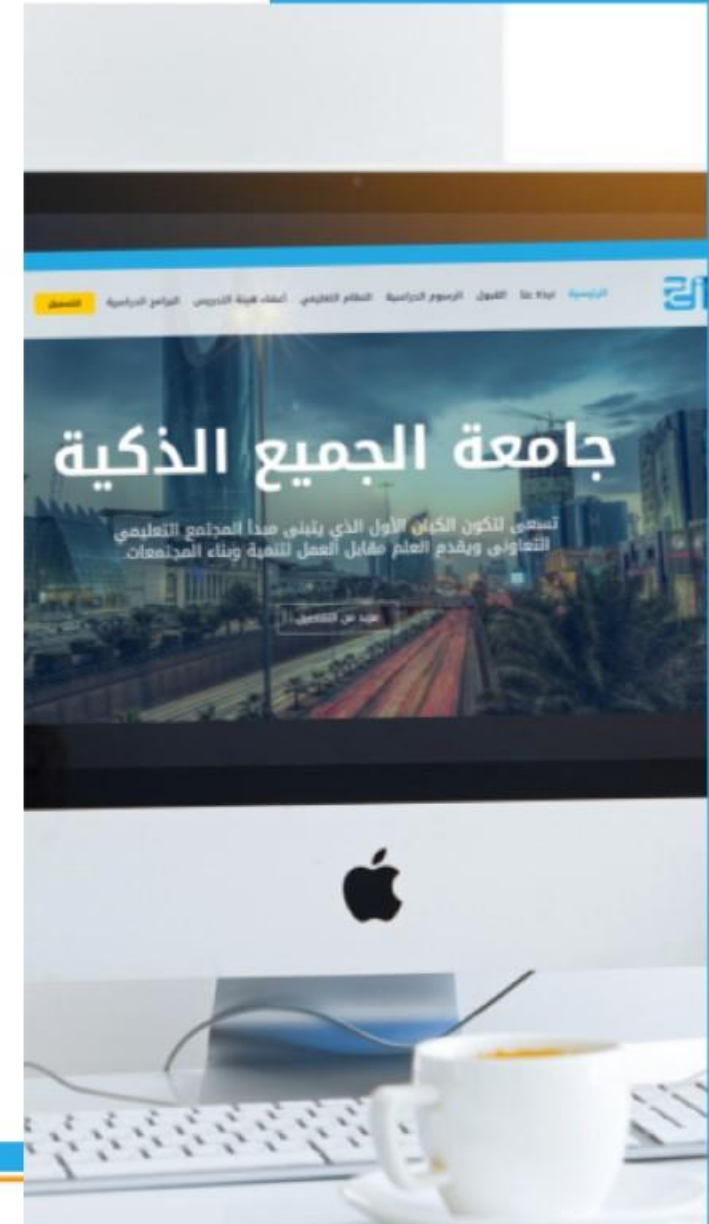
Network Sniffing

- Let's look at a simple example. Say you have a device (Host 1) that needs to communicate with another device (Host 2) on the same subnet. Host 1 will know Host 2's IP address (**192.168.168.3** in our example). But to communicate with Host 2, Host 1 also needs to know Host 2's MAC address.
- Enter the ARP table. Host 1 can use ARP to discover Host 2's MAC address.
- Since Host 1 doesn't know exactly where Host 2 is, Host 1 broadcasts an ARP protocol request to all the devices on the local subnet asking, "What's the MAC address for Host 2's IP address?". All the hosts on the network will receive the message, and most will discard it.
- They're not Host 2, so they don't need to do anything. Host 2, though, will respond to Host 1 with, "What's up? My MAC address is 00:14:20:01:23:47."

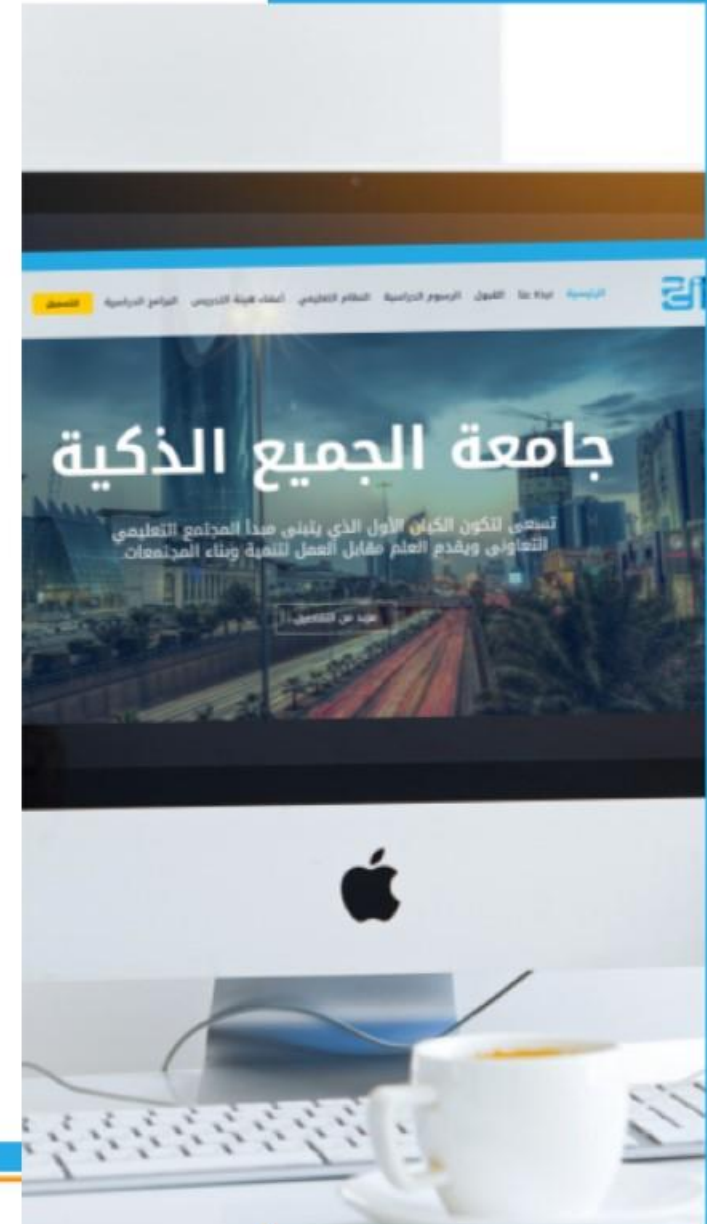
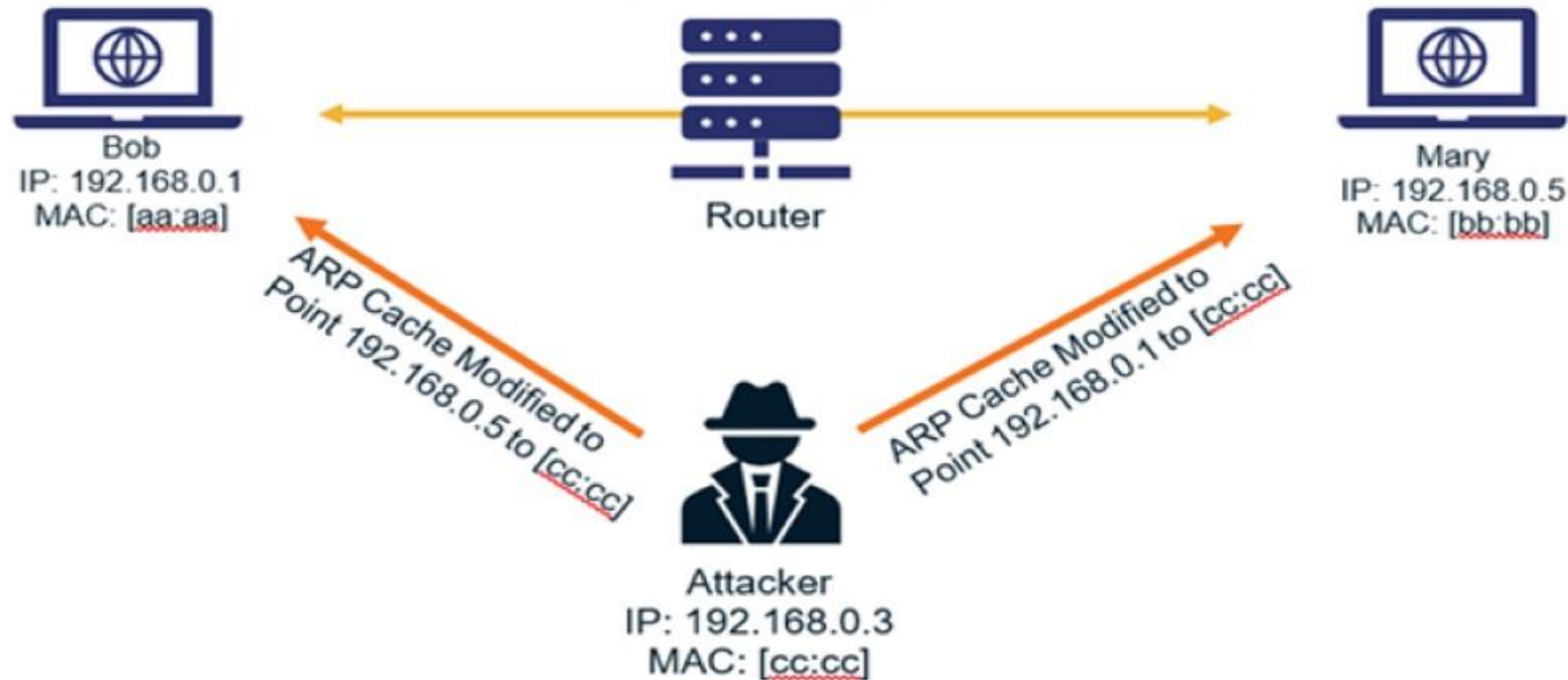


