Lecture 5

Secure Access for Network Devices

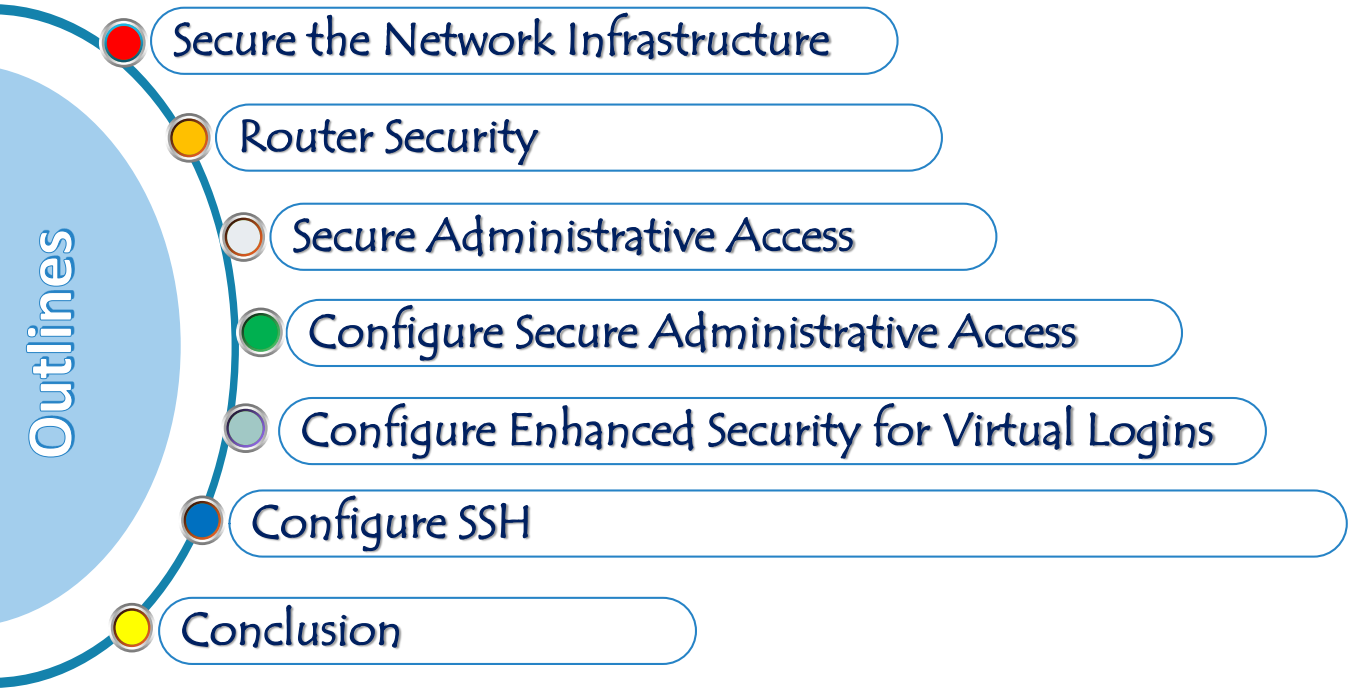
Presented By

Dr.Marwa Sharaf El-Din

Attention !

THE CONTENTS OF THIS PRESENTATION FOR EDUCATION PURPOSE ONLY

Outlines

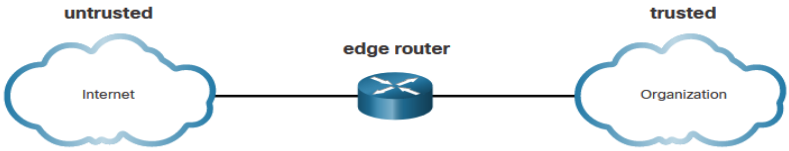


- Secure the Network Infrastructure
- Router Security
- Secure Administrative Access
- Configure Secure Administrative Access
- Configure Enhanced Security for Virtual Logins
- Configure SSH
- Conclusion

Secure the Network Infrastructure

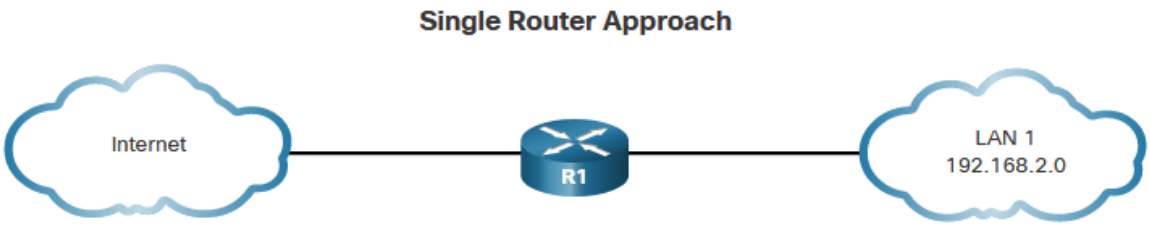
Secure the Network Infrastructure

- ✓ **Securing the network infrastructure** is critical to overall network security.
- ✓ **The network infrastructure** includes routers, switches, servers, endpoints, and other devices.
- ✓ **Routers** are a primary target for attacks because these devices direct traffic into, out of, and between networks.
- ✓ The **edge router** shown in the figure is the last router between the internal network (Trusted network) and an untrusted network, such as the internet. All an organization's internet traffic goes through an edge router, which often functions as the first and last line of defense for a network.



