(29th October 2025) - JAGUAR COHORT

Made by Chris Cownden

4th Lab Recap Guide:

Recording is here , Transcript is here

Timestamps

00:00 TCP, HTTP, and OSI Model

18:27 VPNs: Secure Remote Access

42:55 Network Troubleshooting Basics

01:01:03 Backing Up SSH Configurations

01:02:23 Troubleshooting Tips and Rules

01:16:39 Firewall Ports and Protocols Explained

01:27:56 ARP Spoofing Demo

01:42:05 Setting Targets and Monitoring

01:48:57 ARP: Network Traffic Inspection Tool

Recommended Resources

- What is client server computing ?
- What is a Server? Servers vs Desktops Explained
- Learn Microsoft Active Directory (ADDS) in 30mins
- 60 Linux Commands you NEED to know (in 10 minutes)

Linux Commands Cheatsheet

Find this cool web guide that shows 400+ Linux commands https://linux-commands.labex.io/

(29th October 2025) - JAGUAR COHORT

Made by Chris Cownden

Other Recordings To Date

Date	Order	Recordings	Lab Recap Guides
Wednesday 29th October	Lab 4	RECORDING	THIS ONE
Wednesday 22nd October	Lab 3	RECORDING	RECAP GUIDE
Sunday 19th October	2nd Sunday	RECORDING	
Wednesday 15th October	Lab 2	RECORDING	RECAP GUIDE
Wednesday 8th October	Lab 1	RECORDING	RECAP GUIDE
Sunday 5th October	1st Sunday	RECORDING	

Terminology used in today's session

Remote Connection: Accessing one computer/system from another over a network, commonly using SSH or RDP.
SSH (Secure Shell): Secure protocol for command-line remote access, usually running on port 22/TCP.
Telnet: Unsecured command-line remote access protocol, typically on port 23/TCP (not recommended for use).
RDP (Remote Desktop Protocol): Windows graphical remote access protocol, operates on port 3389/TCP.
Port Number: Numeric identifier for network services (e.g., 80 for HTTP, 22 for SSH).
TCP/UDP: Transport layer protocols for reliable (TCP) or best-effort (UDP) network communication.
Workstation: A client PC or device on the network, typically used to connect to servers.
Kali Linux: Security-focused Linux distribution used for hacking and testing.
Ubuntu: Popular Linux operating system, often used as a server or workstation.
Firewall: Network device or software that controls traffic based on rules (e.g., port/protocol).
VPN (Virtual Private Network): Secure, encrypted "tunnel" connection for remote access

over the internet.
Ping: Network diagnostic tool to test connectivity between devices.
Network Card (Ethernet Adapter): Hardware enabling devices to connect to a network with unique MAC address.
ARP (Address Resolution Protocol): Resolves IP addresses to MAC addresses for local network delivery.
ARP Spoofing/Poisoning: Attack technique falsifying MAC address associations in an ARP cache.
Putty: Windows application for SSH and Telnet remote access sessions.
User Account: Individual network identity with specific access rights (e.g., labadmin, user01).
Configuration File: File containing service or system settings, often modified for security or access.
Home Directory: User's default folder location in the file system.

Understanding TCP & UDP

Feature	**TCP (Transmission Control Protocol)**	**UDP (User Datagram Protocol)**
Connection	Connection-oriented (handshake before data transfer)	Connectionless (no setup, just send)
Reliability	Reliable and guarantees delivery, order, and no duplicates	Unreliable and no guarantee of delivery or order
Speed	Slower due to error checking and acknowledgments	Faster, less overhead
Use Cases	Web browsing (HTTP/HTTPS), email, file transfers	Streaming, gaming, voice/video calls
Error Checking	Yes – resends lost packets	Minimal – ignores lost packets

(29th October 2025) - JAGUAR COHORT

Made by Chris Cownden

Examples of TCP & UDP

Port	Protocol	TCP	UDP	Description
20	FTP (Data)	✅	❌	Transfers file data between client and server
21	FTP (Control)	✅	❌	Handles commands for file transfers
22	SSH (Secure)	✅	❌	Secure command-line and remote login
23	Telnet (Insecure)	✅	❌	Unencrypted remote command-line access
25	SMTP	✅	❌	Sends outgoing email
53	DNS	✅	✅	Translates domain names to IPs (UDP for queries, TCP for large transfers)
67	DHCP (Server)	❌	✅	Assigns IP addresses automatically (server listens for requests)
68	DHCP (Client)	❌	✅	Client listens for DHCP server replies to get its IP
69	TFTP	❌	✅	Simplified file transfer (no authentication)

(29th October 2025) - JAGUAR COHORT

Made by Chris Cownden

80	HTTP	✅	❌	Web traffic (non-secure websites)
110	POP3	✅	❌	Retrieves emails from server
123	NTP	❌	✅	Network time synchronization
143	IMAP	✅	❌	Retrieves and manages emails on server
161/162	SNMP	❌	✅	Network monitoring and management
389	LDAP	✅	✅	Directory services like Active Directory
443	HTTPS	✅	❌	Secure web traffic (SSL/TLS)
445	SMB	✅	❌	File sharing and network communication (Windows)
993	IMAPS	✅	❌	Secure IMAP email
995	POP3S	✅	❌	Secure POP3 email
3389	RDP	✅	❌	Remote Desktop Protocol (Windows)
5060/5061	SIP	✅	✅	Voice over IP (VoIP) signaling

