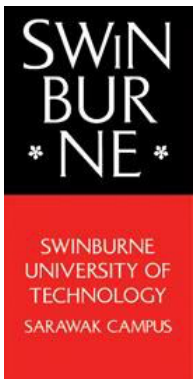

Swinburne University of Technology Hawthorn Campus
Department of Computing Technologies

COS30015 IT Security

Assignment 2 - *Semester 2, 2024*

Part A Incident Forensic Analysis

Student Name: Marco Giacoppo

Student ID: 104071453

Due Date: AEST 23:59 on 31/10/2024.

Add your answers in the appropriate locations by replacing <answer> with your answer.

Impact at STARFLEET

1. What type of threat does this appear to be?

   This could be a ransomware attack where malicious software encrypts user's files, making them not being able to access until a ransom is paid.

2. What is the indicator associated with this threat type?

   The primary indicator would be the inability to open or access files, because as we can see the extension says locked.

3. What main MITRE ATT&CK technique is associated with this incident type?

   The main MITRE ATT&CK technique could be T1486 – Data Encrypted for Impact, which refers to ransomware encrypting files to disrupt availability.

Unknow file identified

1. Is agent.exe a normal file?

   No, agent.exe is not a typical system file. It could be malicious, given that the user doesn't recall downloading it and it is located suspiciously on the desktop.

2. What type of file is agent.exe?

   This can be investigated through hash checks. The provided hash (d806e3e0c84b0b7208fb4ba9df5cd7b8851abce5c0bbb3ee330560aaa139f 243) should be checked against online malware tools to identify if it's a known malware.

3. Analysing the agent.exe-12345678.pf file, has agent.exe been executed before?

   According to the prefetch file, agent.exe has been executed once.

4. How many times has the file been executed?

   Based on the prefetch log, agent.exe has been executed once, as mentioned in the analysis of the prefetch file.

5. What does this file allow an adversary to do?

   Without further analysis of the file itself, it's likely that agent.exe was used to establish remote access or initiate malicious activity, as it's associated with suspicious behaviour on Chris Pike's machine.

Signs of tampering

1. Can you make sense of this command? What is last part decoded?

   I decoded the command in CyberChef and it translates to:

   Set-ExecutionPolicy unrestricted

   This command modifies the PowerShell execution policy to allow scripts to run without restrictions, which is a common method used by attackers to bypass script restrictions.

2. What does this command do?

   It changes the PowerShell execution policy to unrestricted, allowing any PowerShell script to run, even if it's unsigned or potentially malicious.

What was disabled

1. What does this script do?

   This script translates to Set-MpPreference -DisableRealtimeMonitoring $true, where it disables Windows Defender's real-time monitoring, which would allow malware to run without detection.

2. Is the previous command and this script potentially related?

Yes, the previous command sets PowerShell to unrestricted, and this script disables Defender's protection, making it easier for malicious software like agent.exe to run.

3. Could it have allowed system changes which would allow agent.exe to be ran?

   Yes, by disabling Defender's real-time protection and setting the execution policy to unrestricted, the system becomes vulnerable to executing malicious files like agent.exe.

4. What device was this script copied from?

   The script appears to have been copied from the device with IP address 192.168.100.20, which seems to be another internal device within the STARFLEET network.

Signs of movement

1. What type of event is this?

   The log refers to Event ID 4624, which is related to a successful logon event. This event type typically indicates that someone successfully logged into a machine.

2. Does this event confirm someone logged onto this device?

   Yes, this event confirms that someone successfully logged into the device. The log shows a successful login attempt for Chris Pike's account.

3. Where did the connection occur from?

   The log indicates that the connection originated from 192.168.100.20, which is an internal address in the Starfleet network.

4. What does the type/port indicate?

   The connection was made over port 3389, which is the default port for Remote Desktop Protocol (RDP). This suggests that the attacker used RDP to access the machine remotely.

5. What main MITRE ATT&CK tactic is represented here?

   The main MITRE ATT&CK tactic here is T1021.001 – Remote Services: Remote Desktop Protocol (RDP).

