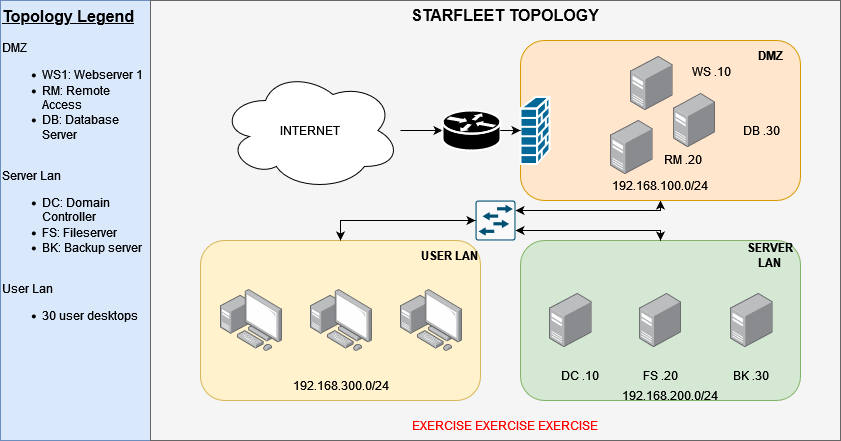
Assignment 2

Part A

STARFLEET has asked for help to deal with an unfolding cyber incident. The need your help to understand what has occurred in the incident to recover. To assist, they have collected a range of artefacts across their environment.

STARFLEET has provided their network topology to assist with the analysis.



Analyse the following artefacts and answer the associated questions.

Impact at STARFLEET

|  |
| --- |
| A user, Chris Pike, has reported that they are unable to open files on their computer.    Inspecting their computer, it appears that all their files has been impacted. Further investigation confirms that no files can be opened. |
| 1. What type of threat does this appear to be? 2. What is the indicator associated with this threat type? 3. What main MITRE ATT&CK technique is associated with this incident type? |

Unknow file identified

|  |
| --- |
| A file called agent.exe has been found on Chris’ desktop. Chris does not recall ever downloading or running this program. The team has collected the hash for you to investigate this file.  d806e3e0c84b0b7208fb4ba9df5cd7b8851abce5c0bbb3ee330560aaa139f243  Chris’ manger, Michael Burnham, has asked whether we can tell if the file was executed. The associated prefect file has been provided for agent.exe.  agent.exe-12345678.pf  ---------------------  Executable Name: agent.exe  Hash Path: 12345678  Executable Size: 12499.456 KB  Prefetch File Version: 30 (Windows 10)    Run Count: 1  Last Run Times:  - 2025-04-10 14:35:33    Volume Information:  - Volume Serial Number: ABCD-1234  - Volume Creation Time: 2023-01-01 00:00:00    Referenced Files and Directories:  - C:\Windows\System32\kernel32.dll |
| 1. Is agent.exe a normal file? 2. What type of file is agent.exe? 3. Analysing the agent.exe-12345678.pf file, has agent.exe been executed before? 4. How many times has the file been executed? 5. What does this file allow an adversary to do? |

Signs of tampering

|  |
| --- |
| A command has been traced to agent.exe. CMD was used to run the following command.  powershell -EncodedCommand U2V0LUV4ZWN1dGlvblBvbGljeSB1bnJlc3RyaWN0ZWQ=  Note: line formatting makes the above command look like it is over two lines, it is one single line |
| 1. Can you make sense of this command? What is last part decoded? What does this command do? |

What was disabled

|  |
| --- |
| After discussing with Michael Burnham, she’s very curious how agent.exe could have been executed. She said that Defender is running on their devices.  A PowerShell script called RunMe.PS1 was found with agent.exe. Inspecting the contents, the following was found.  U2V0LU1wUHJlZmVyZW5jZSAtRGlzYWJsZVJlYWx0aW1lTW9uaXRvcmluZyAkdHJ1ZQ== |
| 1. What does this script do? 2. Is the previous command and this script potentially related? 3. Could it have allowed system changes which would allow agent.exe to be ran? What device was this script copied from? |

Signs of movement

|  |
| --- |
| It appears the RunMe.PS1 was copied from a device internal to STARFLEET. If true, the IT manager Mr Suru remarked that this is concerning. That means someone has connected to Chris’ computer.  The following Sysmon log entry was captured to help determine this.  Event:  System:  Provider Name: Microsoft-Windows-Security-Auditing  EventID: 4624  Version: 2  Level: 0  Task: 12544  Opcode: 0  Keywords: 0x8020000000000000  TimeCreated SystemTime: 2025-04-10T12:01:00.000Z  EventRecordID: 12345  Correlation:  Execution ProcessID: 1234 ThreadID: 5678  Channel: Security  Computer: UserLan-PC8  Security:  EventData:  SubjectUserSid: S-1-5-18  SubjectUserName: UserLan-PC8$  SubjectDomainName: WORKGROUP  SubjectLogonId: 0x3e7  TargetUserSid: S-1-5-21-1234567890-123456789-1234567890-1001  TargetUserName: Chris Pike  TargetDomainName: UserLan-PC8  TargetLogonId: 0x12345  LogonType: 10  LogonProcessName: User32  AuthenticationPackageName: Negotiate  WorkstationName: UserLan-PC8  LogonGuid: {00000000-0000-0000-0000-000000000000}  TransmittedServices: -  LmPackageName: -  KeyLength: 0  ProcessId: 0x44c  ProcessName: C:\Windows\System32\svchost.exe  IpAddress: 192.168.200.10  IpPort: 3389  ImpersonationLevel: %%1833  RestrictedAdminMode: -  TargetOutboundUserName: -  TargetOutboundDomainName: -  VirtualAccount: %%1843  TargetLinkedLogonId: 0x0  ElevatedToken: %%1842 |
| 1. What type of event is this? 2. Does this event confirm someone logged onto this device? 3. Where did the connection occur from? 4. What does the type/port indicate? What main MITRE ATT&CK tactic is represented here? |