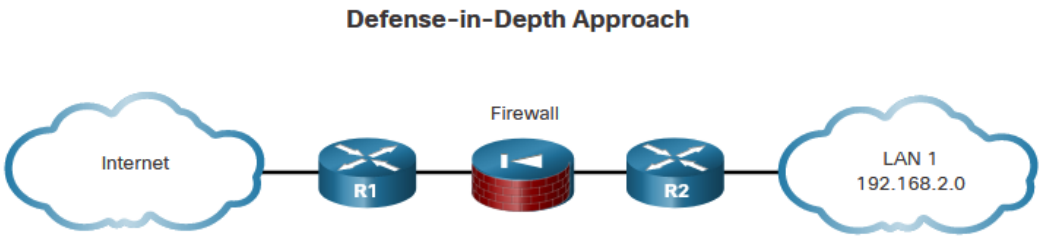
Edge Router Security Approaches

- ✓ **Single Router:** A single router connects the protected network or internal local area network (LAN), to the internet.
- ✓ All security policies are configured on this device.



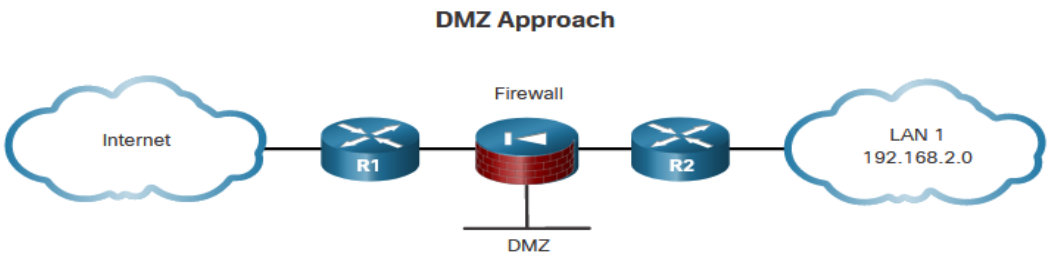
Edge Router Security Approaches (Cont.)

- ✓ **Defense-in-Depth:** This uses multiple layers of security prior to traffic entering the protected LAN.
- ✓ There are **three primary layers of defense**: **the edge router**, **the firewall**, and **an internal router** that connects to the protected LAN.



Edge Router Security Approaches (Cont.)

- ✓ **Demilitarized Zone (DMZ):** The **DMZ** can be used for servers that must be accessible from the internet or another external network.
- ✓ The **DMZ** can be set up between **two routers**, with an internal router connecting to the protected network and an external router connecting to the unprotected network.



Router Security

Router Security

Three areas of router security must be maintained:

- **Physical:** Place the router and physical devices that connect to it in a secure locked room that is accessible only to authorized personnel. Install an uninterruptible power supply (UPS) or diesel backup power generator.
- **Operating System:** Configure the router with the maximum amount of memory possible. The availability of memory can help mitigate DoS attacks. Use the latest, stable version of the operating system that meets the feature specifications of the router or network device. Keep a secure copy of router operating system images and router configuration files as backups.
- **Router Hardening:** Ensure that only authorized personnel have access and that their level of access is controlled. Disable unused ports and interfaces. Disable unnecessary services. A router has services that are enabled by default. Some of these services can be used by an attacker to gather information about the router and the network.

Secure Administrative Access

Secure Administrative Access

- ✓ **Securing administrative access** is important. If **an unauthorized person gains administrative access to a router**, that person could alter routing parameters, disable routing functions, or discover and gain access to other systems within the network.

- ✓ **Several tasks are involved in securing administrative access to an infrastructure device:**
  - Restrict device accessibility
  - Log and account for all access
  - Authenticate access
  - Authorize actions
  - Ensure the confidentiality of data

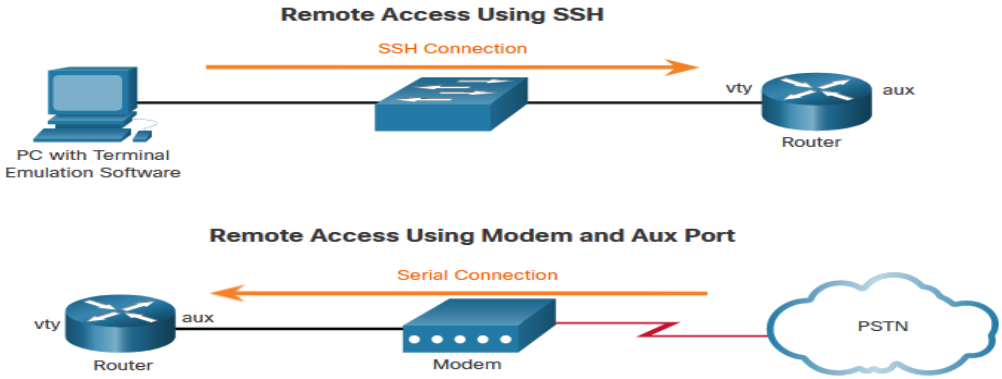
Secure Local Access

A router can be accessed for administrative purposes locally or remotely:

- **Local access: The administrator** must have physical access to **the router** and use **a console cable** to connect to **the console port**.
- **Local access** is typically used for initial configuration of the device.

