INTERNSHIP REPORT

WEEK # 4
M. USAMA SHAHBAZ

CONTENTS

ABOUT THE COMPANY

The **Digital Empowerment Network Pakistan** appears to be an initiative focused on improving digital literacy and empowering individuals through training and resources in areas such as cybersecurity, cloud computing, AI, and other digital technologies. These kinds of programs typically aim to bridge the digital skills gap by offering educational programs and certifications to help participants gain practical knowledge and skills that are relevant to today's job market, especially in tech-related fields.

Here's a general breakdown of what such a network could involve:

1. **Educational Programs**: Courses or training programs in areas like cybersecurity, cloud computing, AI, software quality assurance (SQA), and more.
2. **Certifications**: Certifications that help validate the skills learned during the courses, making participants more competitive in the job market.
3. **Community Development**: Initiatives to promote digital literacy in underprivileged communities, helping individuals learn how to use technology to better their lives.
4. **Networking Opportunities**: Connecting learners with professionals, mentors, and industry experts, helping them to grow their career prospects.

Since the details are based on general expectations from such networks, it's advisable to visit their official website or contact them directly to gain more specific information about their mission, vision, and services.

CONFIGURING FIREWALLS AND INTRUSION DETECTION SYSTEMS

1.Objective: Protect the network by setting up firewalls and IDS.

2.Description:

Implement firewalls and intrusion detection systems to monitor and control incoming and outgoing network traffic. Detect and prevent unauthorized access and attacks.

3.Key Steps:

- Selecting appropriate firewall and IDS solutions.
- Configuring firewall rules and policies.
- Setting up IDS to monitor network traffic.
- Analyzing IDS alerts and responding to threats.
- Regularly updating and maintaining the configurations

INTRODUCTION TO FIREWALLS AND INTRUSION

DETECTION SYSTEMS

In today's digital landscape, where cyber threats are increasingly sophisticated and prevalent, organisations must prioritise robust security measures to protect their networks. Two critical components of a comprehensive security strategy are Firewalls and Intrusion Detection Systems (IDS). These technologies work in tandem to create a secure environment for both data and users, ensuring that sensitive information remains protected against unauthorised access and cyber attacks. Firewalls serve as the first line of defence in network security. They are designed to monitor and control incoming and outgoing network traffic based on predetermined security rules. By acting as a barrier between a trusted internal network and untrusted external networks, firewalls filter out potentially harmful traffic. This filtering process can be based on various criteria, including IP addresses, protocols, and ports, effectively preventing unauthorised users from accessing the network. Firewalls can be implemented in hardware, software, or a combination of both, providing flexibility in deployment according to organisational needs. Their ability to enforce policies and control traffic helps mitigate risks associated with data breaches, malware infections, and other cyber threats. Intrusion Detection Systems (IDS) are crucial for monitoring network traffic and identifying suspicious activities that may indicate a security breach. IDS can analyse various

data packets traversing the network and use signature-based detection to identify known threats or anomaly-based detection to flag unusual behaviour that deviates from established norms. Upon detecting a potential intrusion, an IDS generates alerts for system administrators, enabling them to respond swiftly to potential threats. While firewalls focus on preventing unauthorised access, IDS complements this by providing visibility into ongoing network activities, helping organisations detect and respond to incidents in real-time. The necessity of implementing both firewalls and IDS cannot be overstated. Firewalls provide a proactive defence by controlling traffic at the perimeter, significantly reducing the attack surface. However, they are not infallible; sophisticated attackers can sometimes bypass firewalls through various techniques, such as social engineering or exploiting application vulnerabilities. This is where IDS becomes invaluable. By continuously monitoring network traffic and system behaviour, IDS can detect breaches that may have slipped past the firewall, offering an additional layer of protection. Moreover, the integration of firewalls and IDS enhances an organisation's overall security posture. By working together, these technologies create a defence-in-depth strategy, which is essential in modern cybersecurity frameworks. Organisations can not only prevent unauthorised access but also have the capability to detect and respond to security incidents promptly. This is particularly important in today's regulatory environment, where organisations are required to comply with various data protection laws, such as GDPR and HIPAA, that mandate stringent security measures

CONFIGURING FIREWALL RULES AND POLICIES

● Update the system to ensure that all packages and dependencies are current, enhancing security, stability, and compatibility with new software.

```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get update
[sudo] password for kali:
Get:1 https://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 https://kali.download/kali kali-rolling/main amd64 Packages [20.1 MB]
Get:3 https://kali.download/kali kali-rolling/main amd64 Contents (deb) [48.8 MB]
Get:4 https://kali.download/kali kali-rolling/contrib amd64 Packages [110 kB]
Get:5 https://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [268 kB]
Get:6 https://kali.download/kali kali-rolling/non-free amd64 Packages [195 kB]
Get:7 https://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [875 kB]
Get:8 https://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [10.8 kB]
Get:9 https://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb) [22.8 kB]
Fetched 70.5 MB in 45s (1,552 kB/s)
Reading package lists... Done
```

