Assignment 2 PART B - SITE REP for the STARFLEET Incident

Student ID: 104837257
Student Name: Arun Ragavendhar Arunachalam Palaniyappan
Assignment Name: Assignment 2 Part B – SITE REP
Date: 01 /06/2025
Tutor: Yasas Akurudda Liyanage Don

<table>
<tr><th colspan="3">STARFLEET SITREP</th></tr>
<tr><td>Impacted STARFLEET Accounts</td><td>Student ID</td><td>Arun Ragavendhar Arunachalam Palaniyappan (104837257)</td></tr>
<tr><td rowspan="2">**Chris Pike** – His account was the initial entry point. After falling for a phishing email, he downloaded a fake job offer file that stole his credentials. The attacker used these to access RM.20 (Remote Access Machine in the DMZ) from a Tor exit node (171.25.193.25), which hides the attacker’s real location. This marked the start of the breach.
Admin – The Admin account on the Domain Controller was brute-forced from RM.20. Multiple password attempts were made until a successful RDP login gave the attacker full SYSTEM-level access to the server (192.168.200.10), allowing full control.
Klingon – This account was used to download a confidential file (*starfleet_secrets.txt*) from inside the STARFLEET network to an external IP address (80.67.167.81). There is no sign of a normal login, which suggests the account was fake, hijacked, or created by the attacker for stealthy data theft.</td><td>Class</td><td>Friday – 06:30 PM to 08:30 PM</td></tr>
<tr><td>Tutor</td><td>Yasas Akkurudha Liyanage Don</td></tr>
<tr><td>Incident Timeline</td><td colspan="2">Impacted STARFLEET Hosts</td></tr>
<tr><td>**1. 09 April 2025 – 15:45:12 UTC**
Chris Pike received a phishing email from **phish@fakeemail.com**, faking a STARFLEET contact. The email was delivered from **183.81.169.238**, a public IP</td><td colspan="2">**1) RM.20 – Remote Access Machine (DMZ Gateway)**
IP Address: 192.168.100.20</td></tr>
</table>

from Vietnam. It linked to a fake job offer hosted on a suspicious domain; this was the attacker’s first trick to steal credentials. This log had incorrect time stamps in PDT, but the exact timestamp as per the logs have been mentioned here. **This event marked the start of the attack chain.**

2. 09 April 2025 – 13:23:14 UTC

Chris Pike opened the attached Word document. The file silently ran a hidden script that captured his STARFLEET username and password. This was the exact moment the attacker harvested his valid credentials.

3. 10 April 2025 – 10:24:01 UTC

The attacker logged into STARFLEET’s Remote Access Machine in the DMZ (RM.20) using Chris Pike’s stolen credentials. The connection came from 171.25.193.25, an exit node from the Tor network, clearly showing that the attacker was hiding their real location while gaining initial access.

4. 10 April 2025 – 11:26:01 UTC

The attacker moved laterally from the DMZ machine (RM.20) to STARFLEET’s Domain Controller (192.168.200.10). Using a brute-force attack from inside the network, they cracked the **Admin** account password and gained full SYSTEM-level access, unlocking complete control over STARFLEET’s internal systems.

5. 10 April 2025 – 12:01:00 UTC

The attacker used Chris Pike’s stolen credentials to log into his personal workstation (UserLan-PC8). This was a full user login, and shows that the attacker was now actively operating inside STARFLEET’s internal network, preparing to disable security tools and launch ransomware.

Impact: High – This system was the attacker’s entry point into STARFLEET, allowing them to step from external access into the internal network undetected.

The attacker first logged into RM.20 using the stolen credentials of Chris Pike. The login came from a Tor exit node (171.25.193.25), masking their true location and making the intrusion hard to trace. RM.20 is located in the DMZ zone and is meant to act as a controlled gateway for remote access. Once inside this system, the attacker had a direct line to the internal Server LAN and quickly used it to attempt further intrusions. RM.20 was not isolated properly and had unnecessary access to critical systems like the Domain Controller, which helped the attacker escalate the attack.

2) DC-10 – Domain Controller (Server LAN)

IP Address: 192.168.200.10

Impact: Critical – This system gave the attacker total control of STARFLEET. Every major part of the attack was launched or coordinated from here.

