CSL3351 – Incident Detection and Response

Assignment 2: Incident Detection Case Study

Glen TEAKLE 10532981

Joondalup Campus/Online

Dr Leslie Sikos

Contents

[Executive Summary 3](#_Toc135083914)

[Lockheed Martin Cyber Kill Chain and MITRE ATT&CK Framework 3](#_Toc135083915)

[Introduction 4](#_Toc135083916)

[Technical Details 4](#_Toc135083917)

[Cyber-attack 1 - Malicious file upload – SUCCESS 4](#_Toc135083918)

[Cyber-attack 2 - Attempted SSH login as ROOT user – FAILED 6](#_Toc135083919)

[Cyber-attack 3 -Login as Root user – FAILURE 7](#_Toc135083920)

[Possible Cyber-attack 4 -Encryption of Data – Inconclusive 9](#_Toc135083921)

[Tools and Countermeasures 10](#_Toc135083922)

[Running Sheet 11](#_Toc135083923)

[Timeline of Events 15](#_Toc135083924)

[References 16](#_Toc135083925)

# Executive Summary

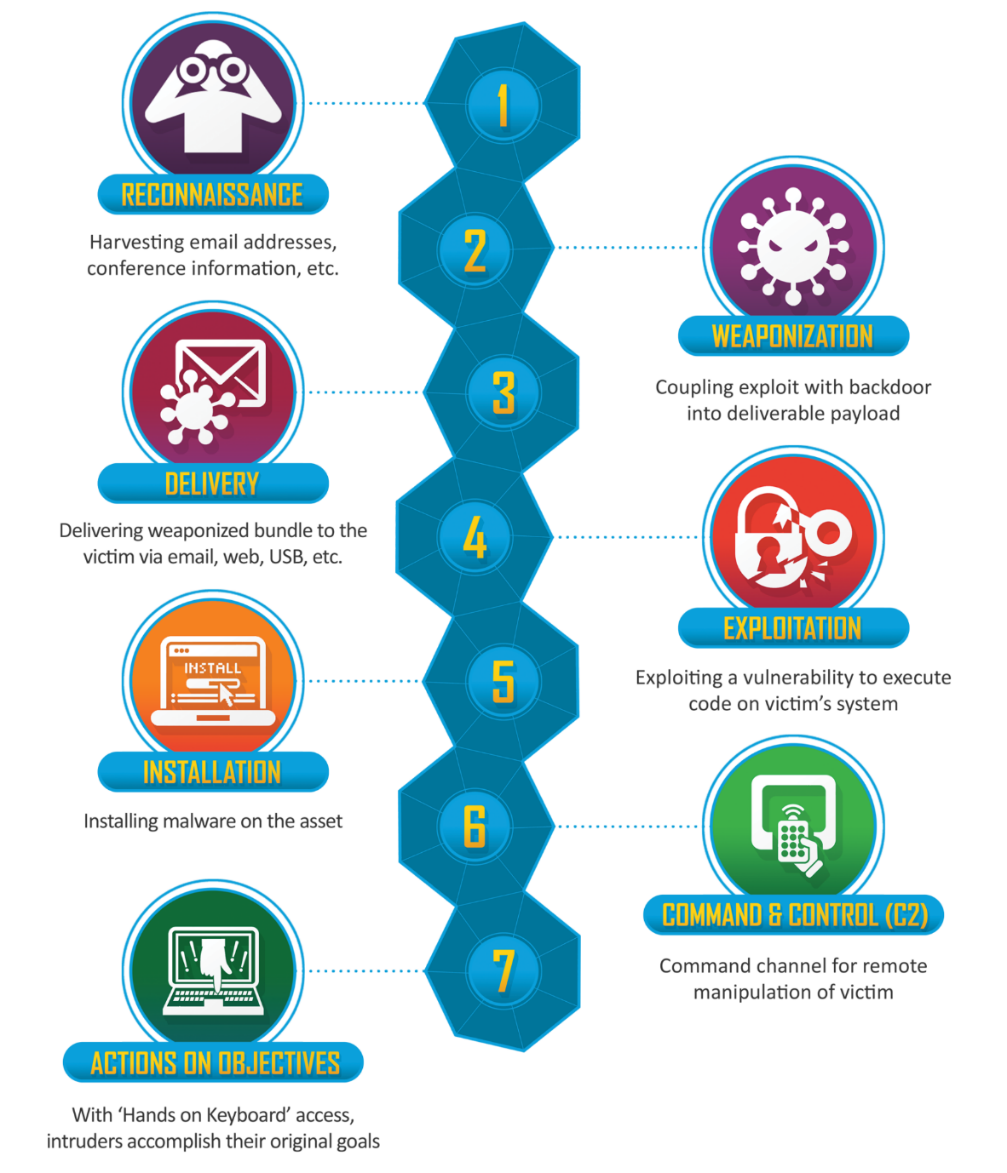
A supplied dataset was investigated using Elasticsearch in the ELK stack. Given the timeframe 29/9/21 10:00 – 01/10/21 14:00; the purpose was to identify and analyse any evidence of cyber-attacks during this timeframe. Technical details of any found attacks are given and they are categorized against both the relevant Lockheed Martin Cyber Kill Chain phases (see Figure 1) and MITRE ATT&CK Framework's attack techniques (Figure 2). Mitigation strategies, prevention and countermeasures are discussed regarding each found cyber-attack, along with justification for each. Also included is a running sheet which details the actions taken during the investigation, for means of repeatability. Lastly, a timeline of chronological events (cyber-attacks) is included.

