LAB Assignment 2

Secure Network Communications

NETSEC

Spring 2020

2020-03-10

Submitted by:

Ranjana Ghimire, Justas Narusas, Efstathios Psyllakis

Group 221

MAC ADDRESS:

2 Traffic Interception in Local Area Networks

Question 1

Write down three examples of network protocols that operate in a clear-text manner with no inherent protection and very briefly describe what they are used for.

Some protocols which work in clear-text manners are FTP,TELNET,HTTP,SMTP,SNMP.

- **HTTP**
  HTTP is an underlying protocol used to transfer data over the web. Because of its clear-text manner, it can expose username and passwords in web mail as well as store user information in cookies.
- **FTP**
  FTP is used to upload and download files between 2 hosts.
- **SMTP**
  SMTP is used to deliver email from one email server to another.

2.1 Question 1

What do you see in your VM? Is there a difference when using HTTP and HTTPS?

The HTTP websites “msn.com”, “scratchpads.eu” were broadcasted on driftnet compared to HTTPS which they were not because HTTPS is an encrypted connection.
HTTPS uses TLS(SSL) to encrypt the normal HTTP protocol (“Why is HTTP not secure?,” n.d.).

2.2 Question 3

Do you get the same results as previously? Explain your results

We had completely different results as there was no output on driftnet with regard to HTTP sites.

2.4 Question 4

What is the MAC address registered for the default gateway of the ‘Windows7’ VM? Does this MAC belong to one of your group’s machines?

10.11.200.1 = default gateway MAC 00-0e-0c-64-be-50
No, it does not belong.

2.5 Question 5

What is the MAC address associated with the default gateway of the system now? Which is the device that is the real owner of this MAC address?

IP 10.11.200.1 MAC: 08-00-27-18-21-21
The Kali device is the real owner of this MAC address.

2.5 Question 6

Can the 'Windows7' VM communicate with other hosts on the internet (e.g. browsing popular websites)? Add a 'LinuxClient' VM to your topology. Is the 'Windows7' VM able to communicate with other hosts in the same network? Explain why or why not for both questions.

Windows cannot communicate with other hosts on the internet, such as "google.com", because of the arp command the original MAC address is changed and as a result, network availability problems occur. Yes, we used the ping command on Windows, and we were able to communicate with LinuxClient.

2.5 Question 7

Can you perform an arp poisoning attack against the LinuxClient VM? Why or why not?

There was no denial of service observed compared to Windows machines and we could browse on google.

Does Linux behave differently than Windows when it comes to gratuitous ARP replies?

In the case of Linux, the ARPtable will get updated in cases for gratuitous arp frames even if the APR table already has an entry.

2.6 Question 8

Examine the captured packets (both IP and MAC address protocol header fields) and describe the actual path that the "request" packet followed. For easier examination apply the Wireshark filter 'Issue a single piip.src == '

The ping command does not work because of DSV's firewall.

2.6 Question 9

Does the Eve ('Kali 1') VM also capture the reply packets? Why or why not?

It does not capture the reply packets due to DSV's firewall setting as in Question 8.

2.6 Question 10

Use the command 'tracert' in the 'Windows7' VM to enumerate the intermediate nodes between the VM and a public IP address (e.g. tracert –d 8.8.8.8). Examine the command output along with the captured packets in Wireshark. Do you notice anything interesting in the results? Can you explain it based on how the 'tracert' command operates?

Tracert sends multiple requests to the destination. We cannot perform this command properly because DSV's Firewall blocks the connection.

2.7 Question 11

What message appears in the victim's browser?

"The connection was reset. The connection to the server was reset while the page was loading."

2.8 Question 12

Can the attacker extract the user credentials from the intercepted request? How can this be accomplished?

Yes, the credentials could be extracted but not from the request. It can be accomplished by searching the HTTP history and checking for the response.

2.9 Question 13

Which HTTP query parameter did you modify?

We modified the GET query.

2.10 Question 14

Provide a screenshot of the modified web page the user received and a short comment on what you have changed.

We managed to remove some <div></div> that included images in the HTML.

3 Symmetric Encryption - Block Ciphers

3.3 Question 1

What can be considered as the secret key of the ROT13 cipher? Does this cipher use substitution or transposition as an encryption technique? Based only on the intercepted known ciphertext, is the attacker capable of retrieving the plaintext and if yes, how?

The part of the command given “tr a-mn-zA-MN-Z n-za-mN-ZA-M >“ can be considered as the secret key. The Substitution encryption technique is used, and the plain text can be retrieved with a Brute force attack.

3.4 Question 2

What is the size of the generated key? Can you identify and describe any security weaknesses with the above approach?

