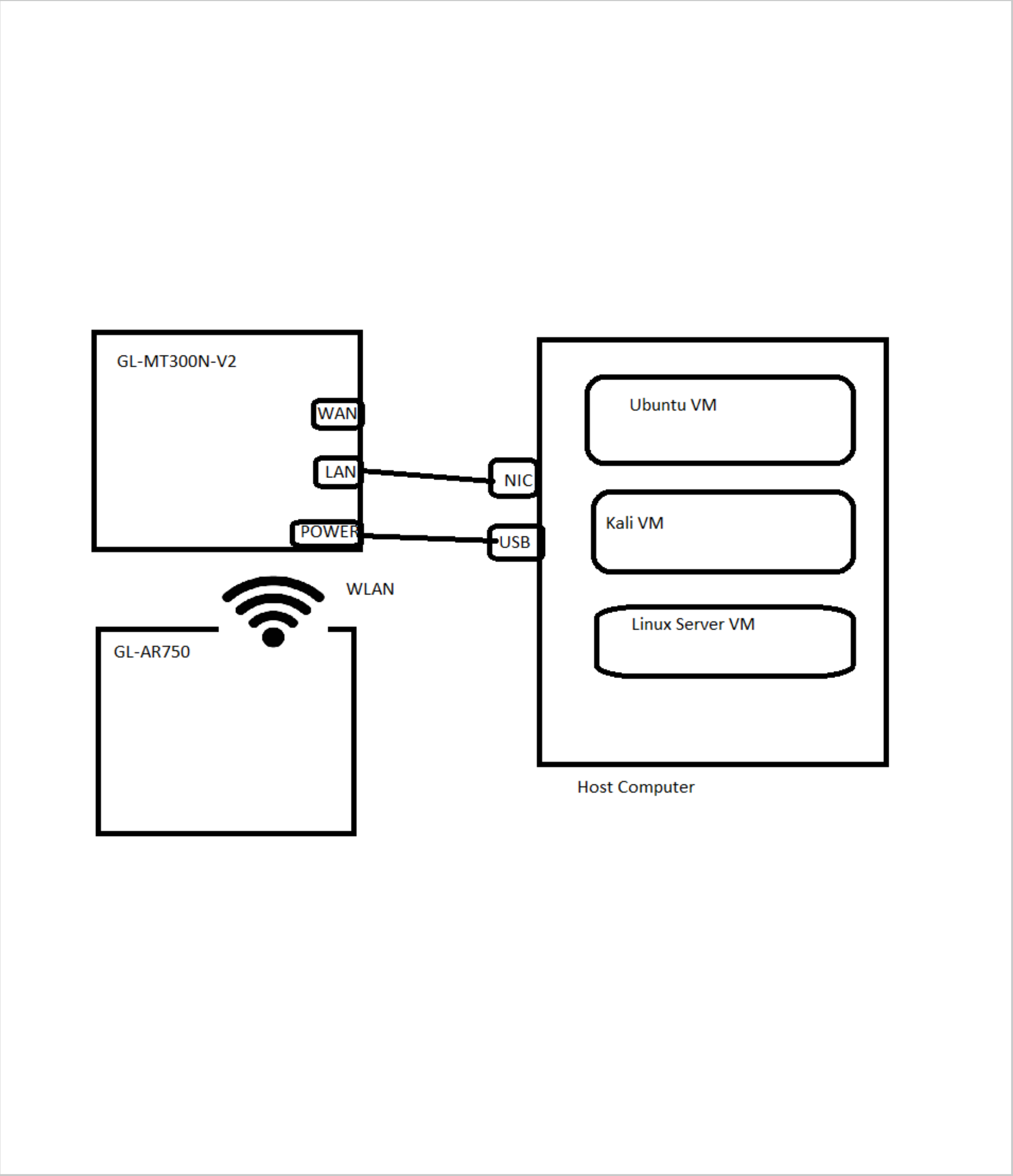
NETW200 Fundamentals of Information Technology and Networking II Course Project

The IoT is growing exponentially!

This project covers 6 areas:

- Importing Virtual Appliances into VMware
- Network Segmentation using Subnetting and V-LAN's
- Network Vulnerability Assessment
- Authentication Management
- Network Traffic Monitoring
- IP Routing & Network Expansion



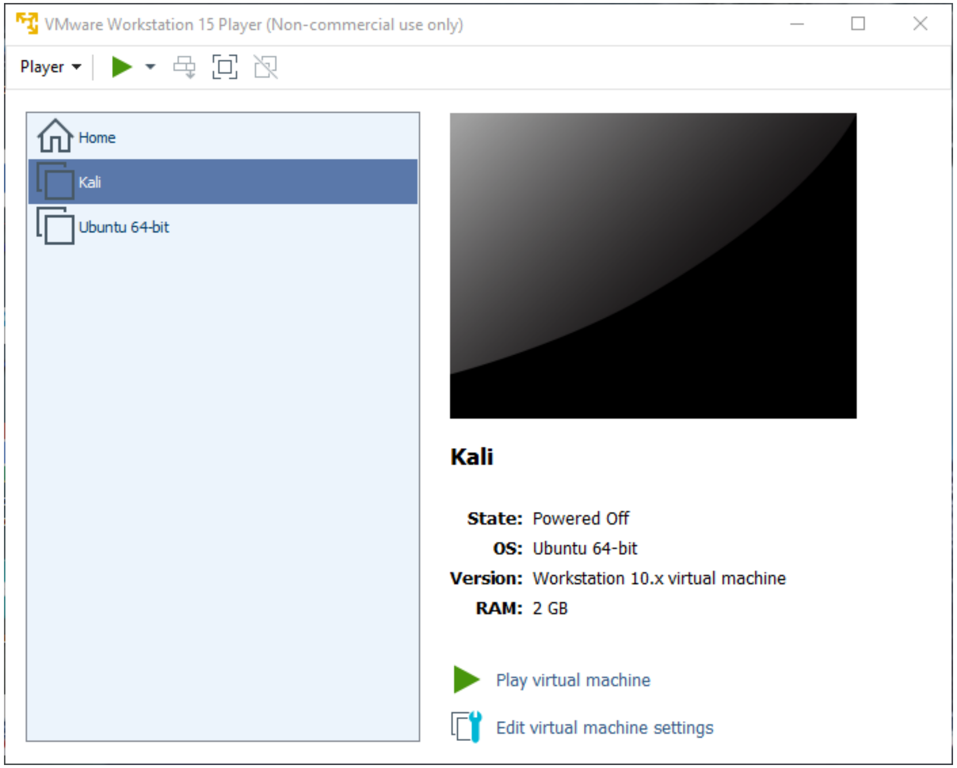
Initial diagram

A small network that supports both IPv4 and IPv6. The network is made up of two travel routers, one Host Machine, and three Guest VMs. The Host Machine and Guest VMs will dynamically obtain their IP addresses from the travel routers.

VMware player environment with both VMs

VMware Player environment with Ubuntu and Kali VMs.

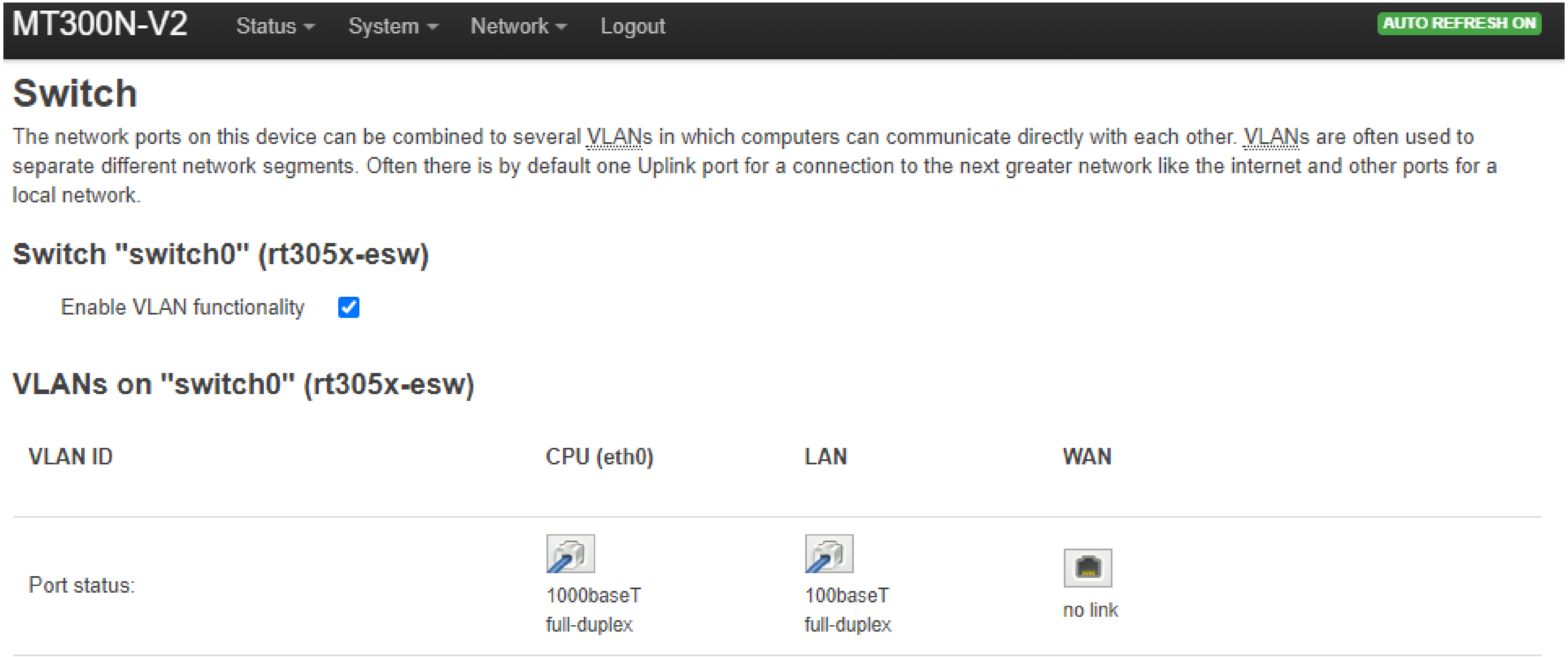
- The Ubuntu OS was installed from an ISO image.
- The Kali Linux OS was imported as an OVF file.



VMware Workstation 15 Player (Non-commercial use only)
Player
Home
Kali
Ubuntu 64-bit
Play virtual machine
Edit virtual machine settings

Kali

State: Powered Off
OS: Ubuntu 64-bit
Version: Workstation 10.x virtual machine
RAM: 2 GB



Switch

The network ports on this device can be combined to several VLANs in which computers can communicate directly with each other. VLANs are often used to separate different network segments. Often there is by default one Uplink port for a connection to the next greater network like the internet and other ports for a local network.

