

Assignment Two

by

Alan Hubbard

S326012

for

Dr Bharanidharan Shanmugam

HIT333 Cyber Security

PART B - TASK 1

Download “smb3-aes-128-ccm.pcap” from the following link

https://wiki.wireshark.org/SampleCaptures#SMB3_encryption. Analyse the pcap file using wireshark and list down all information you can read from the packets. (05 marks)

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.160.64.139	10.160.65.202	SMB2	172	Negotiate Protocol Request
2	0.000356	10.160.65.202	10.160.64.139	SMB2	318	Negotiate Protocol Response
3	0.007518	10.160.64.139	10.160.65.202	SMB2	190	Session Setup Request, NTLMSSP_NEGOTIATE
4	0.007801	10.160.65.202	10.160.64.139	SMB2	318	Session Setup Response, Error: STATUS_MORE_PROCE
5	0.012641	10.160.64.139	10.160.65.202	SMB2	430	Session Setup Request, NTLMSSP_AUTH, User: SUSE
6	0.013995	10.160.65.202	10.160.64.139	SMB2	142	Session Setup Response
7	0.020596	10.160.64.139	10.160.65.202	SMB2	180	Tree Connect Request Tree: \\WS2016\encrypted
8	0.020693	10.160.65.202	10.160.64.139	SMB2	150	Tree Connect Response
9	0.024612	10.160.64.139	10.160.65.202	SMB2	268	Encrypted SMB3

Frame 1: 172 bytes on wire (1376 bits), 172 bytes captured (1376 bits) on interface unknown, id 0
 Ethernet II, Src: Xensourc_44:52:5c (00:16:3e:44:52:5c), Dst: RealtekU_e8:f0:9a (52:54:00:e8:f0:9a)
 Internet Protocol Version 4, Src: 10.160.64.139, Dst: 10.160.65.202
 Transmission Control Protocol, Src Port: 38166, Dst Port: 445, Seq: 1, Ack: 1, Len: 106
 NetBIOS Session Service
 SMB2 (Server Message Block Protocol version 2)

First and second frame “Negotiate Protocol Request” and “Response” is used to negotiate the protocol version and the server provides a valid a list of authentication methods

6	0.013995	10.160.65.202	10.160.64.139	SMB2	142	Session Setup Response
7	0.020596	10.160.64.139	10.160.65.202	SMB2	180	Tree Connect Request Tree: \\WS2016\encrypted
8	0.020693	10.160.65.202	10.160.64.139	SMB2	150	Tree Connect Response
9	0.024612	10.160.64.139	10.160.65.202	SMB2	268	Encrypted SMB3

Frame 6: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface unknown, id 0
 Ethernet II, Src: RealtekU_e8:f0:9a (52:54:00:e8:f0:9a), Dst: Xensourc_44:52:5c (00:16:3e:44:52:5c)
 Internet Protocol Version 4, Src: 10.160.65.202, Dst: 10.160.64.139
 Transmission Control Protocol, Src Port: 445, Dst Port: 38166, Seq: 505, Ack: 595, Len: 76
 Source Port: 445
 Destination Port: 38166
 [Stream index: 0]
 [Conversation completeness: Incomplete (8)]
 [TCP Segment Len: 76]
 Sequence Number: 505 (relative sequence number)
 Sequence Number (raw): 1517249317
 [Next Sequence Number: 581 (relative sequence number)]
 Acknowledgment Number: 595 (relative ack number)
 Acknowledgment number (raw): 743360153
 1000 = Header Length: 32 bytes (8)
 Flags: 0x018 (PSH, ACK)
 Window: 8233
 [Calculated window size: 8233]
 [Window size scaling factor: -1 (unknown)]
 Checksum: 0x713b [unverified]
 [Checksum Status: Unverified]
 Urgent Pointer: 0
 Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
 TCP Option - No-Operation (NOP)
 TCP Option - No-Operation (NOP)
 TCP Option - Timestamps: TSval 162696628, TSecr 3180665814
 [Timestamps]
 [SEQ/ACK analysis]
 [This is an ACK to the segment in frame: 5]
 [The RTT to ACK the segment was: 0.001354000 seconds]
 [Bytes in flight: 76]

Frames 3 to 6 is setting up the session and frame 6 includes and ACK to frame 5.