After gaining access to RM.20, the attacker launched a brute-force attack and successfully guessed the Admin account password ("1q2w3e4r5t6y"). This allowed them to log into the Domain Controller with full administrative rights. From DC-10, they could remotely control every other STARFLEET system, disable security features, and push scripts without needing further user logins. This system was used to launch attacks on Chris Pike’s workstation and MrSuru’s machine. It also allowed the attacker to operate using SYSTEM-level access across the network. Control over this one system gave them full power over the entire STARFLEET environment.

6. 10 April 2025 – Between 12:01:00 UTC and 14:35:33 UTC

A PowerShell command was executed on Chris's system to set the execution policy to **Unrestricted**. This disabled script-blocking protections and allowed any script, including malicious ones, to run freely without interruption.

7. 10 April 2025 – Between 12:01:00 UTC and 14:35:33 UTC

Soon after, another PowerShell script called RunMe.ps1 was used to disable Windows Defender's real-time protection. This command, run using Set-MpPreference, turned off key defences, giving the attacker full control to drop malware without being blocked.

8. 10 April 2025 – 14:35:33 UTC

With all defences bypassed, the attacker executed agent.exe, a ransomware payload. All files on Chris Pike's device were encrypted and locked, marking the first visible impact of the attack on a user system.

9. 25 April 2025 – 06:26:12 UTC

The attacker, already holding SYSTEM access on MrSuru's machine through the domain controller, initiated a brute-force attack directly from localhost. They targeted both MrSuru and the Admin accounts by guessing passwords, trying to gain direct login access.

10. 25 April 2025 – 06:29:19 UTC

After 17 failed login attempts, the brute-force attack stopped. MrSuru's account was locked out, as confirmed by Event ID 4740. Although login failed, this showed the attacker was still attempting to gain user-level access, even while operating with SYSTEM privileges.

11. 25 April 2025 – 06:30:12 UTC

3) UserLan-PC8 – Chris Pike's Workstation

IP Address: 192.168.300.X

Impact: High – This system was fully compromised through valid user login.

The attacker disabled key security protections and executed ransomware, leading to total data loss on this host. They logged into Chris Pike's computer using his stolen username and password. This was a full user-level login. Once inside, the attacker ran a PowerShell command to remove script restrictions, allowing any script to run without warning. Then, they executed another command to disable Windows Defender's real-time protection, leaving the system exposed. Finally, they launched the ransomware program agent.exe, which encrypted every file on the machine and made the device unusable.

4) DESKTOP-CRPG57R – MrSuru's Device (Internal Workstation)

IP Address: 192.168.300.Y

Impact: High - This machine was not successfully breached through user login, but it still became a target for malware and evidence destruction due to the attacker's SYSTEM-level control.

The attacker launched a brute-force attack from inside MrSuru's machine, targeting both the MrSuru and Admin accounts. After 17 wrong password attempts, MrSuru's account got locked. But the attacker didn't stop there, they already had full SYSTEM access, which let them run commands without logging in. They used a hidden batch file named AAAAAAAAAAAAAAAA.bat, which ran in a loop using timeout.exe to stay active. Also, before running the .bat file, the attacker had shut down the event logging service and deleted the log files to hide the failed login attempts and everything else that happened after running the .bat file.

Windows Event Logging Service was forcefully shut down on MrSuru's system. This action was carried out using SYSTEM-level access, as shown by Event ID 1100. This step was likely taken by the attacker to prevent further activity from being recorded in the logs, which is a common defence evasion technique.

12. 25 April 2025 – 06:55:09 UTC

The attacker deleted the Windows Event Logs. This happened shortly after they had shut down the event logging service using SYSTEM-level access. The purpose was to **erase evidence of the brute-force attempts made earlier on the MrSuru and Admin accounts**, preventing investigators from tracing the login failures.

13. 25 April 2025 – 07:34:53 UTC

The attacker opened the batch file AAAAAAAAAAAAAAAA.bat using Notepad (PID 6640), likely to check or make changes before running it. This shows they were interacting with the file manually. The attacker edited or updated the malicious script **for 16 minutes** before running it.

14. 25 April 2025 – 07:50:06 UTC

The attacker has SYSTEM Access. The batch file AAAAAAAAAAAAAAAA.bat is executed through cmd.exe (PID 8576) and it launched timeout.exe and conhost.exe at the same moment, On **MrSuru's** system. The script ran in a loop and had persistence enabled.

15. 25 April 2025 – 07:52:37 UTC

Shortly after, STARFLEET investigators captured memory using RamCapture64.exe (PID 416). This snapshot was taken while the batch script was still running. The file no longer exists on disk, proving it ran directly from memory and was never saved on the disk. **This event marked the end of the attack chain.**

5) Starfleet File Server – SAMBA Target (Inferred from Logs)

IP Address: Not explicitly recorded, part of internal Server LAN

Impact: High – This system was used for quiet data exfiltration without compromising any user accounts.

