SEC 285 Project: Network and Security

Tyler Brainer

Introduction

In this project I learned and demonstrated various forms of security measures. I learned how to utilize tools to implement and configure cryptography, firewalls, multifactor authentication, and vulnerability assesments.

Cryptography

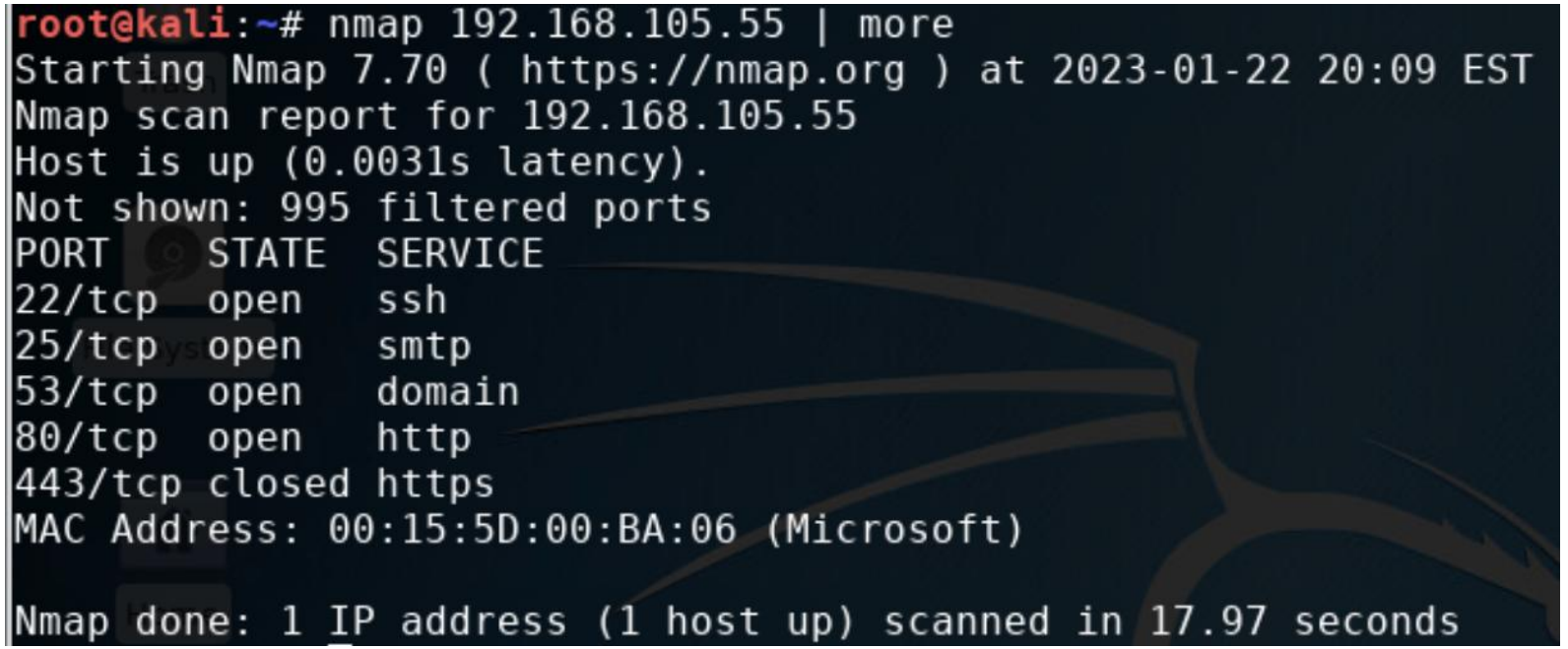
I used a kali Linux CLI to create a file and encrypt it with gpg.
I then decrypted the file showing the plaintext after decryption

```
root@kali:~# cat testfile.txt
This is a test file that we will encrypt with gpg
root@kali:~# cat testfile.txt.gpg
[binary data]
root@kali:~#
```

```
root@kali:~# ls test*
testfile.txt.gpg
root@kali:~# gpg testfile.txt.gpg
gpg: WARNING: no command supplied.  Trying to guess what you mean ...
gpg: AES256 encrypted data
gpg: encrypted with 1 passphrase
root@kali:~# ls test*
testfile.txt  testfile.txt.gpg
root@kali:~# cat testfile.txt
This is a test file that we will encrypt with gpg
```

