Lab Work Portfolio

by

Team Struggle Bus

Donald MacKenzie(246230M) Kārlis Siders (2467273S) Khena Dungu(2462068D) Declan McBride(2399448M) Rishabh Mathur(2465899M) Lau Hok Yee(2551157L)

Week 1 Portfolio

Exercise 1: The Spanning Tree Protocol (STP) is being captured in this sample. It is a Layer 2 network protocol used in a local area network (LAN) to prevent problems like bridge loops and broadcast radiation in a network topology. No cyber-attack could be identified in this example.

Exercise 2: The protocol captured is the Address Resolution Protocol (ARP). It is a communication protocol used for discovering the MAC address of a device, by using its IP address. The results are stored in an ARP table, for easy address look-up. The communication is broadcast and a cyber attack can be seen in this example.

The attack is an **ARP Storm** because 622 ARP requests are sent in less than half a minute. This sample is likely to be provided from the attacking machine since all packets are ARP requests and there are no ARP replies. It suggests that the attacker is hiding their identity and replies are not being received to ensure all bandwidth is being used to continue the attack.

The MAC Address for every 'Sender' IP is the same. For every request, the sender is most likely to spoof an IP address and ask to be replied by the request to the spoofed address. As such, more than 600 ARP requests quickly build up an ARP table of incorrect data (same MAC address for many different IP addresses), filling up the buffer and causing the network to crash. This could also be a part of an ARP scan, which tries to find out as many IP addresses as there are in the network.

Exercise 3: Configuration Test Protocol/loopback (LOOP), Cisco Discovery Protocol (CDP), Domain Name System (DNS), Internet Protocol v4 (IPv4), User Datagram Protocol (UDP), Address Resolution Protocol (ARP) and Internet Control Message Protocol (ICMP) are being captured in this sample. For communication, LOOP is a layer 2 "ping" equivalent and uses Ethernet as its transport protocol. CDP is a Layer 2 protocol that enables networking applications to learn about directly connected devices nearby. DNS is the phonebook of the Internet by translating domain names to IP addresses for browsers to load Internet resources. IPv4 is the underlying technology to connect our devices to the web. A unique numerical IP address will be assigned when a device is connected to the Internet. UDP is a communication protocol between applications on the Internet especially for time-sensitive transmission by establishing low-latency and loss-tolerating connections. ARP is a communication protocol used for discovering the link layer address like a MAC address together with a known internet layer address, i.e., IPv4 address. ICMP is a network level protocol used by network devices to diagnose network communication issues.

Malformed information is caused by UDP length being longer than IP payload length. Thus, the cyber attack is a **Teardrop attack** (DoS). Data payload is fragmented and sent over but the size is bigger than expected because the IP fragments overlap. This overlap is caused by the fragment offset being 24 at frame 9, instead of 36, which is the payload of the first fragment at frame 8.

Week 2 Portfolio

Analysis of the Email
Content:

- Subject line lacks information
- Automated email: “Dear User” - non-personalised greeting is being used
- Grammar issues - “Glasgow Cyber Security team” should read “Glasgow Cyber Security Team”
- Email body is also lacking information and extremely generic, could mean anything
- No university branding in the email, entirely plain text

Link:

- Hovering over the link “www.gla.ac.uk/security.info” directs to www.digitalkingdomsecurity.com
- .info file extension is very rare
- If you manually direct your browser to gla.ac.uk/security.info, you hit a 404 error

Meta-data:

- Supposedly sent from the University, but sent to a non-organisation email address

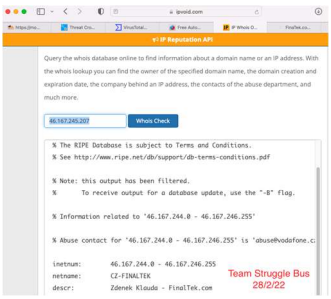
Conclusions:

- Potentially could be Clone phishing, but seems implausible an organisation would actually send an email so sparse of detail if members of the organisation were actually victims of a cyber attack.
- Not enough detail to be spear phishing.
- Could be whaling, but it’s impossible to know without more context about the receiver of the email.
- Not smishing - done through email.

