Lab One

CS6035 – Introduction to Information Security

Griselda Conejo Lopez
[*gcl6@gatech.edu*]

Yuxiang Liu
[*yliu858@gatech.edu*]

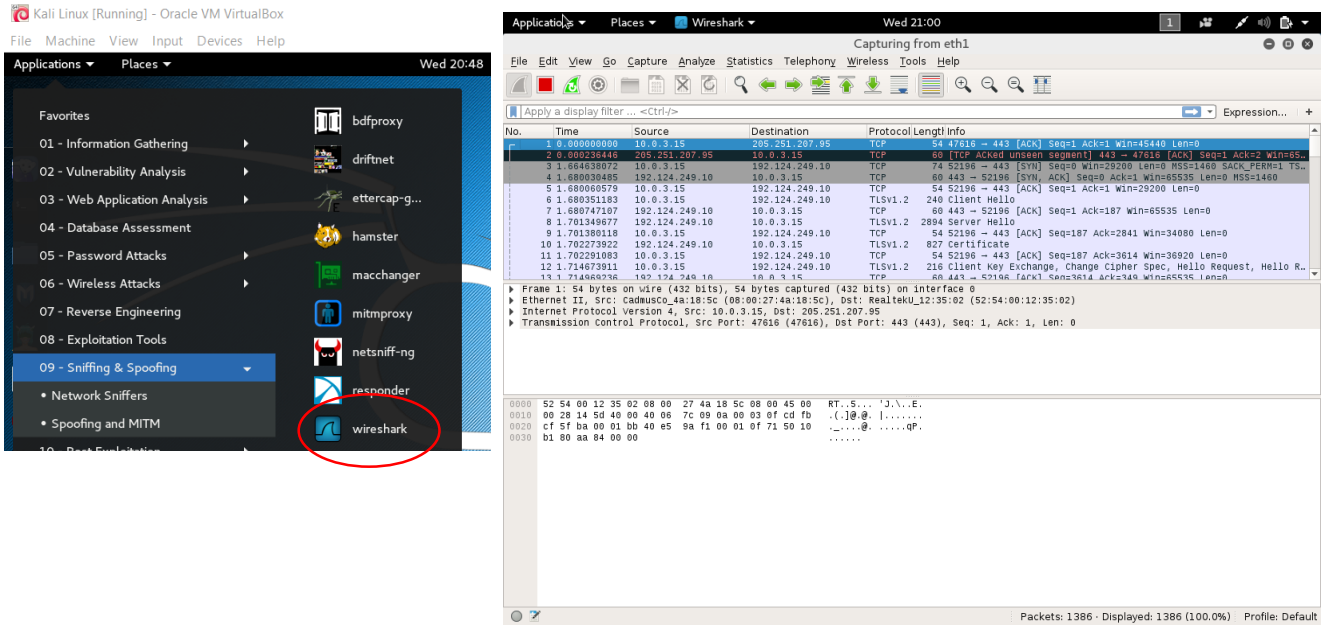
Kaushik Santhanam
[*ksanthanam7@gatech.edu*]

MARCH 11, 2016

Set up Kali Linux (2 Points)
Set up a Kali system any way you wish (virtual or otherwise), but we recommend you set it up as a virtual system.

What to submit:

- A screenshot of one security tool included in Kali Linux embedded into your solutions document. [1 point]



- Explain the utility of the tool you've selected above. [1 point]

Wireshark is a network protocol analyzer that lets us see what is happening on the network at a microscopic level (structure of different networking protocols). It is commonly used as a packet analyzer for network troubleshooting, analysis, software and communications protocol development, and education. Wireshark has a rich feature set which includes the following: [1,2]

- Deep inspection of hundreds of protocols, with more being added all the time
- Live capture and offline analysis
- Standard three-pane packet browser
- VoIP analysis
- Read/write many different capture file formats: tcpdump (libpcap), Pcap NG, Catapult DCT2000, Cisco Secure IDS iplog, Microsoft Network Monitor, and many others
- Live data can be read from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI, and others (depending on your platform)
- Decryption support for many protocols, including IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, and WPA/WPA2
- Coloring rules can be applied to the packet list for quick, intuitive analysis

DNS Architecture (4 Points)
This exercise will explore the architecture of the Domain Name System and how it can be exploited by an attacker.

What to submit:

- In a DNS packet, what is the Transaction ID and how is it used? [0.5 point]

DNS packets have a structure that is:

Transaction ID	Flags	Header
Question count	Answer resource record count	
Authority resource record count	Additional resource record count	
Question entries		
Answer resource records		
Authority resource records		
Additional resource records		

The DNS packet header starts with a Transaction ID that is used to link a request and the corresponding reply. The Transaction ID is a 16-bit field used to identify a specific DNS transaction. It is created by the message originator and the responder copies the transaction ID into its response message. This enables the DNS client to match responses received from a DNS server to the requests that were sent to the server. [3]

- What OSI layer four protocol does DNS use? Why? [0.5 point]