Switch "switch0" (rt305x-esw)

Enable VLAN functionality ☑

VLANs on "switch0" (rt305x-esw)

VLAN ID	CPU (eth0)	LAN	WAN
Port status:	1000baseT full-duplex	100baseT full-duplex	no link

Travel Router VLAN Configuration

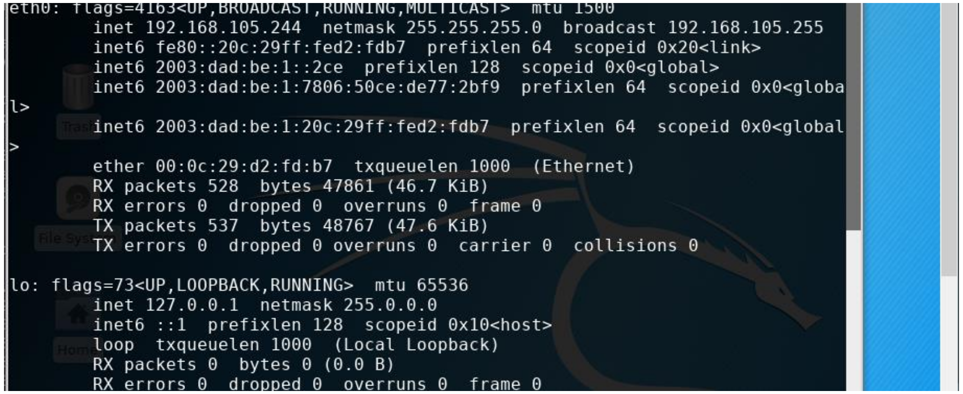
Can 2 OS's communicate with each other?

How do you the two VMs can communicate with each other?

- After ensuring bridging was enabled on both VMs, I performed 2 successful pings using the IPv4 addresses of Kali and Ubuntu

- The purpose of bridging the Kali Linux Network Adapter.
- After enabling bridging allowed the VM to operate as any other node on my home network.

Kali VM IPv4 address

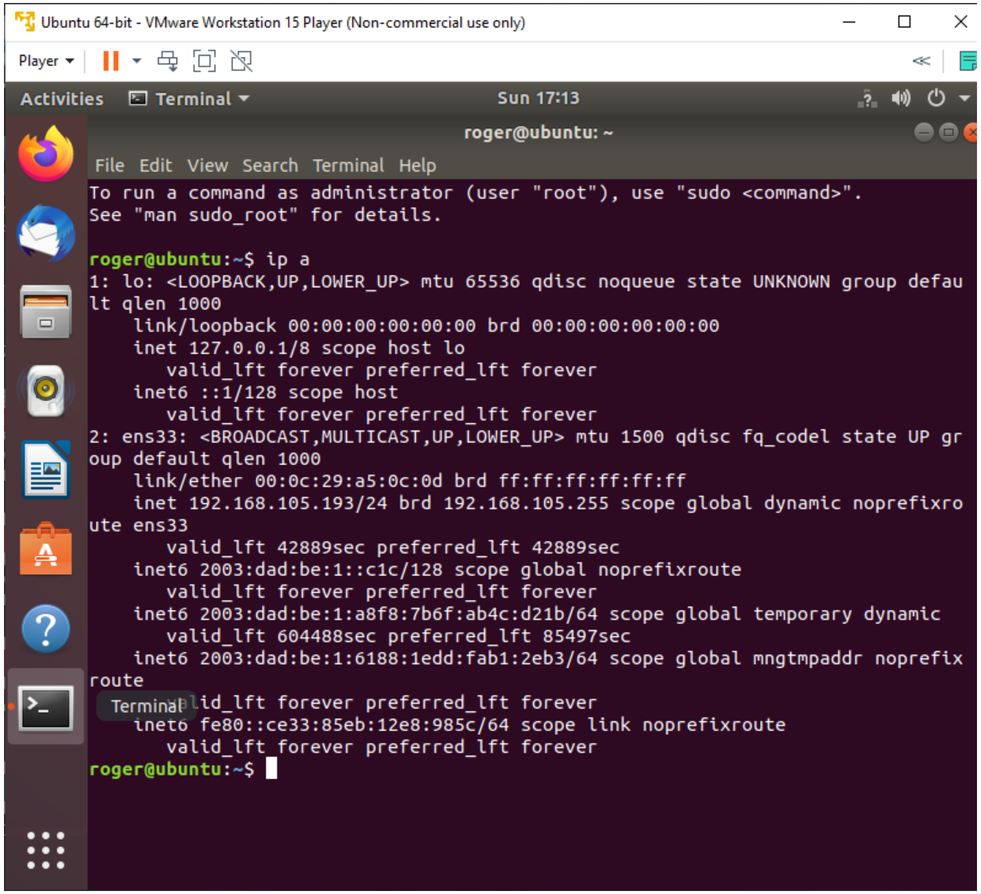


```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.105.244  netmask 255.255.255.0  broadcast 192.168.105.255
        inet6 fe80::20c:29ff:fed2:fdb7  prefixlen 64  scopeid 0x20<link>
        inet6 2003:dad:be:1::2ce  prefixlen 128  scopeid 0x0<global>
        inet6 2003:dad:be:1:7806:50ce:de77:2bf9  prefixlen 64  scopeid 0x0<globa
l>
        inet6 2003:dad:be:1:20c:29ff:fed2:fdb7  prefixlen 64  scopeid 0x0<global
>
        ether 00:0c:29:d2:fd:b7  txqueuelen 1000  (Ethernet)
        RX packets 528  bytes 47861 (46.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 537  bytes 48767 (47.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
```

- The Kali Terminal window with correct IPv4 address from Travel Router, 192.168.105.244

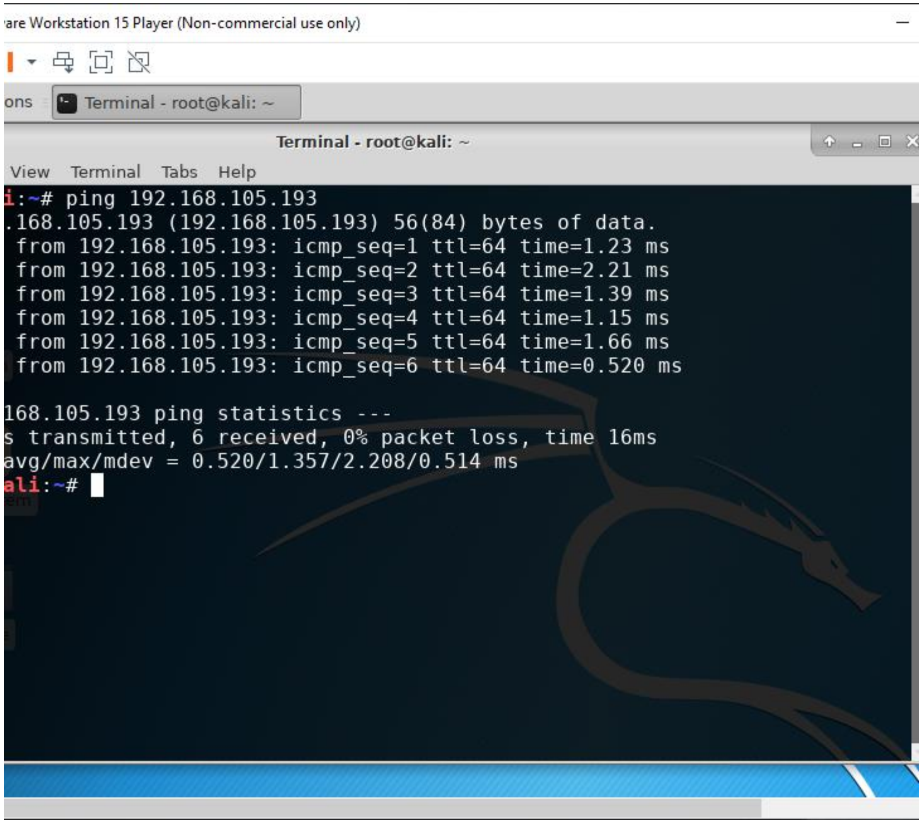
Ubuntu VM IPv4 address

- The Ubuntu Terminal window with correct IPv4 address from Travel Router, 192.168.105.193

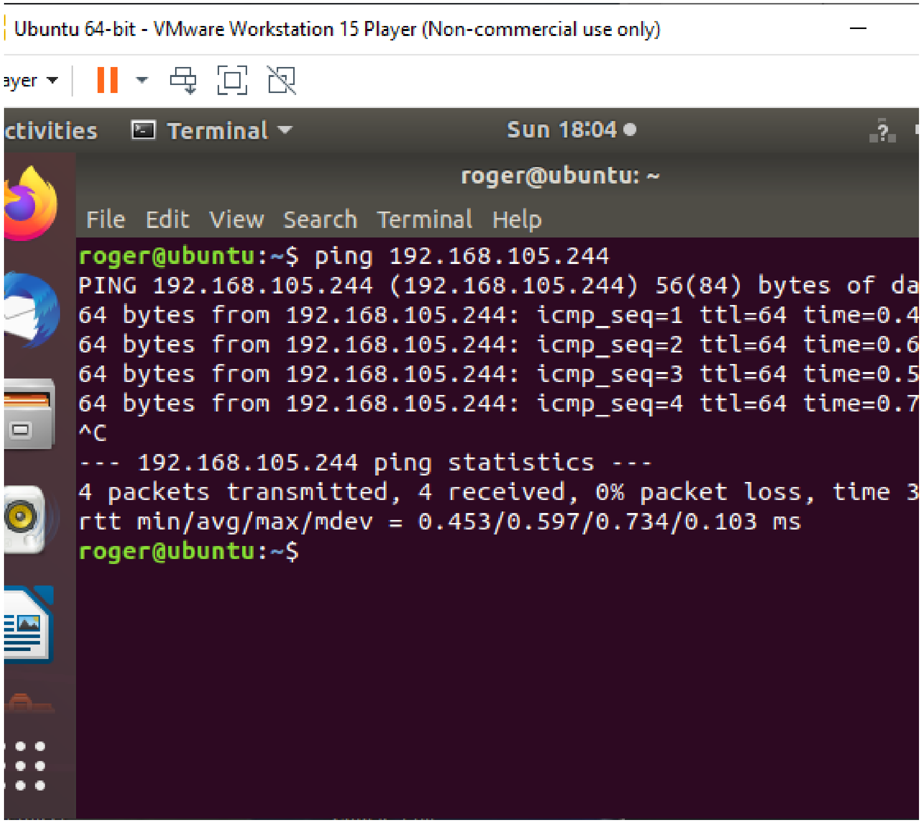


```
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

roger@ubuntu:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defau
lt qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether 00:0c:29:a5:0c:0d brd ff:ff:ff:ff:ff:ff
    inet 192.168.105.193/24 brd 192.168.105.255 scope global dynamic noprefixro
ute ens33
       valid_lft 42889sec preferred_lft 42889sec
    inet6 2003:dad:be:1::c1c/128 scope global noprefixroute
       valid_lft forever preferred_lft forever
    inet6 2003:dad:be:1:a8f8:7b6f:ab4c:d21b/64 scope global temporary dynamic
       valid_lft 604488sec preferred_lft 85497sec
    inet6 2003:dad:be:1:6188:1edd:fab1:2eb3/64 scope global mngtmpaddr noprefix
route
       valid_lft forever preferred_lft forever
    inet6 fe80::ce33:85eb:12e8:985c/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
roger@ubuntu:~$
```