8080	HTTP (Alternate)	✅	❌	Used for web traffic when 80 is unavailable

Recap of ISO Model = HTTPS Example

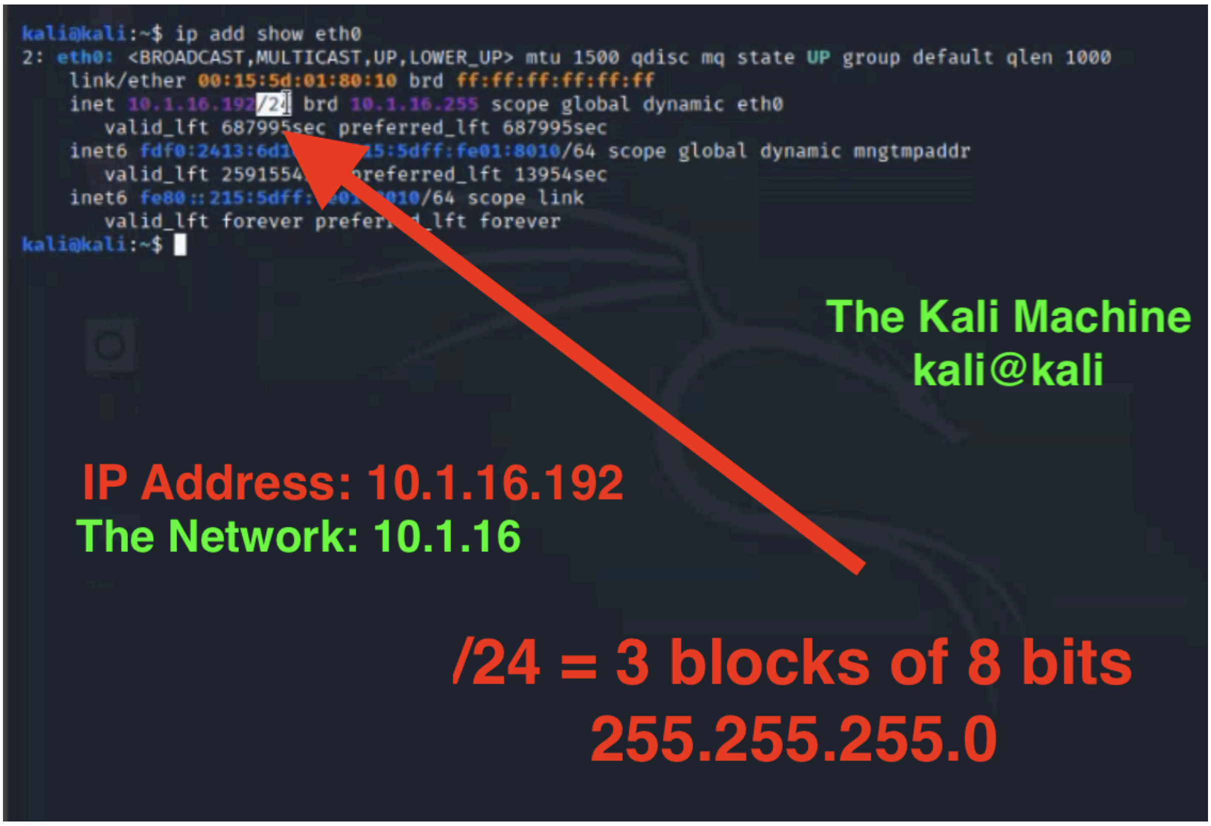
OSI Layer	What it Does	How HTTPS Data is Handled	Devices / Examples
7 – Application	Provides interface to user apps	Browser requests `https://example.com`, encrypts data via TLS	PC, Laptop, Smartphone
6 – Presentation	Formats, encrypts, compresses data	TLS encrypts HTTP data into HTTPS TLS = Transport Layer Security	Same device as above (browser handles it)
5 – Session	Manages sessions and connections	Browser sets up secure session with server (handshake, keys)	Client PC & Web Server
4 – Transport	Ensures reliable delivery	TCP breaks HTTPS data into segments, adds port number 443	Router, PC, Server
3 – Network	Routes packets to destination	IP adds source & destination addresses; finds best path	Router, Layer 3 switch
2 – Data Link	Frames data for physical network	Ethernet/Wi-Fi frames HTTPS packets for LAN	Switch, Wi-Fi access point, NIC (Network Interface Card)
1 – Physical	Transmits raw bits	Bits travel over cable, fiber, or radio	Cables, Fiber, Wireless radios