Stateful Firewall

I scanned for open ports on the network and then specified policy rules with INPUT DROP to filter through the ports to block traffic tat does not meet the rules


root@kali:~# nmap 192.168.105.55 | more
Starting Nmap 7.70 (https://nmap.org) at 2023-01-22 20:09 EST
Nmap scan report for 192.168.105.55
Host is up (0.0031s latency).
Not shown: 995 filtered ports
PORT STATE SERVICE
22/tcp open ssh
25/tcp open smtp
53/tcp open domain
80/tcp open http
443/tcp closed https
MAC Address: 00:15:5D:00:BA:06 (Microsoft)
Nmap done: 1 IP address (1 host up) scanned in 17.97 seconds

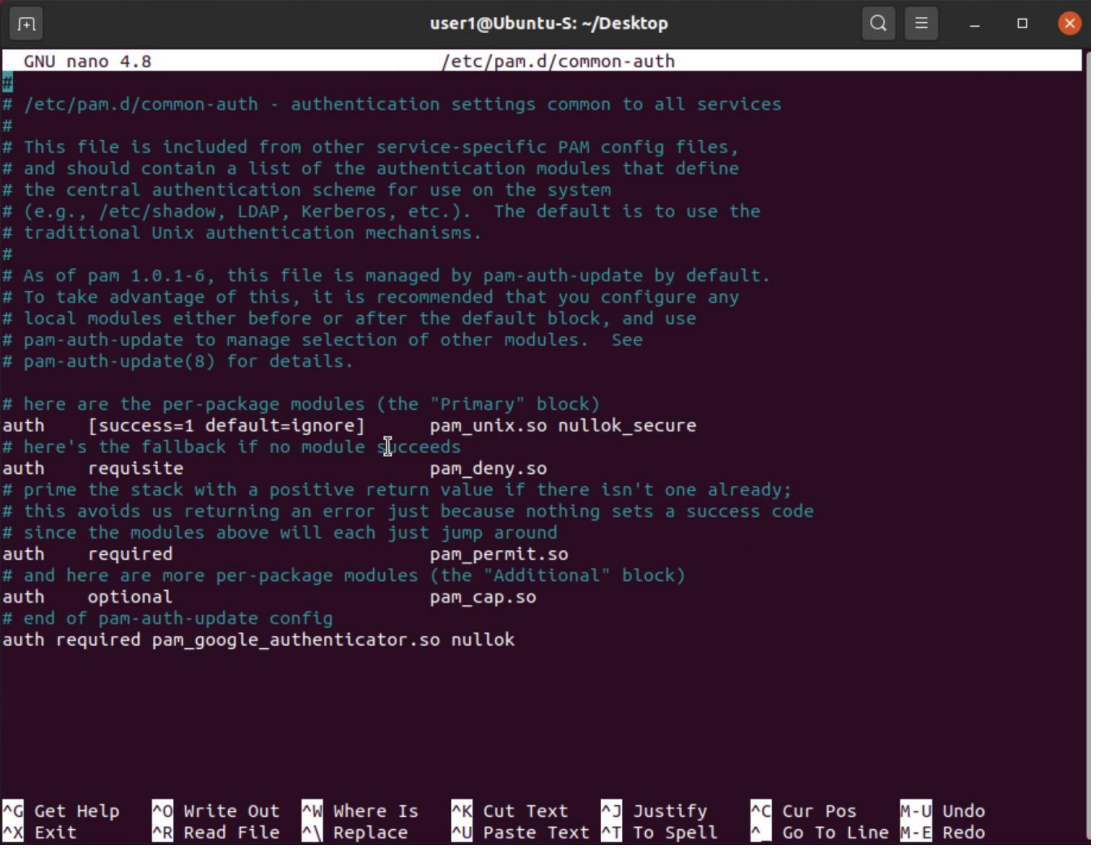
BYOD Security Policy

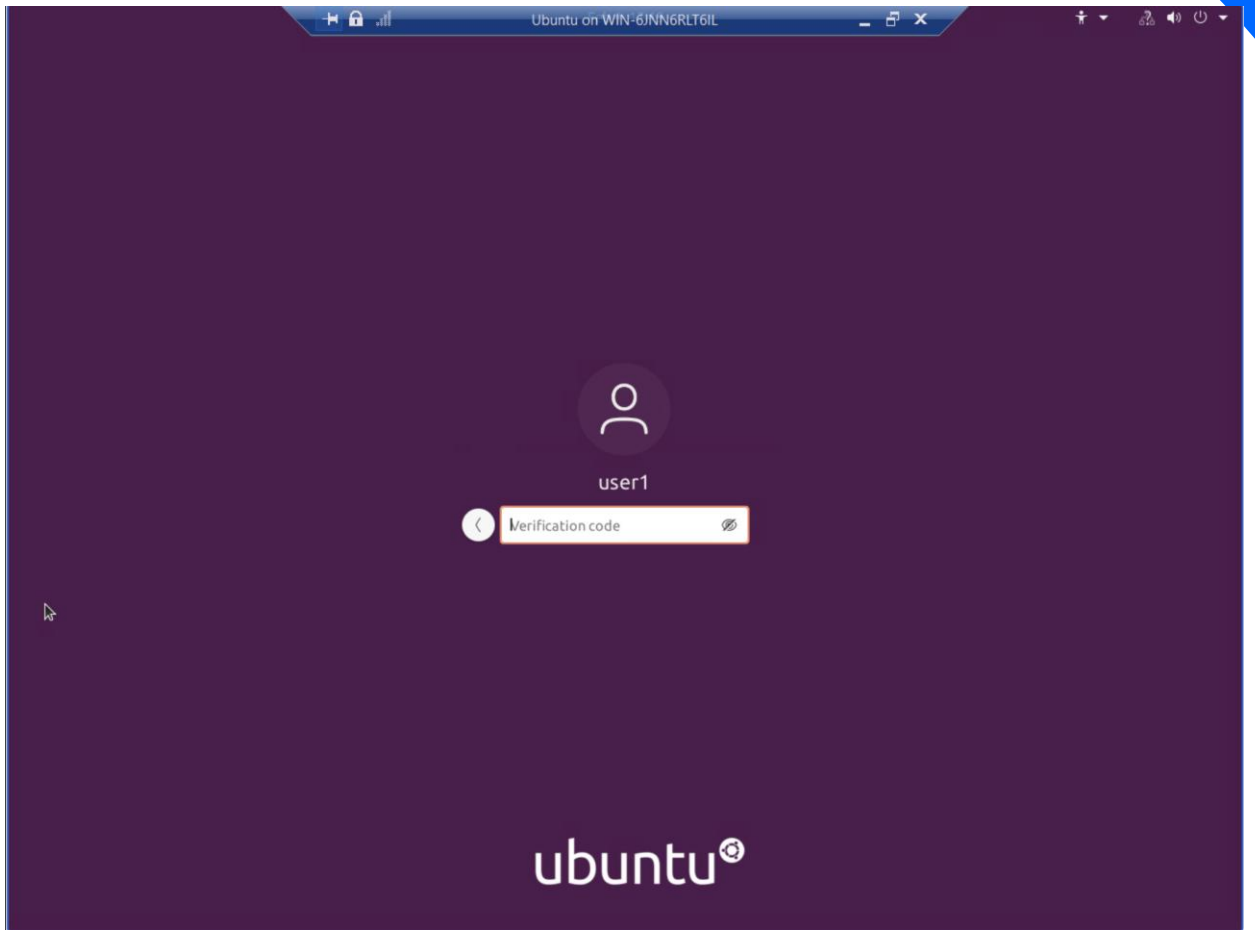
I created a policy for Bring Your Own Device (BYOD) that established who is in charge of enforcing the rules, requirements of encryption and passwords for devices. This policy lists what is allowed on the network and what is not.