## Lockheed Martin Cyber Kill Chain and MITRE ATT&CK Framework

The Lockheed Martin Cyber Kill Chain is a visual representation of specific cyber-attack phases, as shown in Figure 1. All stages are not necessarily incorporated in a cyber-attack as shown in this report.

Figure **1**.

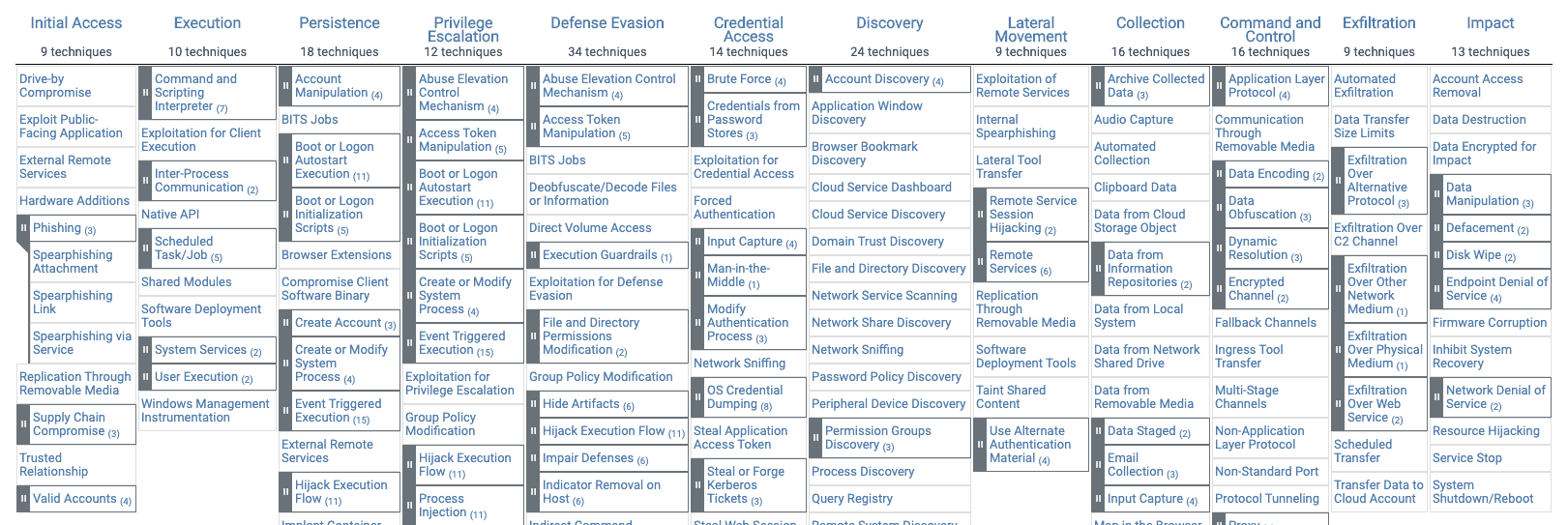
*The Lockheed Martin Cyber Kill Chain*

****

Shown below in Figure 2, the MITRE ATT&CK framework is a visual representation of cyber-attack techniques and tactics. There are 14 categories, each with their own sub-techniques.