Checking if 2 Devices are on the same network

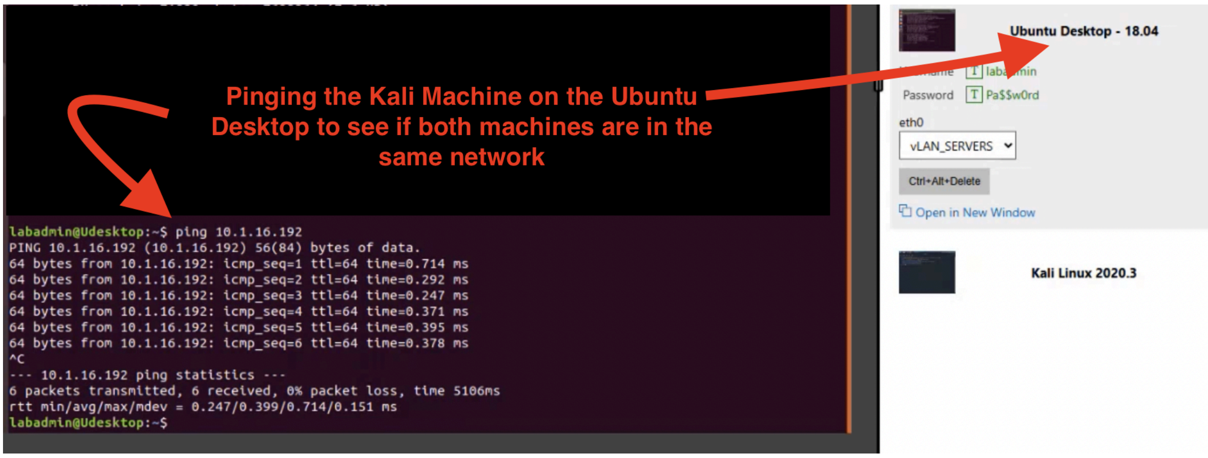
1. On the Kali Linux, write command ip add show eth0 to show IP address for eth0
2. Go to the Ubuntu Desktop and ping the Kali Linux eth0 IP address (10.1.16.192)
3. If it works it will show results and confirm they are in the same network
4. You can check by writing the command ipconfig on Ubuntu to see the ip address (10.16.1.9)

(29th October 2025) - JAGUAR COHORT

Made by Chris Cownden



```
kali@kali:~$ ip add show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:15:5d:01:80:10 brd ff:ff:ff:ff:ff:ff
    inet 10.1.16.192/24 brd 10.1.16.255 scope global dynamic eth0
       valid_lft 687995sec preferred_lft 687995sec
    inet6 fdf0:2413:6d1[illegible]15:5dff:fe01:8010/64 scope global dynamic mngtmpaddr
       valid_lft 2591554[illegible]preferred_lft 13954sec
    inet6 fe80::215:5dff:fe01:8010/64 scope link
       valid_lft forever preferred_lft forever
kali@kali:~$
```



```
labadmin@Udesktop:~$ ping 10.1.16.192
PING 10.1.16.192 (10.1.16.192) 56(84) bytes of data.
64 bytes from 10.1.16.192: icmp_seq=1 ttl=64 time=0.714 ms
64 bytes from 10.1.16.192: icmp_seq=2 ttl=64 time=0.292 ms
64 bytes from 10.1.16.192: icmp_seq=3 ttl=64 time=0.247 ms
64 bytes from 10.1.16.192: icmp_seq=4 ttl=64 time=0.371 ms
64 bytes from 10.1.16.192: icmp_seq=5 ttl=64 time=0.395 ms
64 bytes from 10.1.16.192: icmp_seq=6 ttl=64 time=0.378 ms
^C
--- 10.1.16.192 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5106ms
rtt min/avg/max/mdev = 0.247/0.399/0.714/0.151 ms
labadmin@Udesktop:~$
```