Ping connectivity test between two VMs – Ubuntu & Kali



```
i:~# ping 192.168.105.193
.168.105.193 (192.168.105.193) 56(84) bytes of data.
 from 192.168.105.193: icmp_seq=1 ttl=64 time=1.23 ms
 from 192.168.105.193: icmp_seq=2 ttl=64 time=2.21 ms
 from 192.168.105.193: icmp_seq=3 ttl=64 time=1.39 ms
 from 192.168.105.193: icmp_seq=4 ttl=64 time=1.15 ms
 from 192.168.105.193: icmp_seq=5 ttl=64 time=1.66 ms
 from 192.168.105.193: icmp_seq=6 ttl=64 time=0.520 ms

168.105.193 ping statistics ---
s transmitted, 6 received, 0% packet loss, time 16ms
avg/max/mdev = 0.520/1.357/2.208/0.514 ms
ali:~# 
```



```
roger@ubuntu:~$ ping 192.168.105.244
PING 192.168.105.244 (192.168.105.244) 56(84) bytes of da
64 bytes from 192.168.105.244: icmp_seq=1 ttl=64 time=0.4
64 bytes from 192.168.105.244: icmp_seq=2 ttl=64 time=0.6
64 bytes from 192.168.105.244: icmp_seq=3 ttl=64 time=0.5
64 bytes from 192.168.105.244: icmp_seq=4 ttl=64 time=0.7
^C
--- 192.168.105.244 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3
rtt min/avg/max/mdev = 0.453/0.597/0.734/0.103 ms
roger@ubuntu:~$
```

Network Segmentation Benefits

When a network is segmented into smaller networks, traffic on one network is separated from other network traffic.

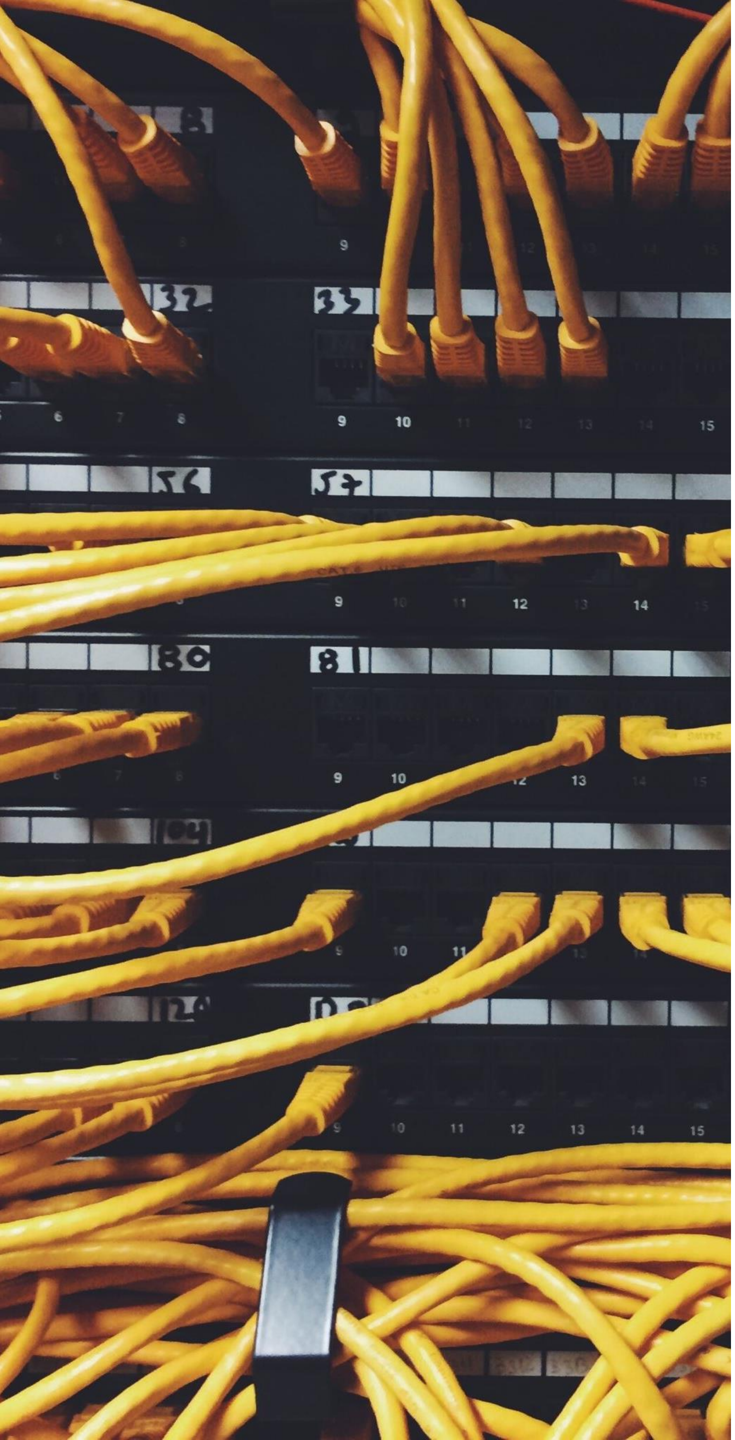
- Enhanced Security
- Improve Performance
- Simplify Troubleshooting

Determining how to segment a network

Along geographic boundaries

Along departmental boundaries

Based on device types



Subnetting

- To be able to communicate with a modern network, a device is required to have a unique identifier known as an Internet Protocol (IP) address. As organizations expand, it is the role of the network engineer to segment the original IP address into smaller Ips to ensure new devices, LAN, and WAN segments will be addressed.
- Subnetting always leads to more networks. However, each network or subnet loses two IP addresses; the network-ID, the first IP address on the subnet, and the broadcast-ID, the last IP address on the subnet. The range of addresses between these two are the usable addresses that can be assigned to devices.

Subnetting example

	Network Address 192.168.2.0/26	First Usable Host Address	Last Useable Host Address	Broadcast Address
First subnet	192.168.2.0	192.168.2.1	192.168.2.62	192.168.2.63
Second subnet	192.168.2.64	192.168.2.65	192.168.2.126	192.168.2.127
Third subnet	192.168.2.128	192.168.2.129	192.168.2.190	192.168.2.191
Fourth subnet	192.168.2.192	192.168.2.192	192.168.2.254	192.168.2.255

Vulnerability Assessment

- Assessing the security posture of the Linux-Server VM (also called Metasploitable) and examining the list of exploits available for the identified vulnerabilities.
- Using the two of the most popular security tools in the industry; Network Mapper (Nmap) and Open Vulnerability Assessment System (OpenVAS). These are used to conduct a vulnerability assessment of a server in a testing or production environment.

Types of Hackers:

- **White hat hackers** are IT security experts hired by companies to identify security vulnerabilities. Also called ethical hackers.
- **Black hat hackers** are groups or individuals that often time are malicious, cause damage, theft data, or privacy.
- **Gray hat hackers** go by of their own code of ethics. Sometimes by means of illegal activity, but their intent is to educate and help.

Attempt methods used by Hackers:

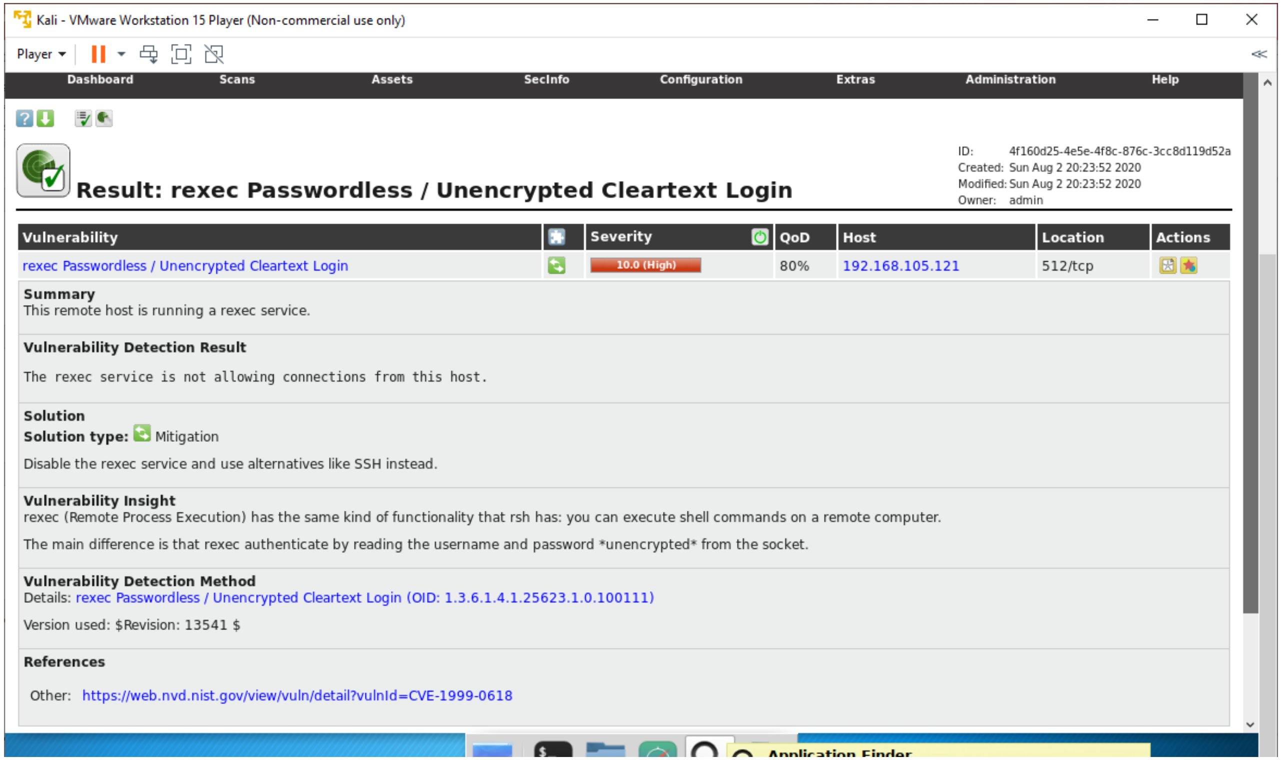
1. **Vulnerability scanning, or vulnerability assessment**, is used to identify vulnerabilities in a network. Two types of vulnerability scans are:
   - Authenticated scanning: Attackers are given the same access as a trusted user would.
   - Unauthenticated scanning: Attackers start on the perimeter of the network, looking for vulnerabilities that do not require trusted privileges.
2. **Penetration testing** uses security tools to find network vulnerabilities and attempts to exploit them.
3. **Red team-blue team exercise** has the red team conduct the attack, and the blue team attempts to defend the network.