Figure **2.**

*MITRE ATT&CK Framework.*



# Introduction

This case study was undertaken using Elasticsearch (ELK stack) to search through a dataset contained in the timeframe 29/9/21 10:00 – 01/10/21 14:00. “Beats”, which are like categories of searches, were used for searching, namely: Filebeat (logs and files), Packetbeat (network data and traffic), Auditbeat (audit data for Linux) and Metricbeat (OS host monitoring and system/service).

Any evidence of cyber-attacks was searched for in the dataset using key words, search terms and specific fields contained within the data ie user, login, http, file, destination IP, email and source IP. Interesting results were further investigated using available related terms and fields, to determine if there was a cyber-attack present. All results are contained in this report.

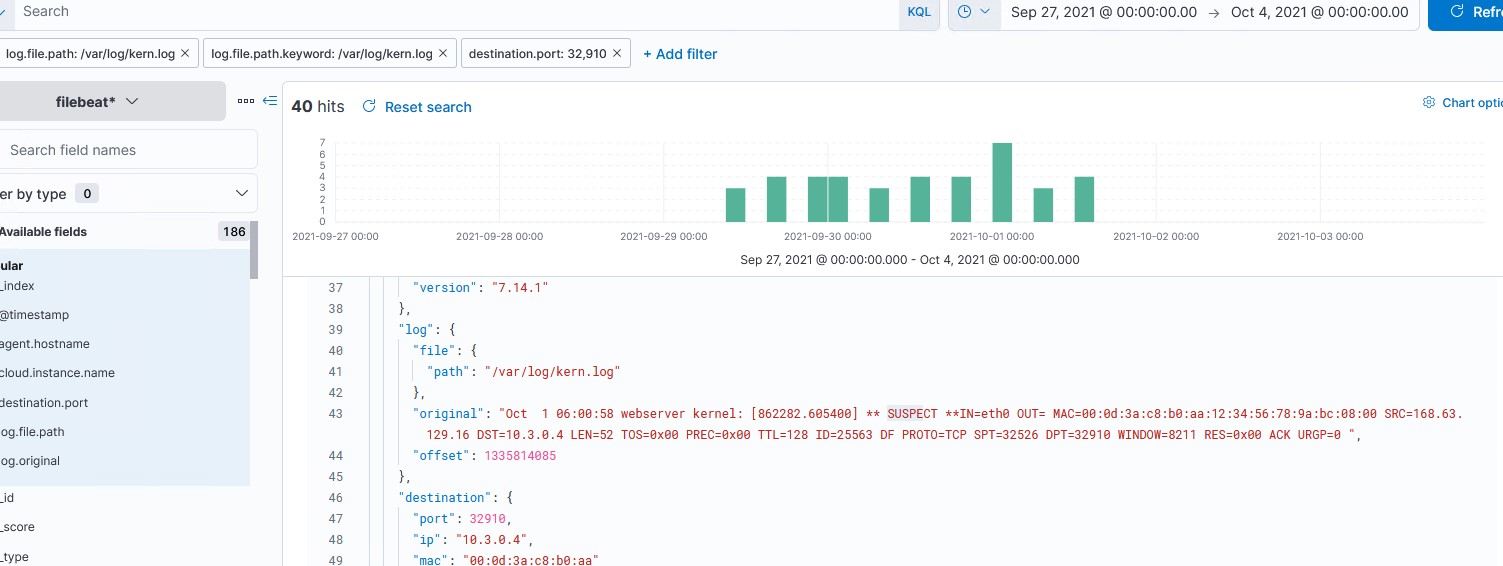
# Technical Details

## Cyber-attack 1 - Malicious file upload – SUCCESS

Between 29/9/21 11:51 and 1/10/21 7:32 a malicious file was successfully uploaded as “/var/log/kern.log “. Event “log:original” shows a long string of text containing the word “suspect” confirming the upload (see Figure 1.) This file was uploaded 36 times to the IP 10.3.0.4.

Figure **1**.

*Screenshot of malicious file upload*.