The Starfleet file server stored the sensitive document **starfleet_secrets.txt** and appears to be part of the internal Server LAN. While its IP was not directly recorded, the file was accessed using SMB and an account named **Klingon**. Since there were no login events linked to this account, and the name doesn't follow STARFLEET's usual naming style, it was likely fake or taken over. This kind of access, points to a shared file server, and not a personal computer. In workplaces like STARFLEET, these servers usually sit in the Server LAN to manage secure file access. The attacker used this system to quietly download internal documents without needing to compromise a user's device.

Each of these STARFLEET systems was picked for a reason. The attacker used the DMZ Remote Access machine to break in, RM.20 to crack the Admin account, the Domain Controller to gain full control, Chris's device to run ransomware, MrSuru's machine to execute memory-only scripts, and the file server to steal sensitive documents. Every move was calculated to push the attack forward.

Important Finding to Note:

Once the attacker cracked the Admin password on the Domain Controller, they gained full SYSTEM-level control across STARFLEET. From there, they didn't need user logins, as they could run commands on any machine remotely. That's how they launched malware and wiped logs on MrSuru's system without ever accessing his user account. In fact, Chris Pike's was the only user account stolen. Everything else was done using that one Admin-level access. No further account breaches were needed.

Identified IOCs and their linked MITRE ATT&CK Tactics and Techniques

IOC Type	IOC Description	Linked MITRE Tactic	MITRE Technique ID & Name
File Name	**Lockheed_Martin_JobOpportunities.docx** – The phishing attachment sent to Chris Pike, containing an embedded script that stole credentials.	**Initial Access**	T1566 – Phishing
	agent.exe – A ransomware program that was run on Chris's system. It locked all files after execution.	**Impact**	T1486 – Data Encrypted for Impact
	RunMe.ps1 – A PowerShell script used to turn off Defender's real-time protection before malware launch.	**Defense Evasion**	T1562.001 – Disable or Modify Tools
	AAAAAAAAAAAAAAAA.bat – A hidden batch file that ran from memory to trigger multiple malicious actions.	**Persistence**	T1053.005 – Scheduled Task or Job
	starfleet_secrets.txt – A sensitive STARFLEET file that was downloaded by the attacker through SMB.	**Exfiltration**	T1041 – Exfiltration Over C2 server
File Hash	`0160375e19e606d06f672be6e43f70fa70093d2a30031affd2929a5c446d07c1`– SHA-256 hash of the phishing DOCX file sent to Chris Pike in the fake job email.	**Initial Access**	T1566 – Phishing
	`d806e3e0c84b0b7208fb4ba9df5cd7b8851abce5c0bbb3ee330560aaa139f243`– Hash of the ransomware binary agent.exe, matching known malware samples.	**Impact**	T1486 – Data Encrypted for Impact
PowerShell Commands	**Set-MpPreference -DisableRealtimeMonitoring $true** – Turns off Defender, letting malware run freely.	**Defense Evasion**	T1059.001 – PowerShell
	Set-ExecutionPolicy Unrestricted – Removes restrictions, allowing any script to run.	**Defense Evasion**	T1059.001 – PowerShell