Secure Remote Access

- **Remote access:** Although the **aux port** option is available, the most common remote access method involves allowing **Telnet, SSH, HTTP, HTTPS, or SNMP** connections to the router from a computer.
- **The computer** can be on the local network or a remote network.



Configure Secure Administrative Access

Configure Passwords

- ✓ To secure **user EXEC mode** access, enter line console configuration mode using the **line console 0** global configuration command.
- ✓ Specify **the user EXEC mode** password using the **password** *password* command.
- ✓ Enable user EXEC access using the **login** command.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# line console 0
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)# end
Sw-Floor-1#
```

Configure Passwords (Cont.)

- ✓ To have **administrator access** to all IOS commands including configuring a device, you must gain **privileged EXEC mode access**.
- ✓ To secure **privileged EXEC access**, use the **enable secret** *password* global config command.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# enable secret class
Sw-Floor-1(config)# exit
Sw-Floor-1#
```

Configure Passwords (Cont.)

- ✓ To secure **vty lines**, enter line vty mode using the **line vty 0 15** global config command.
- ✓ Specify **the vty password** using the **password** *password* command.
- ✓ **Enable vty access** using the **login** command.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# line vty 0 15
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)# end
Sw-Floor-1#
```

Encrypt Passwords

- ✓ **Strong passwords** are only useful if they are secret.

- ✓ **There are several steps that can be taken to help ensure that passwords remain secret on a Cisco router and switch including these:**
  - Encrypting all plaintext passwords
  - Setting a minimum acceptable password length
  - Deterring brute-force password guessing attacks
  - Disabling an inactive privileged EXEC mode access after a specified amount of time.

Encrypt Passwords (Cont.)

- ✓ To encrypt all plaintext passwords, use the **service password-encryption** global config command.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# service password-encryption
Sw-Floor-1(config)#
```

- ✓ Use the **show running-config** command to verify that passwords are now encrypted.

```
Sw-Floor-1(config)# end
Sw-Floor-1# show running-config
!
(Output omitted)
!
line con 0
password 7 094F471A1A0A
login
!
line vty 0 4
 password 7 094F471A1A0A
 login
line vty 5 15
 password 7 094F471A1A0A
 login
!
!
end
```

Configure Enhanced Security for Virtual Logins

Enhance the Login Process

- ✓ **Login blocking** is enabling a detection profile that lets you configure a network device to react to repeated failed login attempts by refusing further connection requests.
- ✓ **Access control lists (ACLs)** can be used to **permit legitimate connections from addresses of known system administrators.**
- ✓ Use the **banner** global configuration mode command to specify appropriate messages. **Banners** protect the organization from a legal perspective.

```
Router(config)# banner { motd | exec | login } delimiter message delimiter
```

```
This equipment is privately owned and access
is logged. Disconnect immediately if you are
not an authorized user. Violators will be
prosecuted to the fullest extent of the law.
User Access Verification:

Username:
```

Configure Login Enhancement Features

- ✓ The **login block-for** command can defend against DoS attacks by disabling logins after a specified number of failed login attempts.
- ✓ The **login quiet-mode** command maps to an ACL that identifies the permitted hosts.
- ✓ The **login delay** command specifies the number of seconds the user must wait between unsuccessful login attempts.
- ✓ The **login on-success** and **login on-failure** commands log successful and unsuccessful login attempts.

```
R1(config)# login block-for seconds attempts tries within seconds
R1(config)# login quiet-mode access-class {acl-name | acl-number}
R1(config)# login delay seconds
R1(config)# login on-success log [every login]
R1(config)# login on-failure log [every login]
```

Enable Login Enhancements

✓ To help a **Cisco IOS device** provide DoS detection, use the **login block-for** command, which must be issued before any other login command. The **login block-for** command monitors login device activity and operates in two modes:

- **Normal mode:** Also called **watch mode**, the router keeps **count of the number of failed login attempts** within **an identified amount of time**.
- **Quiet mode:** Also called **the quiet period**. If the number of **failed logins exceeds the configured threshold**, all login attempts using Telnet, SSH, and HTTP are denied for **the time specified** in the **login block-for** command.

```
R1(config)# ip access-list standard PERMIT-ADMIN
R1(config-std-nacl)# remark Permit only Administrative hosts
R1(config-std-nacl)# permit 192.168.10.10
R1(config-std-nacl)# permit 192.168.11.10
R1(config-std-nacl)# exit
R1(config)# login quiet-mode access-class  PERMIT-ADMIN
```