**Relevant/Interesting Results**

destination IP 10.3.0.4

source IP 168.63.129.16

iptables “ACK” and “PSH”

**Relation to the Lockheed Martin Kill Chain**

*Stage 3: Delivery* – *Delivery of weaponised package to the victim*. The file was delivered via upload. A vulnerability in the iptables rules that allows for multiple connections may have been exploited.

*Stage 5: Installation* – *Installing malware on the asset*. The uploaded file may be auto-executing or it may require user interaction to execute. The contents and intent of the file are unknown, although “webserver kernel” is included in the file log description.

**Relation to the MITRE ATT&CK Framework**

This attack relates to the following MITRE ATT&CK techniques:

* *Execution* – User Execution – Malicious File. It remains unclear what the file contained or what its intentions were. User interaction may be required to activate the malware.
* *Defense Evasion* - Masquerading. The uploaded file may not be a “log” file and could be disguised as an “exe” or some other extension to trick a user into opening it (hence the “suspect” tag). This can be achieved by editing the file in a hex editor to alter the first few bytes.
* *Resource Development* - Stage Capabilities - Upload Malware. The file was uploaded to the IP 10.3.0.4 and from there any number of harmful events/activities could occur including: malicious script execution or backdoor installation.

## Cyber-attack 2 - Attempted SSH login as ROOT user – FAILED

Repeated failed attempts between 29/9/21 10:12 and 1/10/21 13:59 at logging into a mailserver using SSH. Results show 8,800 authentication/login failures under the username “root” from Yangzhou, China. This was likely a brute force botnet attack against the mailserver password.

**Relevant/Interesting Results**

destination.as.organization.name: Chinanet.

source IP- 61.177.173.20- China.

**Relation to the Lockheed Martin Kill Chain**

*Stage 1: Reconnaissance* – *Researching, identifying and gaining information to use in the attack ie email addresses, IP addresses etc*.

The attacker would have initially used a scanning tool such as Nmap to search identify such things as:

* The target IP.
* Any open ports available for access.
* Running services and versions on the system.

Known vulnerabilities of the mailserver could then be searched for using this information to gain access using SSH.

*Stage 2: Weaponization – Combining malware with a deliverable payload*.

With open ports found, the attacker could plan their brute force attack using a wordlist of common passwords. They could also search an online database (such as https://cve.mitre.org) for common vulnerabilities related to the service versions found. This attack also made use of an SSH which the attacker could have configured through the upload of a php file to the server to gain access to the mailserver remotely.

**Relation to the MITRE ATT&CK Framework**

This attack relates to the following MITRE ATT&CK techniques:

* *Initial Access* – Valid Accounts: misuse of credentials to gain initial access. Access controls may be avoided, continuous access may be used to control other services remotely such as VPN’s or other network devices. Access to the mailserver could have resulted in the attacker discovering an inactive email account/user and taking advantage of it.
* *Privilege Escalation* – Abuse Elevation Control Mechanism. Gaining higher-level permissions to elevate privileges. Admin access would likely result in the attacker being able to perform tasks previously unavailable to standard users.
* *Credential Access –* Brute Force: using brute force techniques (such as wordlists, common passwords) to gain access to accounts. This technique can lead to password guessing, cracking, spraying or credential stuffing.
* *Resource Development –* Acquire Infrastructure – Botnet: the use of a network of compromised systems that can be used in the brute force attack. A follow-on technique may be large scale phishing.
* *Resource Development* – Compromise Accounts: if root access is gained, the attacker may compromise other existing accounts in the system. The attacker may impersonate the root or another user to gain trust in other users and perform social engineering for further cyber-attacks on social media, email or cloud accounts.

## Cyber-attack 3 -Login as Root user – FAILURE

On the 29/9/21 between 10:15 and 14:12 there were 45 attempts from source IP 209.141.59.200 to login to an unconfirmed source through an SSH as a ROOT user. All attempts failed and were logged as “authentication failure”. This attack was likely another brute force attempt on the password for the ROOT user, from a different IP. With the smaller amount of login attempts in contrast to the previous attack (45 compared to 8,800 ) this attack was likely human interaction.

**Relevant/Interesting Results**

user:name: root

process:executable: \usr\bin\sshd

source IP: 209.141.59.200

acct: root

terminal: sshd

message\_type: user\_login

result: fail

event:type: authentication\_failure

**Relation to the Lockheed Martin Kill Chain**

*Stage 1: Reconnaissance* – *Researching, identifying and gaining information to use in the attack ie email addresses, IP addresses etc*.