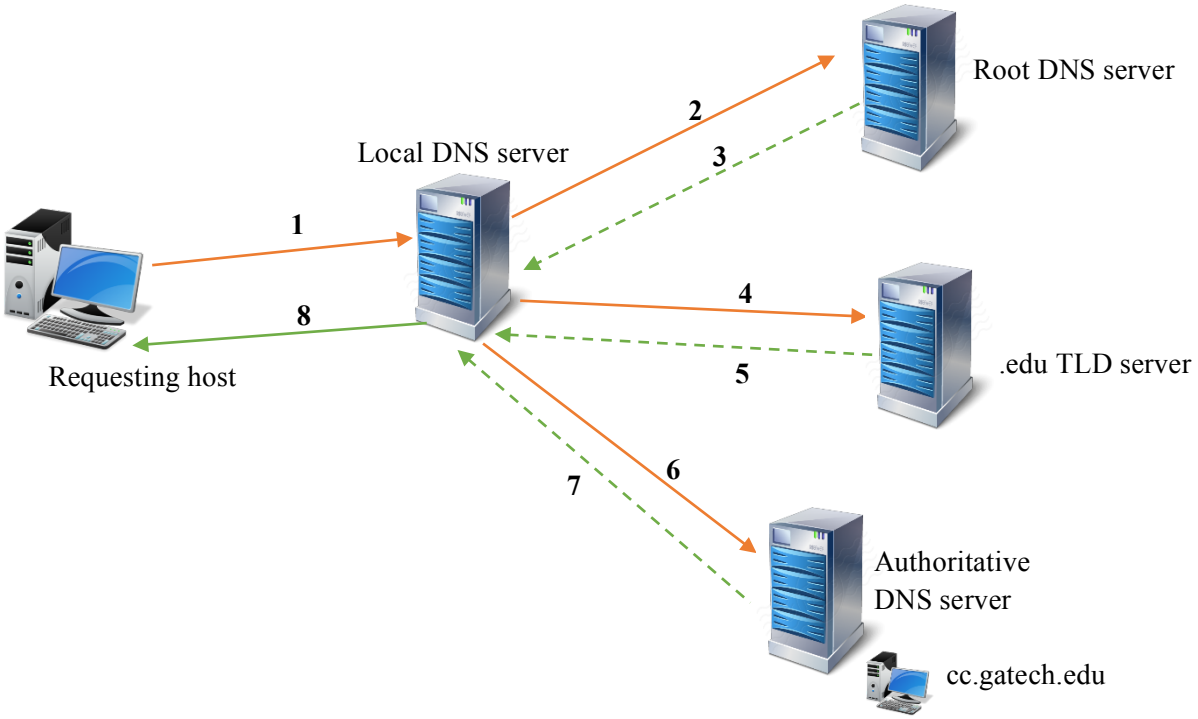
DNS is a protocol that sits at the application layer of the OSI model that makes use of the whole TCP/IP stack [4]. DNS works on a client-server model and it uses primarily UDP protocol (on port 53) for transport layer communication since it does not demand the transfer of large amounts of data or a payload. DNS uses UDP protocol because when browsing a website, before establishing the TCP connection to communicate with the protocol HTTP with the server, the client needs to get the IP address of the URL using a DNS query, DNS then uses UDP and TCP transport to query other distributed DNS servers to answer client questions like "what are the IP addresses associated with www.gatech.edu?" [5].

- Draw a diagram showing the full trip for a recursive DNS query for www.cc.gatech.edu. Label each entity involved (i.e., requesting host, local DNS server, root server, TLD server, and authoritative server). Assume that nothing is cached. Note that you do not have to label each entity with its IP address or hostname. Just the labels mentioned in the previous sentence will do. [1 point]

The full trip for the recursive DNS query is: [6]

1. Requesting host requests its local DNS server to solve the DNS query '*www.cc.gatech.edu*'
2. The local DNS server asks the root DNS server for the IP address of '*www.cc.gatech.edu*'

3. The root DNS server finds the suffix as '.edu' and returns a list of IP addresses of the TLD servers responsible for '.edu' to the local DNS server
4. The local DNS server sends the same query for '*www.cc.gatech.edu*' to one of the TLD servers which were provided by the root DNS server
5. The .edu TLD server finds the suffix '*gatech.edu*' and returns the IP address of the authoritative DNS server for Gatech to the local DNS server.
6. The local DNS server sends the same query for '*www.cc.gatech.edu*' to authoritative DNS server provided by the .edu TLD server
7. The authoritative DNS server responds with the IP address of 'c*c.gatech.edu*'
8. The requesting host receives the IP address of its desired query

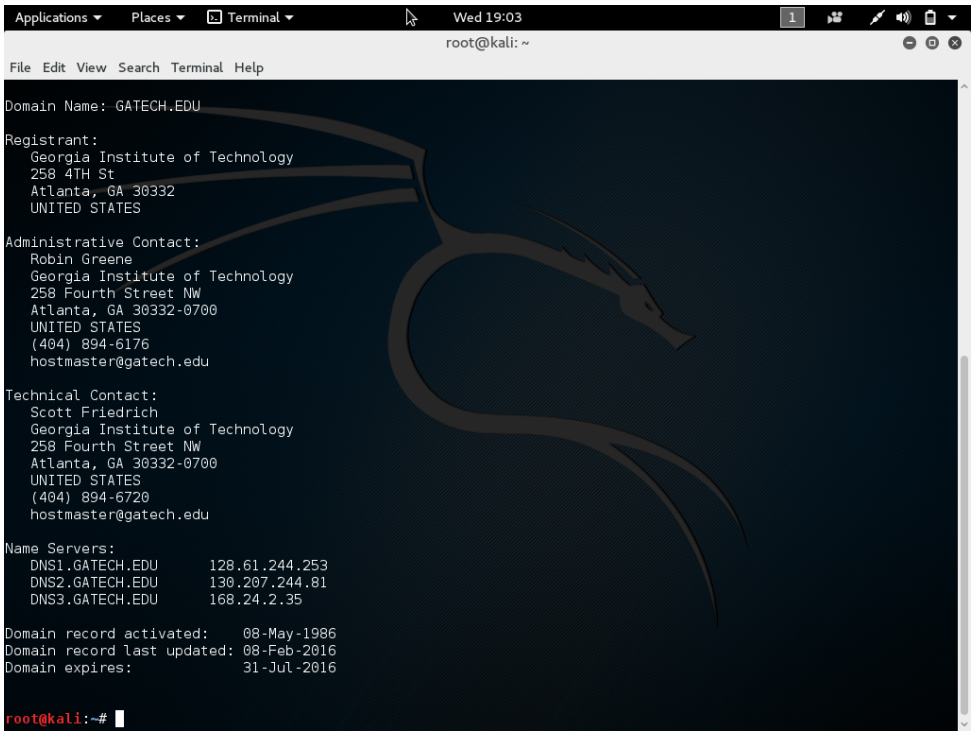


- Using the terminal of your Kali server, type "whois gatech.edu" Include the output in your submission. Now type "traceroute www.cc.gatech.edu" How could this information be useful to an attacker? [0.5 point]