Log Failed Attempts

- ✓ There are **three commands** that can be configured to help an administrator detect a password attack. **Each lets a device to generate syslog messages** for **failed** or **successful** **login** attempts.
- ✓ The **first two commands**, **login on-success log** and **login on-failure log**, generate syslog messages for successful and unsuccessful login attempts.
- ✓ An alternative to the **login on-failure log** command is the **security authentication failure rate** command can be configured to generate a log message when the login failure rate is exceeded.

```
R1(config)# login on-success log [every login]
R1(config)# login on-failure log [every login]
```

```
R1(config)# security authentication failure rate threshold-rate log
```

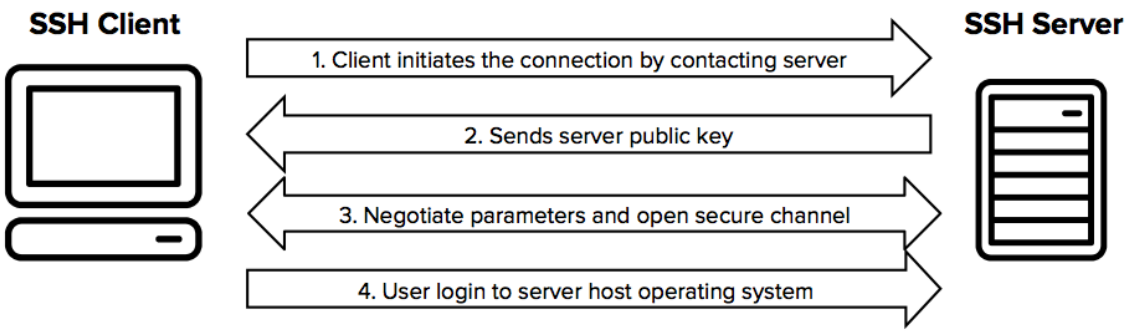
Log Failed Attempts (Cont.)

- ✓ Use the **show login** command to verify the **login block-for** command settings and current mode.

- ✓ The **show login failures** command displays additional information regarding the failed attempts, such as the IP address from which the failed login attempts originated.

```
R1# show login failures
Total failed logins: 22
Detailed information about last 50 failures

Username     SourceIPAddr     lPort Count TimeStamp
admin        1.1.2.1          23    5     15:38:54 UTC Wed Dec 10 2008
Admin        10.10.10.10      23    13    15:58:43 UTC Wed Dec 10 2008
admin        10.10.10.10      23    3     15:57:14 UTC Wed Dec 10 2008
cisco        10.10.10.10      23    1     15:57:21 UTC Wed Dec 10 2008

R1#
```

Configure SSH


SSH Client
SSH Server
1. Client initiates the connection by contacting server
2. Sends server public key
3. Negotiate parameters and open secure channel
4. User login to server host operating system

Enable SSH

Configure **a Cisco device** to support **SSH** using the following **six steps**:

Step 1. Configure a unique device hostname.
Step 2. Configure the IP domain name.
Step 3. Generate a key to encrypt SSH traffic.
Step 4. Verify or create a local database entry.
Step 5. Authenticate against the local database.
Step 6. Enable vty inbound SSH sessions.

```
Router(config)# hostname R1
R1(config)# ip domain name span.com
R1(config)# crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.span.com % The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
Dec 13 16:19:12.079: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#
R1(config)# username Bob secret cisco
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# exit
```

Enable SSH

```
Router(config)# hostname R1
R1(config)# ip domain name span.com
R1(config)# crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.span.com % The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
Dec 13 16:19:12.079: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#
R1(config)# username Bob secret cisco
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# exit
```

Enhance SSH Login Security

- ✓ To verify the optional **SSH command settings**, use the **show ip ssh** command.
- ✓ Use the **ip ssh time-out** *seconds* global configuration mode command to modify the default 120-second timeout interval.
- ✓ This configures **the number of seconds** that SSH can use to authenticate a user. By default, a user logging in has **three attempts** to enter the correct password before being **disconnected**.
- ✓ To configure a different number of consecutive SSH retries, use the **ip ssh authentication-retries** *integer* global configuration mode command.

```
R1# show ip ssh
SSH Enabled - version 2.0
Authentication methods:publickey,keyboard-interactive,password
Authentication timeout: 120 secs; Authentication retries: 3
(output omitted)

R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# ip ssh time-out 60
R1(config)# ip ssh authentication-retries 2
R1(config)# ^Z
R1#
*Feb 16 21:23:51.237: %SYS-5-CONFIG_I: Configured from console by console
R1# show ip ssh
SSH Enabled - version 2.0
Authentication methods:publickey,keyboard-interactive,password
Authentication timeout: 60 secs; Authentication retries: 2
(output omitted)
```

Enhance SSH Login Security

```
R1# show ip ssh
SSH Enabled - version 2.0
Authentication methods:publickey,keyboard-interactive,password
Authentication timeout: 120 secs; Authentication retries: 3
(output omitted)

R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# ip ssh time-out 60
R1(config)# ip ssh authentication-retries 2
R1(config)# ^Z
R1#
*Feb 16 21:23:51.267: %SYS-5-CONFIG_I: Configured from console by console
R1# show ip ssh
SSH Enabled - version 2.0
Authentication methods:publickey,keyboard-interactive,password
Authentication timeout: 60 secs; Authentication retries: 2
(output omitted)
```

Connect a Router to an SSH-Enabled Router

✓ **To verify the status of the client connections**, use the **show ssh** command. There are two different ways to connect to an SSH-enabled router. By default, when SSH is enabled, a Cisco router can act as **an SSH server** or **SSH client**. **As a server**, a router can accept SSH client connections. **As a client**, a router can connect via SSH to another SSH-enabled router.