The attacker would have initially used a scanning tool such as Nmap to search identify such things as:

* The target IP.
* Any open ports available for access.
* Running services and versions on the system.

Known vulnerabilities of the mailserver could then be searched for using this information to gain access using SSH.

*Stage 2: Weaponization – Combining malware with a deliverable payload*.

With open ports found, the attacker could plan their brute force attack using a wordlist of common passwords. They could also search an online database (such as https://cve.mitre.org) for common vulnerabilities related to the service versions found. This attack also made use of an SSH which the attacker could have configured through the upload of a php file to the server to gain access to the mailserver remotely.

**Relation to the MITRE ATT&CK Framework**

This attack relates to the following MITRE ATT&CK techniques:

* *Initial Access* – Valid Accounts: misuse of credentials to gain initial access. Access controls may be avoided, continuous access may be used to control other services remotely such as VPN’s or other network devices. This technique can lead to access of other accounts (default, domain, local or cloud). Access to the unconfirmed source could have resulted in any number of subsequent attacks. The source could have been a webpage, email account, user account, webserver/mailserver, database etc.
* *Resource Development* – Compromise Accounts: if root access is gained, the attacker may compromise other existing accounts in the system. The attacker may impersonate the root or another user to gain trust in other users and perform social engineering for further cyber-attacks on social media, email or cloud accounts.
* *Initial Access* – Phishing: emails may be sent from the compromised root account to other users to gain further access/privileges.
* *Initial Access -* Trusted Relationship: the attacker may continue to abuse their gained privileges to breach third party users known to the original victim. These third parties may themselves have higher access granted to them for internal management (ie IT service contractors, physical security) and may exist on the same network as the initial breach.
* *Credential Access –* Brute Force: using brute force techniques (such as wordlists, common passwords) to gain access to accounts. This technique can lead to password guessing, cracking, spraying or credential stuffing.
* *Privilege Escalation* – Abuse Elevation Control Mechanism: Gaining higher-level permissions to elevate privileges. Admin access would likely result in the attacker being able to perform tasks previously unavailable to standard users. This technique can lead to bypassing user account controls and an elevated prompt.

## Possible Cyber-attack 4 -Encryption of Data – Inconclusive

Evidence of encryption was found in the dataset but not enough to confirm or deny a cyber-attack. Multiple instances of hashing algorithms were discovered including: SHA1, SHA256, RSA, SHA1. This could have been an example of someone (disgruntled user) trying to encrypt data they were not authorised to access, or highly sensitive data that was unprotected. This act could be damaging if there were no backups of the encrypted files and could ultimately lead to a ransomware attack. The error code “47, illegal parameter” indicates a violation of security guidelines regarding SSL/TLS connections.

**Relevant/Interesting Results**

Port 443

Source IP - 52.230.25.243

Destination IP - 10.0.0.4

Ingress

Encryption SHA1 “FDD969AC34642572E46A25CF35CC8BE93C4E99D0”

Organization – Let’s Encrypt

Signature algorithm – Sha256-RSA

Alerts – severity: “fatal”, code “47”, type: “illegal\_parameter”, source: “server”.

**Relation to the Lockheed Martin Kill Chain**

Although not identified as an actual attack, this act can still be related to the following stages in relation to a ransomware attack:

*Reconnaissance - Researching, identifying and gaining information to use in the attack ie email addresses, IP addresses etc*.

Identifying which files/folders to encrypt and if there are backups present.

*Weaponization – Combining malware with a deliverable payload*.

Collecting all encrypted data into an encrypted folder to hold for “ransom”.

*Delivery – Delivery of weaponised package to the victim*.

Contacting the victim (usually by email) to inform them their files have been encryptedand are inaccessible.

*Exploitation – Activating the code to trigger the malware on target system.*

The initial access of the data and subsequent encryption.

*Actions on Objectives – The attacker achieving their objective and possibly moving on to another target.*

If the ransom is paid, the attack is successful. The encrypted data may then be unencrypted and returned to the owner, but this is not always the case.

**Relation to the MITRE ATT&CK Framework**

* *Impact –* Data Encrypted for Impact: encryption of data to compromise its Confidentiality, Integrity or Availability (CIA). This can lead to a ransomware attack. If malware is used for encryption, it can move through the target network and employ other techniques such as gaining access to other accounts or internal defacement.
* *Collection –* Archived collected Data: the encryption of data before possible exfiltration.