What is ARP Spoofing (ARP Poisoning)

- An ARP spoofing, also known as ARP poisoning, is a type of attack in which a malicious actor sends falsified ARP (**Address Resolution Protocol**) messages over a local area network.
- This results in the linking of an attacker's MAC address with the IP address of a legitimate computer or server on the network. Once the attacker's MAC address is connected to an authentic IP address, the attacker will begin receiving any data that is intended for that IP address.
- ARP spoofing can enable malicious parties to intercept, modify or even stop data in-transit.
- ARP spoofing attacks can only occur on local area networks that utilize the Address Resolution Protocol.

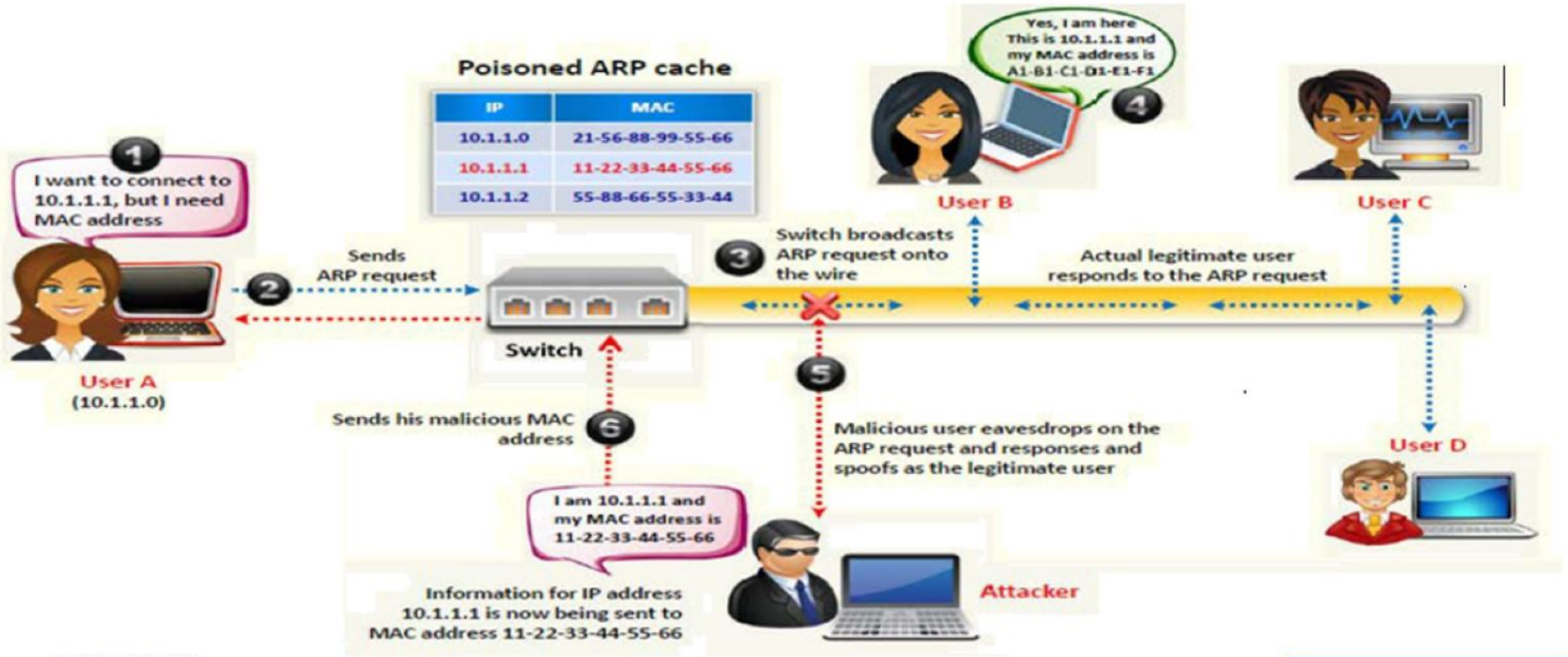


ARP Spoofing Attack



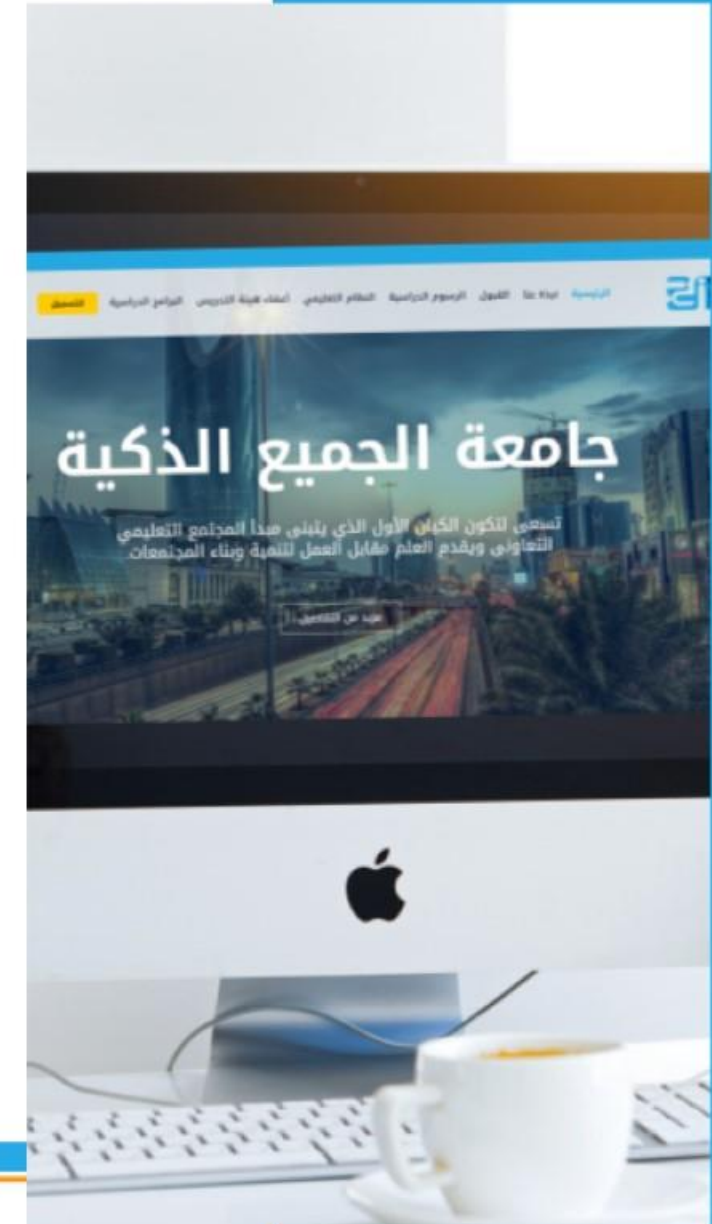
Chapter 05