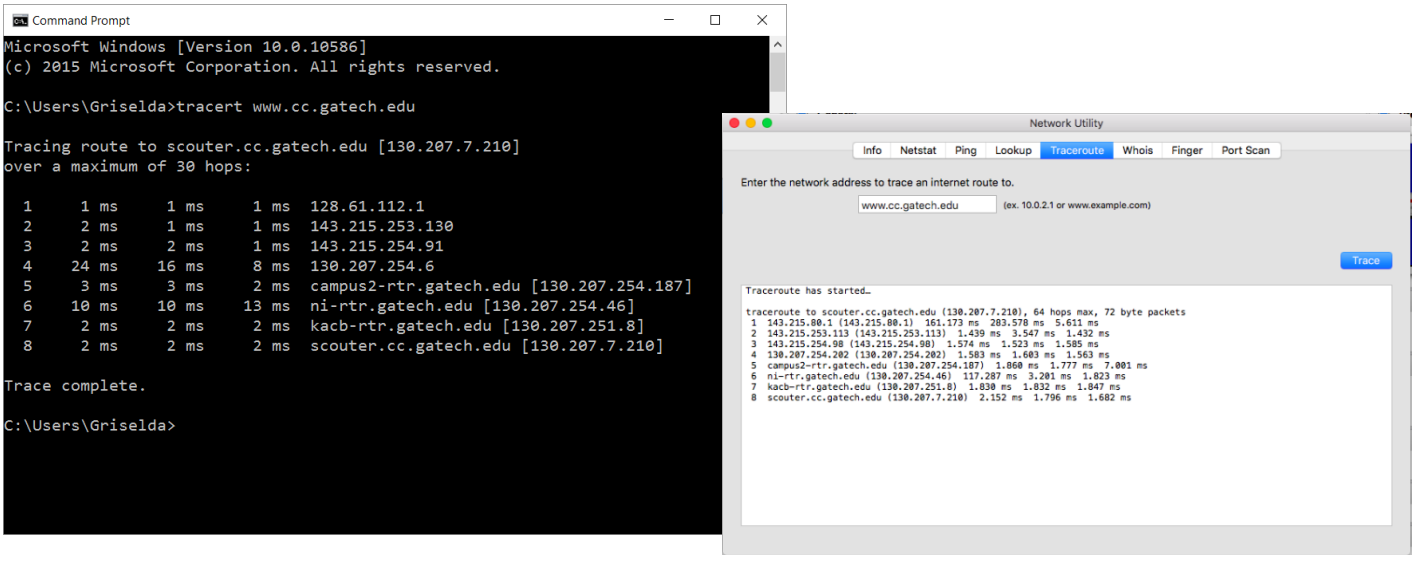
Traceroute sends packets to a destination, asking each router along the way to reply when it passes on the packet. This will shows the path that packets take when we send them between our location and a destination [7]. An attacker can use the traceroute output to create and approximate network diagram, determine the physical location of some of the routers the packets are passing through, to gather network information such as gateways and other internal systems, and for firewall discovery, since frequently dropped packets are evidence of a firewall. The whois command looks up the registration record associated with a domain name, showing information about who registered and owns a domain name, including their contact information. [8]. An attacker can use

the whois database and the nslookup tool to determine the IP address ranges, DNS server addresses, etc. for the target institution.

Output for ‘whois gatech.edu’:



Output for traceroute www.cc.gatech.edu:



- What is the impact to end users if they query a DNS server with a poisoned cache? [0.5 point]

Cache poisoning is a type of attack in which corrupt data is inserted into the cache database of the DNS name server [9], a single fake entry into a caching server can redirect a large number of end users. Since the browser resolves the address of the domain automatically, there is no reason for the end user to be suspicious. The impact of a poisoned cache is that end users can be redirected to some other website (of the attacker's choosing and set up to appear legitimate) without even knowing it, tricking them into accepting content coming from a non-authentic server or download malicious content, opening the door for computer worms or other malware, even man-in-the-middle attacks and denial-of-service attacks.

- Explain the process for performing a poisoning attack. Be sure to note why it works. [0.5 point]

When a DNS caching server gets a query from a subscriber for a domain, it looks to see whether it has an entry cached. If not, it will ask authoritative DNS servers and wait for their responses. To verify if the response is the answer to the corresponding question, it will check the following parameters: Source IP Address; Source Port Number; whether the answer matches the question asked; whether unique transaction number matches. An attack succeeds if the attacker can beat a legitimate authoritative DNS server by sending fake query response and arrives at the caching server first with the correct parameters. [10]

- Now that you understand the weaknesses of the basic Domain Name System, what is one way it could be improved? [0.5 point]

It could be improved with Domain Name System Security Extensions (DNSSEC) that use cryptographic digital signatures signed with a trusted public key certificate to determine the authenticity of data. [11]

SSL/TLS and Traffic Analysis (6 Points)
In this section you will use the network analysis tool Wireshark to watch SSL/TLS at work when connecting to a secure web site (using HTTPS)

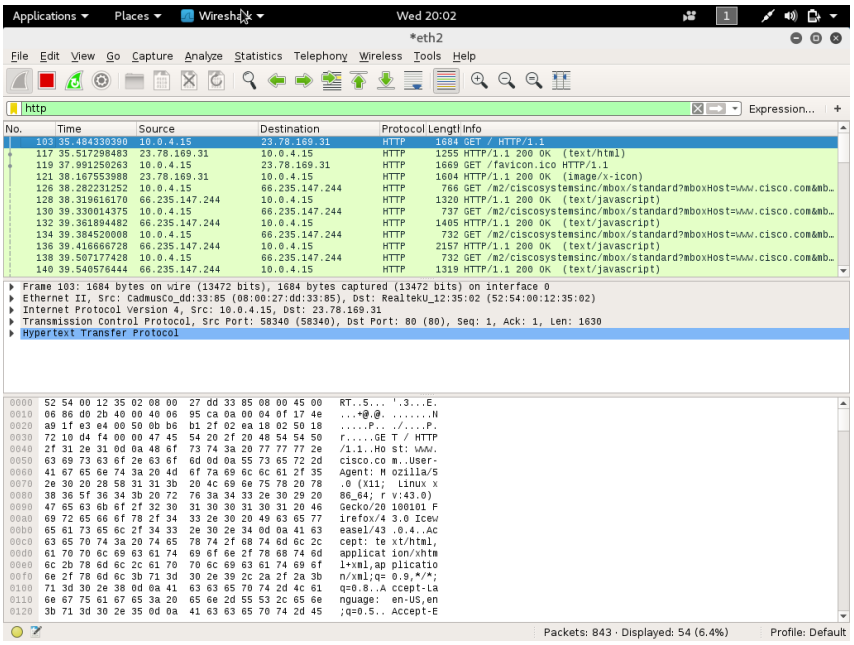
What to submit:

- What is different when visiting the site using HTTP versus HTTPS? (Protip: To see HTTP traffic, use Wireshark to filter on "http". To see HTTPS traffic, use Wireshark to filter on "ssl" traffic.) [1 point]

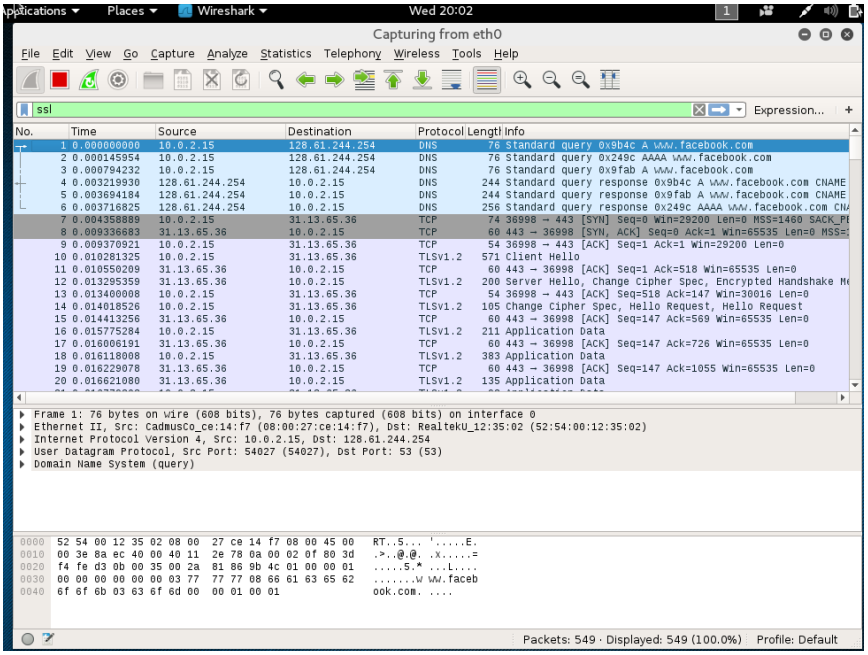
HTTP stands for Hyper Text Transfer Protocol. It is used for transferring data between server and client. It does not have encryption. On the other hand, HTTPS stands for Hyper Text Transfer Protocol SECURE. It is also used for the same purpose, but it does this in a secure manner by encryption. The server and the client agree upon a code so that the information shared between them through the HTTPS connection cannot be read by anyone else. This is done using TLS also

known as Transport layer security. The website encrypts the session with a digital certificate (SSL Certificate) that contains unique, authenticated information about the certificate owner and a Certificate Authority verifies the identity of the certificate owner when it is issued. HTTP uses port 80 by default whereas HTTPS used port 443 by default. Both use TCP and both are request/receive protocols with ACKs. [12]

