Assignment Two

by

Alan Hubbard

S326012

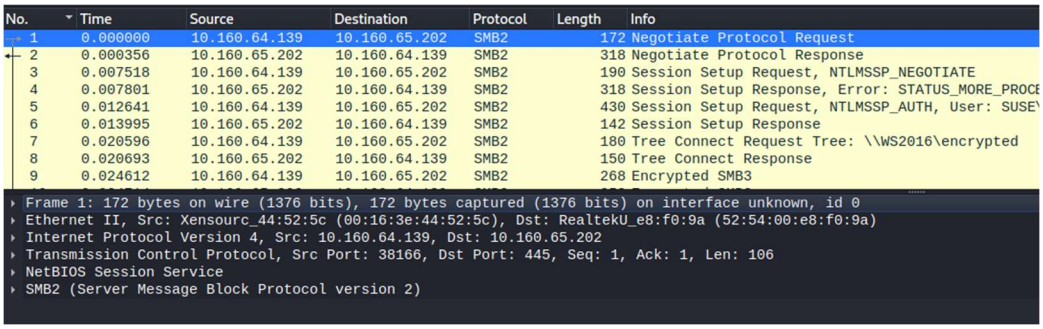
for

Dr Bharanidharan Shanmugam

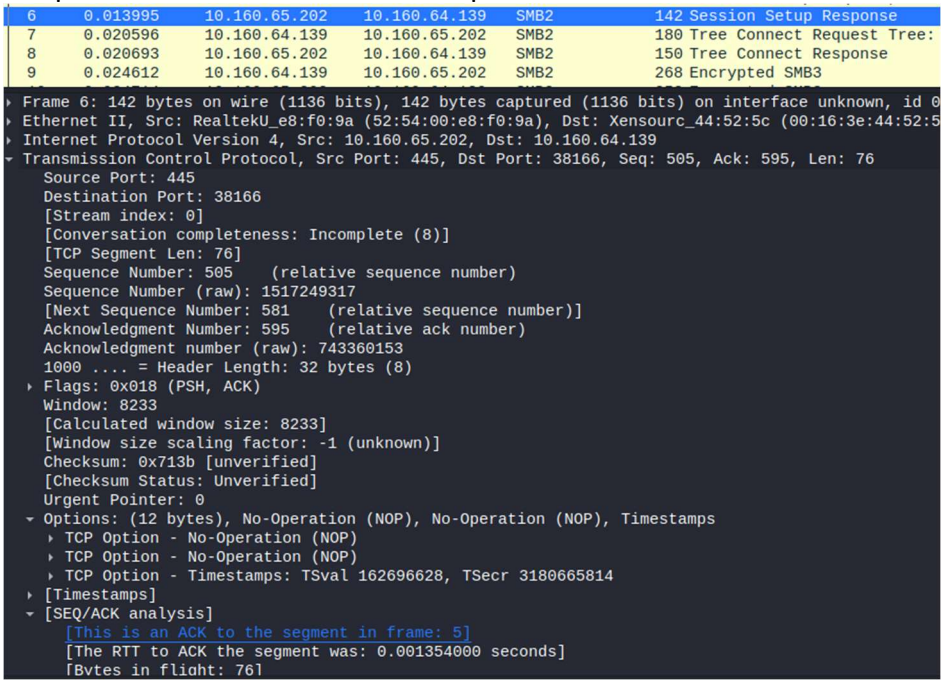
HIT333 Cyber Security

**PART B - TASK 1**

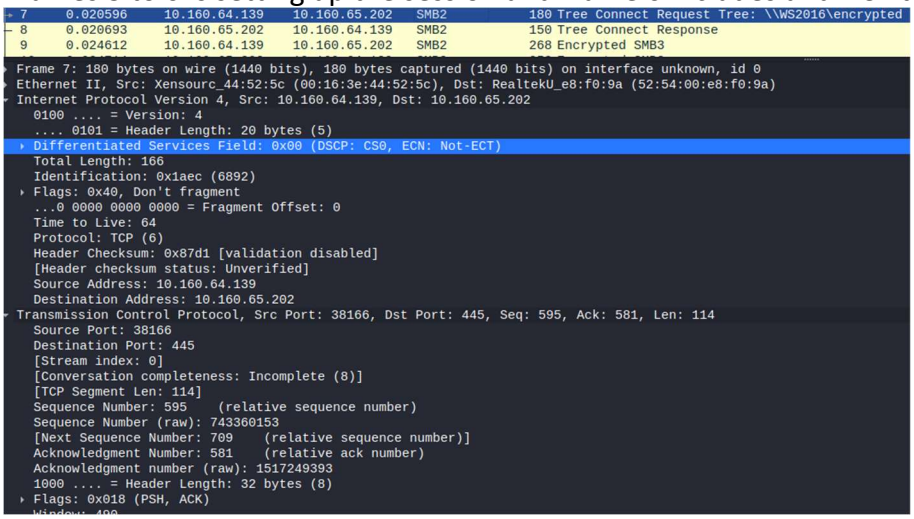
Download “smb3-aes-128-ccm.pcap” from the following link https://wiki.wireshark.org/SampleCaptures#SMB3_encryption. Analyse the pcap file using wireshark and list down all information you can read from the packets. **(05 marks)**