# Tools and Countermeasures

*Cyber-attack 1*.

* To prevent malicious files being uploaded to a server, file contents should be verified upon successful upload. Files can be altered using a hex editor to change their appearance and may not be what they claim to be.
* Anti-virus software can also be used to scan and detect uploaded files for malware.
* Windows 10 contains “Attack Surface Reduction” rules that prevent potentially malicious files from executing.
* Application control, restricting program execution and regular user training are further mitigation strategies for this attack.

*Cyber-attack 2*.

* Regular updates/patching of system software.
* Investigating failed login attempts (such as this attack) to determine the source.
* Employing multi-factor authentication (MFA) and regular changing of user passwords.
* Password policies should be in use to enforce this and should also contain rules such as: no reusing old passwords and no using the same password for work/private accounts.
* Application storage of credentials should be hashed or saved securely.
* Default usernames/passwords should be changed if in use.
* Regular checks of inactive accounts that can be removed/deactivated.
* Lock out policy that prevents further password guessing attempts after a certain number has failed.
* If an account has been breached, it should be reset.

*Cyber-attack 3*.

* The TCP protocol uses a 3-way handshake which includes SYN, SYN-ACK and ACK. Configuring the iptables to limit the number of connections would help to mitigate this type of attack.
* User training and awareness regarding phishing.
* MFA should be in place.
* Network segmentation to isolate other areas of the network.

*Cyber-attack 4*.

* Limiting access to certain files/folders.
* Password protecting all sensitive data would ensure nothing is encrypted by an unauthorised user.
* Implementing a Disaster Recovery Plan (DRP) in case backup files are needed to restore systems.
* Regular system scans to detect user/file activity.

