**Practical 1b : Network Protocols**

**Objectives:** Use Remote Desktop to connect to remote servers

Understanding SMTP, POP3, ARP and DNS

Basic ping sweeps, port scans and banner grabbing

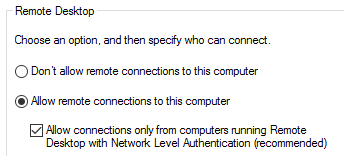
**Exercise Using Remote Desktop to connect to a remote system**

**Description :**

You will enable Remote Desktop services on the Win10 virtual machine so that any other system is able to do a remote connection to it.

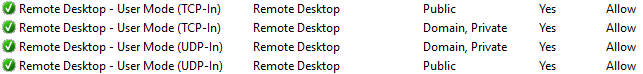
In Win10 VM:

1. Login as user admin.
2. Right-click on the Windows icon in the lower left corner and select System.
3. Click on “Advanced system settings”.
4. Click on the Remote tab.
5. Under Remote Desktop, select “Allow remote connections to this computer”.



Note : If your HostPC (your laptop or desktop) is unable to do a Remote Desktop connection with an encryption error, you may need to uncheck this box to allow your HostPC to connect.

1. Click on Select Users. View who is currently allowed to connect to the Win10 through Remote Desktop. Click Cancel.
2. Click OK.
3. In a Command Prompt, run “netstat -an” to see the ports that are opened. You should see that Port 3389, which is the default port number for Remote Desktop, is opened.
4. In the Cortana search textbox, type “firewall advanced” and run Windows Firewall with Advanced Security.
5. Click on Inbound Rules.
6. Enable the “Remote Desktop – User Mode (TCP-in)” rule for Public profile.



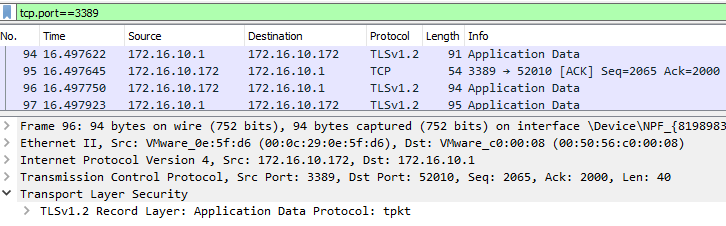
1. Run Wireshark and start capturing packets.

In Host PC (this refers to your laptop or desktop) :

1. In the Cortana search textbox, type “remote” and run Remote Desktop Connection.
2. For Computer, type in the IP address of your Win10 VM.
3. For username, click “More Choices” or “Show Options”. For username, use “192.168.10.67\admin”, changing the IP to your Win10-VM-IP.
4. Login to your Win10 VM as admin and password “1qwer$#@!”
5. You may be asked about the certificate of the Win10 VM as it is not from a trusted Certificate Authority. Click Yes to accept it.
6. You now have remote access to the Desktop of your Win10 VM. You can run commands and applications just as if you are at the Win10 VM.
7. To exit Remote Desktop, click the cross icon in the top bar to close the connection.

In Win10 VM:

1. Stop the Wireshark capture.
2. Do a search to find the packet containing the password “1qwer$#@!”. You should not be successful, as Remote Desktop Connection encrypts the network traffic.



The packets in the Remote Desktop connection are encrypted

Note : Remote Desktop should only be enabled when necessary.

In Win10 VM to disable Remote Desktop:

1. In System, click on “Advanced system settings”. Click the Remote tab.
2. Select “Don’t allow connections to this computer”. Click OK.

**Exercise Address Resolution Protocol (ARP) Spoofing**

**Description:**

Each network card has a physical address, also known as a MAC address. Computers communicate with each other by sending packets to MAC addresses. When a packet addressed to IP address “134.2.15.45” arrives in the network, it must find the corresponding MAC address.

Address Resolution Protocol works by sending a broadcast to all computers in the network segment to ask who has the IP address 134.2.15.45. The correct computer will reply with its MAC address.

ARP Spoofing can occur when a system informs that a certain IP address is at its MAC address, which is wrong.

IP 192.168.10.99 is at MAC address 33-33-33-33-33-33!