7	0.020596	10.160.64.139	10.160.65.202	SMB2	180	Tree Connect Request Tree: \\WS2016\encrypted
8	0.020693	10.160.65.202	10.160.64.139	SMB2	150	Tree Connect Response
9	0.024612	10.160.64.139	10.160.65.202	SMB2	268	Encrypted SMB3

Frame 7: 180 bytes on wire (1440 bits), 180 bytes captured (1440 bits) on interface unknown, id 0
 Ethernet II, Src: Xensourc_44:52:5c (00:16:3e:44:52:5c), Dst: RealtekU_e8:f0:9a (52:54:00:e8:f0:9a)
 Internet Protocol Version 4, Src: 10.160.64.139, Dst: 10.160.65.202
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 166
 Identification: 0x1a0c (6892)
 Flags: 0x40, Don't fragment
 ... 0 0000 0000 0000 = Fragment Offset: 0
 Time to Live: 64
 Protocol: TCP (6)
 Header Checksum: 0x87d1 [validation disabled]
 [Header checksum status: Unverified]
 Source Address: 10.160.64.139
 Destination Address: 10.160.65.202
 Transmission Control Protocol, Src Port: 38166, Dst Port: 445, Seq: 595, Ack: 581, Len: 114
 Source Port: 38166
 Destination Port: 445
 [Stream index: 0]
 [Conversation completeness: Incomplete (8)]
 [TCP Segment Len: 114]
 Sequence Number: 595 (relative sequence number)
 Sequence Number (raw): 743360153
 [Next Sequence Number: 709 (relative sequence number)]
 Acknowledgment Number: 581 (relative ack number)
 Acknowledgment number (raw): 1517249393
 1000 = Header Length: 32 bytes (8)
 Flags: 0x018 (PSH, ACK)
 Window: 100

Frame 7 and 8 are paired as “Tree Connect Request” and “Tree Connect Response”. The TCP Src and Dst Ports are mirrored between each of the paired handshakes.

TASK 6

QR code has different vulnerabilities and it could easily exploit. With the help of www.grstuff.com explain how an attacker could use a QR code to direct a victim to a malicious website? **(05 marks)**

QR (Quick Response) Codes provide users the ability to quickly be redirected to sites or applications that they see, by using an inbuilt camera on an internet connected device. This is seen to meet the needs of many and the desire to quickly consume information or gain access, which has been met by the IT industry and wider markets.

However, due to the expedited nature of the link, personal device connection often overlooks tell-tale signs of malicious content. As the URL is not usually fully visible, cyber criminals can use QR Codes to direct users to malicious URLs, which may have been used in conjunction with phishing attacks. Further, to make QR Codes seem more attractive, they may also use legitimate advertisements and replace the QR Code with their own.

The methods to compromise a users’ device or personal information are similar to traditional attacks, such as unknowingly downloading malicious software (viruses, keyloggers, sniffing tools, etc) and redirection to malicious or inappropriate sites.

Methods to mitigating this risk include;

- confirming or verifying QR Code authenticity with other sources,
- visually checking legitimacy. This will require some familiarity with QR Codes.
- Verifying URLs security. I.e., HTTPS://

IEEE Computer Society. (19 October 2022) Risks of Using QR Codes,
<https://www.computer.org/publications/tech-news/trends/qr-code-risks>

G2. (21 April 2022) Are QR Codes Safe? Best Practices to Ensure QR Code Security
<https://learn.g2.com/qr-code-security>

TechTarget. (05 August 2022) Understanding QR code security issues for enterprise devices
<https://www.techtarget.com/Understanding-QR-code-security-issues>.

TASK 7

You can download the EXIF tool from <https://exiftool.org/>. You can select one model from the link (https://exiftool.org/sample_images.html) and use images and find any interesting information in the metadata. (Note: You can select only one For eg. Acer or Google etc., but you must analyse all the images using the EXIF tool) **(10 Marks)**

2 Files have only 29 lines of data output from EXIF tool. - AcerDX650.jpg and AcerX960.jpg
These same 2 files also have "Artists" in the metadata however the text was unreadable.
Also the two smallest files sizes.

Smallest File – 503 bytes

Largest – 39 kB

6 Files include a Warning: [minor] Unrecognized MakerNotes

AcerCP-8660.jpg

AcerCR8530.jpg

AcerCS6530.jpg

AcerCS6530.jpg

AcerCU-6530.jpg

AcerM900.jpg

File AcerE101.jpg contains GPS Positioning Data. The location is at a port in the Vasileostrovsky District, St Petersburg, Russia.

GPS Position: 59 deg 56' 49.96" N, 30 deg 11' 35.39" E

See attached excel file for full metadata extraction.

TASK 8

Based on your personal experiences or those of someone you know (you may have to interview other students or a friend), write a paragraph regarding a computer attack that occurred.

- When did it happen and what was the attack?
- What type of damage did it inflict?
- List the reason or reasons you think that the attack was successful.
- How was the computer fixed after the attack?
- What could have prevented it?

(05 Marks)

In 2019, a sporting club was the target of a deliberate attack to transfer funds from them. The spear phishing attack identified exploited a vulnerability within the banking system, where previous banking signatories were not removed from the account. They further exploited the dislocated nature of the committee which operated from different areas of the country.

False invoices were sent to the club treasurer and simultaneously contacted via sms, posing as the club president. The “president” claimed they were with a merchant awaiting the collection of goods, however, could not transfer the funds themselves, requiring the treasurer’s assistance. The appearance of haste and distress are likely to have aided in the success of the scammers.