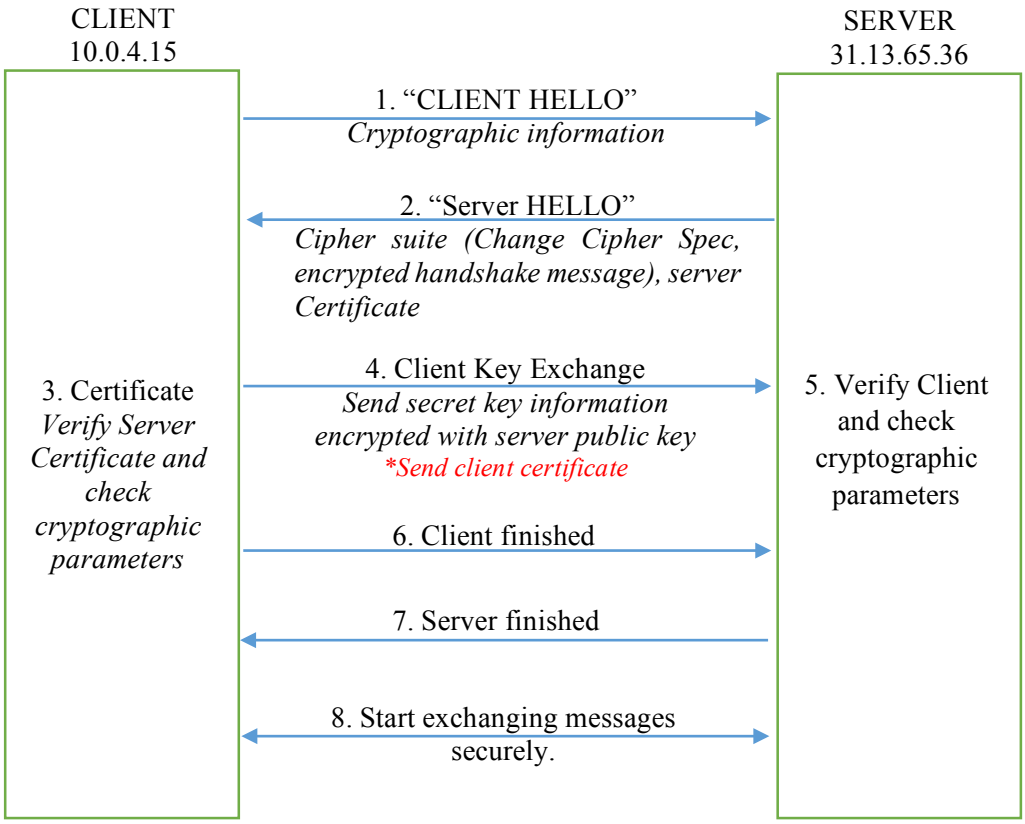
Visiting http://www.cisco.com



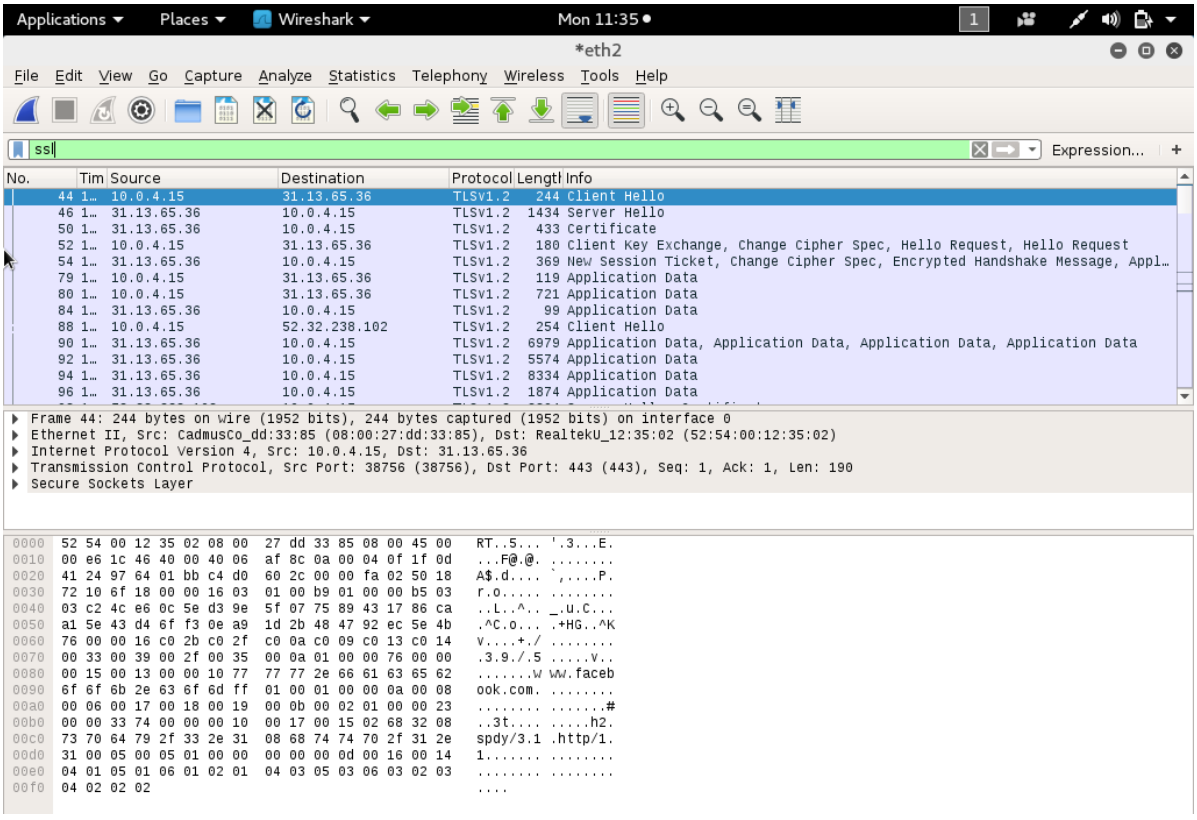
Visiting https://www.facebook.com



- Draw a diagram showing the SSL/TLS handshake procedure you observed. Attach a screenshot of the Wireshark capture that shows the first few packets of the handshake. [2 points]

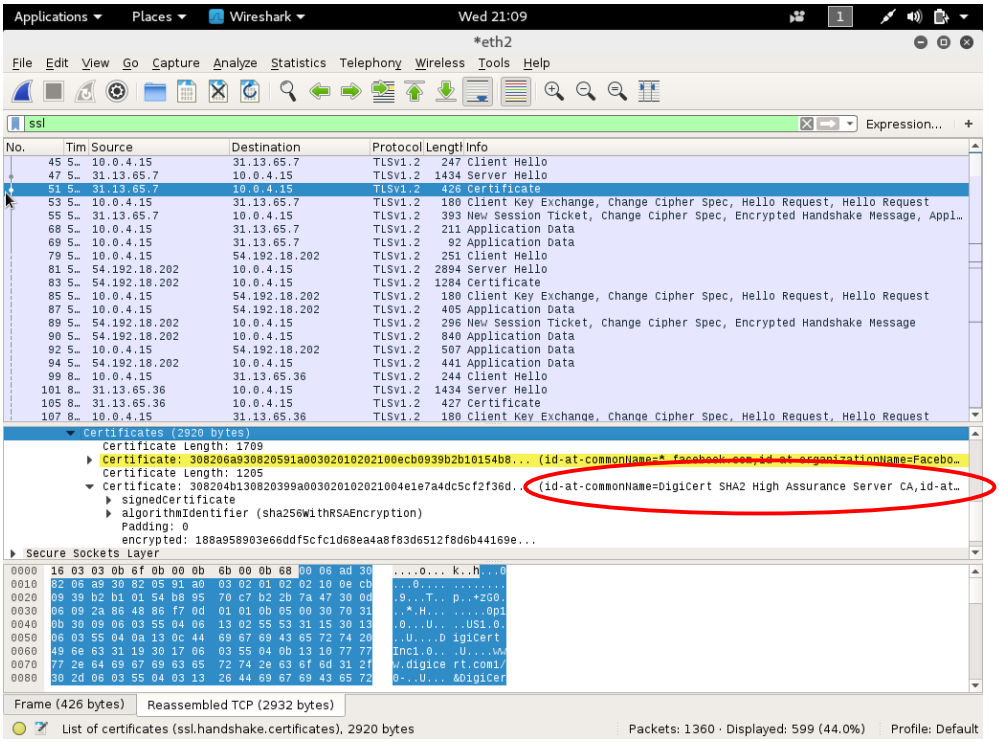


* In this SSL/TLS handshake, the server did not request a client certificate.