**Kali Linux**

IP : 192.168.10.188

MAC : 33-33-33-33-33-3

**Host PC**

IP : 192.168.10.40

MAC : 22-22-22-22-22-22

**Win10 VM**

IP : 192.168.10.99

MAC : 11-11-11-11-11-11

Kali Linux is doing an ARP Spoof to trick Host PC to send packets meant for Win10 VM to Kali Linux instead

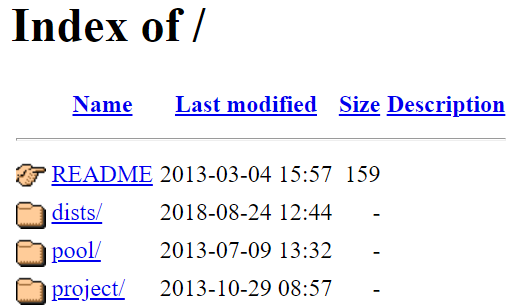
In order to do ARP Spoofing, you need three systems in the same network. You will configure your two VM images to be on the same network as your Host PC.

1. Check that both your Kali and Win10 VM are in NAT.
2. In Win10 VM, run “arp -a” to view the current entries in the ARP table.
3. In Kali VM, run “sudo arp -a” to view the current entries in the ARP table.
4. In Kali, run Wireshark and start capturing packets.
5. In one of your VMs, ping the other VM.
6. Stop the Wireshark capture.
7. Run “arp -a” again on both VMs. The system you just pinged should be listed in the ARP table.
8. In the Wireshark capture, type “arp” in the Filter textbox to view the ARP packets.

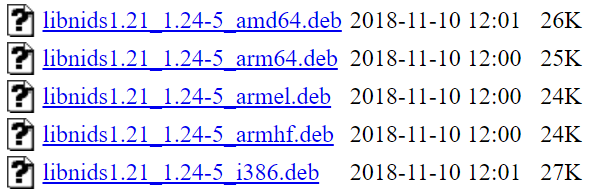
You will now try to use ARP Spoof to make the Host PC think that the Kali VM is the Win10 VM. By default, the arpspoof command is not installed on Kali. Arpspoof command is contained in the dsniff package. One easy method to download and install software on Kali Linux is to use the commands “apt-get update” and “apt-get install dsniff”. We will instead try the more manual method of downloading the required software packages from Kali website and installing them.

In Kali (install the arpspoof command) :

1. In Kali, open the Web Browser and browse to http.kali.org. You will a see a web page like the following :



1. Click on “pool”. Click on “main”.
2. The first software package we are looking for is called “libnids”. Click on “libn”, and click on “libnids”. (you can do a Control-F to find for the string “libnids”)
3. Download the libnids*nnnn*\_amd64.deb package. (Our Kali is 64-bit AMD architecture)



You should see later versions of libnids

1. In a terminal on Kali, change directory to where you have downloaded the file (normally in the directory /home/kali/Downloads).
2. Install the software package by running the following command :

sudo dpkg -i libnids*nnnn*\_amd64.deb (replace *nnnn* with the version number)

1. In the Web Browser, browse to http.kali.org/pool/main. The next software package we are looking for is called “dsniff”. Click on “d”, and click on “dsniff”.
2. Download the dsniff\_*nnnn*\_amd64.deb package.
3. Install the software package by running the following command :

sudo dpkg -i dsniff\_*nnnn*\_amd64.deb (replace *nnnn* with the version number)

1. Check that the arpspoof command is now available :

sudo arpspoof (Note : the sudo before arpspoof is important!)

On Host PC, Win10 VM and Kali VM :

1. Run “ipconfig /all” or “ip addr” to check the IP address and MAC address of all three systems. Fill the table below.

For the Host PC, make sure you record down the IP address and MAC address that is in the same subnet as the IP addresses of the Win10 and Kali VMs. It should normally be the VMnet8 interface (for NAT)

|  |  |  |
| --- | --- | --- |
| System | MAC address | IP address |
| Host PC | **C8-09-A8-CD-F5-BA** | **192.168.126.1** |
| Win10 VM | **00-0C-29-9c-F8-65** | **192.168.126.130** |
| Kali VM | **00:0c:29:30:7d:60** | **192.168.126.129** |

On Host PC

1. Ping your Win10 VM.
2. Run “arp -a” to view the ARP entry for your Win10 VM. Check that the MAC address belongs to your Win10 VM.