Username: labadmin
Password: Pa$$w0rd

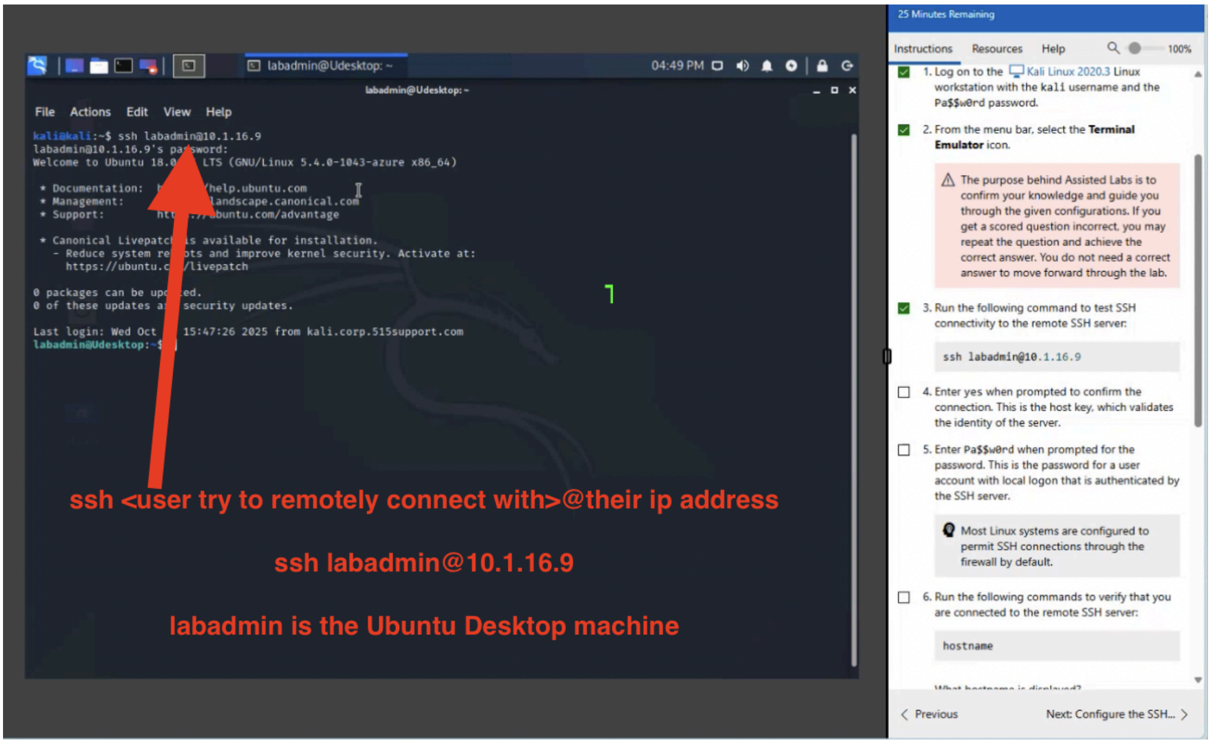
Remotely connect to another device using SSH

This is a great skill to have because if you have 20 devices on the same network and you want to access one for security purposes, you can securely connect to other devices, safely control and move files on other devices, automate tasks, and even securely access internal network services all without leaving your chair.

(29th October 2025) - JAGUAR COHORT

Made by [Chris Cownden]

1. Check the IP address you want to connect to (use "ipconfig")
2. Then write out the SSH command to connect to it (see image)
3. Once admin password is added it says "Welcome to Ubuntu which means the Kali Machine has been successful and securely connected to the Ubuntu Machine on the same network
4. To verify, use command "hostname" and it will tell you which machine you are currently operating with.
5. As long as you are the admin, you can control that device



```
kali@kali:~$ ssh labadmin@10.1.16.9
labadmin@10.1.16.9's pa sword:
Welcome to Ubuntu 18.0   LTS (GNU/Linux 5.4.0-1043-azure x86_64)

 * Documentation:  h    /help.ubuntu.com
 * Management:          landscape.canonical.com
 * Support:        htt     ubuntu.com/advantage

 * Canonical Livepatc  is available for installation.
   - Reduce system re  ots and improve kernel security. Activate at:
     https://ubuntu.c  /livepatch

0 packages can be upd  ed.
0 of these updates ar  security updates.

Last login: Wed Oct    15:47:26 2025 from kali.corp.515support.com
labadmin@Udesktop:~$
```

☑ 1. Log on to the Kali Linux 2020.3 Linux workstation with the kali username and the Pa$$w0rd password.

☑ 2. From the menu bar, select the **Terminal Emulator** icon.

⚠ The purpose behind Assisted Labs is to confirm your knowledge and guide you through the given configurations. If you get a scored question incorrect, you may repeat the question and achieve the correct answer. You do not need a correct answer to move forward through the lab.

☑ 3. Run the following command to test SSH connectivity to the remote SSH server:

```
ssh labadmin@10.1.16.9
```

☐ 4. Enter yes when prompted to confirm the connection. This is the host key, which validates the identity of the server.

☐ 5. Enter Pa$$w0rd when prompted for the password. This is the password for a user account with local logon that is authenticated by the SSH server.

Most Linux systems are configured to permit SSH connections through the firewall by default.

☐ 6. Run the following commands to verify that you are connected to the remote SSH server:

```
hostname
```

What hostname is displayed?