# Running Sheet

|  |  |  |
| --- | --- | --- |
| TIMESTAMP | ACTION/ SEARCH COMMAND | RESULT/OUTCOME |
| 1/05/23  7:59 PM | Opened Elastic Search in Azure VM  Clicked on “Analytics” then “Discover” and changed timeframe to “Last 2 years” | 428,917 hits displayed with “heartbeat” as the selected Beat |
| 1/05/23  8:13 PM | Changed Beat to “packetbeat” | Results displayed 17,948,803 hits |
| 1/05/23  8:14 PM | Added “\_index” filter  Selected “packetbeat-7.14.1-mailcow” | Results displayed 8,237,400 hits |
| 1/05/23  8:20 PM | Added “source.ip: 172.22.1.1” to filter | Results displayed 169,080 hits |
| 1/05/23  8:27 PM | Added “destination.ip: 172.22.1.249” to filter | Results displayed 169,080 hits |
| 1/05/23  8:30 PM | Removed “packetbeat-7.14.1-mailcow” from filter | Results displayed 169,080 |
| 1/05/23  8:40 PM | Added “http.request.method: GET” to search | Results displayed 109,434 hits |
| 1/05/23  8:45 PM | Added “{"1": "warning: .\*\\[([0-9a-f\\.:]+)\\]: SASL .+ authentication failed", "2": "-login: Disconnected \\(auth failed, .+\\): user=.\*, method=.+, rip=([0-9a-f\\.:]+),", "3": "-login: Aborted login \\(tried to use disallowed .+\\): user=.+, rip=([0-9a-f\\.:]+), lip.+", "4": "SOGo.+ Login from '([0-9a-f\\.:]+)' for user .+ might not have worked", "5": "mailcow UI: Invalid password for .+ by ([0-9a-f\\.:]+)", "6": "([0-9a-f\\.:]+) \"GET \\/SOGo\\/.\* HTTP.+\" 403 .+", "7": "Rspamd UI: Invalid password by ([0-9a-f\\.:]+)", "8": "-login: Aborted login \\(auth failed .+\\): user=.+, rip=([0-9a-f\\.:]+), lip.+", "9": "NOQUEUE: reject: RCPT from \\[([0-9a-f\\.:]+)].+Protocol error.+"}” to filter | Results displayed 72,906 hits.  Interesting terms in results:  Authentication failed  Aborted login  Login: disconnected  Mailcow UI: Invalid password  Login: Aborted login  Tried to use disallowed  Might not have worked |
| 1/05/23  8:45 PM | Removed “source.ip: 172.22.1.1” and “destination.ip: 172.22.1.249” from filter and added “http.request.method: \*” to search | Results displayed 2,721,650 hits |
| 1/05/23  9:10 PM | Added “destination.ip: 20.92.232.1” to filter | Results displayed 2,289,568 hits |
| 1/05/23  9:42 PM | Added “source.ip: 10.2.0.4” to filter | Results displayed 484,970 hits |
| 2/05/23  10:50 AM | Added “\_index: filebeat-7.14.1” to filter | Results displayed 2,069,914 hits  Interesting keywords/terms in results:  var/log/kern.log  suspect  iptables “ACK” and “PSH”  Source port 9200  Destination port 59280  Dest IP 10.3.0.4  Related IP 20.92.232.1 |
| 2/05/23  10:58 AM | Added “/var/log/kern.log” to filter | Results displayed 2,032,452 hits |
| 2/05/23  10:58 AM | Added “destination.port: 59,280” to filter | Results displayed 841,039 hits |
| 2/05/23  11:18 AM | Added “source.port: 9,200” to filter | Results displayed 841,012 hits |
| 2/05/23  11:20 AM | New search for “http.request.method: \*” | Results displayed 75,597 hits  Interesting result:  “log.file.path: /hostfs/var/log/nginx/access.log” |
| 2/05/23  11:23 AM | Google search for “nginx access” | Clicked on <https://nginx.org/en/docs/http/ngx_http_access_module.html>  Discovered nginx is related to “limiting access to certain client addresses” |
| 2/05/23  11:31 AM | Added “log.file.path: /hostfs/var/log/nginx/access.log” to filter | Results displayed 38,160 hits |
| 2/05/23  1:30 PM | New search in “filebeat”  Added “user.name: root” and  “cloud.instance.name: mailserver” to filter | Results displayed 14,785 hits  Interesting results:  @timestamp.system.auth.ssh.method: repeated 2 times: [failed password]  process.name: sshd  log.file.path: /hosts/var/log/auth.log |
| 2/05/23  1:35 PM | Added “@timestamp: Oct 1, 2021 @ 13:07:55:000” to filter | Results showed 2 hits |
| 2/05/23  1:35 PM | Removed “@timestamp: Oct 1, 2021 @ 13:07:55:000” from filter  Changed date range to 29/9/21 10AM-01/10/21 2PM | Results showed 9,267 hits  Results showed 11,152 hits |
| 2/05/23  2:10 PM | Switched to PACKETBEAT, cleared filters and added:  Server.domain: elastic.taxing.systems  destination.ip: 20.92.232.1  \_type.doc  \_index: packetbeat-7.14.1-webserver | Results showed 401,953 hits |
| 2/05/23  4:05 PM | Cleared filters and added:  Error.message: Get <http://stack.taxing.systems:9600>: dial tcp 52.230.25.243:9600: connect: connection refused | Results displayed 37, 294 hits  Interesting fields:  “error.type:io.message:”Get \<http://stack.taxing.systems:9600\>: dial tcp 52.230.25.243:9600: connect: connection refused” |
| 5/05/23  9:35 PM | New search for “http.response.status.code :\*” | Results showed 2,366,824 hits |
| 7/05/23  9:00 PM | Cleared filters and added:  server.domain: elastic.taxing.systems  destination.ip: 20.92.232.1  source.ip: 10.2.0.4  http.request.method:post  \_index:packetbeat-7.14.1-mailcow  user\_agent.original: Go-http-client/1.1 | Results showed 360,442 hits.  Interesting event fields:  method:post  transport:tcp  protocol:http  direction:egress |
| 7/05/23  9:15 PM | Added field:  method:post | Results showed 400 hits |
| 7/05/23  9:30 PM | Cleared filters and added:  log.file.path: /var/log/kern.log  log.file.path.keyword: /var/log/kern.log  destination.port: 32910 | Results showed 40 hits |
| 7/05/23  10:05 PM | New search in PACKETBEAT for:  Destination.domain.keyword: 52.230.25.243 | Results showed 43 hits |
| 7/05/23  10:14 PM | Added new fields:  related.ip: 10.0.0.4  related.ip: 185.142.236.36 | Results showed 13 hits  Field “tls.server.hash.sha1” showed a sha1 hash value “FDD969AC34642572E46A25CF35CC8BE93C4E99D0” |
| 7/05/23  10:16 PM | Opened <https://10015.io/tools/sha1-encrypt-decrypt> and attempted to decrypt sha1 hash value | Decryption failed |
| 7/05/23  10:18 PM | Added field: tls.server.hash.sha1: FDD969AC34642572E46A25CF35CC8BE93C4E99D0 | Results showed 7 hits |
| 8/05/23  11:55 AM | Google search for “Microsoft-corp-msn-as-block” | Not sure what this is but is listed as Field: “source.as.organization.name”  Navigated to <https://cleantalk.org/blacklists/as8075> to try to identify meaning of “Microsoft-corp-msn-as-block” |
| 8/05/23  12:38 PM | New search in “filebeat” for “user\_agent.original : \*” | Results showed 2,720,820 hits with fields:  Go-http-client/1.1  Elastic-Heartbeat/7.14.1  WALinuxAgent/2.4.0.2  Rspamd-3.0  Curl/7.6.4.0 |
|  |  |  |
| 8/05/23  1:45 PM | Cleared fields and added:  event.type: access  suricata.eve.http.url: /  suricata.eve.http.http\_method: GET | Results showed 26 hits |
| 9/05/23  10:02 AM | Cleared filters, ran new search for: “destination.ip.keyword: mail” in FILEBEAT | Results returned 19,634 hits  Event “message” showed various fields of interest including:  “dovecot: managesieve-login: Disconnected: Connection closed”  Numerous Docker container events with the heading “ofelia\_job\_exec\_dovecot” |
| 10/05/23  9:45 PM | New search in AUDITBEAT  Added fields:  auditd.message\_type  event.action  event.category  event.outcome  event.type  user.effective.name | Returned 40,674 hits  Interesting field results:  user:name: root  process:executable: \usr\sbin\sshd  source IP: 209.141.59.200  acct: root  terminal: sshd  op: login  secondary: root  message\_type: user\_login  result: fail  event:type: authentication\_failure  action: logged-in  outcome: failure |
|  | Added field “source IP 209.141.59.200” | Results showed 77 hits |
|  | Changed date range to 27/9/21 – 1/10/21 | Results showed 45 hits |