Scanning tools used for network vulnerability

NMAP (network mapper) is designed to scan large networks and provide information about a network and its hosts.

Nessus performs more sophisticated scans than NMAP. It can provide information about the types of vulnerabilities available and if security patches exist to protect against the identified vulnerabilities. It can even identity unencrypted sensitive data saved on the hosts.

Metasploit combines known scanning and exploit techniques to explore potentially new attack routes.



ID: 4f160d25-4e5e-4f8c-876c-3cc8d119d52a
Created: Sun Aug 2 20:23:52 2020
Modified: Sun Aug 2 20:23:52 2020
Owner: admin

Result: rexec Passwordless / Unencrypted Cleartext Login

Vulnerability		Severity	QoD	Host	Location	Actions
rexec Passwordless / Unencrypted Cleartext Login		10.0 (High)	80%	192.168.105.121	512/tcp	

Summary
This remote host is running a rexec service.

Vulnerability Detection Result

```
The rexec service is not allowing connections from this host.
```

Solution
Solution type: Mitigation

Disable the rexec service and use alternatives like SSH instead.

Vulnerability Insight
rexec (Remote Process Execution) has the same kind of functionality that rsh has: you can execute shell commands on a remote computer.

The main difference is that rexec authenticate by reading the username and password *unencrypted* from the socket.

Vulnerability Detection Method
Details: rexec Passwordless / Unencrypted Cleartext Login (OID: 1.3.6.1.4.1.25623.1.0.100111)

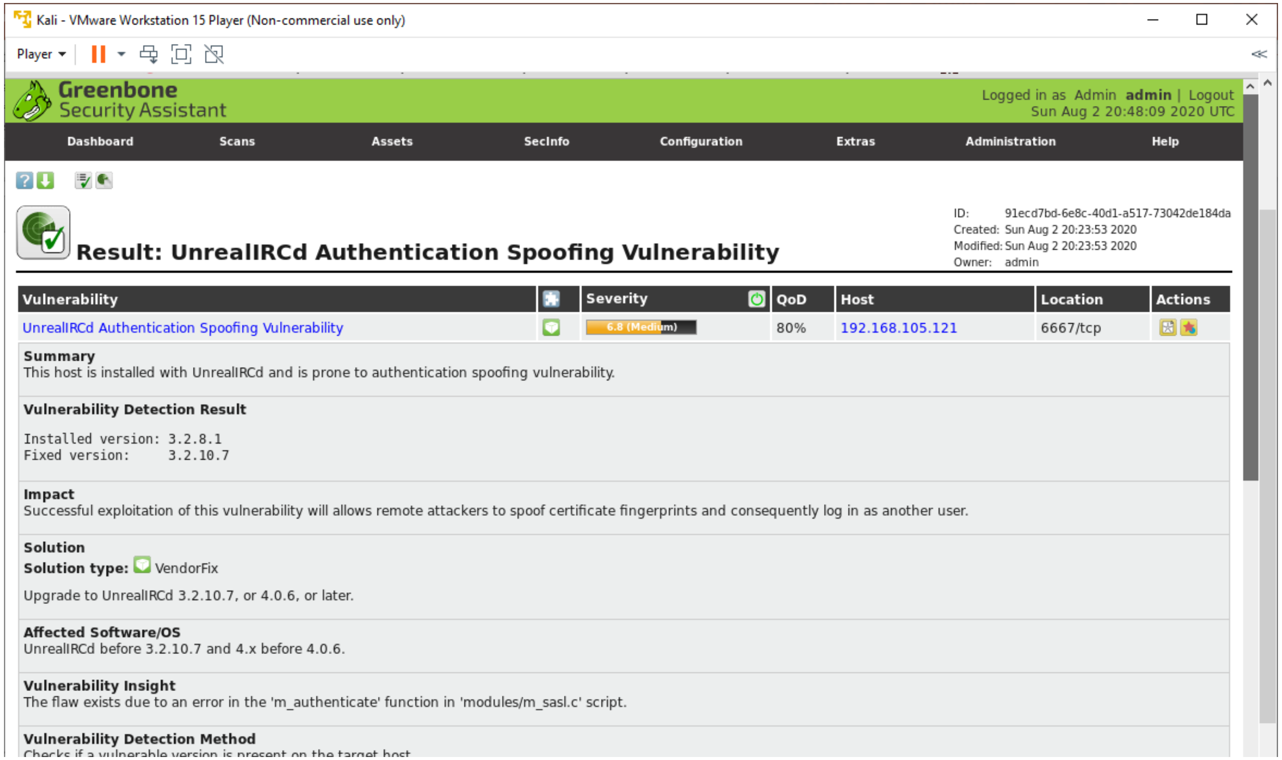
Version used: $Revision: 13541 $

References

Other: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0618

Solution: Disable rexec service and use alternate like SSH instead

High Severity Rating Vulnerability



Kali - VMware Workstation 15 Player (Non-commercial use only)
Player
Greenbone
Security Assistant
Logged in as Admin admin | Logout
Sun Aug 2 20:48:09 2020 UTC
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help

Result: UnrealIRCd Authentication Spoofing Vulnerability

ID: 91ecd7bd-6e8c-40d1-a517-73042de184da
Created: Sun Aug 2 20:23:53 2020
Modified: Sun Aug 2 20:23:53 2020
Owner: admin

Vulnerability		Severity	QoD	Host	Location	Actions
UnrealIRCd Authentication Spoofing Vulnerability		6.8 (Medium)	80%	192.168.105.121	6667/tcp	

Summary
This host is installed with UnrealIRCd and is prone to authentication spoofing vulnerability.

Vulnerability Detection Result

```
Installed version: 3.2.8.1
Fixed version:     3.2.10.7
```

Impact
Successful exploitation of this vulnerability will allows remote attackers to spoof certificate fingerprints and consequently log in as another user.

Solution
Solution type: VendorFix

Upgrade to UnrealIRCd 3.2.10.7, or 4.0.6, or later.

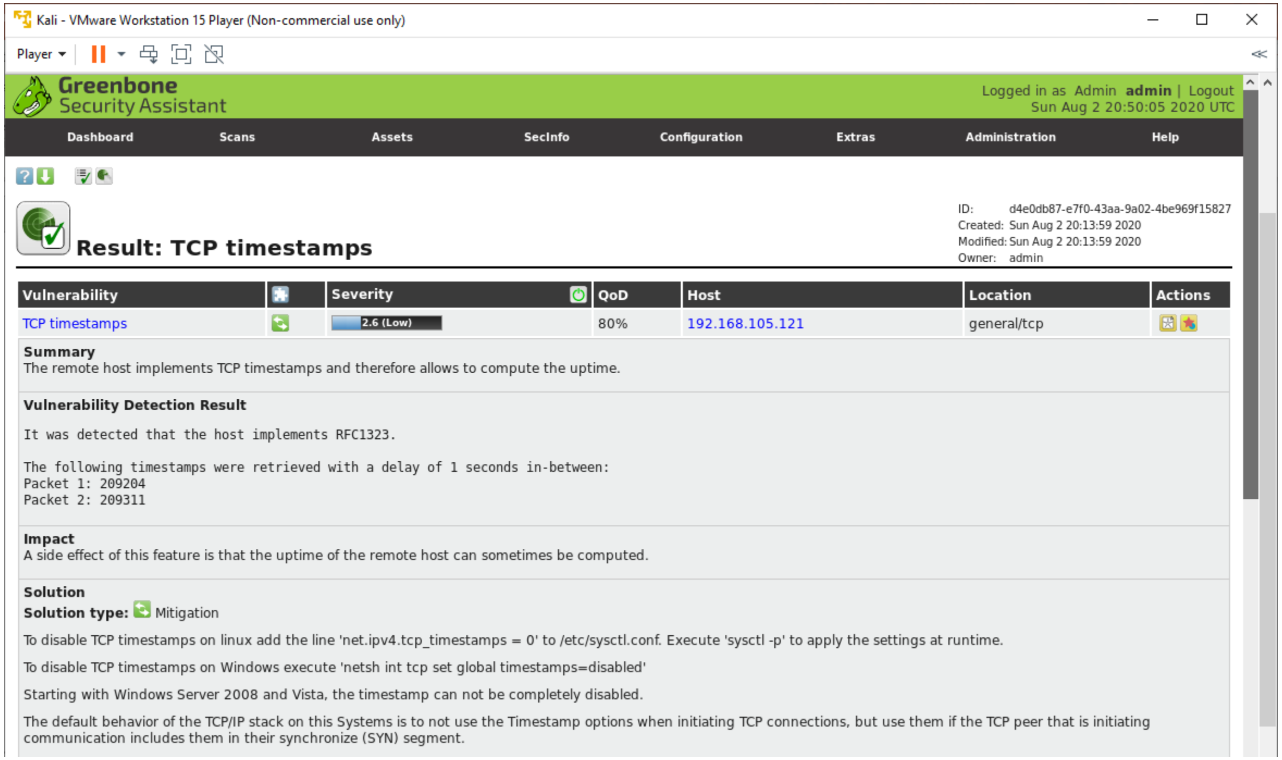
Affected Software/OS
UnrealIRCd before 3.2.10.7 and 4.x before 4.0.6.

Vulnerability Insight
The flaw exists due to an error in the 'm_authenticate' function in 'modules/m_sasl.c' script.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host

Solution: Upgrade to UnrealRCd 3.2.10.7. or 4.0.6 or later.

Medium Severity Rating Vulnerability



Kali - VMware Workstation 15 Player (Non-commercial use only)
Player
Greenbone Security Assistant
Logged in as Admin admin | Logout
Sun Aug 2 20:50:05 2020 UTC
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help

Result: TCP timestamps

ID: d4e0db87-e7f0-43aa-9a02-4be969f15827
Created: Sun Aug 2 20:13:59 2020
Modified: Sun Aug 2 20:13:59 2020
Owner: admin

Vulnerability		Severity	QoD	Host	Location	Actions
TCP timestamps		2.6 (Low)	80%	192.168.105.121	general/tcp	

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result

```
It was detected that the host implements RFC1323.

The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 209204
Packet 2: 209311
```

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution
Solution type: Mitigation

To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.

To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'

Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.

The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.

Solution: Staring with Windows Server 2008 and Vista, the timestamp can not be completely disabled.