Other indicators identified

1. What can be summarised from the events recorded in the log file?

   The DC.log.txt shows multiple failed login attempts to the Admin account via RDP from 192.168.100.20. Eventually, a successful login was made using the Admin account.

2. Was the attack successful?

   Yes, the attacker successfully logged into the Admin account after several failed attempts.

3. What account was targeted?

   The Admin account was targeted.

4. Where did the connection originate from?

   It was from the IP address 192.168.100.20

5. What does the type/port indicate?

   The connection was made over port 3389, indicating the use of Remote Desktop Protocol as I mentioned earlier.

6. What main MITRE ATT&CK tactic is represented here?

   The main MITRE ATT&CK tactic is T1078 – Valid Accounts, where the attacker uses legitimate credentials to gain access.

7. Should a connection of this type be allowable between these two servers?

   No, such connections over RDP between internal systems should be restricted to prevent unauthorized access.

Impacted Account

1. What is the original password used to access the DC?

   The original password is 1q2w3e4r5t6y. I found it by inputting the cipher output, then changed the Box Height to 4 to see if there's anything that's readable. Once I found 1q2w3e4r5t6y, I hashed it using SHA-512 where it gave the same hash value.

2. What Cipher was used obtain the original password?

   The cipher that was used is the Caesar Box Cipher.

Initial Access

1. It appears the adversary logged into the Remote Access machine using a STARFLEET user account. What account was used?

   Based on the log provided in the assignment, the account used to gain initial access was Chris Pike's account.

2. What IP address was used to access the Remote Access machine (be careful to defang this IP address)

The IP address used to access the Remote Access machine was 171[.]25[.]193[.]25

3. What is interesting about this IP address?

   The IP address 171.25.193.25 is notable because it appears to be an external IP.

4. What remote access method was used?

   The method used was Remote Desktop Protocol (RDP), as indicated by the use of port 3389.

Missing Data

1. What file was uniquely downloaded which could be a sensitive data leak?

   The file starfleet_secrets.txt was uniquely downloaded and could be a sensitive data leak.

2. What IP downloaded this file? (be careful to defang this IP address)

   The IP address that downloaded the file is 80[.]67[.]167[.]81

3. What is interesting about this IP address?

   It appears to be an external IP, indicating that the data was exfiltrated outside the STARFLEET network. This suggests that the file may have been downloaded outside the internal network.

4. Who downloaded this file?

   The user associated with this download is Klingon.

Incoming mail

1. Who is the proper sender of the email? (be careful to defang this domain)

   The email appears to be from mail[.]fakeemail[.]com

2. What was IP address of this sender? (be careful to defang this IP address)

   The IP address from the sender is 183[.]81[.]169[.]238.

3. What is interesting about this IP?

   The IP address 183[.]81[.]169[.]238. Could be traced to a location that is inconsistent with legitimate communications from the Starfleet.com domain. This suggests that the email might have been spoofed.

Patient zero

1. What is the name of the file?

   The file name provided is Lockheed_Martin_JobOpportunities.docx, which appears to be a malicious document used in the attack.

2. What is the SHA256 hash of the file?

   The hash provided in the log for this file is 0160375e19e606d06f672be6e43f70fa70093d2a30031affd2929a5c446d07c1.

3. Is the file safe?

   No, the file is not safe. It is likely with an exploit that allows the adversary to compromise the system once Chris Pike opens it.

4. How can you verify if the file is safe?

   The file's hash (SHA256) should be checked against a malware database.

5. What threat group did this file come from?

   Based on the context of the assignment, the file could be associated with a known Advanced Persistent Threat (APT) group that specializes in spear-phishing campaigns

6. How might this file be analysed safely?

   This file could be analysed safely using a sandbox environment, such as Cuckoo Sandbox, or by performing static and dynamic analysis in a controlled VM with no internet connection.

Easter Eggs (HD Only)

1. Easter Egg 1: <answer>
2. How did you find Easter Egg 1?

   <answer>

3. Easter Egg 2 (both name and content): <answer>
4. How did you find Egg 2?

   <answer>