ssh <user try to remotely connect with>@their ip address

ssh labadmin@10.1.16.9

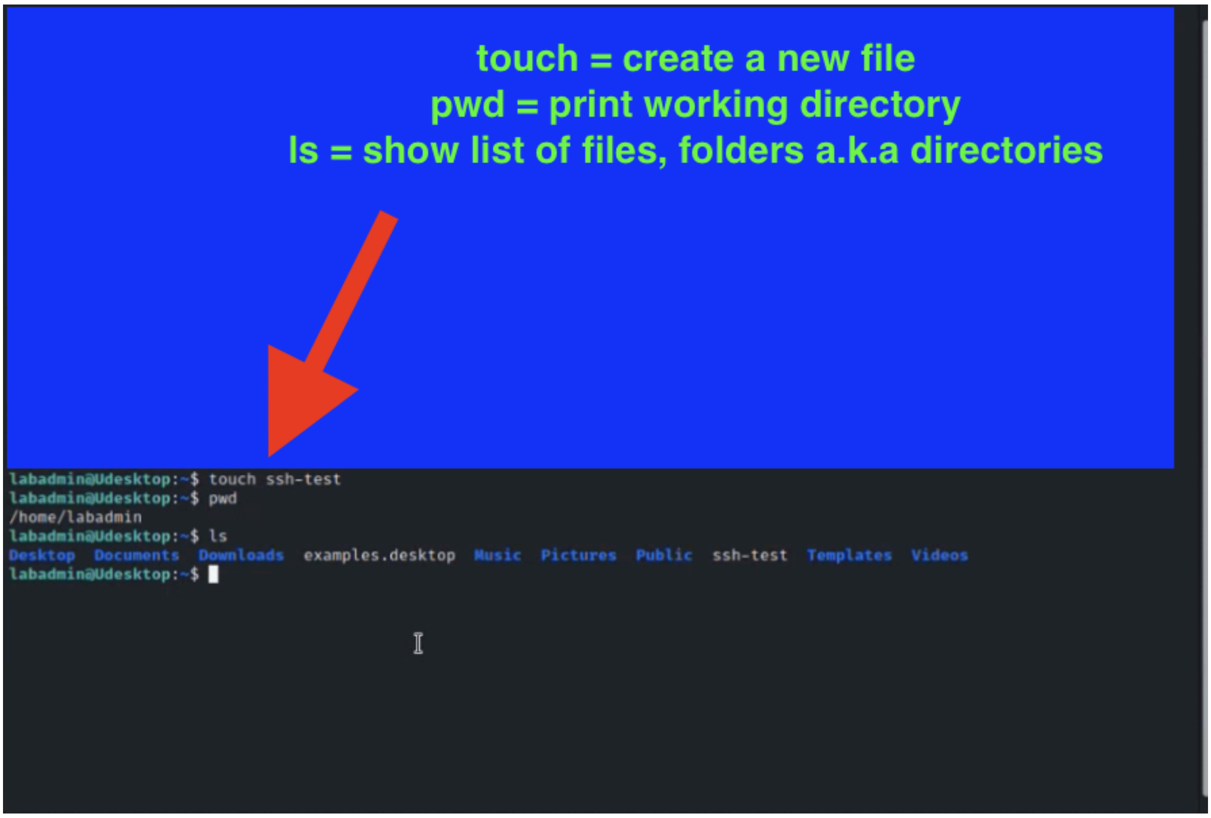
labadmin is the Ubuntu Desktop machine

Creating a file on another device in your network with SSH

1. Firstly, follow instructions above to SSH to Ubuntu Desktop via Kali Linux so that you are operating as Ubuntu while writing commands in the Kali Linux machine
2. To create a file using the command "touch"
3. "touch ssh-test" (creating a file called ssh-text)
4. Check to see where you are creating the file by printing the working directory. Use command "pwd"
5. It will say /home/labadmin = this is the labadmin folder in the home directory.
6. Use command "ls" to see the full list of files in the labadmin folder. It should show the file
7. Now go to Ubuntu Desktop and you'll see the file ssh-test is in this location /home/labadmin/ssh-test

(29th October 2025) - JAGUAR COHORT

Made by Chris Cownden



touch = create a new file
pwd = print working directory
ls = show list of files, folders a.k.a directories

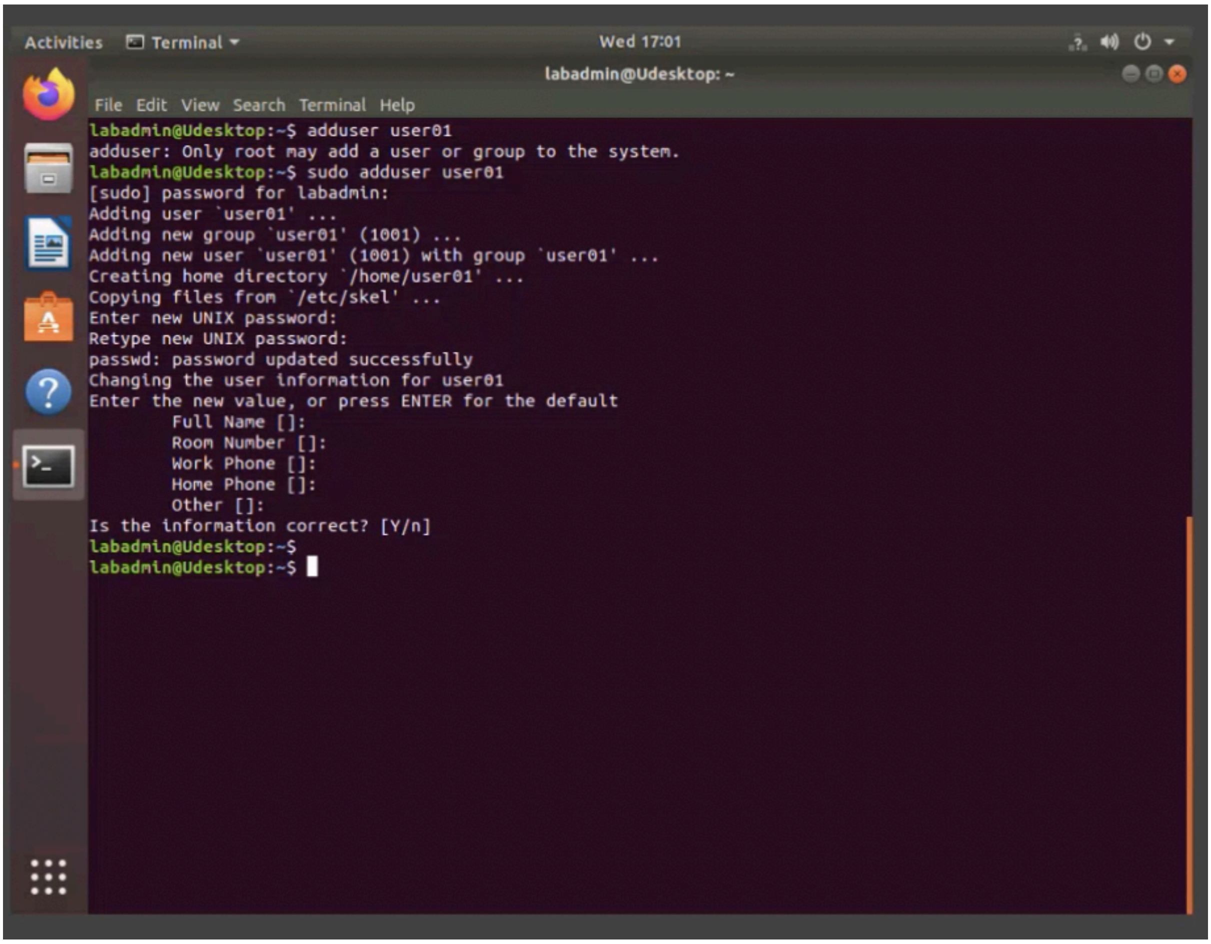
```
labadmin@Udesktop:~$ touch ssh-test
labadmin@Udesktop:~$ pwd
/home/labadmin
labadmin@Udesktop:~$ ls
Desktop  Documents  Downloads  examples.desktop  Music  Pictures  Public  ssh-test  Templates  Videos
labadmin@Udesktop:~$ 
```