Investigation with security tools:
IPVoid (www.ipvoid.com)
Introduction: A range of different tools available for analysis of URLs and IP (v4 and v6) addresses. The purpose of all tools is mainly to acquire information about these URLs/IP addresses.
In addition, there is an abundance of other tools available relevant to DNS, text, encryption, passwords, and more.
Differently from other tools, IPVoid does not gather any user feedback on whether sites are malicious or not, it only gives factual information, e.g., blacklists that the address appears in, that users can then use to decide for themselves whether a website/host is malicious or not.

Results:

1. IPVoid whois search on 46.167.245.207 points to Zdenek Klauda at FinalTek.com, which seems to be a generic platform to purchase web hosting in Czechia

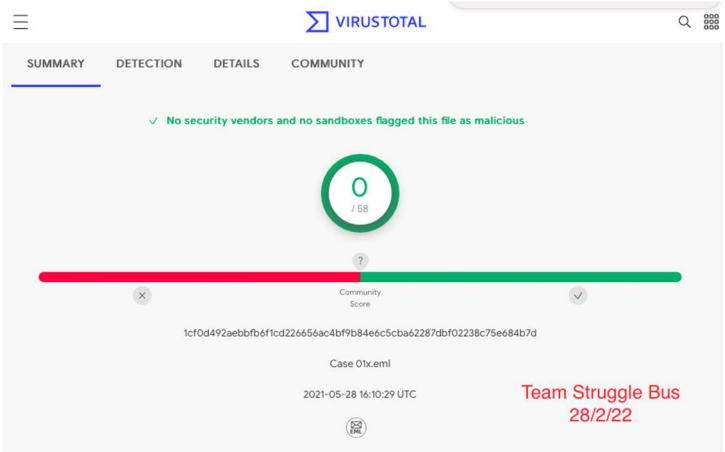


2. IPVoid blacklist check on 46.167.245.207 shows that it is possibly safe
3. Geolocation: Hovorcovice, Czech Republic (50.1804, 14.5205)

Virustotal (www.virustotal.com)
Introduction: “Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community”
It uses a community of users (end users and cyber security professionals) to create a pool of information on potentially harmful content.
It seems to have a larger focus on being user friendly for those with less knowledge on cyber security terms and practices.
It allows users to scan any suspicious files and is the first option when you open the site so shows that this would be the site's primary use.

Results:

1. Virustotal found no issues with the file, it does not contain malware



Checkphish (www.checkphish.ai)
Introduction: The engine helps in detecting phishing emails by analysing and evaluating how a user would look and understand at emails using techniques such as neuro linguistic programming(NLP), computer vision, and deep learning.
The engine keeps on learning from millions of high quality, proprietary image and text samples in its datasets, which helps in making a highly accurate detection.

Results:

1. email was sent from Czechia (inserted IP from email header: localhost (emkei.cz. [46.167.245.207])

Week 3 Portfolio

Questions:

- **What type of keywords would you use if you are searching for dogs? (Answer format: a list) RegEx**:
    - Dog* (Includes Dog, doggy, dogs, doggies, etc)
    - Pet
    - Woof
    - Pup* (includes Pup, Pups, Puppy, etc)
    - D*g
    - Pug*
    - Shiba*
    - Canine*
    - Hound*
    - Pooch*
    - Tail*
    - Mutt*
    - *.mp4
    - *.mov
    - *.jp*g
    - *.gif
    - *.pdf
    - Owner*

- **Is there anything noticeable in the extracted files?**
    - The user has recently deleted four files with dog-related material. Two copies of a PDF about Dogs, two copies of an image of a bulldog.
    - An entire folder containing 138 files (some images and pdfs) was deleted shortly before the computer was seized.
    - Additionally, a partition of the disk seems to have been deleted (Volume 1)
    - The group are inclined to believe that user may have been using the images to hide some secretive or key information with help of steganography, which is a data hiding method where a file is stored in another file to create the impression that there is no secretive information inside it. But it would be hard to make that conclusion only on the basis of the information that is provided, and investigating it further would be outside the scope of this exercise.
    - There is a password-protected PDF file called *disc1.pdf.* Password: pup.