The size of the generated key is 32 bits. The major weakness of this technique is the way that the encryption key will be shared across Bob and Alice without being intercepted.

3.5 Question 3

How many attempts are needed at most and on average to break the employed encryption assuming no knowledge of the symmetric key? (If you have a book, please refer to it)

The attacker at most has to try 4.3 x 10^9 alternative keys by performing a brute-force attack in order to break the encryption and on average half of this number as long as our key length is 32bits (Stallings, 2011).

4 Message Integrity

4.1 Question 1

What are the hash values of the file? What are the hash algorithms' output sizes? Briefly explain why a larger output size of a hash algorithm is preferable.

MD5 - d41d8cd98f00b204e9800998ecf8427e - 32
SHA1 - da39a3ee5e6b4b0d3255bfef95601890afd80709 - 40

4.3 Question 2

Does the above method of sending the hash value in plain form guarantee the integrity of the file? Can the attacker, in theory, modify the file and still be accepted by the server and how?

No, it does not guarantee the integrity of the file. The attacker can modify the file as long as he has access to the hash value in plain. He could use it to decrypt the message, modify it, encrypt it again and then resend it.

5 Public Key Cryptography

5.1 Question 1

What is the public exponent used (in this case)? What does it mean?

The public exponent is 65537 (0x10001).

5.1 Question 3

Is there any security concern with respect to the generated file that contains the key pair? Hint: Type: $ openssl genrsa –help // for examining other available parameters when creating it

One of the parameters of openssl genrsa is '-out' which means to output the key to a file. If this file falls under the non-trusted party, then it poses a security risk.

5.2 Question 4

Which of the security qualities in the CIA triad are protected with the above scheme / performed steps?

The above steps secure the confidentiality of the information. Integrity cannot be guaranteed until hash values are generated and availability is limited to confidential personnel with decrypting keys.

5.2 Question 5

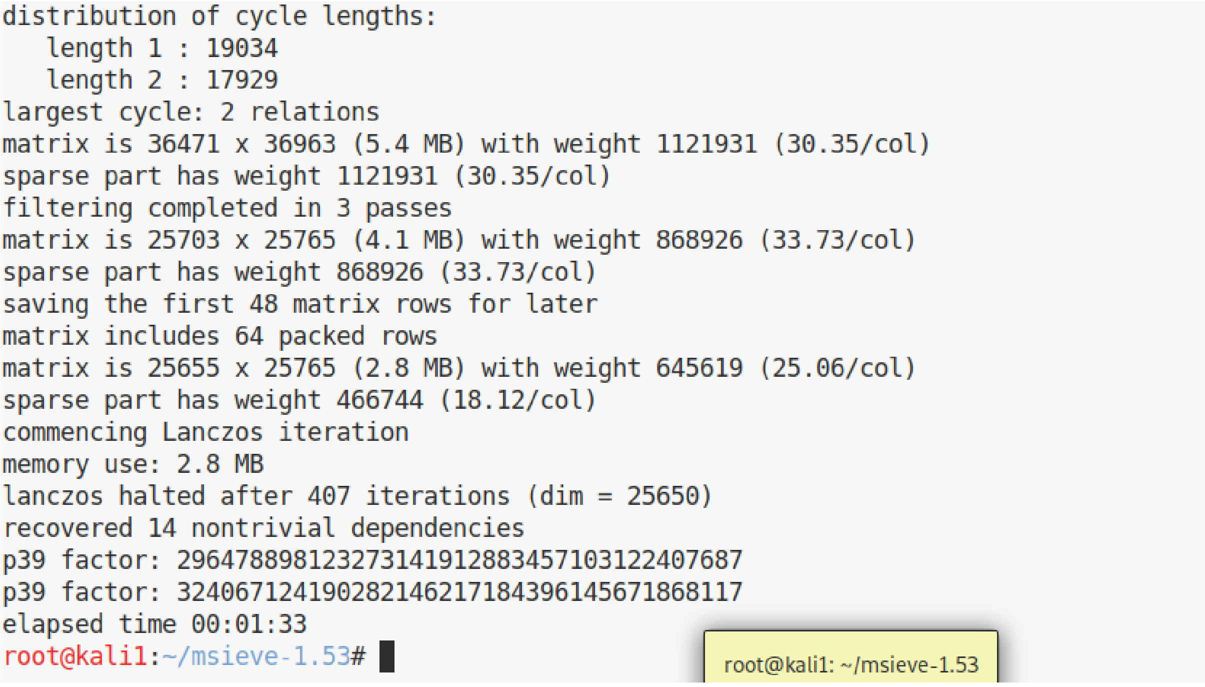
How can the intercepting host mount a Man in the Middle attack so as to be able to decrypt the encrypted transmitted message? Describe briefly the steps that need to be performed on the intercepting host.