● Install ufw

```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install ufw
```

● Now Enable ufw

```
┌──(kali㉿kali)-[~]
└─$ sudo ufw enable
Firewall is active and enabled on system startup
```

● Setup basic rules.

```
┌──(kali㉿kali)-[~]
└─$ sudo ufw allow 22/tcp
Rule added
Rule added (v6)
```

● Check the existing rules in the firewall.

```
┌──(kali㉿kali)-[~]
└─$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW IN    Anywhere
22/tcp (v6)                ALLOW IN    Anywhere (v6)
```

SETTING UP INTRUSION DETECTION SYSTEMTOMONITOR NETWORK TRAFFIC

● Install suricata.

● Check the status of suricata and make sure it is inactive.

● List down the IDS configuration to check the files.

```
┌──(kali㉿kali)-[~]
└─$ sudo ls -al /etc/suricata
total 116
drwxr-xr-x   3 root root  4096 Oct  2 10:02 .
drwxr-xr-x 192 root root 12288 Oct  2 10:02 ..
-rw-r--r--   1 root root  3327 Jun 26 03:23 classification.config
-rw-r--r--   1 root root  1375 Jun 26 03:23 reference.config
drwxr-xr-x   2 root root  4096 Oct  2 10:02 rules
-rw-r--r--   1 root root 85757 Jun 27 08:29 suricata.yaml
-rw-r--r--   1 root root  1643 Jun 26 03:23 threshold.config
```

● Open the suricata.yaml file to set up the IDS configuration. Search HOMENET
and change its ip to the systems ip as we are using the same system to ping the ip.
To check the system ip, open another terminal and write ip a s to check the ip.

```
┌──(kali㉿kali)-[~]
└─$ ip a s
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:1e:36:4a brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.108/24 brd 192.168.100.255 scope global dynamic noprefixroute eth0
       valid_lft 85116sec preferred_lft 85116sec
    inet6 fe80::43fe:b377:d656:b11/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

● Now search af-packet and make sure it has the same ethernet connection as of the ip address your are using.

```
# Linux high speed capture support
af-packet:
  - interface: eth0
```

● Setup custom rules in the rules file.

```
File  Actions  Edit  View  Help

  GNU nano 8.1                          /etc/suricata/rules/local.rules *
alert icamp any any → $HOME_NET any (msg:"ICMP Ping"; sid:1; rev:1; )
```

● Add rules file path in the suricata.yaml file

```
rule-files:
  - suricata.rules
  - /etc/suricata/rules/local.rules
```

● After setting up the configuration and rules, update suricata.

```
─(kali⊛kali)-[~]
─$ sudo suricata-update
/10/2024 -- 11:19:02 - <Info> -- Using data-directory /var/lib/suricata.
/10/2024 -- 11:19:02 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
/10/2024 -- 11:19:02 - <Info> -- Using /etc/suricata/rules for Suricata provided rules.
/10/2024 -- 11:19:02 - <Info> -- Found Suricata version 7.0.6 at /usr/bin/suricata.
/10/2024 -- 11:19:02 - <Info> -- Loading /etc/suricata/suricata.yaml
/10/2024 -- 11:19:02 - <Info> -- Disabling rules for protocol pgsql
/10/2024 -- 11:19:02 - <Info> -- Disabling rules for protocol modbus
/10/2024 -- 11:19:02 - <Info> -- Disabling rules for protocol dnp3
/10/2024 -- 11:19:02 - <Info> -- Disabling rules for protocol enip
/10/2024 -- 11:19:02 - <Warning> -- No index exists, will use bundled index.
/10/2024 -- 11:19:02 - <Warning> -- Please run suricata-update update-sources.
/10/2024 -- 11:19:02 - <Info> -- Fetching https://rules.emergingthreats.net/open/suricata-7.0.6/emerging.
```

● Now download suricata from the list sources and configure.

● Start suricata.

● Now check the status of suricata.

● Now ping your ip and check the logs in suricata.

● Monitor the logs and disable the suricata after monitoring.

CONCLUSION

In conclusion, the configuration of firewalls and Intrusion Detection Systems (IDS) is crucial for bolstering the cybersecurity posture of organizations. Firewalls act as the first line of defense, meticulously controlling network traffic based on predefined security rules to prevent unauthorized access and mitigate threats. Meanwhile, IDS provides continuous monitoring, enabling the detection of suspicious behavior and facilitating timely responses to potential breaches. This layered approach not only reduces the attack surface but also enhances the organization's ability to respond effectively to emerging threats. Throughout this internship, I have gained valuable hands-on experience in implementing and managing these essential security technologies, highlighting the importance of maintaining updated configurations and monitoring logs to ensure their ongoing effectiveness against evolving cyber threats