Network Sniffing

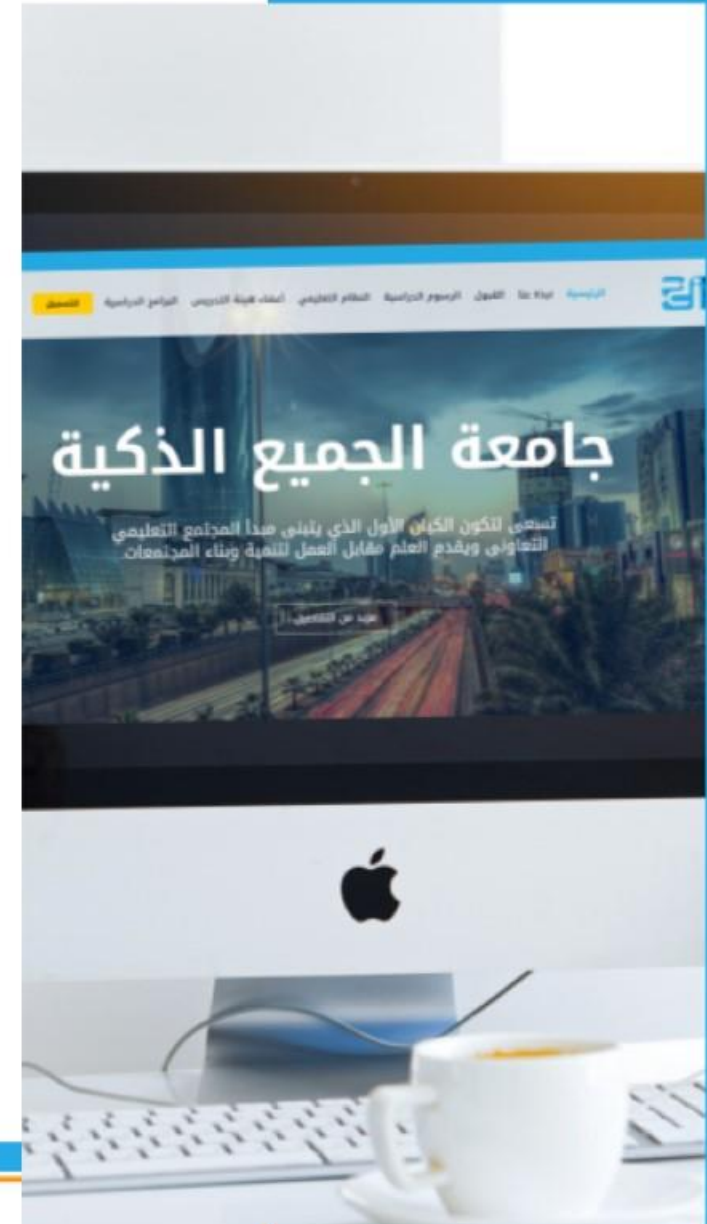


The attack works as follows:

1. The attacker must have access to the network. He scan the network to determine the IP addresses of at least two devices—let's say these are a workstation and a router.
2. The attacker uses a spoofing tool, such as Arpspoof or Driftnet, to send out forged ARP responses.
3. The forged responses advertise that the correct MAC address for both IP addresses, belonging to the router and workstation, is the attacker's MAC address. This fools both router and workstation to connect to the attacker's machine, instead of to each other.
4. The two devices update their ARP cache entries and from that point onwards, communicate with the attacker instead of directly with each other.
5. The attacker is now secretly in the middle of all communications.