Encoded Commands	U2V0LU1wUHJlZmVyZW5jZSAtRGlzYWJsZVJlYWx0aW1lTW9uaXRvcmluZyAkdHJ1ZQ== and U2V0LUV4ZWN1dGlvblBvbGljeSB1bnJlc3RyaWN0ZWQ= (both decoded to security disabling commands)	**Defense Evasion**	T1059.001 – PowerShell
External IP	**171.25.193.25** – A known Tor exit node used to remotely access STARFLEET's DMZ system (RM.20) via RDP.	**Initial Access**	T1133 – External Remote Services
External IP	**80.67.167.81** – IP address used to download the secrets.txt file from inside STARFLEET.	**Exfiltration**	T1041 – Exfiltration Over C2 server
Email Sender	**phish@fakeemail.com** – The spoofed address pretending to be from STARFLEET's HR department.	**Initial Access**	T1566 – Phishing
Email Sender IP	**183.81.169.238** – Public IP based in Vietnam, used to send the phishing email.	**Initial Access**	T1566 – Phishing
Accounts	**Chris Pike** – His credentials were stolen and reused by the attacker to log in and move across systems.	**Valid Accounts**	T1078 – Valid Accounts
	Admin – The attacker guessed this password through brute-force and gained full control of the Domain Controller.	**Credential Access**	T1110 – Brute Force
	Klingon – A suspicious account used to access and download **starfleet_secrets.txt;** not found in normal login records. Same activity also facilitated data exfiltration over SMB.	**Valid Accounts**	T1078 – Valid Accounts
		Exfiltration	T1041 – Exfiltration Over C2 server
Host Activity	The attacker used RDP to move from RM.20 (DMZ) → Domain Controller → Chris Pike's PC → MrSuru's system.	**Lateral**	T1021.001 – Remote Services: RDP
		Movement Execution	T1059 – Command and Scripting Interpreter
Registry Edit	Registry changes found in memory show that PowerShell settings were modified to weaken system defences.	**Persistence**	T1012 – Query Registry
		Evasion	T1012 – Query Registry
Log Events	Windows event logs were shut down and later deleted using SYSTEM-level access, hiding all activity trails.	**Defense Evasion**	T1070 – Indicator Removal

Remediation Advice

Remediation advices and the MITRE ATT&CK TTPs which they can block, remove or alert against, are shared below:

1. **Enforce Multi-Factor Authentication (MFA) for Remote Access**

Tactic: Initial Access / Credential Access
Technique: T1078 – Valid Accounts, T1133 – External Remote Services

The entire attack began with a stolen password, but it succeeded only because there was no second layer of security. If STARFLEET had enabled MFA on its DMZ Remote Access system, the attacker would have been blocked even after stealing Chris Pike's credentials. A login attempt from the attacker would have triggered a second authentication request, most likely a mobile prompt or token that only Chris could approve. This would not just stop the attack but also notify Chris of suspicious activity. That single alert could have triggered an early investigation and avoided every step that followed. MFA should be enforced especially for all RDP services, admin panels, and web-based logins.

2. **Set Strong Password Policies for All Admin Accounts**

Tactic: Credential Access
Technique: T1110 – Brute Force

The Admin account on the Domain Controller used a weak, guessable password: "1q2w3e4r5t6y." The attacker cracked it with brute-force attempts from within the network. To prevent this, STARFLEET must enforce complex password rules, such as minimum 18 characters, including upper and lowercase letters, numbers, and special characters, with no common patterns. Accounts should lock after five wrong password attempts. This would block the attacker quickly and alert the security team right away. This one step would have stopped the attacker from gaining SYSTEM-level access to the Domain Controller and taking control of the entire network, as they only cracked the password after 15 brute force attempts.

3. **Disable RDP from External Networks or Strictly Limit It**

Tactic: Initial Access / Lateral Movement
Technique: T1133 – External Remote Services, T1021.001 – Remote Services: RDP

The attacker first entered STARFLEET through Remote Desktop Protocol (RDP) using a Tor exit node. This shows that RDP was exposed to the internet without any proper filtering. STARFLEET must close all remote access ports like RDP by default. If RDP is absolutely necessary, it should only be allowed through a secured VPN tunnel, with a strict set of whitelisted IPs. Logs of every remote login attempt must be collected and reviewed regularly. Any RDP session from a public or suspicious IP, especially from privacy networks like Tor, should immediately trigger alerts for review. Without these basic restrictions, remote access becomes an open door for hackers.

4. **Isolate the Domain Controller from Other LAN Zones**

Tactic: Lateral Movement
Technique: T1021.001 – Remote Services: RDP

RM.20, a remote access system in DMZ, was able to directly reach the Domain Controller. This should never be allowed. STARFLEET must redesign its internal network using segmentation. Remote systems, user devices, servers, and critical infrastructure like the Domain Controller must be placed in separate VLANs. Each segment should have strict firewall rules that block unnecessary communication. For example, a DMZ system like RM.20 should never be able to initiate a connection to the Domain Controller. If proper segmentation had been in place, the attacker's lateral movement would have been blocked or at least slowed down, giving defenders more time to respond.

5. **Turn on Centralised Logging and Real-Time Monitoring**

Tactic: Defense Evasion
Technique: T1070 – Indicator Removal, T1059.001 – PowerShell

The attacker disabled event logging and deleted event logs on MrSuru's system to hide their actions. This worked because STARFLEET relied on logs stored only on the affected machines. To fix this, all systems must send logs to a central logging server or SIEM tool that stores them separately. These logs should be write-only from the endpoint's side, meaning attackers cannot delete them even if they gain SYSTEM access. The system must also trigger alerts for risky actions like PowerShell policy changes, Windows Defender being disabled, or unusual login locations. If this had been in place, STARFLEET investigators could have spotted the attack early and retrieved unaltered logs even after the local machines were compromised.