Low Severity Rating Vulnerability

Vulnerability assessment

- Hosts found in the Nmap scan result:
- Router 192.168.105.1, Linux Server VM 192.168.105.121, HP laptop 192.168.105.153, Kali VM 192.168.105.244

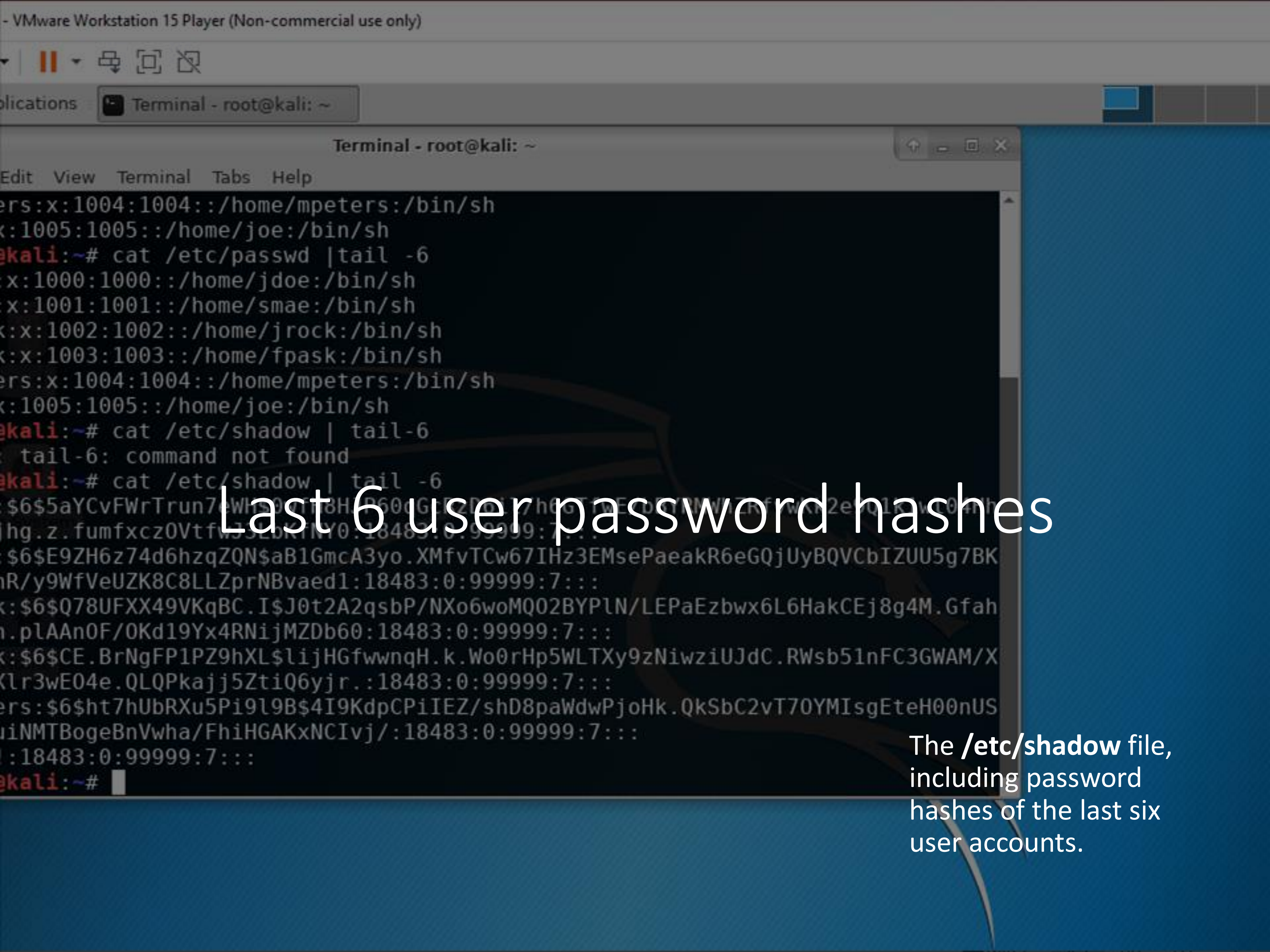
- Ranking of vulnerabilities is important to bring the most crucial weaknesses to your attention.

Password Management

To access resources, a user or device is required to have a unique credential set. The most common credential set is username and password. Network administrators audit their servers' password databases to uncover weak passwords before an attacker discovers.

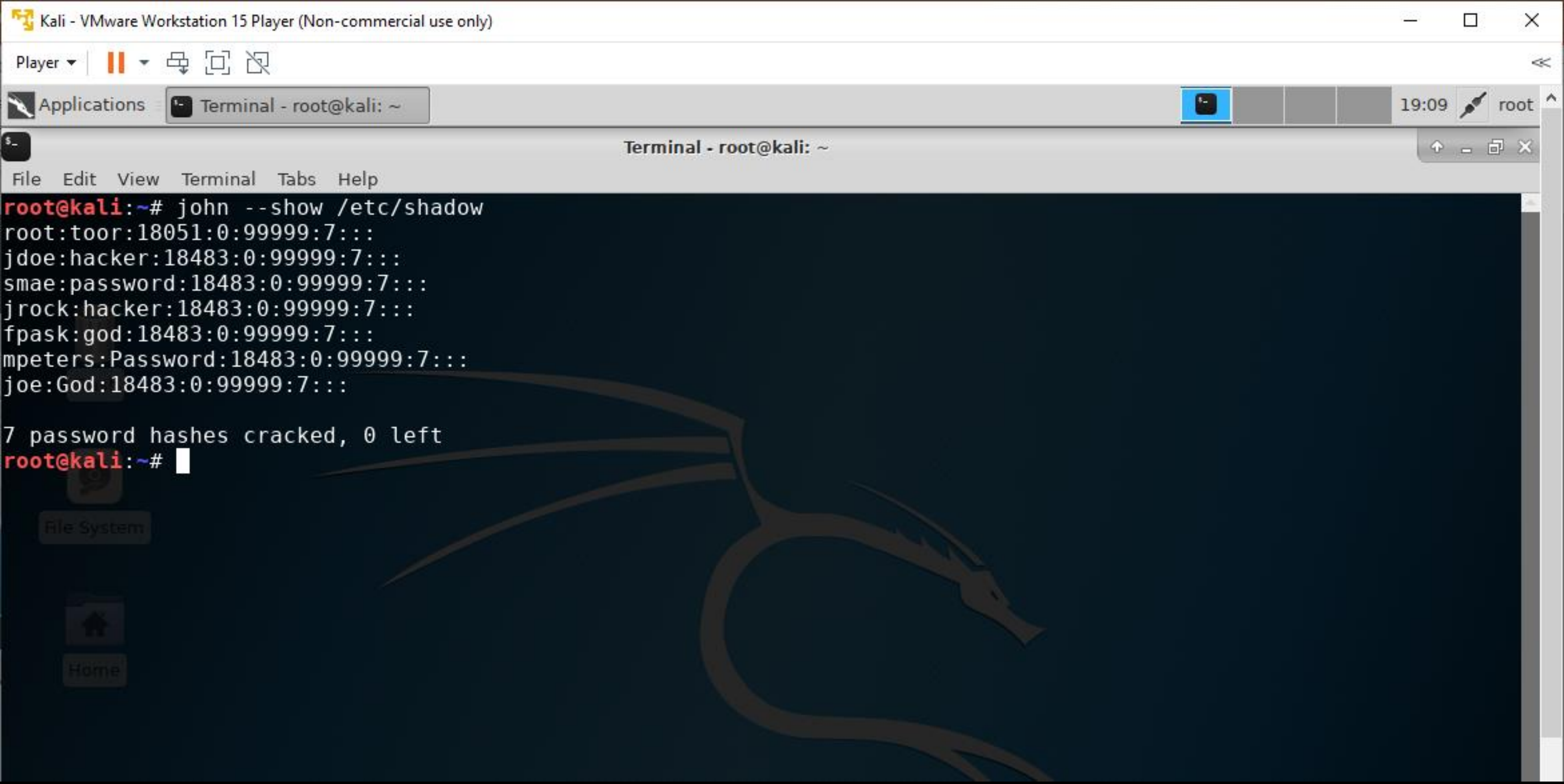
Strong passwords protect against password attacks including dictionary, rainbow table, and brute-force attacks.

Last 6 user password hashes



```
ers:x:1004:1004::/home/mpeters:/bin/sh
x:1005:1005::/home/joe:/bin/sh
@kali:~# cat /etc/passwd |tail -6
:x:1000:1000::/home/jdoe:/bin/sh
:x:1001:1001::/home/smae:/bin/sh
k:x:1002:1002::/home/jrock:/bin/sh
k:x:1003:1003::/home/fpask:/bin/sh
ers:x:1004:1004::/home/mpeters:/bin/sh
x:1005:1005::/home/joe:/bin/sh
@kali:~# cat /etc/shadow | tail-6
: tail-6: command not found
@kali:~# cat /etc/shadow | tail -6
:$6$5aYCvFWrTrun7eWh[illegible]
jhg.z.fumfxczOVtf[illegible]Y0:18483:0:99999:7:::
:$6$E9ZH6z74d6hzqZQN$aB1GmcA3yo.XMfvTCw67IHz3EMsePaeakR6eGQjUyBQVCbIZUU5g7BK
nR/y9WfVeUZK8C8LLZprNBvaed1:18483:0:99999:7:::
k:$6$Q78UFXX49VKqBC.I$J0t2A2qsbP/NXo6woMQO2BYPlN/LEPaEzbwx6L6HakCEj8g4M.Gfah
n.plAAnOF/OKd19Yx4RNijMZDb60:18483:0:99999:7:::
k:$6$CE.BrNgFP1PZ9hXL$lijHGfwwnqH.k.Wo0rHp5WLTXy9zNiwziUJdC.RWsb51nFC3GWAM/X
Xlr3wEO4e.QLQPkajj5ZtiQ6yjr.:18483:0:99999:7:::
ers:$6$ht7hUbRXu5Pi9l9B$4I9KdpCPiIEZ/shD8paWdwPjoHk.QkSbC2vT7OYMIsgEteH00nUS
uiNMTBogeBnVwha/FhiHGAKxNCIvj/:18483:0:99999:7:::
!:18483:0:99999:7:::
@kali:~# 
```

The **/etc/shadow** file, including password hashes of the last six user accounts.