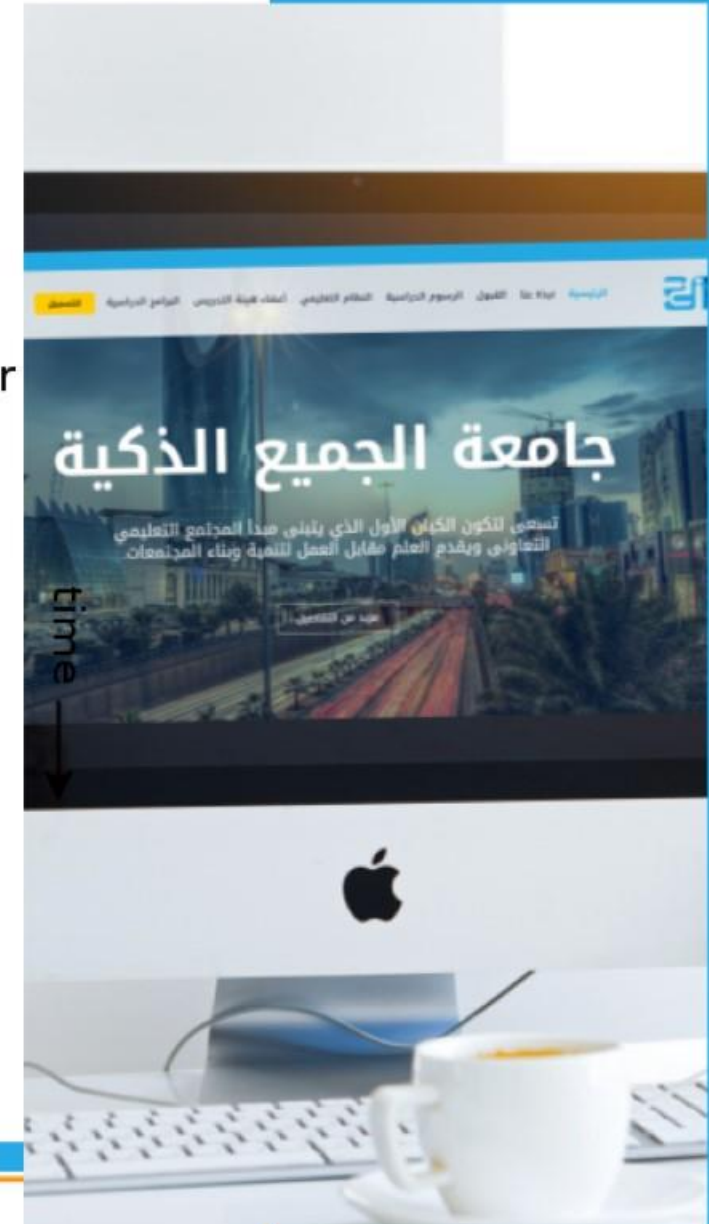
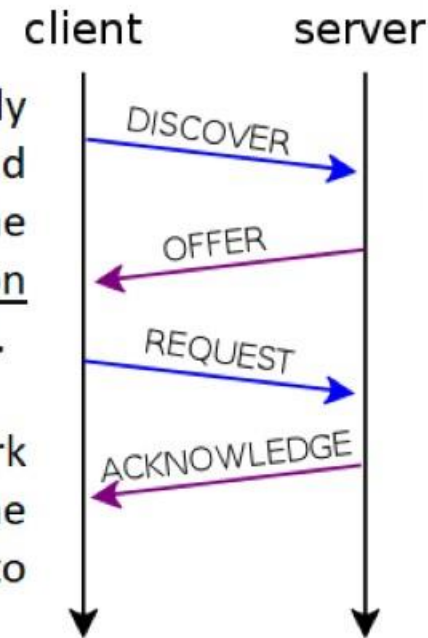
- **DHCP Spoofing Attack**
 - DHCP work
 - DHCP starvation
 - DHCP Spoofing



DHCP servers

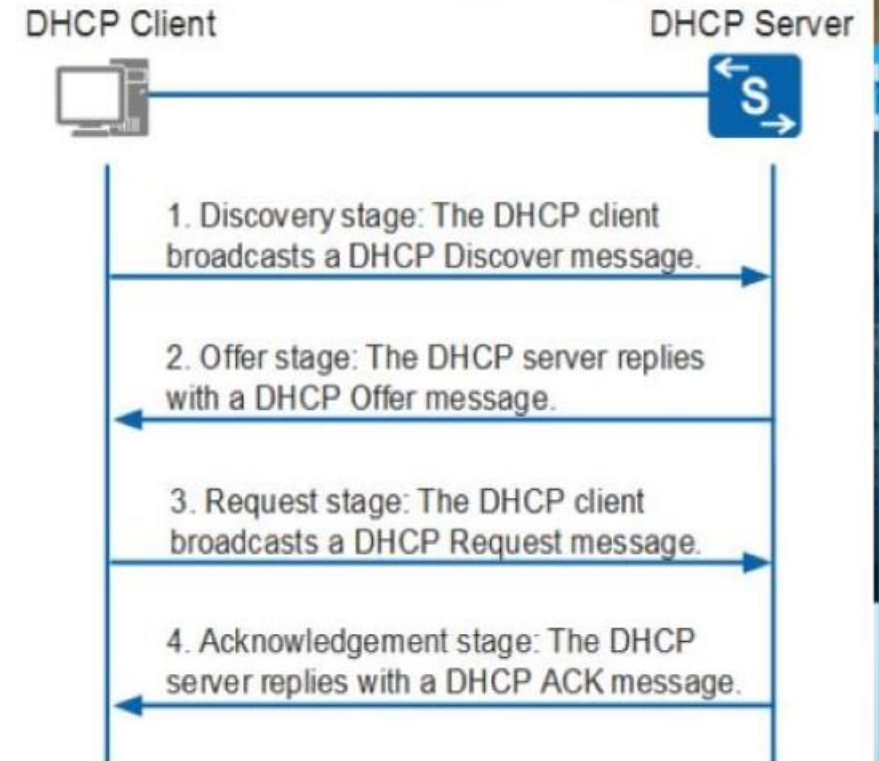
A DHCP Server is a network server that automatically provides and assigns IP addresses, default gateways and other network parameters to client devices. It relies on the standard protocol known as Dynamic Host Configuration Protocol or DHCP to respond to broadcast queries by clients.

A DHCP server automatically sends the required network parameters for clients to properly communicate on the network. Without it, the network administrator has to manually set up every client that joins the network



DHCP servers

1. **DHCP Discover:** The DHCP client sends a broadcast message to reach the DHCP server and start the negotiation process.
2. **DHCP Offer:** The DHCP server responds back to the DHCP client with IP information that can be used once it has been acknowledged.
3. **DHCP Request:** The DHCP client responds back to the DHCP server with a formal request to start using the IP information previously reserved.
4. **DHCP ACK:** The DHCP server acknowledges the DHCP Request message and the DHCP client starts using the assigned IP information.