Check SSH Status

```
R1# show ssh
%No SSHv2 server connections running.
%No SSHv1 server connections running.
R1#
```

Connect from R2 To R1

```
R2# ssh -l Bob 192.168.2.101

Password:

R1>
```

View SSH Connections

```
R1# show ssh
Connection Version Mode Encryption  Hmac       State             Username
0          2.0     IN   aes128-cbc  hmac-sha1  Session started   Bob
0          2.0     OUT  aes128-cbc  hmac-sha1  Session started   Bob
%No SSHv1 server connections running.
R1#
```

Connect a Router to an SSH-Enabled Router

Check SSH Status

```
R1# show ssh
%No SSHv2 server connections running.
%No SSHv1 server connections running.
R1#
```

Connect from R2 To R1

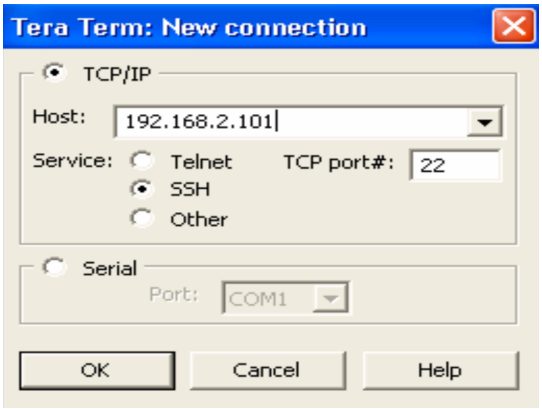
```
R2# ssh -l Bob 192.168.2.101

Password:

R1>
```

View SSH Connections

```
R1# show ssh
Connection Version Mode Encryption  Hmac        State               Username
0          2.0     IN   aes128-cbc  hmac-sha1   Session started     Bob
0          2.0     OUT  aes128-cbc  hmac-sha1   Session started     Bob
%No SSHv1 server connections running.
R1#
```

Connect a Host to an SSH-Enabled Router (Cont.)

- ✓ Connect using **an SSH client** (e.g., PuTTY, OpenSSH, TeraTerm) running on a host.
- ✓ Generally, **the SSH client** initiates an SSH connection to the router.
- ✓ The router SSH service prompts for the correct **username** and **password** combination.
- ✓ After the login is verified, the router can be managed as if the administrator was using a standard Telnet session.

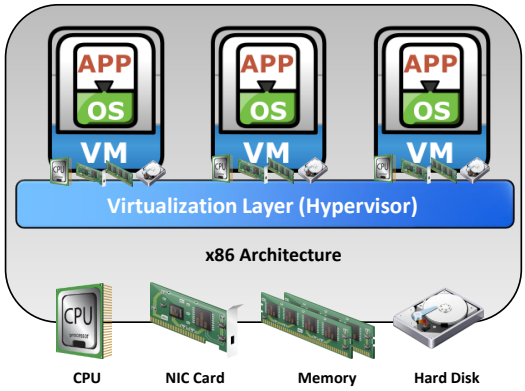


Virtualization

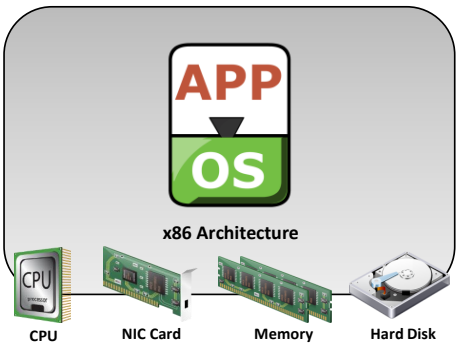
- **Today, virtualization technology change the way of digital content storing, managing and delivering for organizations. Benefits of virtualization such as reduce cost, high efficiency and best utilization of hardware resources.**

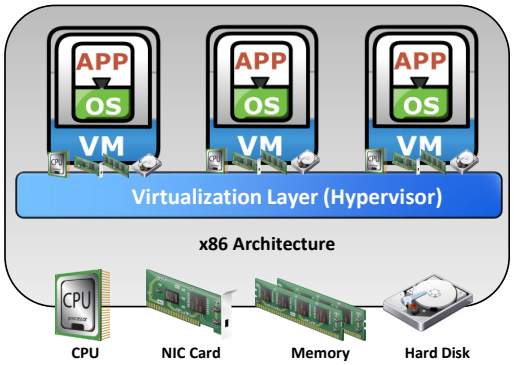
Virtualization

It is a technique of abstracting the physical compute hardware and enabling multiple operating systems (OSs) to run concurrently on a single or clustered physical machine(s).