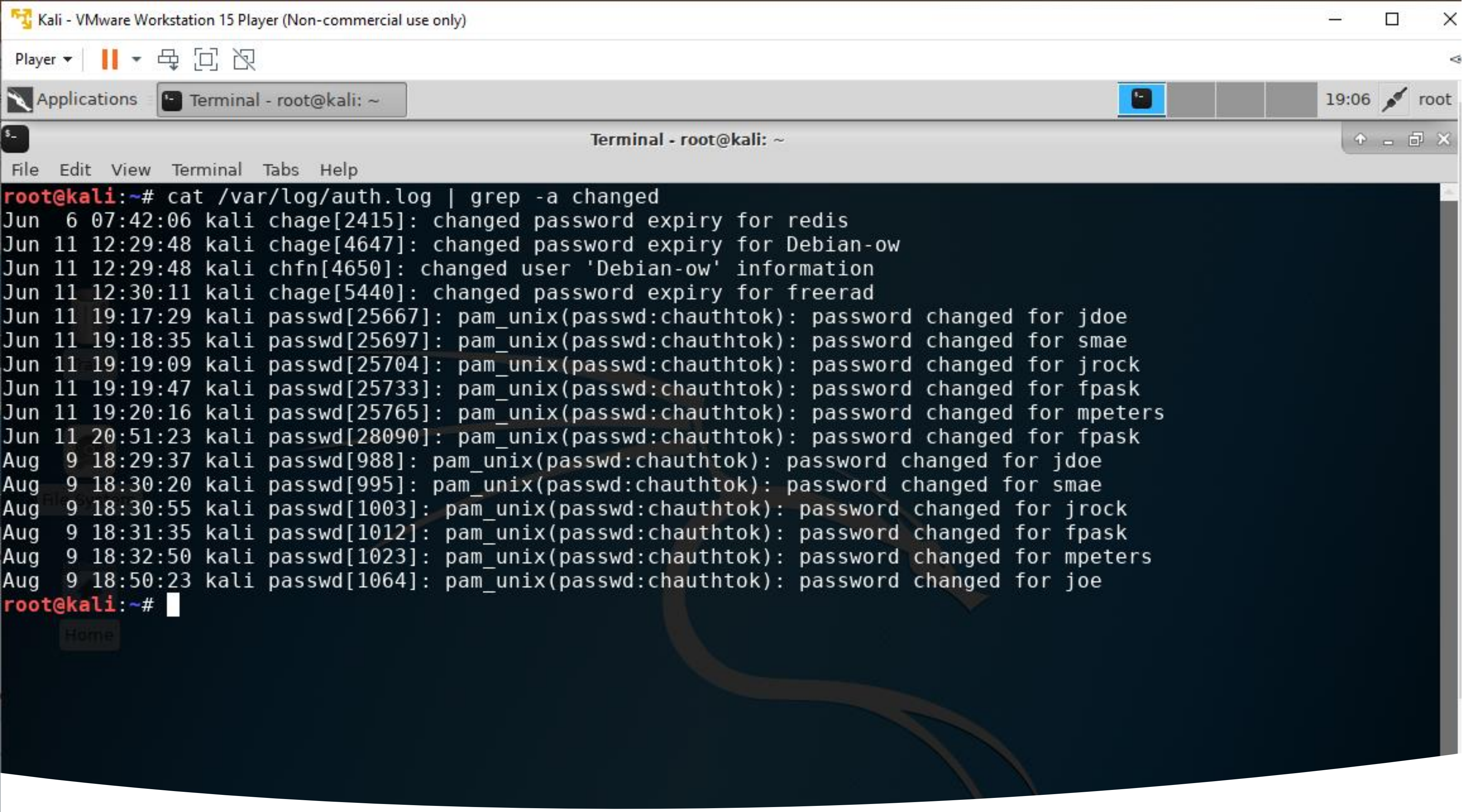


Kali - VMware Workstation 15 Player (Non-commercial use only)
Player
Applications
Terminal - root@kali: ~
19:09
root
Terminal - root@kali: ~
File Edit View Terminal Tabs Help

```
root@kali:~# john --show /etc/shadow
root:toor:18051:0:99999:7:::
jdoe:hacker:18483:0:99999:7:::
smae:password:18483:0:99999:7:::
jrock:hacker:18483:0:99999:7:::
fpask:god:18483:0:99999:7:::
mpeters:Password:18483:0:99999:7:::
joe:God:18483:0:99999:7:::

7 password hashes cracked, 0 left
root@kali:~# 
```

John the Ripper security tool in action

The cracked user passwords by using the John the Ripper security tool one of the most used password cracking tools in IT security, to assess the strength of passwords in your system.



```
root@kali:~# cat /var/log/auth.log | grep -a changed
Jun  6 07:42:06 kali chage[2415]: changed password expiry for redis
Jun 11 12:29:48 kali chage[4647]: changed password expiry for Debian-ow
Jun 11 12:29:48 kali chfn[4650]: changed user 'Debian-ow' information
Jun 11 12:30:11 kali chage[5440]: changed password expiry for freerad
Jun 11 19:17:29 kali passwd[25667]: pam_unix(passwd:chauthtok): password changed for jdoe
Jun 11 19:18:35 kali passwd[25697]: pam_unix(passwd:chauthtok): password changed for smae
Jun 11 19:19:09 kali passwd[25704]: pam_unix(passwd:chauthtok): password changed for jrock
Jun 11 19:19:47 kali passwd[25733]: pam_unix(passwd:chauthtok): password changed for fpask
Jun 11 19:20:16 kali passwd[25765]: pam_unix(passwd:chauthtok): password changed for mpeters
Jun 11 20:51:23 kali passwd[28090]: pam_unix(passwd:chauthtok): password changed for fpask
Aug  9 18:29:37 kali passwd[988]: pam_unix(passwd:chauthtok): password changed for jdoe
Aug  9 18:30:20 kali passwd[995]: pam_unix(passwd:chauthtok): password changed for smae
Aug  9 18:30:55 kali passwd[1003]: pam_unix(passwd:chauthtok): password changed for jrock
Aug  9 18:31:35 kali passwd[1012]: pam_unix(passwd:chauthtok): password changed for fpask
Aug  9 18:32:50 kali passwd[1023]: pam_unix(passwd:chauthtok): password changed for mpeters
Aug  9 18:50:23 kali passwd[1064]: pam_unix(passwd:chauthtok): password changed for joe
root@kali:~# 
```

Account modification in the **Auth.log** File

The **/var/log/auth.log** file with information on account modification.

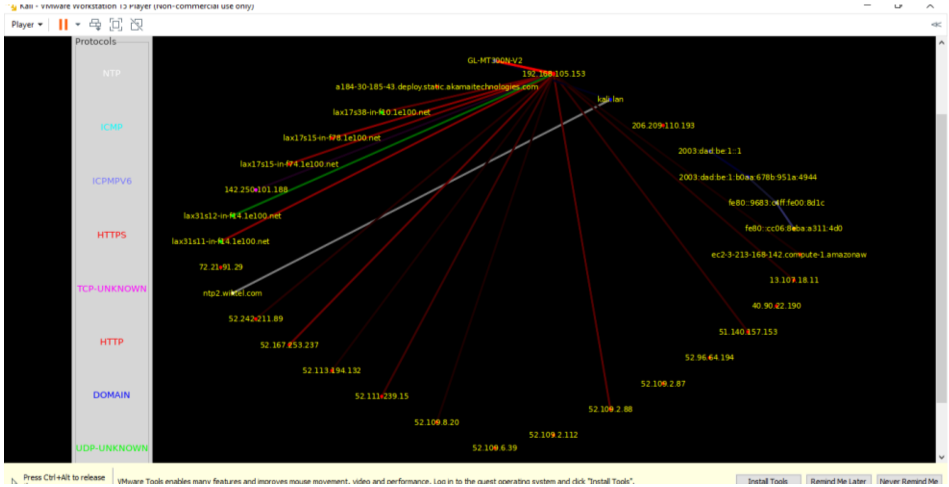
Password management assessment

- Even though ***jdoe*** and ***jrock*** have the same password (i.e., hacker), their password hashes in the /etc/shadow file are different.
- The passwords are salted. When salting is random data unique to the user , it is saved with their password and used in the hashing process of storing and verifying the password.

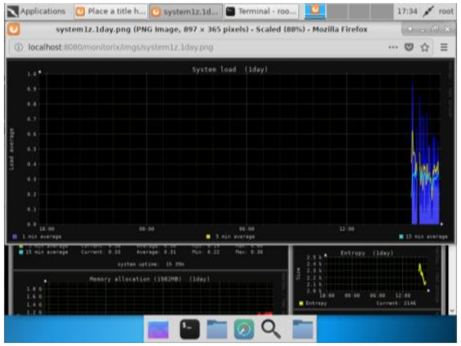
Network Traffic Monitoring

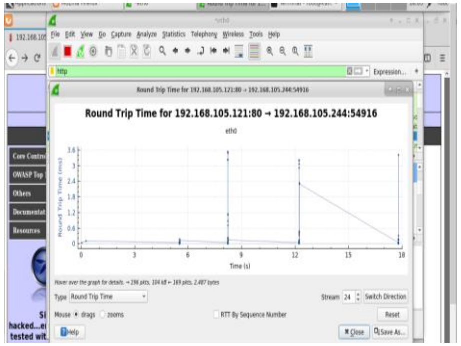
Today's networks must ensure many things and also provide connectivity from source to destination endpoints. Users often use realtime, transaction-based, and non-real-time applications. Each application may require a different level of service. It is crucial for engineers to monitor the network activities to ensure that the network meets the bussinesses needs. Some of the requirements in modern networks include performance, reliability, scalability, adaptability, security, manageability.

Monitorix, Wireshark, and Etherape can be used to monitor the health of a network.



VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click "Install Tools".