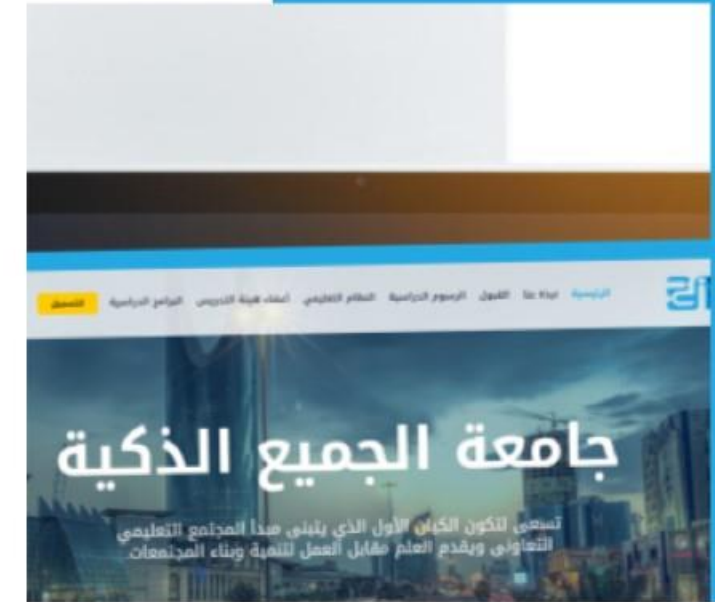
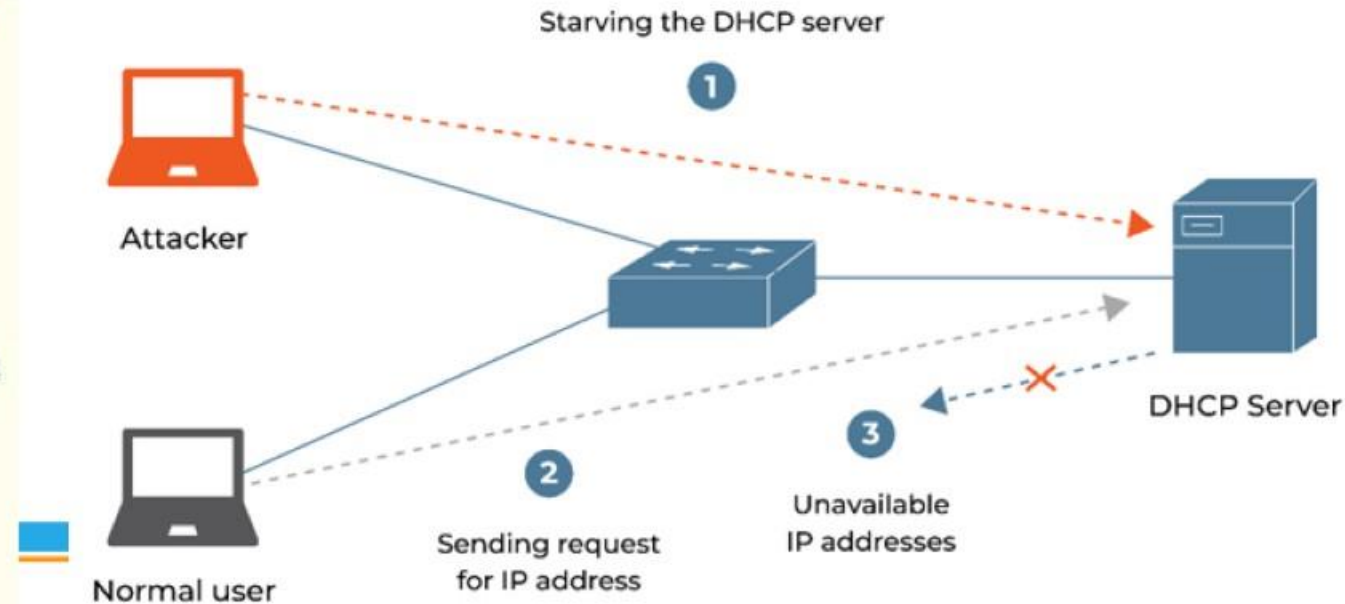
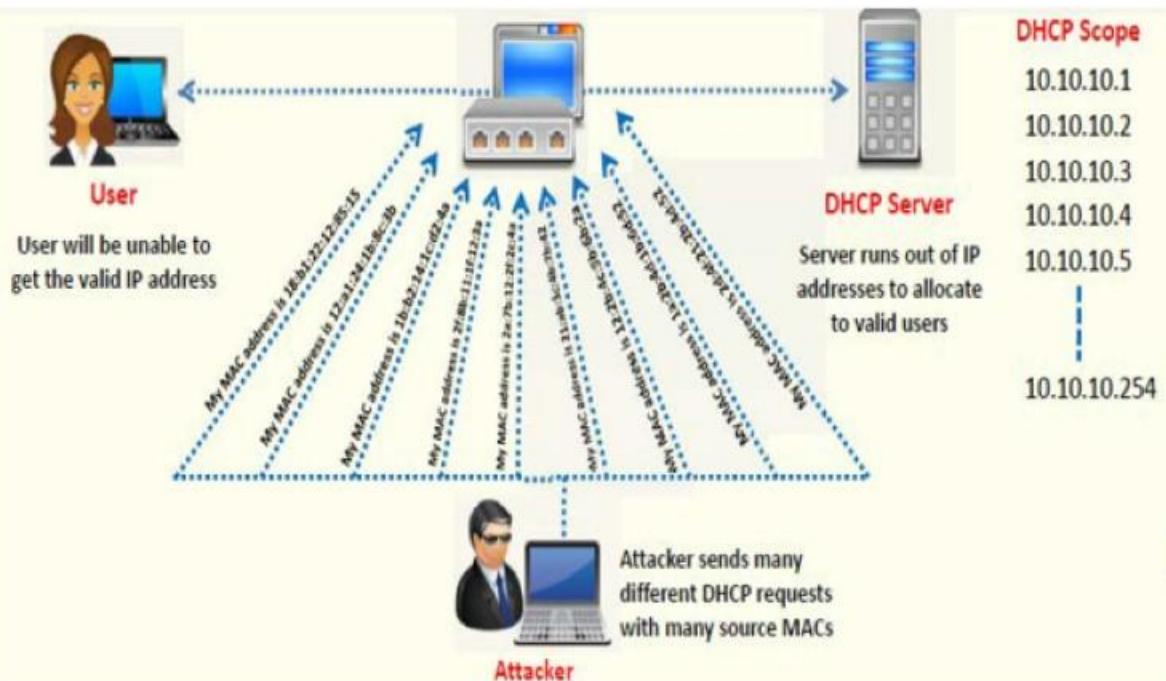


Chapter 05

Network Sniffing

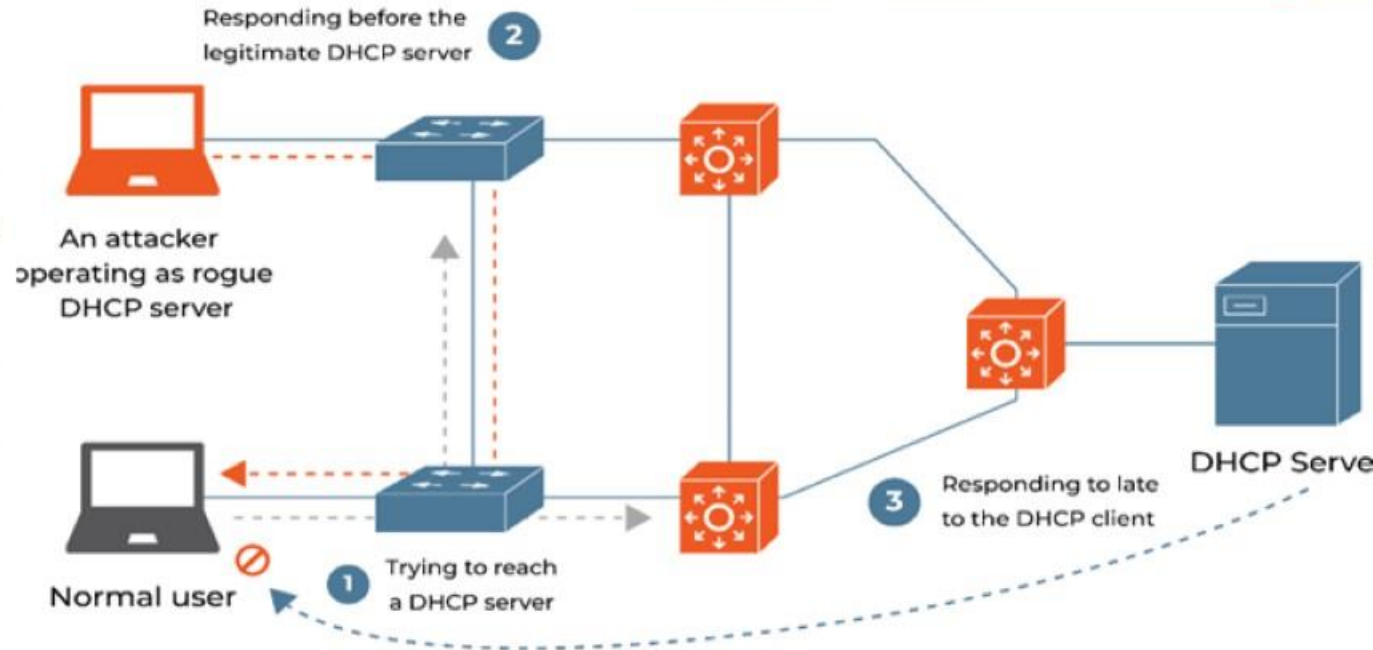
DHCP Starvation Attacks

- The goal of a DHCP starvation attack is to exhaust the address space available to the DHCP server. An attacker can initiate this attack by sending a flood of fake DHCP Discover messages with spoofed MAC addresses.
- As a result, the DHCP server will respond back with a DHCP Offer message to each of the DHCP Discover messages previously received.