In Kali VM

1. Run the following command to make the ARP entry for the Win10 VM in your Host PC to point to your Kali Linux VM.

Change to your Host PC IP

Change to your Win10 VM IP

sudo arpspoof –i eth0 –t 192.168.10.200 192.168.10.67

1. Run Wireshark and start capturing packets. ic

On Host PC

1. Run “arp -a” to view the ARP entry for your Win10 VM. Check that the MAC address now belongs to your Kali.
2. Ping to your Win10 VM. The ping will not be successful.

Because of the “spoofed” entry in the ARP table, all packets meant for the Win10 VM are sent to your Kali VM instead.

In Kali VM

1. Type Control-C to stop the arpspoof.
2. Stop the Wireshark capture.
3. Look at the ICMP packets from your Host PC. Even though the Destination IP is your Win10 IP, the Destination MAC address is your Kali MAC address.
4. Look at the ARP packets. When you run arpspoof, the Kali Linux starts sending ARP packets to the Host PC to update the “spoofed” MAC address.

**Exercise Bettercap, ARP, DNS Spoof and SSL Strip**

Check that the Win10, Kali and web-server VMs are powered on.

Bettercap is a tool that can be used for network monitoring and also network attacks. This time, we will use the apt-get install command to install Bettercap on Kali.

In Win10 VM

1. Run “arp -a” to view the ARP entry for the Gateway.

In Kali VM

1. Run the following commands to install Bettercap.

sudo apt-get update (this command will update the package lists on Kali)

sudo apt-get install bettercap

1. Run Bettercap.

sudo bettercap

1. Type “help” to see the available commands and modules. Most of the modules are nor running.

help

1. View the network information. Currently you will see the IP address of Kali and the IP of the VMware gateway.

net.show

1. Net.probe is a module that will search for other hosts on the same network. View the help for the module net.probe, and set net.probe to be running.

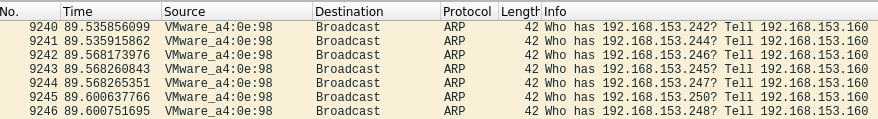
help net.probe

net.probe on

1. Type “help” again to see the net.probe module is running. The net.recon module is also started along with net.probe.

help

1. Run Wireshark and start capturing packets. Look for the ARP packets that the net.probe module is sending out.



ARP broadcast requests sent out to probe for other hosts in the network

1. View the network information again. This time you will see the IP address of the Win10 VM (and other systems in the network) too.

net.show

1. Stop net.probe. You do not need to stop the net.recon module as it is needed by the arp.spoof module.

net.probe off

1. Configure the arp.spoof module to trick the Win10 VM (victim) into thinking the Kali is the gateway.

help arp.spoof

set arp.spoof.targets 192.168.10.67

Change to your Win10 VM IP

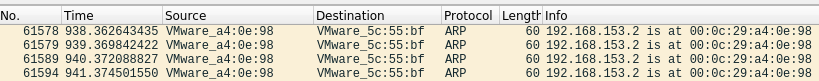
1. Check the settings of the arp.spoof module.

get arp.spoof.\*

1. Start arp.spoof.

arp.spoof on

1. In the Wireshark capture, look at the ARP packets. The arp.spoof module is sending ARP packets to the Win10 VM to tell that the Gateway IP is at the Kali MAC address.



ARP packets sent to Win10 VM to make it think the Gateway IP is at Kali MAC address. You will have different IP and MAC addresses in your packet capture.

In Win10 VM

1. Run “arp -a” to view the ARP entry for the Gateway. Check that the MAC address belongs to your Kali.

Now we will use the dns.spoof module in Bettercap to spoof the domain yahoo.com. When the Win10 VM tries to browse to the domain yahoo.com, it will go to web-server2 instead.