It can happen mainly by intercepting the communication and sending to Alice the malkey generated by the host.
The steps are as follows:

I. The key is generated in a Linux server and placed in a common folder.
II. The key is copied in Alice's client, but before Alice copies the key, another client 'B' copies the key from step I and places its key there
III. Then client B waits for Alice to create a file and put it in a shared folder and when that happens, Client B copies the encrypted file and decrypts with its own key. And in order not to let Linux servers have any idea about it, it creates its own encrypted file using the key of Linux server and places it in a shared folder.
IV. Alice does not know if her file reached the Linux server.
V. Linux server does not know if this is Alice's file
VI. And Client B has now the encrypted file from Alice which he can easily decrypt with his own key.

5.3 Question 6

What are the prime factors of the server's modulus?



```
distribution of cycle lengths:
   length 1 : 19034
   length 2 : 17929
largest cycle: 2 relations
matrix is 36471 x 36963 (5.4 MB) with weight 1121931 (30.35/col)
sparse part has weight 1121931 (30.35/col)
filtering completed in 3 passes
matrix is 25703 x 25765 (4.1 MB) with weight 868926 (33.73/col)
sparse part has weight 868926 (33.73/col)
saving the first 48 matrix rows for later
matrix includes 64 packed rows
matrix is 25655 x 25765 (2.8 MB) with weight 645619 (25.06/col)
sparse part has weight 466744 (18.12/col)
commencing Lanczos iteration
memory use: 2.8 MB
lanczos halted after 407 iterations (dim = 25650)
recovered 14 nontrivial dependencies
p39 factor: 296478898123273141912883457103122407687
p39 factor: 324067124190282146217184396145671868117
elapsed time 00:01:33
root@kali1:~/msieve-1.53# 
```

5.4 Question 7

Having possession of the server's private key, what is the attacker capable of? How can this attack be mitigated by the server?

Having the possession of the server's private key, the attacker is capable of decrypting all the encrypted files of the Linux server as well as sending by encrypted files without knowledge of the server. This can be mitigated by following the process of asymmetric encryption rather than symmetric.

7 Public Key Cryptography - Digital Certificates

7.2 Question 1

What information is contained in a digital certificate request? Why are CSRs digitally signed, and who signs them?

Consists data version, subject, subject public key info, public key algorithm, public key, modulus, exponent, attributes, signature algorithm. CSRs are signed by a digital Certificate Authority, so as to prove the identity of the third party, but in this case, we signed it in the LinuxServer to prove our identity in the web server.

7.2 Question 2

Does a self-signed certificate provide the same security guarantees as a digital certificate signed by a trusted CA? Can you think of a case where a self-signed certificate can be acceptable to use?

The self-signed certificate does not provide the same security guarantees as a digital certificate signed by a trusted CA because it can be modified or generated by a non-trust third party and be used with malicious intent.

7.3 Question 3

Explain briefly why a certificate should have a validity period (e.g. –days 365).

The self-signed certificate can be installed on the web server (Apache2) so as to be able to serve the web pages over an SSL-protected communication channel.
A certificate needs to have a validity period in order to verify if the server is what it says in the certificate and if not then the new certificate needs to be setup after the validity expires. Just like our passport, our passport expires within certain years and after that we need to prove our new validity and get a recent picture for a new passport. Similarly, the renewed certificate will have new information about the server ("Why Do SSL Certificates Expire?," 2016).

7.5 Question 4

What data about the certificate holder does the certificate contain?

- Subject
- Serial Number
- Issuer
- Valid From
- Valid To
- Public Key
- Signature Algorithm
- Signature Value

7.5 Question 5

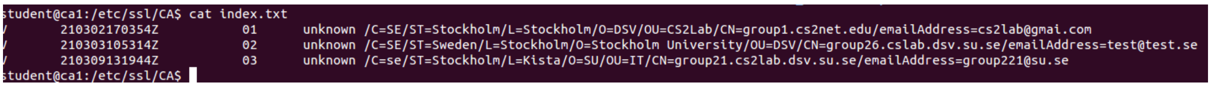
What security risks exist if the certificate is accepted by the user?

If a certificate is not signed by a CA and is accepted, then it means that the user has given “an open door” for the attacker in order to perform an attack.