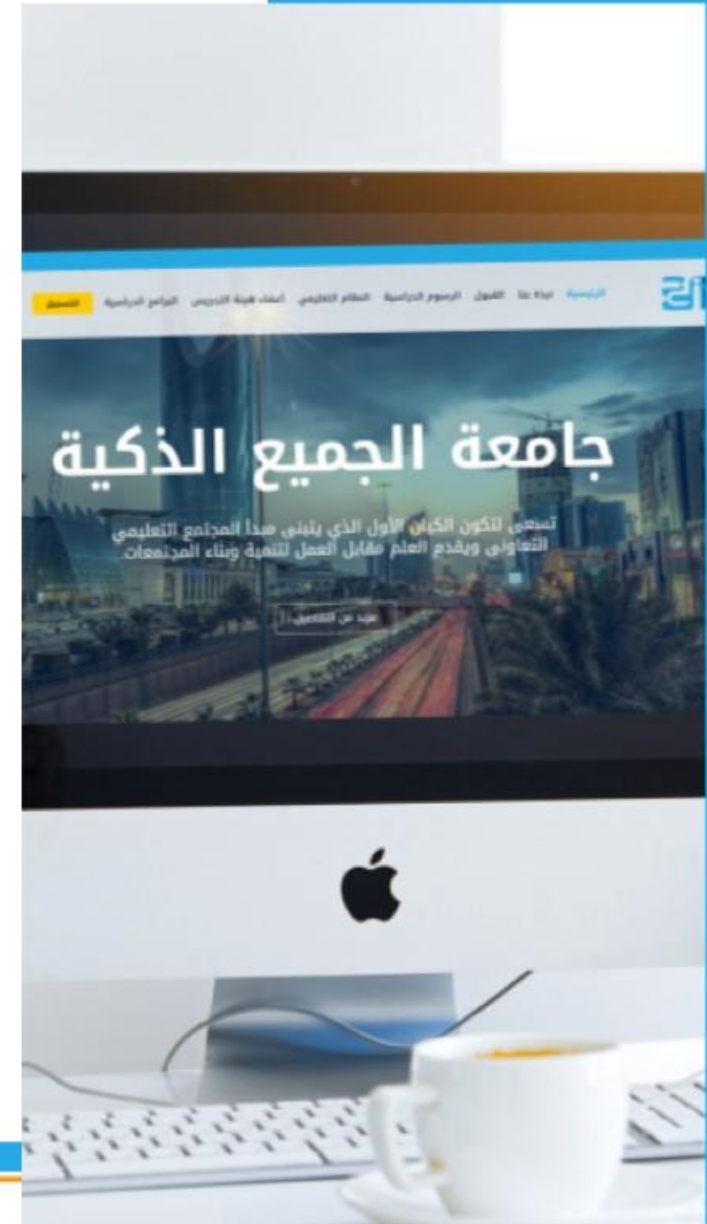
DHCP Server Spoofing Attack

- When an attacker operates a rogue DHCP server, a user can blindly start a DHCP communication with the attacker instead of the legitimate DHCP server on the network.
- This could easily happen when the rogue DHCP server is closer to the DHCP client and replies before the legitimate DHCP server does.



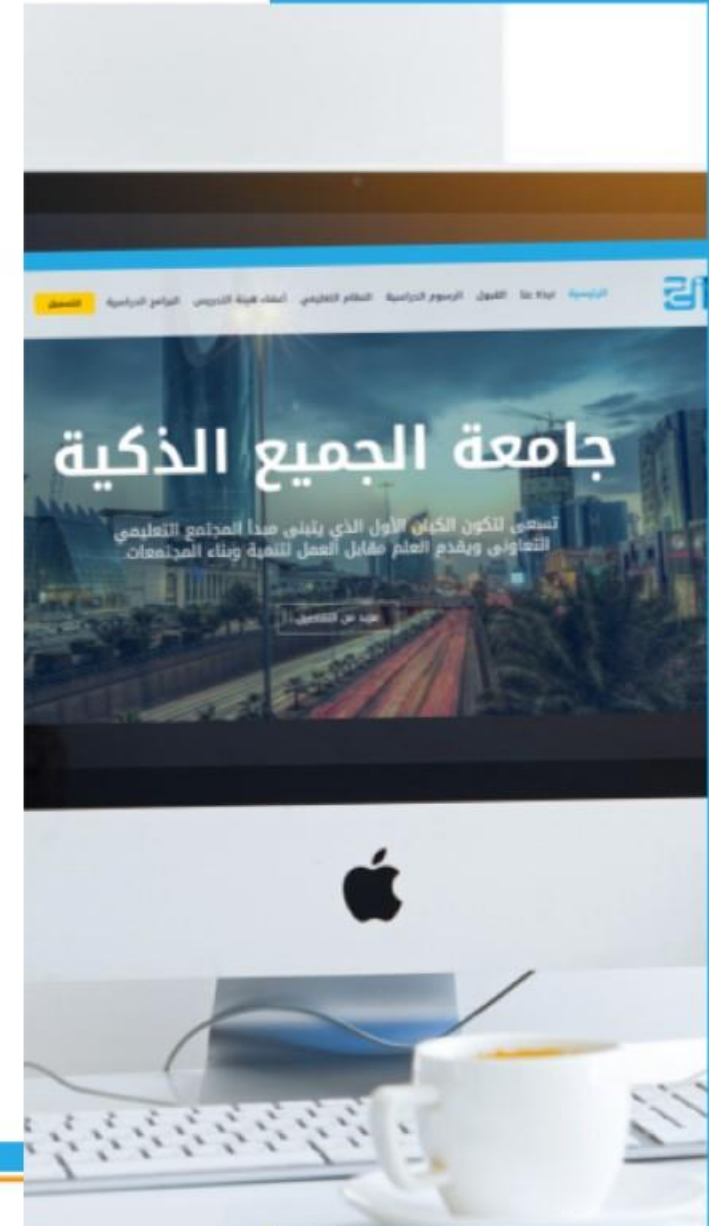
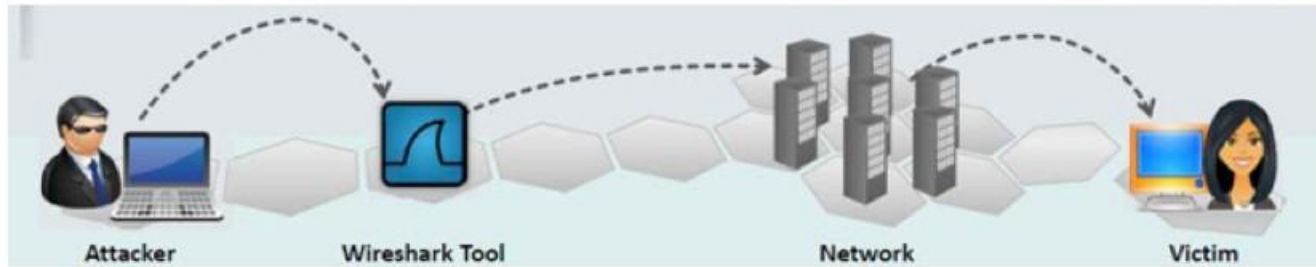
Wireshark is a network packet analyzer. A network packet analyzer presents captured packet data in as much detail as possible.