Before and After Virtualization





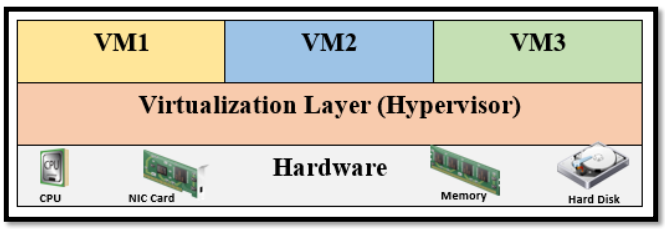
Before Virtualization	After Virtualization
• Runs single operating system (OS) per machine at a time • Couples s/w and h/w tightly • May create conflicts when multiple applications run on the same machine • Underutilizes resources • Is inflexible and expensive	• Runs multiple operating systems (OSs) per physical machine concurrently • Makes OS and applications h/w independent • Isolates VM from each other, hence, no conflict • Improves resource utilization • Offers flexible infrastructure at low cost

Types of Hypervisor

✓ **There are two types of hypervisors as follows:**

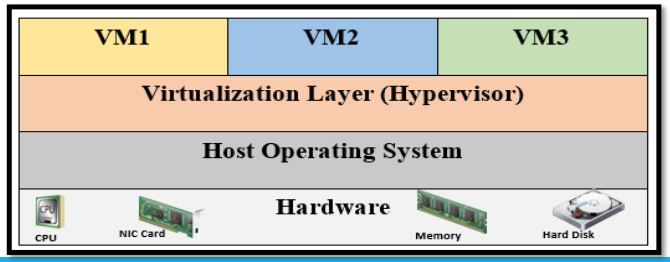
1. **Type 1: Bare-metal Hypervisor**

➢ The Bare-metal Hypervisor straight operates on a physical hardware system, such as VMware ESXi