In Kali VM

1. In the Bettercap prompt, look at the help for the dns.spoof module.

help dns.spoof

1. Configure the dns.spoof module to direct DNS requests for the domain yahoo.com to the IP address of web-server2.

Change to your web-server2 IP

set dns.spoof.address 192.168.10.100

set dns.spoof.domains yahoo.com

1. Check the settings of the dns.spoof module.

get dns.spoof.\*

1. Start dns.spoof.

dns.spoof on

1. In Wireshark, start the packet capture if it is not running yet. Set the filter to “dns”.

In Win10 VM

1. In a Command Prompt, run “ipconfig /flushdns” to clear the DNS cache.
2. Start a web browser. Clear the browsing history.
3. Browse to www.yahoo.com. Instead of going to Yahoo, you are directed to the web page of the web-server2 VM. You may see a warning about the security certificate.
4. In a Command Prompt, run “ipconfig /displaydns” to display the DNS cache. Look at the entries under the domain yahoo.com. The IP address for them is the web-server2 IP.

In Kali VM

1. Stop the Wireshark capture.
2. In Wireshark, look for the DNS request for yahoo.com (you can do a Find Packet for the string “yahoo”).

The dns.spoof module sends a DNS response that the IP address of www.yahoo.com is the web-server2 VM IP.



1. In the Bettercap prompt, stop the dns.spoof and arp.spoof modules.

dns.spoof off

arp.spoof off

In Win10 VM

1. In a Command Prompt, run “ipconfig /flushdns” to clear the DNS cache.
2. In the web browser, clear the browsing history.
3. Check that you can browse to the correct www.yahoo.com.

If the attacker configures the web-server webpage to look like Yahoo, a user who is not careful with security certificate warnings, may be tricked into entering sensitive information like usernames and passwords in the attacker’s website.

SSL Strip is a tool that can intercept HTTP traffic and replaces any redirects or links to HTTPS websites with HTTP, and sits in the middle to intercept the connection.

Kali running Bettercap SSL Strip module in (Attacker)

Win10 connecting to Web Server (Victim)

Web Server

HTTPS

HTTP

Because SSL Strip causes the connection between the Victim and the Attacker to be in HTTP, the Attacker may be able to see HTTP data

In Kali VM

1. In the Bettercap prompt, start the arp.spoof module. The Win10 VM now thinks Kali is the gateway.

arp.spoof on

1. Enable SSL Strip in the http.proxy and https.proxy modules and start both modules

set http.proxy.sslstrip true

set https.proxy.sslstrip true

http.proxy on

https.proxy on

1. In Wireshark, start the packet capture. Set the filter to “http”.

In Win10 VM

1. In a Command Prompt, run “ipconfig /flushdns” to clear the DNS cache.
2. In the web browser, clear the browsing history.
3. Try to browse to different websites eg www.ebay.com or www.google.com.

Some websites may allow you to visit their website using HTTP (no lock icon is displayed in the browser). Other websites may show a warning about the security certificate not matching the site. If you continue, you may still receive some web content in HTTP. Try submitting some data in the forms (eg “basketball”).

A user who is not careful, may fail to notice that the website is in unsecured HTTP.

In Kali VM

1. In Wireshark, look for HTTP packets. Can you find the form data that you submitted?
2. Stop the Wireshark capture.
3. In the Bettercap prompt, stop the https.proxy, http.proxy and arp.spoof modules, and exit Bettercap.

https.proxy off

http.proxy off

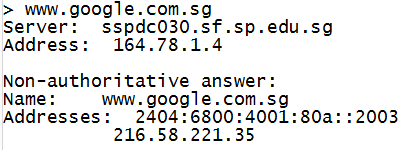
arp.spoof off

exit

**Exercise Domain Name System (DNS) client tools**

In Win10 VM

1. In Command Prompt, type “ipconfig /all”. Look for the IP address of the DNS Server.
2. To find out the IP address of a domain, we can use the nslookup utility:
3. Type “nslookup”.
4. In the nslookup prompt, type a website domain name like “www.google.com.sg” to find the IP address of the website. You may get an output like the following :