- Network administrators use it to troubleshoot network problems
- Network security engineers use it to examine security problems
- Developers use it to debug protocol implementations
- People use it to learn network protocol internals



Chapter 05

Network Sniffing



Chapter 05

Network Sniffing

tv-netflix-problems-2011-07-06.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
343	65.142415	192.168.0.21	174.129.249.228	TCP	66	40555 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519346 TSecr=551811827
344	65.142715	192.168.0.21	174.129.249.228	HTTP	253	GET /clients/netflix/flash/application.swf?flash_version=flash_lite_2.1&v=1.5&n
345	65.230738	174.129.249.228	192.168.0.21	TCP	66	80 → 40555 [ACK] Seq=1 Ack=188 Win=6864 Len=0 TSval=551811850 TSecr=491519347
346	65.240742	174.129.249.228	192.168.0.21	HTTP	828	HTTP/1.1 302 Moved Temporarily
347	65.241592	192.168.0.21	174.129.249.228	TCP	66	40555 → 80 [ACK] Seq=188 Ack=763 Win=7424 Len=0 TSval=491519446 TSecr=551811852
348	65.242532	192.168.0.21	192.168.0.1	DNS	77	Standard query 0x2188 A cdn-0.nflximg.com
349	65.276870	192.168.0.1	192.168.0.21	DNS	489	Standard query response 0x2188 A cdn-0.nflximg.com CNAME images.netflix.com.edge
350	65.277992	192.168.0.21	63.80.242.48	TCP	74	37063 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=491519482 TSecr
351	65.297757	63.80.242.48	192.168.0.21	TCP	74	80 → 37063 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=3295
352	65.298396	192.168.0.21	63.80.242.48	TCP	66	37063 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519502 TSecr=3295534130
353	65.298687	192.168.0.21	63.80.242.48	HTTP	153	GET /us/nrd/clients/flash/814540.bun HTTP/1.1
354	65.318730	63.80.242.48	192.168.0.21	TCP	66	80 → 37063 [ACK] Seq=1 Ack=88 Win=5792 Len=0 TSval=3295534151 TSecr=491519503
355	65.321733	63.80.242.48	192.168.0.21	TCP	1514	[TCP segment of a reassembled PDU]

> Frame 349: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits)

> Ethernet II, Src: Globalsc_00:3b:0a (f0:ad:4e:00:3b:0a), Dst: Vizio_14:8a:e1 (00:19:9d:14:8a:e1)

> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.21

> User Datagram Protocol, Src Port: 53 (53), Dst Port: 34036 (34036)

▼ Domain Name System (response)

[Request In: 348]

[Time: 0.034338000 seconds]

Transaction ID: 0x2188

> Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 4

Authority RRs: 9

Additional RRs: 9

▼ Queries

> cdn-0.nflximg.com: type A, class IN

> Answers

> Authoritative nameservers

0020	00 15 00 35 84 f4 01 c7 83 3f 21 88 81 80 00 01	...5.... .?!.
0030	00 04 00 09 00 09 05 63 64 6e 2d 30 07 6e 66 6c	c dn-0.nfl
0040	78 69 6d 67 03 63 6f 6d 00 00 01 00 01 c0 0c 00	ximg.com
0050	05 00 01 00 00 05 29 00 22 06 69 6d 61 67 65 73	). ".images
0060	07 6e 65 74 66 6c 69 78 03 63 6f 6d 09 65 64 67	.netflix .com.edg
0070	65 73 75 69 74 65 03 6e 65 74 00 c0 2f 00 05 00	esuite.n et.../...

Identification of transaction (dns.id), 2 bytes

Packets: 10299 · Displayed: 10299 (100.0%) · Load time: 0:0.182 · Profile: Default

Chapter 05

Network Sniffing

Display Filtering by Protocol

Example: Type the protocol in the filter box; arp, http, tcp, udp, dns, ip



Monitoring the Specific Ports

```
tcp.port==23
ip.addr==192.168.1.100 machine
ip.addr==192.168.1.100 && tcp.port=23
```

Filtering by Multiple IP Addresses

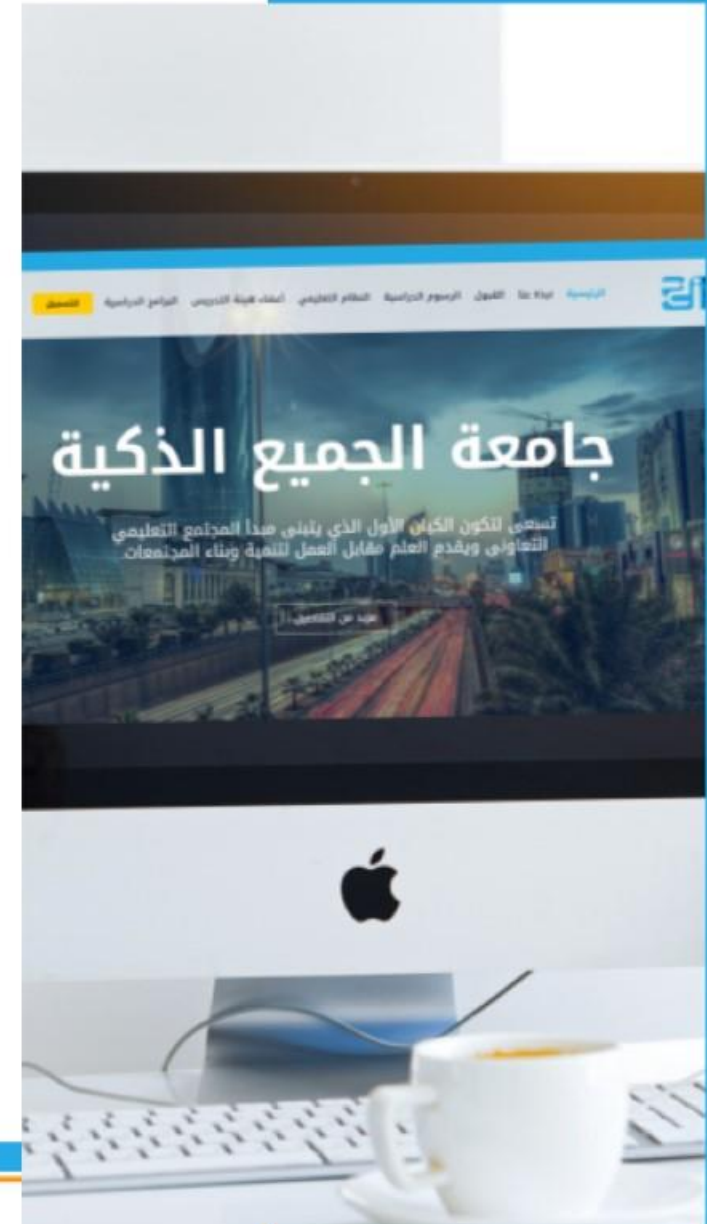
```
ip.addr == 10.0.0.4 or
ip.addr == 10.0.0.5
```

