Name: Muhammad Usman Ali Sadiq

Cyber Security

Company: Code Alpha

Task 03

Network Intrusion Detection System

1.Install Snort

First, ensure that your system is up to date:

```
┌──(kali㉿kali)-[~]
└─$ sudo apt update && sudo apt upgrade -y

[sudo] password for kali:
Get:1 http://mirrors.dotsrc.org/kali kali-rolling InRelease [41.5 kB]
Get:2 http://mirrors.dotsrc.org/kali kali-rolling/main amd64 Packages [20.2 MB]
Get:3 http://mirrors.dotsrc.org/kali kali-rolling/main amd64 Contents (deb) [48.1 MB]
Get:4 http://mirrors.dotsrc.org/kali kali-rolling/non-free amd64 Packages [197 kB]
Get:5 http://mirrors.dotsrc.org/kali kali-rolling/non-free amd64 Contents (deb) [878 kB]
Fetched 69.4 MB in 45s (1,540 kB/s)
60 packages can be upgraded. Run 'apt list --upgradable' to see them.
The following packages were automatically installed and are no longer required:
  freerdp2-x11  libfreerdp-client2-2t64  libfreerdp2-2t64  libjim0.82t64  libllvm18  libwinpr2-2t64  linux-image-6.8.11-amd64
Use 'sudo apt autoremove' to remove them.

Upgrading:
  busybox    firefox-esr      gtk-update-icon-cache  libgtk-4-1       libgtk-4-media-gstreamer  libqt5help5       libxcb-util1  mitmproxy            python3-pyinstaller-hooks-contrib
  easy-rsa   fonts-lyx        init                   libgtk-4-bin     libntfs-3g89t64           libwnck-3-0       libxext-dev   ntfs-3g              usb-modeswitch
  exploitdb  gir1.2-wnck-3.0  init-system-helpers    libgtk-4-common  libqt5designer5           libwnck-3-common  libxext6      python3-cryptography

Installing dependencies:
  libjim0.83

Not upgrading:
  exiv2                libqt6dbus6t64     libqt6opengl6t64         libqt6qmlmodels6  libqt6svg6               libqt6widgets6t64          python3-pypsrp        qt6-qpa-plugins  wireshark
  firmware-linux-free  libqt6gui6t64      libqt6openglwidgets6t64  libqt6quick6      libqt6test6t64           libqt6wlshellintegration6  python3-pyqt6         qt6-wayland      wireshark-common
  libqt6core5compat6   libqt6multimedia6  libqt6printsupport6t64   libqt6sql6-sqlite  libqt6waylandclient6     libqt6xml6t64              qt6-base-dev-tools    qt6ct
  libqt6core6t64       libqt6network6t64  libqt6qml6               libqt6sql6t64      libqt6waylandcompositor6  pyqt6-dev-tools            qt6-gtk-platformtheme  tshark

Summary:
  Upgrading: 26, Installing: 1, Removing: 0, Not Upgrading: 34
  Download size: 115 MB
  Space needed: 20.6 MB / 53.7 GB available

Get:1 http://http.kali.org/kali kali-rolling/main amd64 init-system-helpers all 1.67+kali1 [40.5 kB]
Get:2 http://http.kali.org/kali kali-rolling/main amd64 init amd64 1.67+kali1 [6,596 B]
Get:3 http://kali.download/kali kali-rolling/main amd64 python3-cryptography amd64 43.0.0-1 [935 kB]
Get:4 http://kali.download/kali kali-rolling/main amd64 mitmproxy all 11.0.0-0kali2 [929 kB]
Get:7 http://mirrors.dotsrc.org/kali kali-rolling/main amd64 exploitdb all 20241002-0kali1 [30.1 MB]
Get:5 http://kali.download/kali kali-rolling/main amd64 busybox amd64 1:1.37.0-4 [485 kB]
Get:6 http://kali.download/kali kali-rolling/main amd64 easy-rsa all 3.2.1-1 [70.5 kB]
Get:8 http://http.kali.org/kali kali-rolling/main amd64 libxext-dev amd64 2:1.3.4-1+b2 [104 kB]
Get:9 http://http.kali.org/kali kali-rolling/main amd64 libxext6 amd64 2:1.3.4-1+b2 [50.5 kB]
Get:11 http://kali.download/kali kali-rolling/main amd64 fonts-lyx all 2.4.2.1-1 [190 kB]
Get:13 http://kali.download/kali kali-rolling/main amd64 libwnck-3-0 amd64 43.1-1 [110 kB]
Get:15 http://http.kali.org/kali kali-rolling/main amd64 gtk-update-icon-cache amd64 4.16.3+ds-1 [49.7 kB]
Get:16 http://http.kali.org/kali kali-rolling/main amd64 libgtk-4-common all 4.16.3+ds-1 [2,515 kB]
Get:17 http://http.kali.org/kali kali-rolling/main amd64 libgtk-4-1 amd64 4.16.3+ds-1 [3,145 kB]
```