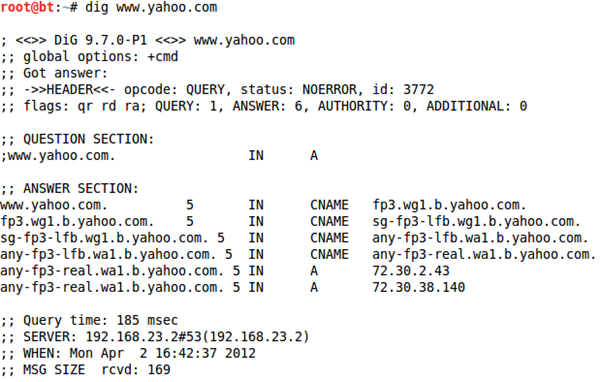
Local DNS Server that will answer your query

IPv4 address for www.google.com.sg

1. Type “exit” to quit nslookup.

In Kali

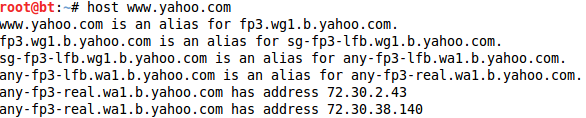
1. To find out the IP address of a domain, we can use the dig or host utilities.
2. Type “dig www.yahoo.com” to find the IP address of www.yahoo.com. You may get an output like the following:



IP addresses for www.yahoo.com

Local DNS Server that is answering your query

1. Type “host www.yahoo.com” to find the IP address of www.yahoo.com. You may get an output like the following:



IP addresses for www.yahoo.com

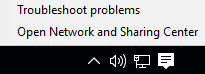
**Exercise DNSChef**

**Description:**

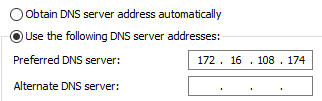
If an attacker can compromise the DNS Server or DNS Cache, and put fake entries in, he can redirect users to fake websites. In this example, we configure the Win10 VM to use Kali as the DNS Server and run DNSChef on Kali to send wrong IP answers when it sees DNS requests for a certain domain.

In Win10 VM ( to set the DNS Server to point to Kali )

1. Right-click on the Network icon in the lower right corner and choose “Open Network and Sharing Center”.



1. Click “Change adapter settings”.
2. Right-click on Ethernet and choose Properties.
3. Select “Internet Protocol Version 4 (TCP/IPv4)” and click Properties.
4. Select “Use the following DNS server addresses” and enter your Kali IP.



Change this to your Kali IP.

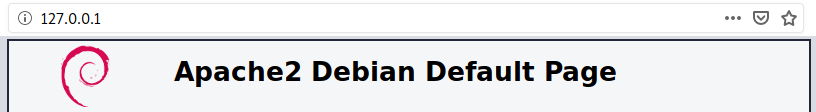
1. Click OK. Click Close.

In Kali

1. Start up the Apache Web Server.

sudo systemctl start apache2

1. Use the web browser to browse to 127.0.0.1. You should see the Apache2 Default page.



1. Check the IP of the current DNS Server (or nameserver).

cat /etc/resolv.conf

1. In a terminal, use DNS Chef to send the IP of your Kali when it sees DNS requests for the domain kali.org. DNS requests for other domains will be forwarded to the normal DNS Server. Enter the following command in a single line :

sudo dnschef -i *KaliIP* --fakedomains kali.org,kali.org.localdomain --fakeip *KaliIP* --nameservers *CurrentDNS-IP*

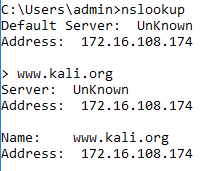
(replace *KaliIP* with your Kali IP, and *CurrentDNS-IP* with the IP of the current DNS Server)

In Win10 VM

1. In a Command Prompt, run the following command to clear any entries in the DNS Cache.

ipconfig /flushdns

1. In the Command Prompt, do a nslookup on www.kali.org. The IP for www.kali.org is returned as the IP of your Kali.



The IP for www.kali.org is now your Kali IP

1. Use a Web Browser to browse to www.google.com. You should be able to browse to Google.
2. Browse to http://www.kali.org. You will be redirected to the Apache Web Server on Kali.

An attacker who manages to redirect users to his IP address will make the fake website look just like the real one. Unsuspecting users may enter sensitive information like usernames and passwords in the attacker’s website.