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




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



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.qrstuff.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 expeditated 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., HTTP**S**://

IEEE Computer Society. (19 October 2022) Risks of Using QRCodes, 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."

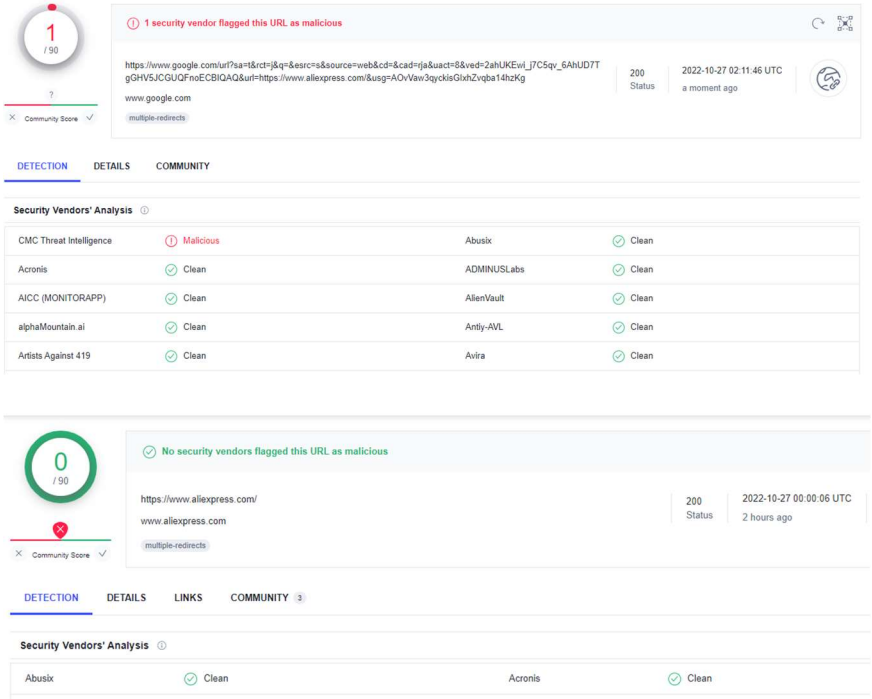
Whilst the attack was targeted and, through social exploitation, specific, the attack could have been prevented through better communication, safeguards, vigilance and diligence. The communication methods between the person posing as the president and the treasurer was one that does not allow suitable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

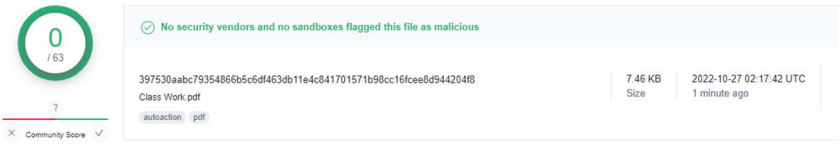
## TASK 9

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.




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.




DETECTION DETAILS BEHAVIOR COMMUNITY

**Security Vendors' Analysis**

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


## Activity Summary

Download Artifacts Full Reports Help

### Detections
NOT FOUND

### Mitre Signatures
4 INFO

### IDS Rules
NOT FOUND

### Sigma Rules
NOT FOUND

### Dropped Files
1 TEXT

### Network comms
NOT FOUND

### Mitre ATT&CK Tactics And Techniques

**Privilege Escalation** TA0004

Process Injection T1055
Spawns processes

**Defense Evasion** TA0005

Masquerading T1036
Creates files inside the user directory

Process Injection T1055
Spawns processes