Then, install Snort:

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

snort is already the newest version (3.1.82.0-0kali1+b1).
The following packages were automatically installed and are no longer required:
  freerdp2-x11  libfreerdp-client2-2t64  libfreerdp2-2t64  libllvm18  libwinpr2-2t64  linux-image-6.8.11-amd64
```

You can verify the installation with:

```
┌──(kali㉿kali)-[~]
└─$ snort -V

   ,,_     -*> Snort++ <*-
  o"  )~   Version 3.1.82.0
   ''''    By Martin Roesch & The Snort Team
           http://snort.org/contact#team
           Copyright (C) 2014-2024 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using DAQ version 3.0.12
           Using LuaJIT version 2.1.1700206165
           Using OpenSSL 3.3.2 3 Sep 2024
           Using libpcap version 1.10.5 (with TPACKET_V3)
           Using PCRE version 8.39 2016-06-14
           Using ZLIB version 1.3.1
           Using LZMA version 5.6.2
```

2. Configure Snort

Step 1: Locate the Snort configuration file

Snort's main configuration file is located at:

```
┌──(kali㉿kali)-[~]
└─$ /etc/snort/snort.conf
```

Open this file in your favorite text editor

```
┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/snort/snort.conf
```

You will need to adjust the network settings to reflect your environment. Look for the line that sets the network variable:

```
var HOME_NET 192.168.19.129/24
```

Step 2: Enable Rules

Snort works based on rule sets, which define patterns of malicious activity. To enable specific rules, navigate to the rule's directory:

```
┌──(kali㉿kali)-[~]
└─$ /etc/snort/rules
```

Enable default rule sets in snort.conf by uncommenting them, for example:

```
┌──(kali㉿kali)-[/etc/snort/rules]
└─$ include $RULE_PATH/community.rules
```

Step 3: Add Custom Rules

You can create custom rules to detect specific activities. Open the local. Rules file to define custom rules:

```
┌──(kali㉿kali)-[/etc/snort/rules]
└─$ sudo nano /etc/snort/rules/local.rules
```

Step 4: Test Snort

Before running Snort, you need to test the configuration to ensure its correctly set up:

```
┌──(kali㉿kali)-[/etc/snort/rules]
└─$ sudo snort -T -c /etc/snort/snort.conf

o")~   Snort++ 3.1.82.0

Loading /etc/snort/snort.conf:
```

3. Run Snort in IDS Mode

Once the configuration is verified, you can run Snort in IDS mode to monitor network traffic:

```
┌──(kali㉿kali)-[/etc/snort/rules]
└─$ sudo snort -A console -i eth0 -c /etc/snort/snort.conf

o")~   Snort++ 3.1.82.0
Loading /etc/snort/snort.conf:
```

- -A console: Output alerts to the console.
- -i eth0: Specifies the network interface to monitor (replace eth0 with your network interface).
- -c /etc/snort/snort.conf: The path to the configuration file.

Snort will now be actively monitoring traffic and will log alerts to the console or a log file.

4. Visualizing Detected Attacks

To visualize detected attacks, you can use third-party tools like **Kibana** or **ELK Stack**. Here's a brief setup using **Kibana** and **Logstash** to visualize Snort logs:

Step 1: Install Logstash and Kibana

In Kali Linux, install **Logstash** and **Kibana**:

```
┌──(kali㉿kali)-[/etc/snort/rules]
└─$ sudo apt install logstash kibana -y
```

Step 2: Configure Logstash

```
┌──(kali㉿kali)-[/etc/snort/rules]
└─$ sudo nano /etc/logstash/conf.d/logstash-snort.conf
```

Add the following configuration to parse Snort logs:

```
input {
    file {
        path ⇒ "/var/log/snort/alert"
        start_position ⇒ "beginning"
    }
}

filter {
    grok {
        match ⇒ { "message" ⇒ "%{SYSLOGTIMESTAMP:timestamp} %{WORD:protocol} %{IP:src_ip} → %{IP:dst_ip}" }
    }
}

output {
    elasticsearch {
        hosts ⇒ ["localhost:9200"]
        index ⇒ "snort-alerts-%{+YYYY.MM.dd}"
    }
}
```

Step 3: Run Logstash and Kibana

Start **Logstash**:

```
┌──(kali㉿kali)-[/etc/snort/rules]
└─$ sudo systemctl start logstash
```

Start **Kibana**:

```
┌──(kali㉿kali)-[/etc/snort/rules]
└─$ sudo systemctl start kibana
```

You can access Kibana through a web browser at http://localhost:5601. Use Kibana's interface to visualize the Snort alerts being ingested from Logstash.