8 Public Key Infrastructure - Certificate Authority

8.3 Question 2

Examine the contents of the index.txt under the '/etc/ssl/CA/. What is the status and the serial of the newly generated certificate?



```
student@ca1:/etc/ssl/CA$ cat index.txt
V       210302170354Z           01      unknown /C=SE/ST=Stockholm/L=Stockholm/O=DSV/OU=CS2Lab/CN=group1.cs2net.edu/emailAddress=cs2lab@gmai.com
V       210303105314Z           02      unknown /C=SE/ST=Sweden/L=Stockholm/O=Stockholm University/OU=DSV/CN=group26.cslab.dsv.su.se/emailAddress=test@test.se
V       210309131944Z           03      unknown /C=se/ST=Stockholm/L=Kista/O=SU/OU=IT/CN=group21.cs2lab.dsv.su.se/emailAddress=group221@su.se
student@ca1:/etc/ssl/CA$
```

8.5 Question 3

Is it a good practice for the root CA to sign digital certificates directly for end users/servers?

As it is stated in the "*Common issues file"* of the course:

"It is definitely not a good idea for a root CA to directly sign end-user certificates. If the root CA's private key somehow got compromised, all the end-user certificates would have to be revoked and new certificates re-issued. It is better to spread the attack surface by having several intermediate CAs, so that if one intermediate CA is compromised the root CA and the other intermediate CAs are not affected. This, of course, does increase the number of entities needed to trust. We trust the root CA, and it in turn says that it trusts the intermediate CAs, and they in turn say that they trust the end users (which in this case are the web servers)."

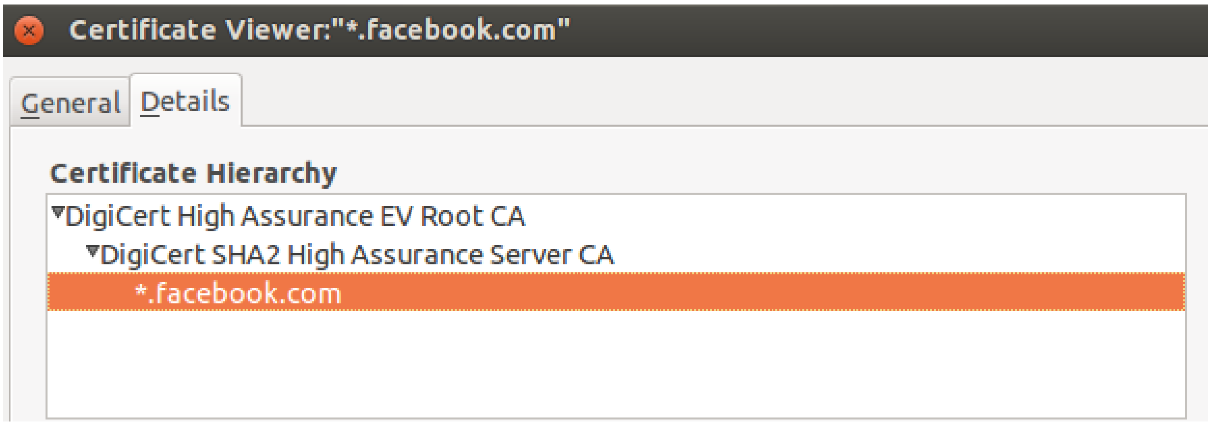
8.6 Question 4

Does Firefox prompt you with a security warning? Why or why not?

No, because the certificate is valid and properly uploaded in Firefox.

8.6 Question 5

Visit any SSL-protected Web page on the Internet (not the web page used in this lab) and provide a screenshot of their certificate hierarchy.



DigiCert High Assurance EV Root CA
  DigiCert SHA2 High Assurance Server CA
    *.facebook.com

9 Public Key Infrastructure - Certificate Revocation

9.1 Question 1

What is the URL of the OCSP server?

OCSP - URI:http://10.11.200.246:8888

9.2 Question 2

What is the error message that Firefox displays on Alice ('LinuxClient') when trying to access the SSL-protected webpage of Bob?

We get a reply:
Secure Connection Failed when trying to access Bob's webpage from Alice's Firefox.

9.2 Question 3

In the case that online connectivity to an OCSP server cannot be established due to various system constraints (e.g. an offline point-of-sale system) how else can the CA inform Alice about Bob's revoked certificate.

We can do a centralized collection of certificates, make sure revoke is performed and push it to Firefox to make the loading of the page sooner.

References

Stallings, W., 2011. Network security essentials: applications and standards, 4th ed. ed. Prentice Hall, Boston.

Why Do SSL Certificates Expire?, 2016. . Hashed SSL Store^{TM}. URL https://www.thesslstore.com/blog/ssl-certificates-expire/ (accessed 3.11.20).

Why is HTTP not secure? | HTTP vs. HTTPS [WWW Document], n.d. . Cloudflare. URL https://www.cloudflare.com/learning/ssl/why-is-http-not-secure/ (accessed 3.11.20).