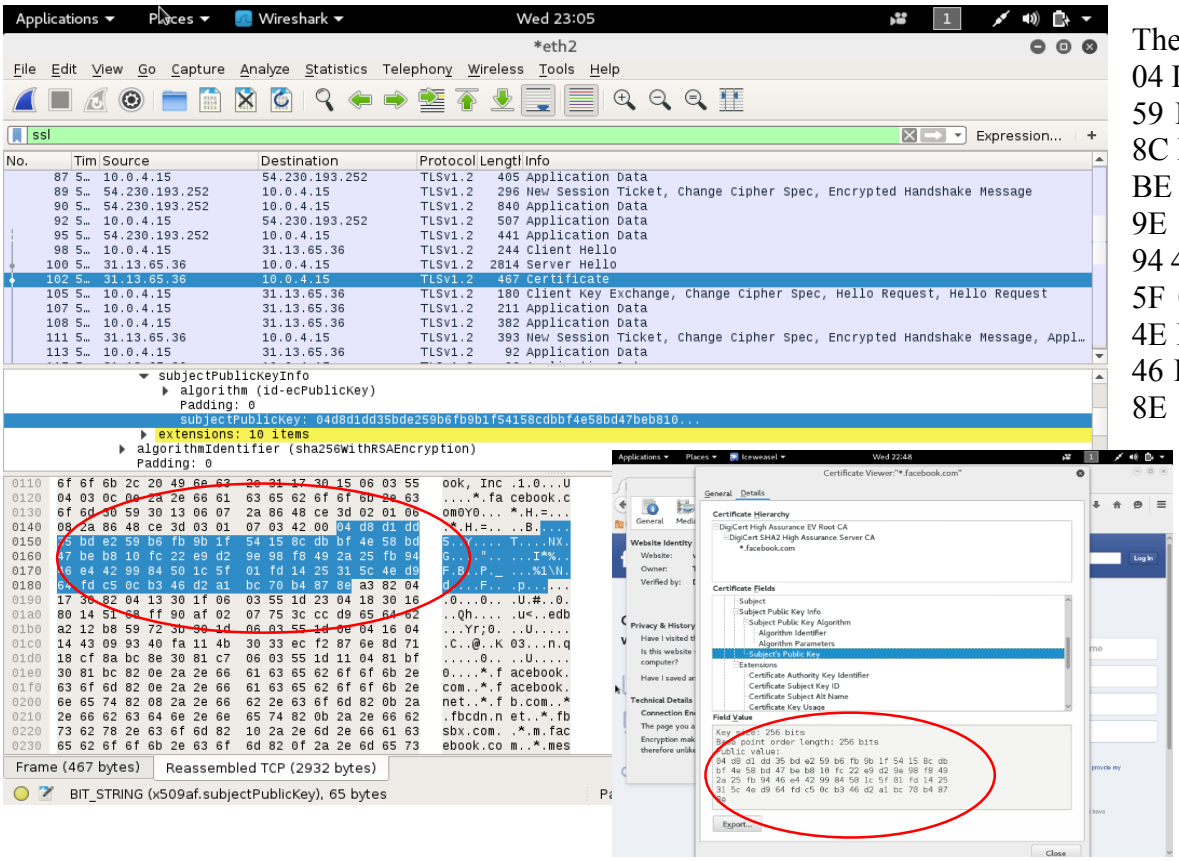


- Which organization(s) issued the certificate of the web server? [1 point]

The certificate was used by DigiCert



- What is the public RSA key of the web server? [1 point]



The public RSA key is: 04 D8 D1 DD 35 BD E2 59 B6 FB 9B 1F 54 15 8C DB BF 4E 58 BD 47 BE B8 10 FC 22 E9 D2 9E 98 F8 49 2A 25 FB 94 46 E4 42 99 84 50 1C 5F 01 FD 14 25 31 5C 4E D9 64 FD C5 0C B3 46 D2 A1 BC 70 B4 87 8E

- If the client (your browser) cannot verify the validity of a remote server's certificate and you choose to trust it anyway, what security properties do you lose? [1 point]

If you choose to trust it, you lose the property of confidentiality and authenticity. This is because, when we cannot verify the validity, it means that the server is not who it says it is. The authenticity of the server is now lost. Some adversary could be posing as the server and this is why their certificate could not be verified. Also, if we choose to trust it and send it all of our login information like username and passwords and other bank information if the site is a banking website or a purchasing website, we could lose all of our information. So the property of confidentiality is also lost. [13]

nmap Security Scanner (4 points)

In this section, you are given two pcap files that contain packets of nmap port scanning traffic. Use Wireshark (or other tools that can view .pcap files) to analyze the network traffic and answer the following questions.

What to submit:

scan_1.pcap file

- What is the IP address of the scanner? [0.25 point]

IP address of the scanner is 192.168.0.9

- What is the IP address of the target? [0.25 point]

IP address of the target is 192.168.0.99

- Which ports were scanned? (Hint: how were they chosen?) [0.25 point]

The ports within the range of 1 to 1024 were randomly scanned

- Which port scanning technique was used? Please justify your answer and describe how the technique works. [0.25 point]

The technique used differentiates between open and closed ports, if the port state is closed it causes a RST to be sent in response to the FIN. The technique used was Xmas scan (-sX). The TCP XMAS scan is used to identify listening ports on the targeted system. The scan manipulates the URG, PSH and FIN flags of the TCP header. If the port is closed on the targeted system, the target will send an RST. If the port is open, the port will ignore the packets [14].