Adding user with SSH on another network

1. Must user command “sudo” to act as a super user
2. sudo adduser user01 = add user by the name user01
3. Prompted to add admin password to verify you as a super user

(29th October 2025) - JAGUAR COHORT

Made by [Chris Cownden]



```
labadmin@Udesktop:~$ adduser user01
adduser: Only root may add a user or group to the system.
labadmin@Udesktop:~$ sudo adduser user01
[sudo] password for labadmin:
Adding user `user01' ...
Adding new group `user01' (1001) ...
Adding new user `user01' (1001) with group `user01' ...
Creating home directory `/home/user01' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for user01
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n]
labadmin@Udesktop:~$
labadmin@Udesktop:~$
```

Open a file with SSH

1. Command “cat” is for opening files
2. cat /etc/ssh/sshd_config
3. Will open the file sshd_config

Assisted Lab: Analyse a ARP Spoofing Attack

Using Kali Linux as the hacking machine to run a program called Ettercap to run ARP Spoofing. The goal with this is to intercept the MAC addresses by changing unique MAC addresses to the same MAC address so that all messages in the network can be read by the hacker.

(29th October 2025) - JAGUAR COHORT

Made by Chris Cownden

What the attacker (Kali Linux) does:

1. **Spoof a MAC:** Kali changes its network interface to claim the same MAC address as the router

2. **Send forged ARP replies:** Kali injects ARP replies into the network, telling MS.10 "the router's IP is at this MAC (Kali's MAC)."

3. **Poison the ARP cache:** MS.10 updates its ARP cache with the attacker's MAC for the router's IP.

4. **Traffic interception:** Now when MS.10 sends frames to the router, they go to Kali first. Kali can read, modify, and then forward the traffic to the real router so MS.10 doesn't notice (classic Man-in-the-Middle).