Filtering by IP Address

```
ip.addr == 10.0.0.4
```

Other Filters

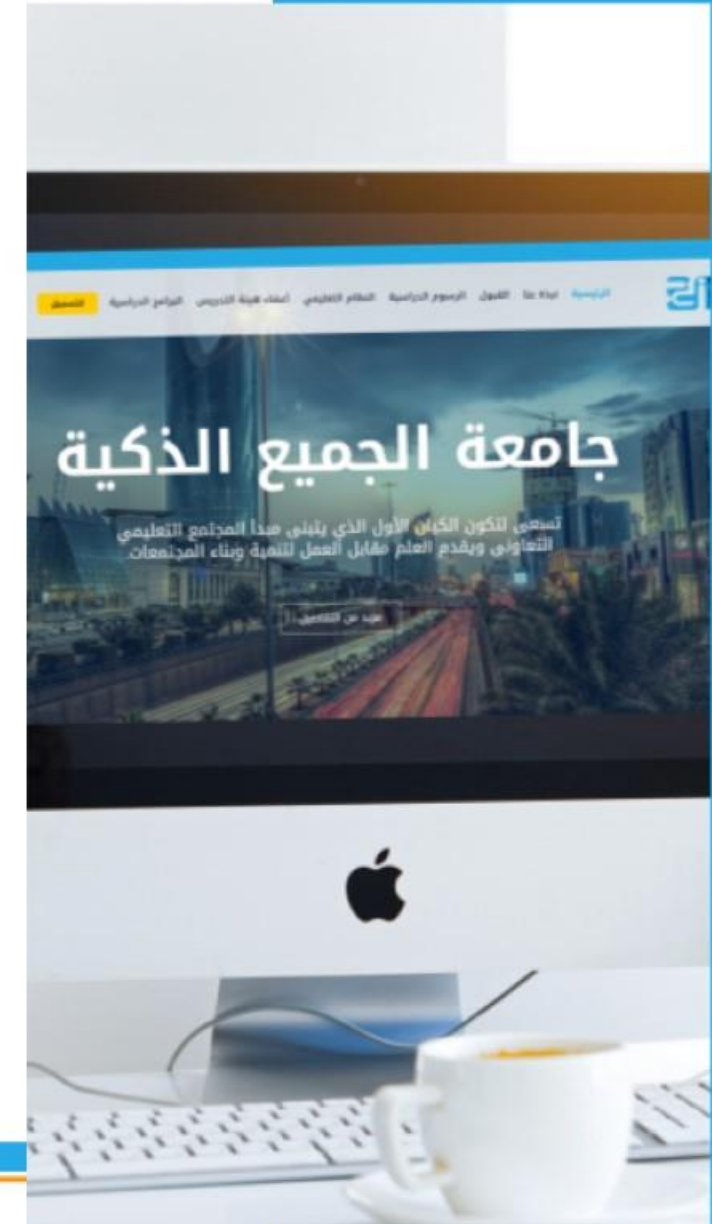
```
ip.dst == 10.0.1.50 && frame.pkt_len > 400
ip.addr == 10.0.1.12 && icmp && frame.number > 15 && frame.number < 30
ip.src==205.153.63.30 or ip.dst==205.153.63.30
```



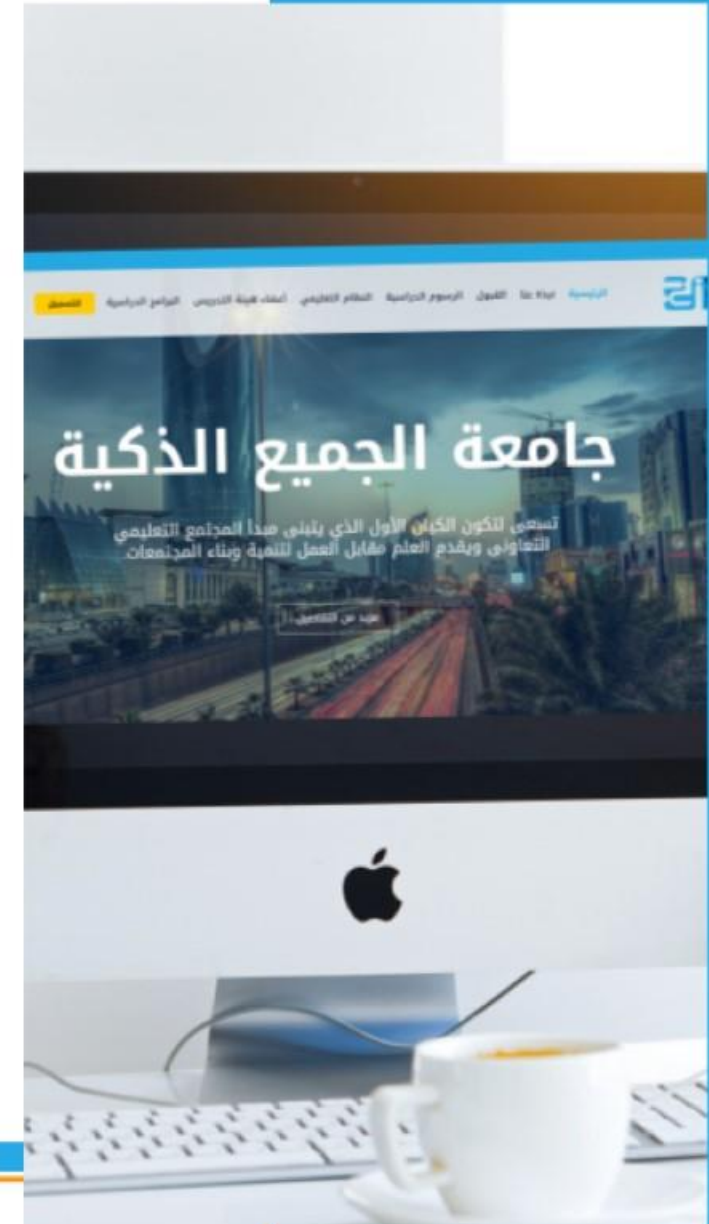
How Can Sniffing Attacks Be Prevented?

There are many ways to protect your network against sniffing attacks. Some key measures include:

- Using **encryption** to protect sensitive data from being intercepted and Never sending sensitive information over an unencrypted connection
- Making sure the wireless network is secured using WPA or WEP encryption
- Regularly updating all software and devices with the latest security patches
- Using a VPN when connecting to public Wi-Fi networks
- Continuously monitoring the network for unusual activity



- <https://www.softwaretestinghelp.com/password-cracker-tools/>
- <https://www.youtube.com/watch?v=ZljJQ1W2ue4>
- <https://wiki.wireshark.org/>



Chapter 05

Any Questions?