Other indicators identified

|  |
| --- |
| Given the developments, Mr Suru has search across the domain for other devices with the RunMe.PS1 file on them. Almost all devices have come back with a positive hit. Most concerning is the Domain Controller.  Sysmon logs have been provided for the Domain Controller. It appears someone has been going after a privileged account.  Analyse the DC.log.txt file.  Note: This file is a simple text file and can be viewed safely |
| 1. What can be summarised from the events recorded in the log file? 2. Was the attack successful? 3. What account was targeted? 4. Where did the connection originate from? 5. What does the type/port indicate? 6. What main MITRE ATT&CK tactic is represented here? 7. Should a connection of this type be allowable between these two servers? |

Impacted account

|  |
| --- |
| After investigating the Sysmon logs on the DC, it appears that the adversary got lucky. The team of STARFLEET have provided the output of a transportation cipher used in Roman times, along with a hash of the original password. Can you crack it?  Cipher output: 1w4tq3r62e5y  Original password hash: 9bf0ec5950285ac82cce6ebca7691c96520645e169a5aaef2bd5ede9036d99624076293916270b97b39ad98a7d13ffcdf4158ba38535c8a02045663b9682731e |
| What is the original password used to access the DC?  What Cipher was used obtain the original password? |

Initial Access

|  |
| --- |
| Seeing that the adversary connected via the Remote Access machine in the DMZ, the team has provided you with an interesting log entry for the Remote Access machine.  Event:  System:  Provider Name: Microsoft-Windows-Security-Auditing  EventID: 4624  Version: 2  Level: 0  Task: 15534  Opcode: 0  Keywords: 0x8020000000000000  TimeCreated SystemTime: 2025-04-10T10:24:01.000Z  EventRecordID: 12360  Correlation:  Execution ProcessID: 1234 ThreadID: 5678  Channel: Security  Computer: Remote  Security:  EventData:  SubjectUserSid: S-1-5-18  SubjectUserName: Remote$  SubjectDomainName: WORKGROUP  SubjectLogonId: 0x3e7  TargetUserSid: S-1-5-21-1234567890-123456789-1234567890-1001  TargetUserName: Chris Pike  TargetDomainName: Remote  TargetLogonId: 0x12345  LogonType: 10  LogonProcessName: User32  AuthenticationPackageName: Negotiate  WorkstationName: Remote  LogonGuid: {00000000-0000-0000-0000-000000000000}  TransmittedServices: -  LmPackageName: -  KeyLength: 0  ProcessId: 0x44c  ProcessName: C:\Windows\System32\svchost.exe  IpAddress: 171.25.193.25  IpPort: 3389  ImpersonationLevel: %%1833  RestrictedAdminMode: -  TargetOutboundUserName: -  TargetOutboundDomainName: -  VirtualAccount: %%1843  TargetLinkedLogonId: 0x0  ElevatedToken: %%1842 |
| 1. It appears the adversary logged into the Remote Access machine using a STARFLEET user account. What account was used? 2. What IP address was used to access the Remote Access machine (be careful to defang this IP address) 3. What is interesting about this IP address? 4. What remote access method was used? |

|  |
| --- |
| The team at STARFLEET is worried that some secrets went missing and were exfiltrated, and possibly made them an interesting target. Analyse the file samba\_log.txt.  The structure of the log is:   * Timestamp: When the log entry was created * Log Level: Severity or verbosity of the log message * Process ID: ID of the process generating the log * Thread ID: ID of the thread within the process (if applicable) * Samba Component: The specific Samba service or module * Message Text: The actual log message * IP Address: IP address of the client * User: The user performing the action * Action: The type of action performed (upload, download, edit, view) * File Name: Name of the file involved |
| 1. What file was uniquely downloaded which could be a sensitive data leak? 2. What IP downloaded this file? (be careful to defang this IP address) 3. What kind of IP is this? 4. Who downloaded this file? |