6. **Deploy Behaviour-Based Detection Tools, Not Just Signature-Based Antivirus**

   Tactic: Defense Evasion / Execution / Persistence
   Technique: T1059.001 – PowerShell, T1562.001 – Disable or Modify Tools, T1053.005 – Scheduled Task or Job

   The malware did not leave behind any files. It used PowerShell commands and a hidden batch file that ran only in memory. Traditional antivirus tools would fail here, because they look for known malware signatures. STARFLEET needs behaviour-based detection tools that focus on actions, not just file names. For example, the system should alert if PowerShell execution policies are suddenly changed, if timeout.exe runs repeatedly in short bursts, or if event logs are shut down. These are clear signs that something is wrong, even if no virus file is found. Modern Endpoint Detection and Response (EDR) systems can do this. If STARFLEET had one in place, these red flags could have triggered a fast response before the files were encrypted or stolen.

7. **Block Access from Known Malicious IPs and Domains**

   Tactic: Initial Access / Exfiltration
   Technique: T1133 – External Remote Services, T1566 – Phishing

   The phishing email came from 183.81.169.238, a public IP from Vietnam, and the attacker logged in from a Tor exit node (171.25.193.25). These are not random IPs; both are known to show up in abuse lists and threat intelligence feeds. STARFLEET’s firewall should regularly update from such feeds and automatically block known Tor exit nodes, flagged SMTP sources, and high-risk IPs. If this was in place, the RDP login from the Tor network would have been blocked instantly, and the phishing email server could have been blacklisted before Chris received the mail.

8. **Run Mandatory Phishing Awareness Sessions**

   Tactic: Initial Access
   Technique: T1566 – Phishing

Chris fell for a fake job offer because he could not recognise a well disguised phishing email. STARFLEET must run mandatory training sessions that teach staff how to spot fake senders, suspicious attachments, and unusual links. This includes running regular fake phishing tests to help staff practise and stay alert. If Chris had been better trained, he might have reported the email instead of opening it, stopping the attack before it even started.

9. **Deploy Lightweight Honeypots and Trap Files**

Tactic: Exfiltration / Credential Access
Technique: T1041 – Exfiltration Over C2, T1078 – Valid Accounts

To spot attackers exploring the network, STARFLEET should place decoy files like a **confidential_bait.docx** or unused admin credentials in key folders. These honeypots do not serve any real function but are monitored closely. If anyone tries to open them, it signals suspicious behaviour. In this attack, such traps could have triggered alerts as soon as the attacker browsed internal shares, giving an early warning.

10. **Run Full Malware Sweep Across All Systems**

Tactic: Impact / Defense Evasion
Technique: T1486 – Data Encrypted for Impact, T1070 – Indicator Removal

Malware like agent.exe and RunMe.ps1 must be fully removed from every affected device. STARFLEET should run both full-disk antivirus scans and memory forensics across all machines. This includes checking for scripts that were run only in memory. All past SYSTEM-level logins must be reviewed to confirm that no backdoors or hidden tasks were left behind. Without this step, the attacker could still have remote control without being noticed.

11. **Reset and Reissue All Credentials Post-Incident**

Tactic: Credential Access / Exfiltration
Technique: T1078 – Valid Accounts, T1041 – Exfiltration Over C2 server

Accounts like Chris Pike, Admin, and suspicious ones like Klingon must be disabled immediately. New accounts should be created with fresh credentials for trusted users only. All passwords, especially those tied to admin roles, must be reset using strong password policies. Inactive or unused accounts should be reviewed and removed to stop attackers from reusing them later. Leaving old accounts in place gives future attackers a head start.

12. **Create an Incident Response Playbook**

Tactic: All Stages (Prevention and Response Support)
Technique: Supports prevention, detection, and containment across all above mentioned techniques

STARFLEET had no clear response workflow when the attack happened. A written playbook must be created that outlines exactly what to do when an incident is detected. This includes who should be alerted, how to quickly disconnect affected devices, and which systems or memory files to preserve for forensic analysis. Regular practice runs (tabletop or simulated attacks) will help reduce confusion, downtime, and errors if another real attack happens.