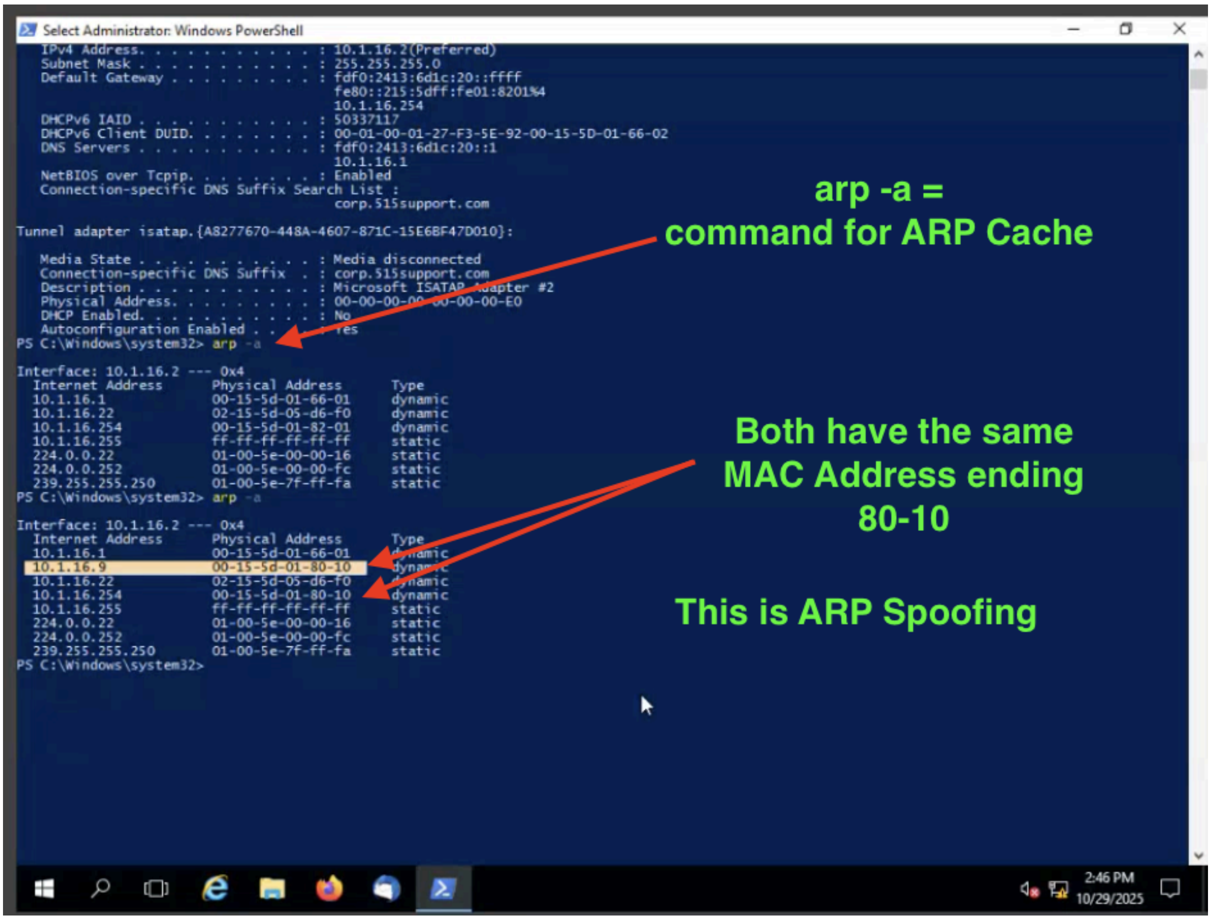
Common Examples:

- **Unsecured Wi-Fi networks:** Hacker intercepts data when you use public Wi-Fi.
- **Fake websites:** Attacker tricks you into visiting a clone of a real site.
- **Email hijacking:** Intercepting emails to steal info or credentials.
- **SSL stripping:** Downgrading secure HTTPS connections to HTTP

Setting Up A Man-In-The-Middle Attack

1. Start on MS10 (This is the machine that will be spoofed)
2. Go to Windows PowerShell to write commands
3. Type command "ipconfig /all" to see all IP addresses and MAC addresses
4. Type arp -a to see the ARP Cache. The ARP Cache shows all the IP addresses and their MAC Addresses
5. Jump to Kali Linux
6. Go to Terminal
7. Main menu, search Ettercap
8. Accept the checkmark on the top bar
9. Click "scan for hosts" on top bar
10. Select the ip address with 10.1.16.2 right click and set to target 1 (MS10)
11. Select 10.1.16.254 and right click and set to target 2 (router)
12. Click the Globe icon on top bar to choose the attack
13. Click ARP Poisoning and click OK
14. Go back to kali@kali tab and write the command "sudo wireshark"
15. Enter password
16. Then a graphical window will appear. Click eth0 (network interface card)
17. Then click the first icon on the top bar. (Hover over it and it will say "Start capturing packets"

18. Minimize it
19. Go back to MS10 and do an ARP Cache with command “arp -a” to show IP addresses and MAC addresses
20. It will show that both 10.1.16.9 & 10.1.16.254 have the same MAC Address which is called ARP Spoofing.
21. That means that both devices will get the same messages across the network
22. Go back to Wireshark and press the red square on the top bar to stop it
23. Go back to Ettercap and click the world icon, then “stop Mitm attack.”



```
   IPv4 Address. . . . . . . . . . . : 10.1.16.2(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fdf0:2413:6d1c:20::ffff
                                       fe80::215:5dff:fe01:8201%4
                                       10.1.16.254
   DHCPv6 IAID . . . . . . . . . . . : 50337117
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-27-F3-5E-92-00-15-5D-01-66-02
   DNS Servers . . . . . . . . . . . : fdf0:2413:6d1c:20::1
                                       10.1.16.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
   Connection-specific DNS Suffix Search List :
                                       corp.515support.com

Tunnel adapter isatap.{A8277670-448A-4607-871C-15E6BF47D010}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : corp.515support.com
   Description . . . . . . . . . . . : Microsoft ISATAP Adapter #2
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
PS C:\Windows\system32> arp -a

Interface: 10.1.16.2 --- 0x4
  Internet Address      Physical Address      Type
  10.1.16.1             00-15-5d-01-66-01     dynamic
  10.1.16.22            02-15-5d-05-d6-f0     dynamic
  10.1.16.254           00-15-5d-01-82-01     dynamic
  10.1.16.255           ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
PS C:\Windows\system32> arp -a

Interface: 10.1.16.2 --- 0x4
  Internet Address      Physical Address      Type
  10.1.16.1             00-15-5d-01-66-01     dynamic
  10.1.16.9             00-15-5d-01-80-10     dynamic
  10.1.16.22            02-15-5d-05-d6-f0     dynamic
  10.1.16.254           00-15-5d-01-80-10     dynamic
  10.1.16.255           ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
PS C:\Windows\system32>
```