- **What type of evidence can we gather?**
    - Dates that files were created or accessed
    - Images
    - Videos
    - Documents
    - Meta-data
    - Underlying data of files (text, hex codes, etc)

    - With Autopsy, a timeline of events that have taken place on the computer can be generated
    - Location data - though there is none in the Disk Image we are working on
    - Communications (such as email files) - though there is none in the Disk Image we are working on

Evidence List

- /img_johndoe.E01/vol_vol2/folder/3103_dogs.pdf
- /img_johndoe.E01/vol_vol2/folder/bulldog-144012__480.jpg
- /img_johndoe.E01/vol_vol2//$CarvedFiles/f0000000.pdf
- /img_johndoe.E01/vol_vol2//$CarvedFiles/f0000384.jpg
- /img_johndoe.E01/vol_vol2/folder/management.pdf
- /img_johndoe.E01/vol_vol2/folder/basicdogtrainingfactsheetnov13.pdf
- /img_johndoe.E01/vol_vol2/folder/basicdogtrainingfactsheetnov13.pdf
- /img_johndoe.E01/vol_vol2/folder/Password Guidance.pdf
- /img_johndoe.E01/vol_vol2/folder/Networking.pdf
- /img_johndoe.E01/vol_vol2/folder/management.pdf/image13.jpg
- /img_johndoe.E01/vol_vol2/folder/management.pdf/image7.jpg
- /img_johndoe.E01/vol_vol2/folder/management.pdf/image10.jpg
- /img_johndoe.E01/vol_vol2/folder/management.pdf/image3.jpg
- /img_johndoe.E01/vol_vol2/folder/hd.jpg
- /img_johndoe.E01/vol_vol2/folder/basicdogtrainingfactsheetnov13.pdf/image1.jpg
- /img_johndoe.E01/vol_vol2/folder/Networking.pdf/image0.jpg
- /img_johndoe.E01/vol_vol2/folder/twerp.jpg
- /img_johndoe.E01/vol_vol2/folder/3103_dogs.pdf/image10.jp
- /img_johndoe.E01/vol_vol2/folder/management.pdf/image9.jpg
- /img_johndoe.E01/vol_vol2/folder/disc1.pdf
- /img_johndoe.E01/vol_vol2/folder/Attacks on Steganographich Images.pdf
- /img_johndoe.E01/vol_vol1/Unalloc_3_0_4128768
- /img_johndoe.E01/vol_vol2/System Volume Information/smartdb_Volume{13fa977c-46ff-11e9-90e9-c49ded1cf670}.sdb

Group Policy

Karlis: Researched all Week 1 exercises and wrote about a third of it, researched and wrote about IPVoid in Week 2, contributed to about a quarter of Week 3 (research and writing). Helped with tidying and proofreading final report. Ensured the team calls regularly for work.
Donald: Researched, carried out and wrote up Week 1 and Week 3 practical work. Helped with final report tidying up/proofreading.
Khena: discussed with the group each week's tasks, got screenshots of our chosen tools for week 2, helped with writing and proofreading the report
Rishabh: Added in details for task in week 2, researching about the security tools, added in the possible keywords, and evidence list for task 3. Helped in proofreading the report.
Lau Hok Yee (Natalie): Researched all Week 1 exercises and wrote about protocols in Exercise 3, researched all Week 2 exercises and formatted Week 2, researched the searching part for Week 3 and added on it.
Declan: Researched and worked on all week 1 exercises. Wrote a significant amount of the week 2 report, and ran the email through several of the tools discussed. In the week 3 report, gathered evidence for the evidence list, added to all other sections of week 3.