Hover over the graph for details. → 196 pkts, 104 kB ← 169 pkts, 2,487 bytes

Type Round Trip Time

Stream 24

Mouse ● drags ○ zooms

□ RTT By Sequence Number

IP Routing

CONFIGURE TWO LOOPBACK INTERFACES ON THE GL-MT300N-V2 TRAVEL ROUTER. ·

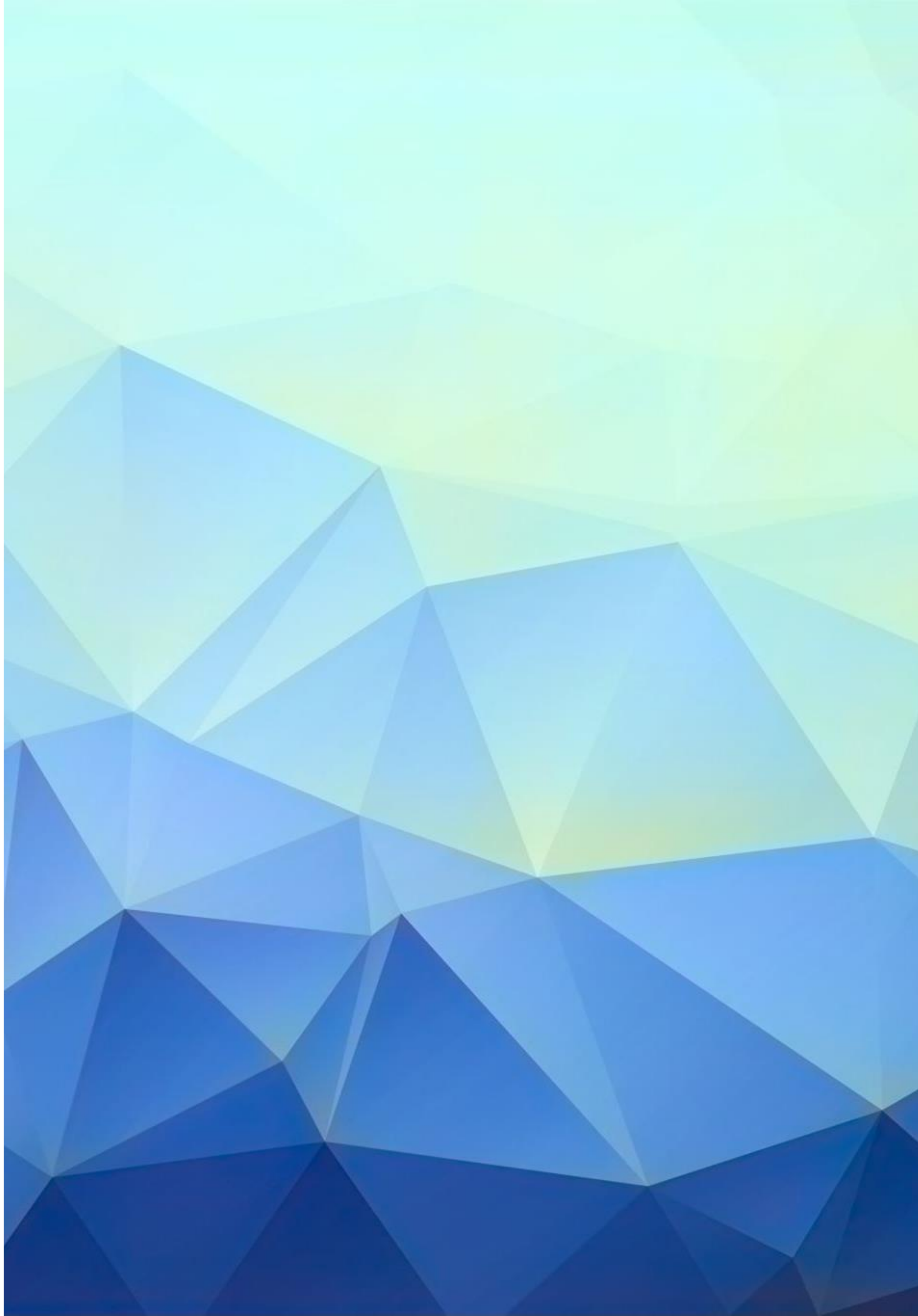
CONFIGURE THE GL AR-750 TRAVEL ROUTER AS A REPEATER TO EXTEND THE REACH OF A WLAN SEGMENT.

TEST CONNECTIVITY BETWEEN THE HOST COMPUTER AND GUEST VMS TO THE NEW LOOPBACK INTERFACES.

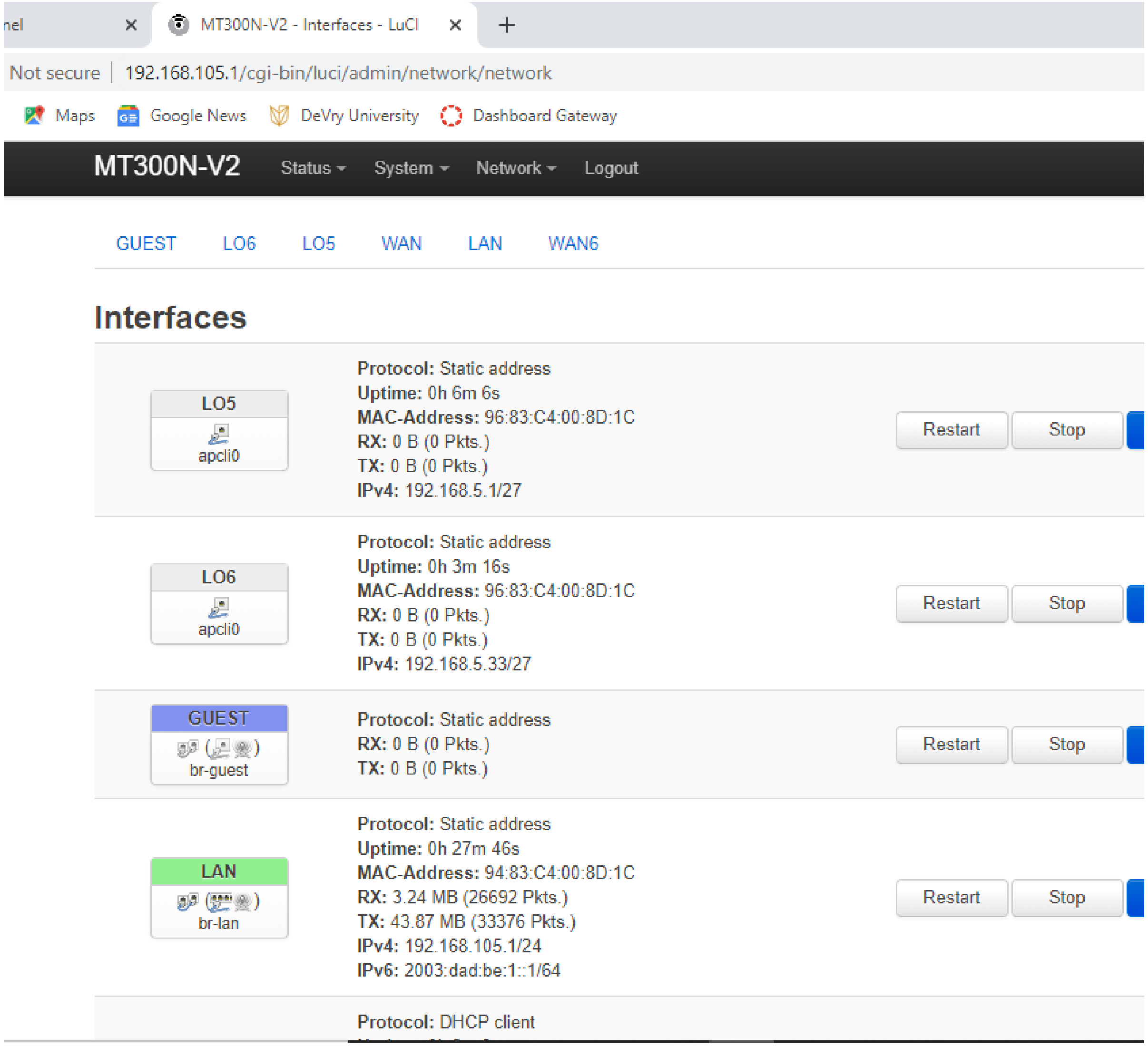
Loopback Interface

The difference between a physical interface and a loopback interface:

A loopback interface is a virtual interface and is used to identify a device and never changes. It will also allow still operate even if one IP address goes down and can only be shutdown if given the command.



IP configurations of Lo5 and Lo6 interfaces



192.168.105.1/cgi-bin/luci/admin/network/network

Interfaces

LO5 (apcli0)

Protocol: Static address
Uptime: 0h 6m 6s
MAC-Address: 96:83:C4:00:8D:1C
RX: 0 B (0 Pkts.)
TX: 0 B (0 Pkts.)
IPv4: 192.168.5.1/27

LO6 (apcli0)

Protocol: Static address
Uptime: 0h 3m 16s
MAC-Address: 96:83:C4:00:8D:1C
RX: 0 B (0 Pkts.)
TX: 0 B (0 Pkts.)
IPv4: 192.168.5.33/27

GUEST (br-guest)

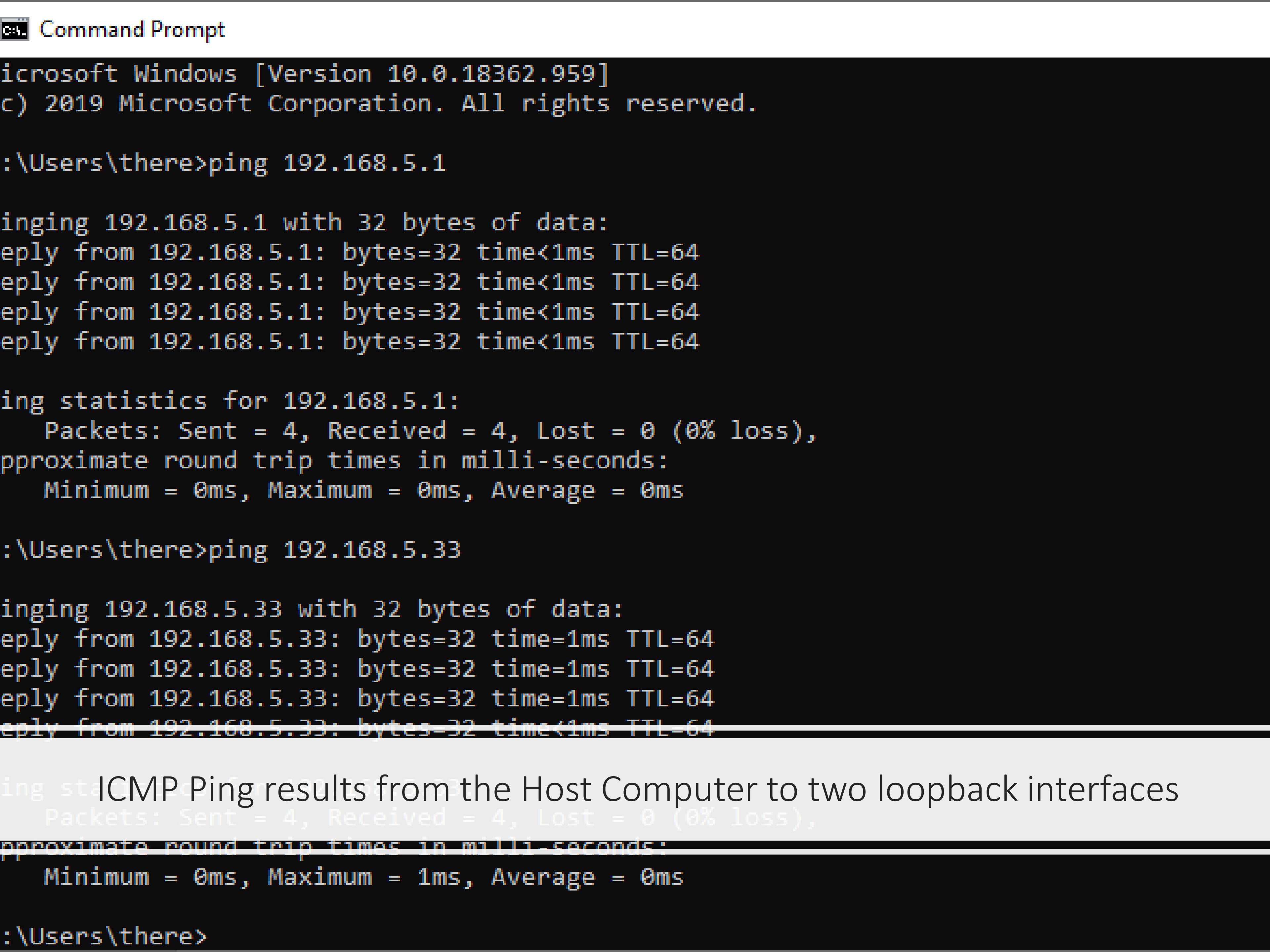
Protocol: Static address
RX: 0 B (0 Pkts.)
TX: 0 B (0 Pkts.)