arp -a =
command for ARP Cache

Both have the same
MAC Address ending
80-10

This is ARP Spoofing

Analogy from today’s session

Think of a busy post office. Each person has a unique mailbox (MAC address), and the post office sorts mail based on addresses. Now, imagine someone sneaky swaps labels on two mailboxes, so mail meant for Bob now gets sent to the wrong box and the sneaky person reads it before letting it reach Bob. ARP cache poisoning in a network works just like that: it tricks computers into sending messages to the attacker instead of the intended recipient, letting the attacker see or change the data before it arrives.

In short: it’s like a fake postman redirecting your letters, so someone can read your mail before you get it.

1. **Unique Mailboxes:** Every computer on the local network has a unique “mailbox” (Mac address) for receiving messages.
2. **Address Book (ARP Cache):** Computers keep an address book that matches an IP address to its correct mailbox (Mac address).
3. **The Switcheroo:** An attacker fools the system by swapping address labels—so info meant for the real recipient gets sent to the attacker first.
4. **Man-in-the-Middle:** The attacker secretly intercepts and can read (or even change) the message, then passes it on so you don’t know anything happened.
5. **Why It Matters:** It’s a way hackers “listen in” or tamper with communications on a network, just like a fake postman handling your mail.

Just like a secure post office needs to check labels, a secure network checks for ARP cache poisoning to keep your data safe.

General Q&A from the session

What types of remote connections were demonstrated in the session?

Two main types were covered: command-line remote connections using SSH/Telnet (mainly for Linux/Unix machines) and GUI-based remote connections using RDP for Windows machines.

Why is SSH preferred over Telnet for remote connections?

SSH encrypts the communication and provides authentication with usernames and passwords, making it secure. Telnet sends credentials in clear text, which can be easily intercepted if someone is sniffing network traffic.

On which port does SSH run, and why is knowing port numbers important?

SSH runs on TCP port 22.

What steps were taken in the lab to set up and test an SSH connection?

(29th October 2025) - JAGUAR COHORT

Made by Chris Cownden

A Kali Linux machine (client) was used to remotely connect to an Ubuntu (server) via SSH. The user logged in using the appropriate credentials and performed actions like checking the hostname and creating a test file on the remote server.

How do internal networks typically structure device communication in businesses?

Workstations (PCs) connect predominantly to servers to access data and services, occasionally to printers. Direct PC-to-PC connections are less common in business but may occur at home.

What is a VPN?

A VPN (Virtual Private Network) creates a secure, encrypted tunnel across the internet for remote users (like those in hotels or working from home) to access company resources as if they were in the office.

How does ARP (Address Resolution Protocol) function in local network communications?

When a device needs to contact another by IP address but doesn't know the MAC, it sends an ARP request. The target responds with its MAC, and communications proceed. This process was explained before demonstrating ARP spoofing attacks.

How do you trigger an ARP Request?

- "ping 192.168.1.10" = ping the IP address
- If the MAC is not in your ARP cache, your system automatically sends an ARP request.
- The device that owns that IP address responds with its MAC address.
- Your device stores the IP and MAC addresses in the ARP cache for future use. (command arp -a for ARP Cache)

What is the command for ARP Caching?

The command is arp -a which shows all.

- ARP stands for Address Resolution Protocol.
- Computers use ARP to translate IP addresses (like `192.168.1.10`) into MAC addresses (hardware addresses like `00:1A:2B:3C:4D:5E`) so they can communicate on a local network.
- The ARP cache is a table your computer keeps temporarily storing these IP-to-MAC mappings.

Why do all MAC Addresses need to be unique?

(29th October 2025) - JAGUAR COHORT

Made by Chris Cownden

- MAC (Media Access Control) addresses are like a device's network fingerprint.
- They identify every device on a local network at the hardware level.
- If two devices have the same MAC, the network can't tell them apart.
- Data might go to the wrong device, causing errors or connection failures.
- Duplicate MAC addresses break this process because the switch doesn't know which port to send the data to.

Why should you NOT use Telnet anymore?

- Telnet sends all data, including usernames and passwords, in plain text.
- Anyone on the network can intercept and read your sensitive information which means that Telnet is an **UNSECURE** service.
- Telnet has known security vulnerabilities that can allow attackers to take control of your device.
- Use SSH instead as it is **SECURE and** encrypts all communication and is much safer.

Keep up the great work team! You've got this!

All the best, Chris Cownden (fellow JAGUAR cohort team player)

Feel free to connect with me here: https://www.linkedin.com/in/chriscownden/