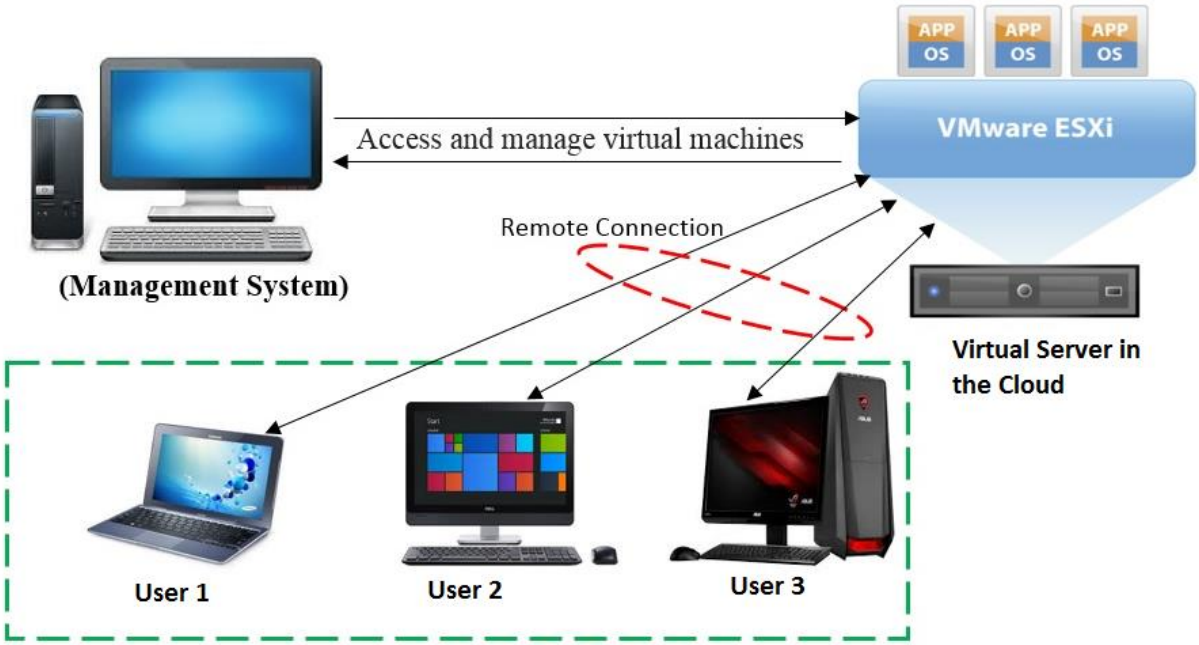


2. **Type 2: Hosted-based Hypervisor**

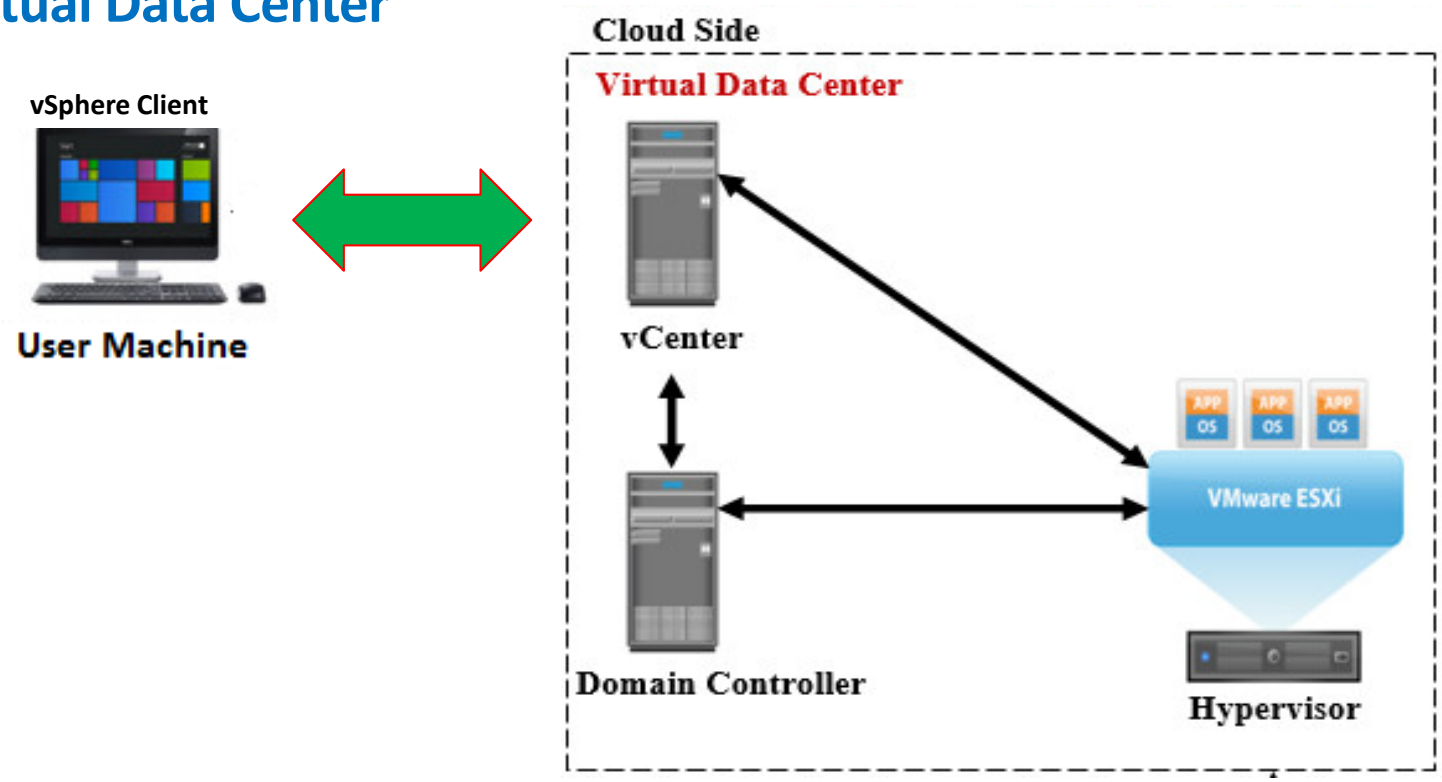
➢ The Hosted based hypervisor runs on top of an already installed standard operating systems such as Linux, Mac, and Windows, such as Virtual box or VMware Workstation