- What is the command and arguments for this scan? Your answer should be what you would type into the shell, e.g. nmap -sT -p443 127.0.0.1. [0.25 point]

nmap –sX –p [-1024] 192.168.0.99

scan_2.pcap file

- What is the IP address of the scanner? [0.25 point]

IP address of the scanner is 192.168.0.9 (additionally, the scanner is posing as 192.168.0.1, 192.168.0.254 and 192.168.0.199 to hide its identity)

- What is the IP address of the target? [0.25 point]

IP address of the target is 192.168.0.99

- Which ports were scanned? (Hint: how were they chosen?) [0.25 point]

The most common 1,000 ports of the nmap-services file with frequency information were randomly scanned.

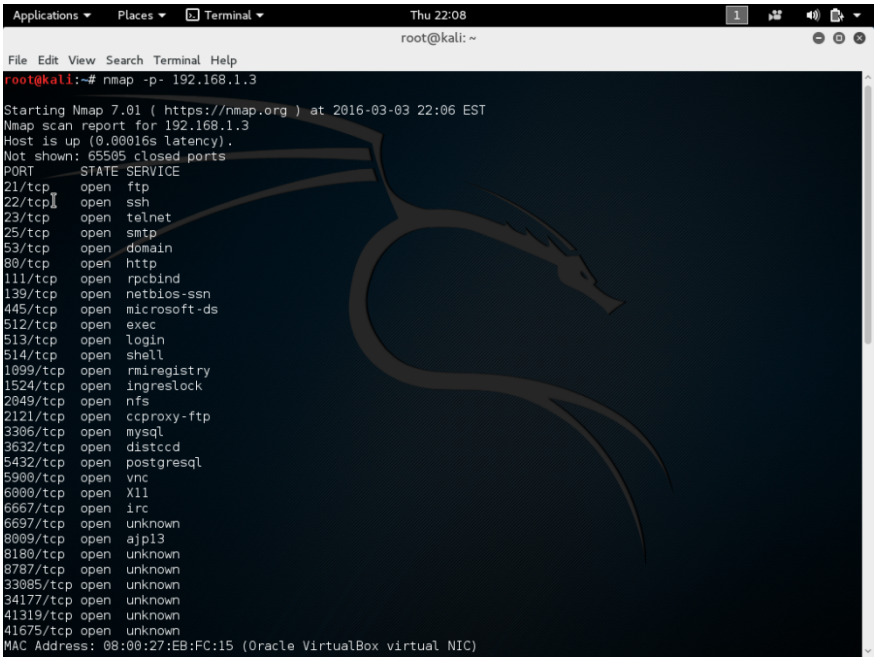
- Which port scanning technique was used? Please justify your answer and describe how the technique works. [0.25 point]

The technique used was the same as in the scan_1.pcap file, the Xmas scan (-sX). However uses an option to cloak a scan with decoys. Decoys make it appear to the remote host that the hosts specified as decoys are scanning the target network too. It is an effective technique for hiding the scanner's IP address. [14]

- What is the command and arguments for this scan? Your answer should be what you would type into the shell, e.g. nmap -sT -p443 127.0.0.1. [0.25 point]

nmap –sX –D 192.168.0.1, 192.168.0.254, 192.168.0.199 192.168.0.99

- Submit the output of a full port TCP SYN scan on across the first network (network1) by running the following command on Kali (scanning Metasploit): nmap –p– 192.168.1.3 [0.5 point]



- Research nmap's different scan techniques. It performs the SYN scan (sS) by default. Why? [0.5 point]

The SYN scan (sS) is the default scan option because it can be performed quickly, scanning thousands of ports per second on a fast network not hampered by restrictive firewalls. It is also relatively unobtrusive and stealthy since it never completes TCP connections (it just sends a SYN packet and waits for a response). It also allows clear, reliable differentiation between the open, closed, and filtered states. [15]

- Choose one other scan technique (i.e. sF, sA, etc.) and discuss its advantages and disadvantages. [0.5 point]

ACK Scan (-sA): It is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered. This scan type sends ACK packets to a host, if an RST comes back, the port is classified "unfiltered", if nothing comes back, the port is said to be "filtered". An ACK scan will never show ports in the "open" state, and so it should be used in conjunction with another scan type to gain more information about firewalls or packet filters.[16]

Advantages: Since the ACK scan does not open any application sessions, the conversation between nmap and the remote device is relatively simple. This scan of a single port is discreet and almost invisible when combined with the other network traffic. [16]

Disadvantages: Since it never tries to connect to a remote device, it can never identify an open port. [16]

iptables Firewall (4 Points)

In this section, you will configure the iptables firewall on your Metasploitable VM and test your settings with Kali Linux.

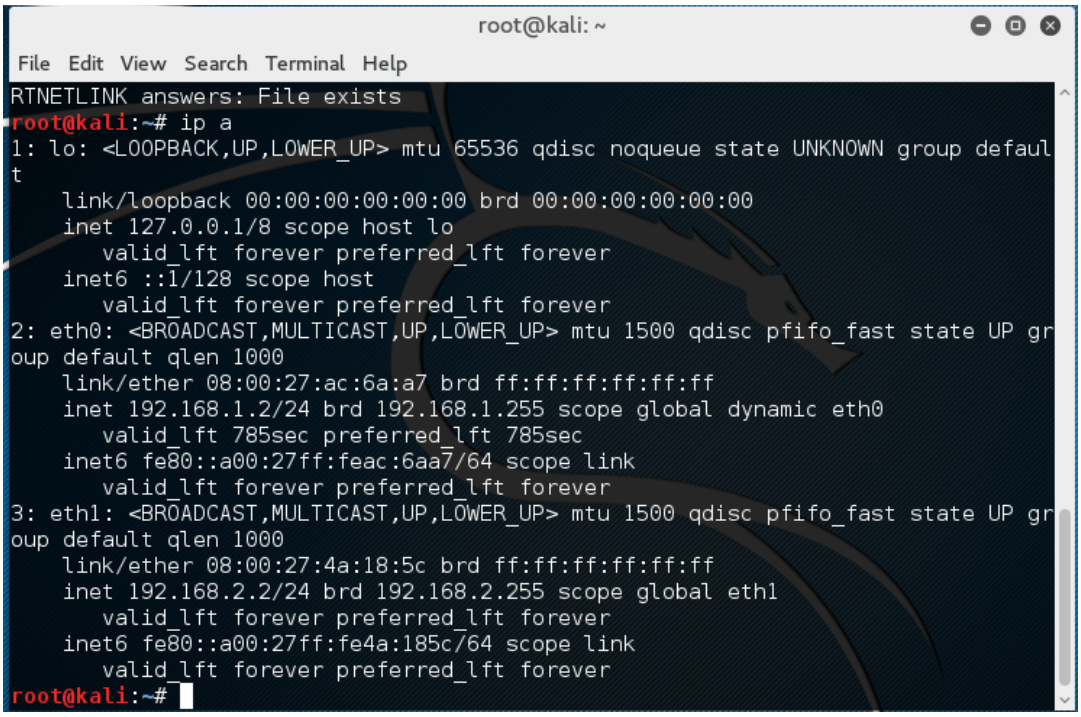
What to submit:

Your task is to configure iptables inside Metasploit with the following settings:

- ✓ Only allow SSH connections from the second (192.168.2.0/24) network
- ✓ Drop all other connections
- ✓ Change the default policy of the FORWARD chain to DROP.

- Provide screenshots of the command '$ ip a' inside of both Kali Linux and Metasploitable to show that the network interfaces are configured correctly. [0.5 point]

'$ ip a' inside Kali:



'$ ip a' inside Metasploitable:

- Provide a screenshot of your final iptables configuration in Metasploitable with the following command: '$ sudo iptables -L' [0.5 point]

'$ sudo iptables -L' inside Metasploitable:

```
msfadmin@metasploitable:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  192.168.2.0/24       anywhere            tcp dpt:ssh state N
EW,ESTABLISHED
REJECT     all  --  anywhere             anywhere            reject-with icmp-po
rt-unreachable

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere            tcp spt:ssh state E
STABLISHED
msfadmin@metasploitable:~$ _
```

Run a basic nmap scan against Metasploitable using both networks (i.e., scan both 192.168.1.3 and 192.168.2.3). The first should return no open ports (they should be all filtered), and the second should return port 22 (SSH) as being open.

```
root@kali:~# nmap -p- 192.168.1.3

Starting Nmap 7.01 ( https://nmap.org ) at 2016-03-04 09:11 EST
Nmap scan report for 192.168.1.3
Host is up (0.00055s latency).
All 65535 scanned ports on 192.168.1.3 are filtered
MAC Address: 08:00:27:EB:FC:15 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 159.64 seconds
root@kali:~#
```

```
root@kali:~# nmap -p- 192.168.2.3

Starting Nmap 7.01 ( https://nmap.org ) at 2016-03-04 09:11 EST
Nmap scan report for 192.168.2.3
Host is up (0.00068s latency).
Not shown: 65534 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 08:00:27:06:F0:8B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 159.74 seconds
root@kali:~#
```

- Is it possible to configure a firewall to block nmap scans, but allow legitimate traffic? Why or why not? [1 point]

It is not possible to configure a firewall to block nmap scans. If you create a firewall that blocks all nmap scans, then it has to be so strict that even legitimate traffic cannot pass through your firewall and the whole purpose of a firewall is lost. The philosophy behind this comes from the fact that you cannot deny your presence on the internet. Firewalls can block or allow broad generic classes of traffic. In this case, nmap can sneak packets which look like legitimate traffic past the firewall. So the only way to block nmap scans is to block all incoming traffic. But then this will not allow legitimate traffic to pass through.

- iptables can be configured to either REJECT or DROP unwanted packets. DROP simply ignores the packet. What does REJECT do? Can you think of any circumstances where it might be better to use REJECT? [1 point]

The REJECT target works basically the same as the DROP target, it prohibits a packet from passing, but it also sends back an error message to the host sending the packet that was blocked (an ICMP destination-unreachable back to the source host). REJECT should be used when we want the other end to know the port is unreachable or the connection has failed after one round-trip time. [17]

- Is a firewall alone sufficient to protect a network? Why or why not? [1 point]

A firewall alone is not enough to protect a network. Firewalls, like locks and walls, only create barriers that reduce the likelihood of someone trying to break-in into the system, they are intended for controlling incoming and outgoing network traffic. However, firewalls lack of any anomaly-detection capabilities, which means they cannot recognize when valid protocols are being used as an attack vehicle, and cannot separate legitimate traffic from malicious traffic. Firewalls are only the first line of defense, a further addition to the range of security is the Intrusion Detection System (IDS) that reports anomalous situations to the system administrator. [18]

REFERENCES

[1] https://www.wireshark.org/
[2] https://en.wikipedia.org/wiki/Wireshark
[3] https://technet.microsoft.com/en-us/library/bb962025.aspx
[4] http://www.exa.unicen.edu.ar/catedras/comdat1/material/TP1-Ejercicio5-ingles.pdf
[5] http://www.tutorialspoint.com/data_communication_computer_network/application_protocols.htm
[6] https://technet.microsoft.com/en-us/library/cc961401.aspx
[7] https://es.wikipedia.org/wiki/Traceroute
[8] http://www.computerhope.com/unix/uwhois.htm
[9] http://www.veracode.com/security/cache-poisoning

[10] http://www.networkworld.com/article/2277316/tech-primers/how-dns-cache-poisoning-works.html
[11] https://en.wikipedia.org/wiki/DNS_spoofing
[12] https://www.instantssl.com/https-tutorials/what-is-https.html
[13] http://www.websense.com/content/support/library/web/hosted/admin_guide/wd_bypass_certif_verif.aspx
[14] https://nmap.org/book/man-port-scanning-techniques.html
[15] https://nmap.org/bennieston-tutorial/
[16] http://www.networkuptime.com/nmap/page3-12.shtml
[17] http://www.chiark.greenend.org.uk/~peterb/network/drop-vs-reject
[18] https://technet.microsoft.com/en-us/library/cc700820.aspx