# Timeline of Events

Cyber-attack 1. Malicious file upload. 36 uploads between 29/9/21 11:51 and 01/10/21 7:32.

Cyber-attack 2. Total 8,800 failed login attempts between 29/09/21 10:12 – 1/10/21 13:59

Cyber-attack 3. 45 failed attempts at logging in through SSH as ROOT user on the 29/9/21 between 10:15 and 14:12

Cyber-attack 4 (possible). Encryption of files/folders between 29/9/21 and 01/10/21.

Cyber-attack 1.

Malicious file upload

29/9/21 11:51 – 01/10/21 7:32

Cyber-attack 2.

Attempted SSH login as ROOT user

29/9/21 10:12 – 1/10/21 13:59

Cyber-attack 3.

Attempted login as ROOT user

29/9/21 10:15 – 14:12

Cyber-attack 4.

File encryption

# References

1OOL5. (n.d.). SHA1 *Encrypt/Decrypt*. https://10015.io/tools/sha1-encrypt-decrypt

CleanTalk. (n.d.). AS8075 MICROSOFT-CORP-MSN-AS-BLOCK. https://cleantalk.org/blacklists/as8075

Deepwatch. (n.d.). *The Cyber Kill Chain*. https://www.deepwatch.com/wp-content/uploads/Cyber-Kill-Chain-deepwatch-source-Lockheed-Martin.png

EC-Council. (n.d.). *The Cyber Kill Chain: The Seven Steps of a Cyberattack*. <https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack/>

Lockheed Martin Corporation (2023). *The Cyber Kill Chain*. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Microsoft. (2019). Kaushal. *SSL/TLS Alert Protocol and the Alert Codes*. https://techcommunity.microsoft.com/t5/iis-support-blog/ssl-tls-alert-protocol-and-the-alert-codes/ba-p/377132

Nginx. (n.d.). *Module ngx\_http\_access\_module*. <https://nginx.org/en/docs/http/ngx_http_access_module.html>

Secure Online Desktop. (2020). *Mitre Att&ck ™: an overview*. https://www.secure-od.com/mitre-attck-an-overview/