Incoming mail

|  |
| --- |
| Chris now recalls the email, the contents of which are provided below for analysis.  From: Kaptian Kirk <captian.kirk@starfleet.com>  To: chrispike@starfleet.com  Subject: A new offer  Date: Wed, 09 April 2025 08:45:12 -0700  Message-ID: <1234567890abcdef@fakeemail.com>  Reply-To: phish@fakeemail.com  X-Mailer: FakeMailer 1.0  Received: from mail.fakeemail.com (mail.fakeemail.com [192.168.1.100])  by smtp.example.com (Postfix) with ESMTP id 1234ABCD  for < chrispike@example.com>; Wed, 09 April 2025 08:45:11 -0700 (PDT)  Received: from unknown (HELO client.fakeemail.com) ([183.81.169.238])  by mail.fakeemail.com with SMTP; Wed, 09 April 2025 08:45:00 -0700  X-Spam-Status: No, score=-1.2 required=5.0 tests=ALL\_TRUSTED  autolearn=disabled version=3.4.0  X-Received: by 2002:a1c:44a0:: with SMTP id z6mr12345678ybd.87.169.123.45  for <chrispike@starfleet.com>; Wed, 09 April 2025 08:45:09 -0700 (PDT)  Content-Type: text/html; charset=UTF-8  Content-Transfer-Encoding: 7bit  <html>  <body>  <h1>Congratulations!</h1>  <p>Dear Candidate,</p>  <p>We are excited to inform you that you have been selected for a fantastic job opportunity!</p>  <p>To view your offer letter and further details, please click the link below:</p>  <p><a href="https://example.com/staging/ NewStarfleetoffers.docx">View Your Offer Letter</a></p>  <p>Best regards,<br>  Human Resources</p>  </body>  </html>  He did remark that it was odd Kirk would send him a job offer given he already worked at Starfleet, but Kirk is a bit of a character. |
| 1. Who is the proper sender of the email? (be careful to defang this domain) 2. What was IP address of this sender? (be careful to defang this IP address) 3. What is interesting about this IP? |

Patient zero

|  |
| --- |
| Investigating the Remote Access device logs in the DMZ, it appears Chris Pike’s account was used to access, then then the subsequent password attack too place. It appears Chris’s account has been compromised.  Chris noted that he received an email recently which seemed odd but didn’t report it. It directed him to download a job offer document. The associated event was captured.  System:  Provider Name: Microsoft-Windows-Sysmon  Guid: {5770385f-c22a-43e0-bf4c-06f5698ffbd9}  EventID: 15  Version: 2  Level: 4  Task: 15  Opcode: 0  Keywords: 0x8000000000000000  TimeCreated SystemTime: 2025-04-09T13:23:14.000Z  EventRecordID: 103456  Correlation:  Execution ProcessID: 1234  ThreadID: 5678  Channel: Microsoft-Windows-Sysmon/Operational  Computer: UserLan-PC8  Security UserID: S-1-5-21-1234567890-123456789-1234567890-1001  EventData:  UtcTime: 2025-04-01 13:23:14.000  ProcessGuid: {a23eae89-c7f3-5915-0000-001083968417}  ProcessId: 1234  Image: C:\Windows\System32\msedge.exe  TargetFilename: C:\Users\ChrisPike\Downloads\ Lockheed\_Martin\_JobOpportunities.docx  CreationUtcTime: 2025-04-01 05:23:14.000  Hash: MD5= a27a9324d282d920e495832933d486ee, SHA256= 0160375e19e606d06f672be6e43f70fa70093d2a30031affd2929a5c446d07c1  Contents:[ZoneTransfer] ZoneId=3 ReferrerUrl:https://example.com/staging/NewStarfleetoffers.docx  HostUrl= https://example.com/  It appears that the adversary used this file as a means to gain credentials to launch their attack campaign. |
| 1. What is the name of the file? 2. What is the SHA256 hash of the file? or 3. Is the file safe? 4. How can you verify if the file is safe? 5. What threat group did this file come from? 6. How might this file be analysed safely? |

Credit Only

|  |
| --- |
| Logs have been collected from Mr Suru’s device; it appears there is a two Credit Easter Eggs there. Analyse the correct log. Mr Suru is concerned someone was trying to access Starfleet. |
| 1. After mounting disk.img, rearrange the following rlao3eusmrcrooso1yps2euou! to “crack” the password, the hash of the correct password is ec6303573605eecba81b389f03bffa662e48442f94e88ac369531bbc033017a7 2. What is the hashing algorithm used (hint: Russian): 3. The password is:   After cracking the hash, complete the following for the second portion:   1. What type of attack (in TTP) is being attempted: 2. How many attempts fail: 3. What is the ID of this: 4. What accounts are caught up in this? 5. Is the attack successful: 6. What is the start time of this attack: 7. What is the end time of this attack: 8. How did you find Easter Egg 2? |

Distinction Only

|  |
| --- |
| A memory capture has been obtained of MrSuru’s device; it appears there are some HD Easter Eggs there. Analyse the memory capture. |
| 1. Easter Egg 1 name: 2. Easter Egg 1 data: 3. How did you find this: 4. Easter Egg 2 name: 5. Easter Egg 2 data: 6. How did you find this: 7. Easter Egg 3 name: 8. Easter Egg 3 data: 9. How did you find this: |