LAN (br-lan)

Protocol: Static address
Uptime: 0h 27m 46s
MAC-Address: 94:83:C4:00:8D:1C
RX: 3.24 MB (26692 Pkts.)
TX: 43.87 MB (33376 Pkts.)
IPv4: 192.168.105.1/24
IPv6: 2003:dad:be:1::1/64

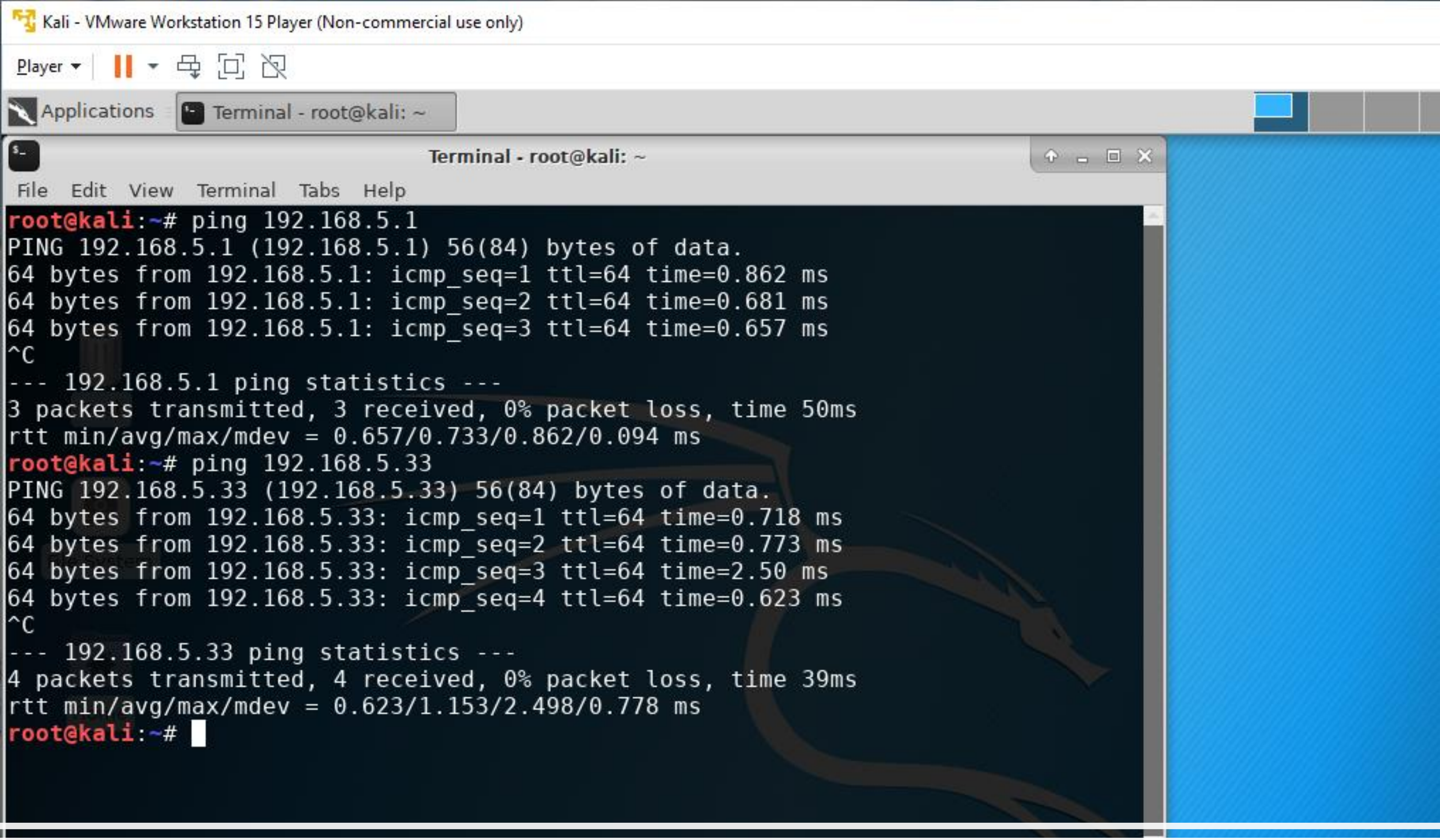
Protocol: DHCP client

Loopback 5 and Loopback 6 interfaces on the GL-MT300N-V2 Router.



```
icrosoft Windows [Version 10.0.18362.959]
c) 2019 Microsoft Corporation. All rights reserved.

:\Users\there>ping 192.168.5.1

inging 192.168.5.1 with 32 bytes of data:
eply from 192.168.5.1: bytes=32 time<1ms TTL=64
eply from 192.168.5.1: bytes=32 time<1ms TTL=64
eply from 192.168.5.1: bytes=32 time<1ms TTL=64
eply from 192.168.5.1: bytes=32 time<1ms TTL=64

ing statistics for 192.168.5.1:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
pproximate round trip times in milli-seconds:
   Minimum = 0ms, Maximum = 0ms, Average = 0ms

:\Users\there>ping 192.168.5.33

inging 192.168.5.33 with 32 bytes of data:
eply from 192.168.5.33: bytes=32 time=1ms TTL=64
eply from 192.168.5.33: bytes=32 time=1ms TTL=64
eply from 192.168.5.33: bytes=32 time=1ms TTL=64
eply from 192.168.5.33: bytes=32 time<1ms TTL=64

ing statistics for 192.168.5.33:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
pproximate round trip times in milli-seconds:
   Minimum = 0ms, Maximum = 1ms, Average = 0ms

:\Users\there>
```

ICMP Ping results from the Host Computer to two loopback interfaces

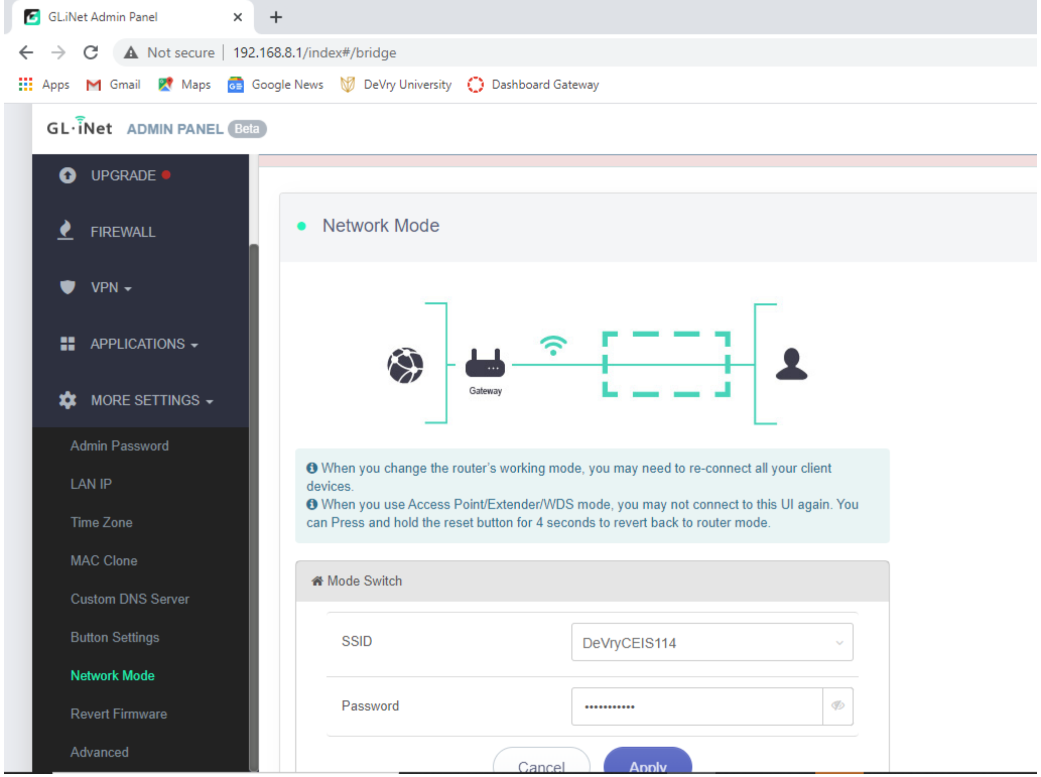


```
root@kali:~# ping 192.168.5.1
PING 192.168.5.1 (192.168.5.1) 56(84) bytes of data.
64 bytes from 192.168.5.1: icmp_seq=1 ttl=64 time=0.862 ms
64 bytes from 192.168.5.1: icmp_seq=2 ttl=64 time=0.681 ms
64 bytes from 192.168.5.1: icmp_seq=3 ttl=64 time=0.657 ms
^C
--- 192.168.5.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 50ms
rtt min/avg/max/mdev = 0.657/0.733/0.862/0.094 ms
root@kali:~# ping 192.168.5.33
PING 192.168.5.33 (192.168.5.33) 56(84) bytes of data.
64 bytes from 192.168.5.33: icmp_seq=1 ttl=64 time=0.718 ms
64 bytes from 192.168.5.33: icmp_seq=2 ttl=64 time=0.773 ms
64 bytes from 192.168.5.33: icmp_seq=3 ttl=64 time=2.50 ms
64 bytes from 192.168.5.33: icmp_seq=4 ttl=64 time=0.623 ms
^C
--- 192.168.5.33 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 39ms
rtt min/avg/max/mdev = 0.623/1.153/2.498/0.778 ms
root@kali:~# 
```

ICMP Ping results from the Kali VM to two loopback interfaces

WLAN SSID

The WLAN SSID of the yellow GL-MT300N-V2 router shown in the extender configuration window of the GL AR-750 router.



Network Mode

When you change the router's working mode, you may need to re-connect all your client devices.

When you use Access Point/Extender/WDS mode, you may not connect to this UI again. You can Press and hold the reset button for 4 seconds to revert back to router mode.

Mode Switch

SSID: DeVryCEIS114

Password: ••••••••••••

Project Conclusion

In this project I investigated a variety of enterprise-level technologies.

- Virtualization, WLANs, network monitoring, Virtual Switching (vSwitch), Routing, and Vulnerability Management.

All these technologies work flawlessly for an organization business needs.