In Kali

1. Use Control-C to stop DNSChef.

In Win10 VM ( to reset back settings )

1. Right-click on Ethernet and choose Properties.
2. Select “Internet Protocol Version 4 (TCP/IPv4)” and click Properties.
3. Select “Obtain DNS Server address automatically”. Click OK. Click Close.
4. In the Command Prompt, do a nslookup on www.kali.org. The actual IP for www.kali.org is now returned.

**Exercise Ping sweep**

**Description**

To do a ping sweep, you can use the ping command to ping each IP address one by one. You can also use special ping sweep software.

If you are doing a ping sweep, remember not to include the broadcast address (eg 172.16.3.255) in the range of IP addresses, as this could cause a large number of packets to be generated and flood the network.

In Kali VM

1. In Kali, look at the man page for fping.
2. Use the fping command to ping the range of IP addresses in your Kali subnet. Which system is alive?

fping --alive --quiet –g 192.168.10.1 192.168.10.254

Change to the range of IPs in your Kali subnet. For example, if your Kali IP is 192.168.10.47, then run fping -g starting from IP 192.168.10.1 to IP 192.168.10.254

1. Look at the man page for hping3.
2. Start a Wireshark capture.
3. Use the hping command to craft one single SYN packet to your Win10 VM.

Change to the IP of your Win10 VM

sudo hping3 –c 1 –S 192.168.10.50

*(You did not specify any port using the -p option, so the SYN packet will go to Port 0)*

1. Stop the Wireshark capture and analyse the packets captured.

Currently your Win10 VM may not reply to the hping3 command as the Windows Firewall may be blocking the SYN packet that is going to Port 0.

1. Start a Wireshark capture.
2. Use the hping command to craft one single SYN packet to Port 80 on your web-server2.

Change to the IP of your web-server2

sudo hping3 –c 1 –S –p 80 192.168.10.47

1. Stop the Wireshark capture and analyse the packets captured.

Because Port 80 on web-server2 receives a SYN packet, it returns a SYN/ACK packet.

**Exercise Basic Port Scans**

**Description:**

Network Mapper (Nmap) is an open source software tool for scanning networks. While many system administrators find the software useful in checking the security of a computer or network, many hackers also use it to discover vulnerabilities in the target network.

Some common Nmap options :

-sT basic port scan : attempt to connect to every port in turn, using the TCP connect().

-sS TCP SYN scan : send packets with SYN flag

-p <port range> only scan specified ports

You are going to run nmap against your web-server2 to see what ports are opened.

In Kali

1. Run the following command to run nmap against your web-server2 to see which ports are opened. It may take a few minutes. You should see a number of ports opened on your web-server2.

Change to the IP of your web-server2

sudo nmap –sS 192.168.10.100

On web-server2

1. Enable and start the Telnet service.

On Kali VM

1. Repeat the nmap scan against your web-server2. Is the Telnet port (23) reported to be opened?
2. Use nmap to run a SYN scan against a range of IP addresses.

Change the range so that the IP of your web-server2 is in the range.

sudo nmap –sS 192.168.10.244-250

Which ports are opened on which systems? What services are running?

**Note : When there is too much network traffic to the servers (eg a whole class of students scanning the same server at the same time), you may not get any reply from the server. Wait a couple of minutes, then try again.**

1. Use nmap to run a SYN scan only on port numbers 22, 25 and 80 against your web-server2

sudo nmap –sS –p22,25,80 192.168.10.100

On web-server2

1. Disable the Telnet service.

**Exercise Banner Grabbing (revision)**

In Kali

1. Use Telnet command to connect to the FTP Server running on your web-server2.

Change to the IP of your web-server2

**telnet 192.168.10.100 21**

Connected to 192.168.10.100.

Escape character is ‘^]’.

You should be able to see the FTP Server software and version that is running on your web-server2. Press Control-] and type “quit” to exit, if necessary.

1. Use Telnet command to connect to the Web Server running on your web-server2. Enter the commands in bold.

**telnet 192.168.10.100 80**

Connected to 172.16.3.250.

Have a space around the slash character between GET and HTTP.

Press Enter twice after this line

Escape character is ‘^]’.

**GET / HTTP/1.1**

What version of web server is running?

Press Control-C to quit, if necessary.

1. You can also use netcat to connect to the Web Server.

**nc 192.168.10.100 80**

Press Enter twice after this line

**GET / HTTP/1.1**

Text

Description automatically generated

*End of Practical*