Virtual Server Using VMware ESXi



Virtual Data Center



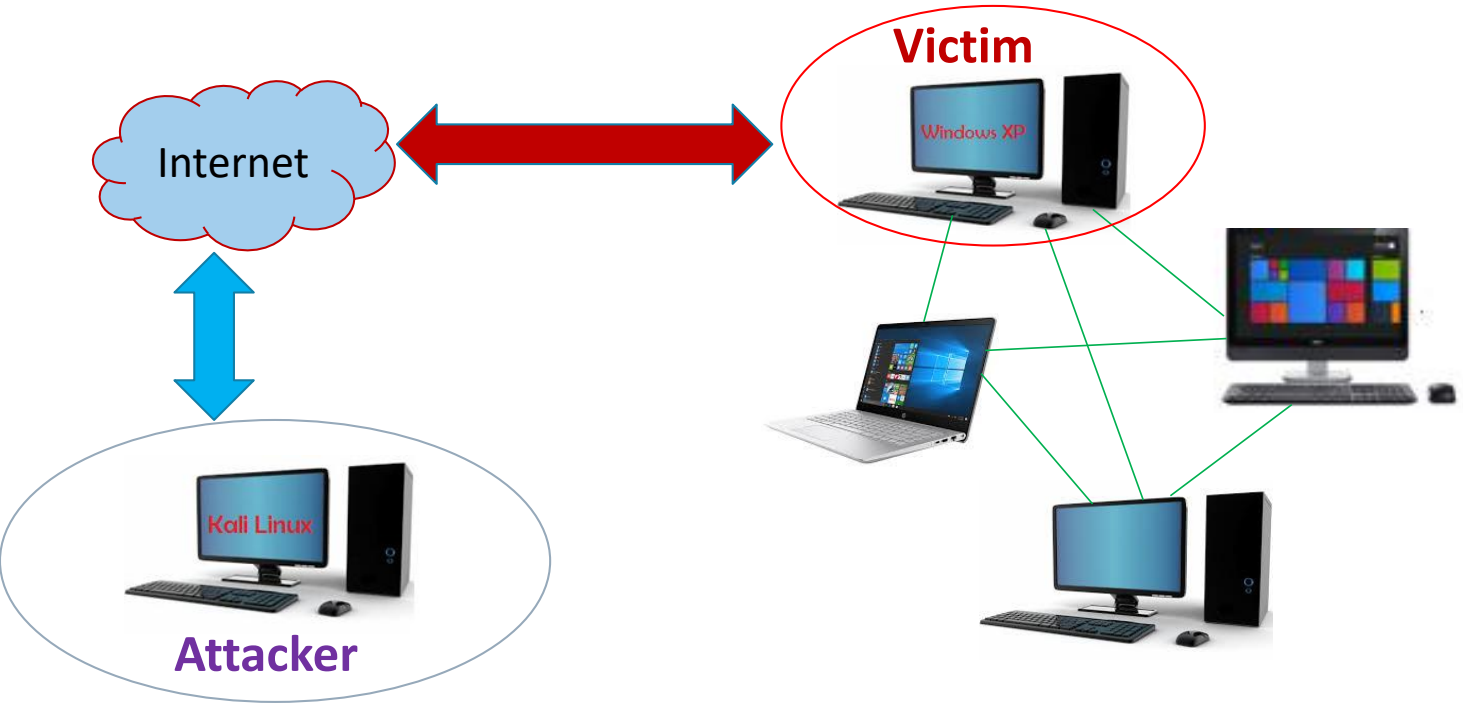
Cloud Networks and Virtualization

The terms “cloud computing” and “virtualization” are often used interchangeably; however, they mean different things. Virtualization is the foundation of cloud computing. Without it, cloud computing, as it is most-widely implemented, would not be possible. Cloud computing separates the application from the hardware. Virtualization separates the operating system from the hardware. The cloud network consists of physical and virtual servers usually found in data centers. Data centers are increasingly using virtual machines (VM) to provide server services to their clients. This allows for multiple operating systems to exist on a single hardware platform. VMs are prone to specific targeted attacks:

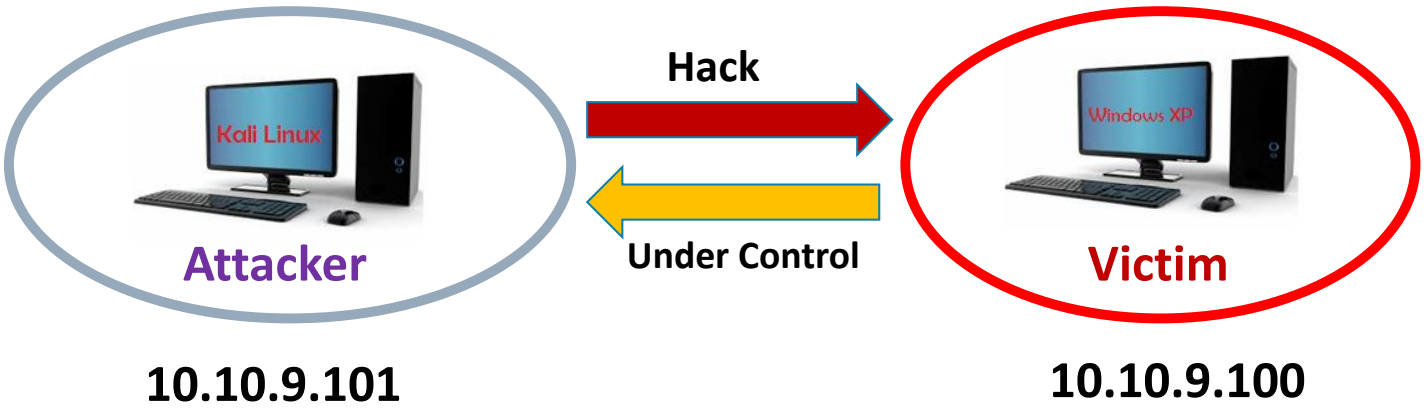
- **Hyperjacking** -An attacker could hijack a VM hypervisor (VM controlling software) and then use it as a launch point to attack other devices on the data center network.
- **Instant On Activation** - When a VM that has not been used for a period of time is brought online, it may have outdated security policies that deviate from the baseline security and can introduce security vulnerabilities.
- **Antivirus Storms** - This happens when all VMs attempt to download antivirus data files at the same time.

Practical Hacking Scenario

Practical Hacking Scenario



Practical Hacking Scenario (cont.)



10.10.9.101

10.10.9.100

Hands On:
Practical Hacking Scenario Demo

Conclusion

In This presentation we covered

- ✓ Secure the Network Infrastructure
- ✓ Router Security
- ✓ Secure Administrative Access
- ✓ Configure Secure Administrative Access
- ✓ Configure Enhanced Security for Virtual Logins
- ✓ Configure SSH


Thank
you


Q&A
You Have Questions We Have Answers