The scammers were able to have over \$10 000 sent to them which ended up in an international bank account. Whilst the money was not recovered from the scammers, the amount was refunded by the banking institution.

Below is a summary email by the treasurer to the bank explaining the situation. Names of people, banks and other organisations have been removed for privacy.

Email:

“SPORTS club had two invoices sent to them for approx 7k each from a scammer. These were fake invoices with the money going to Nigeria via a BANK account. I paid \$10261.00 of the invoices until I became suspicious.

In February we changed the signatories with BANK, had two previous committee members removed from the account and requested dual authorisation for the 2 accounts. The two signatories were not removed with one logging in on the 25 April 2019.

If the dual signatory for internet banking had been in place as requested the likelihood of the false payments would have been detected at the time and thus the situation prevented.”

Whilst the attack was targeted and, through social exploitation, specific, the attack could have been prevented through better communication, safeguards, vigilance and diligence. The communication methods between the person posing as the president and the treasurer was one that does not allow suitable verification of the individual’s identity, therefore

cannot be relied upon. Further, confirmation that the approval to spend the funds was not done by the committee, as required.

By insisting that dual signatory verification was used by the bank account, more than one person would be required to verify the transaction, reducing the likelihood of a successful attack.

Finally, the lack of vigilance and diligence of the treasurer and committee to be wary of such attacks was the reason attacks such as this are successful.

TASK 9

VirusTotal, a subsidiary of Google, is a free online service that analyses files and URLs in order to identify potential malware. VirusTotal scans and detects any type of binary content, including a Windows executable program, Android, PDFs, and images. VirusTotal is designed to provide a “second opinion” on a file and URL that may have been flagged as suspicious by other AV software. In this task, you will use VirusTotal to scan a file and a URL. You can create a file or upload an existing file to check for malicious signatures. URL :

<https://www.virustotal.com/gui/home/upload>

(Note : You must check both file and an URL of your choice) **(05Marks)**

URL: <https://www.aliexpress.com/>

The first image capture is from a Google search redirected link which is why CMC Threat Intelligence may have flagged the URL as malicious. However, when the actual URL was used no flagged were returned.

Screenshot 1: Google Search URL Analysis

1 / 90
1 security vendor flagged this URL as malicious

https://www.google.com/url?sa=t&ct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwLj7C5qy_6AhUD7TgGHV5JCUGQFnoECBIQAQ&url=https://www.aliexpress.com/&usq=AOvVaw3qyckisGlnhZvqba14hzKg

200 Status 2022-10-27 02:11:46 UTC a moment ago

multiple-redirects

Security Vendors' Analysis

CMC Threat Intelligence	Malicious	Abusix	Clean
Acronis	Clean	ADMINUS Labs	Clean
AICC (MONITORAPP)	Clean	AlienVault	Clean
alphaMountain.ai	Clean	Antiy-AVL	Clean
Artists Against 419	Clean	Avira	Clean

Screenshot 2: AliExpress URL Analysis

0 / 90
No security vendors flagged this URL as malicious

https://www.aliexpress.com/

200 Status 2022-10-27 00:00:06 UTC 2 hours ago

multiple-redirects

Security Vendors' Analysis

Abusix	Clean	Acronis	Clean
--------	-------	---------	-------

Class Work.pdf from HIT333 was added to VirusTotal for analysis. No Security Vendors could analyse the file, due to the password protection, however Zenbox did identify Mitre Tactics and Dropped Files.

0
/ 63

?

X Community Score ✓

✓ No security vendors and no sandboxes flagged this file as malicious

397530aabc79354866b5c6df463db11e4c841701571b98cc16fce8d944204f8
Class Work.pdf
autoaction pdf

7.46 KB
Size

2022-10-27 02:17:42 UTC
1 minute ago

DETECTIONDETAILSBEHAVIORCOMMUNITY

Security Vendors' Analysis ⓘ

Acronis (Static ML)	✓ Undetected	Ad-Aware	✓ Undetected
AhnLab-V3	✓ Undetected	ALYac	✓ Undetected
Anity-AVL	✓ Undetected	Arcabit	✓ Undetected
Avast	✓ Undetected	AVG	✓ Undetected

✓ Zenbox

⚠ 0 3 0 0 7 0

Activity Summary

Download Artifacts ▾ Full Reports ▾ Help ▾

⚠ Detections

NOT FOUND

📋 IDS Rules

NOT FOUND

📁 Dropped Files

1 TEXT

🏢 Mitre Signatures

4 INFO

🔍 Sigma Rules

NOT FOUND

🌐 Network comms

NOT FOUND

Mitre ATT&CK Tactics And Techniques ^

Privilege Escalation TA0004

Process Injection T1055

① Spawns processes

Defense Evasion TA0005

Masquerading T1036

① Creates files inside the user directory

Process Injection T1055

① Spawns processes