Double click to open BYOD policy

Multi-factor Authentication

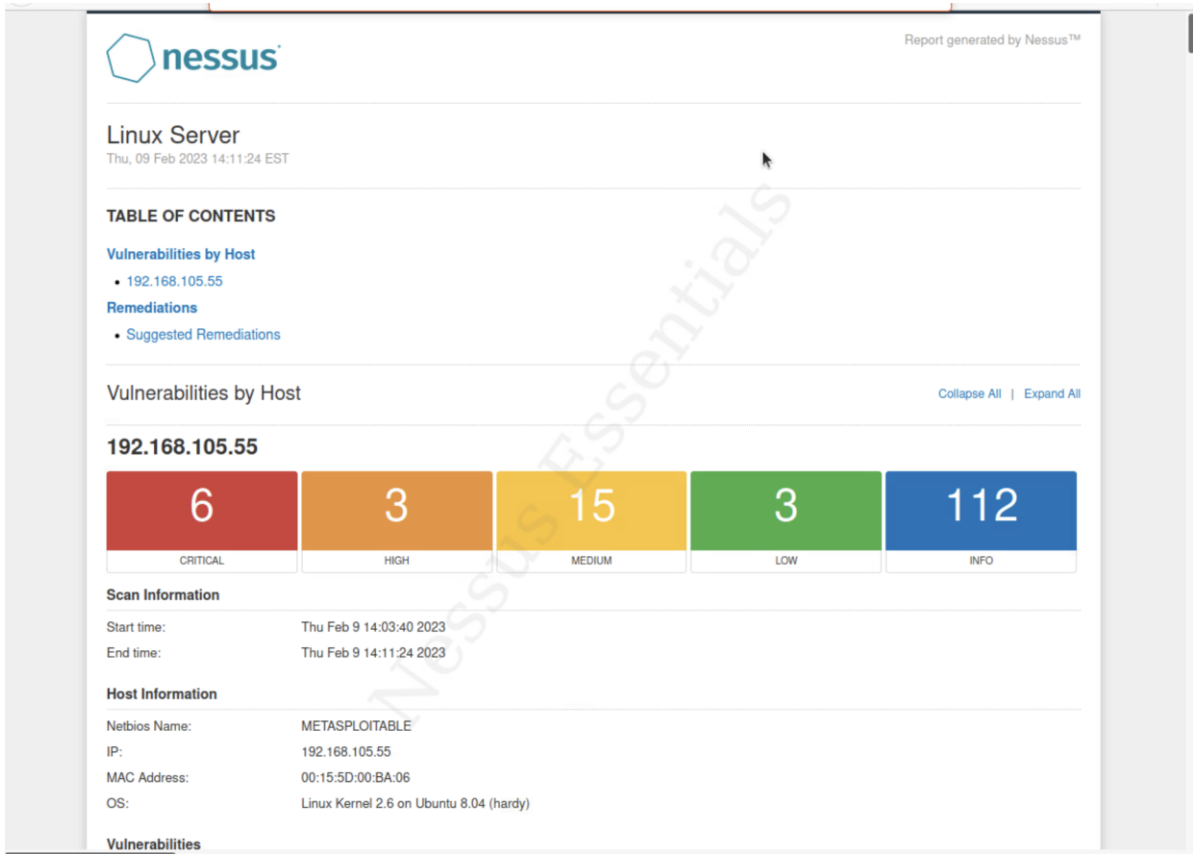
I configure Multi-factor Authentication to be enforced when logging into a Ubuntu VM. This was done by adding the auth required by google authenticator in the common-auth file. The google authenticator app generates a code and requires it to login.

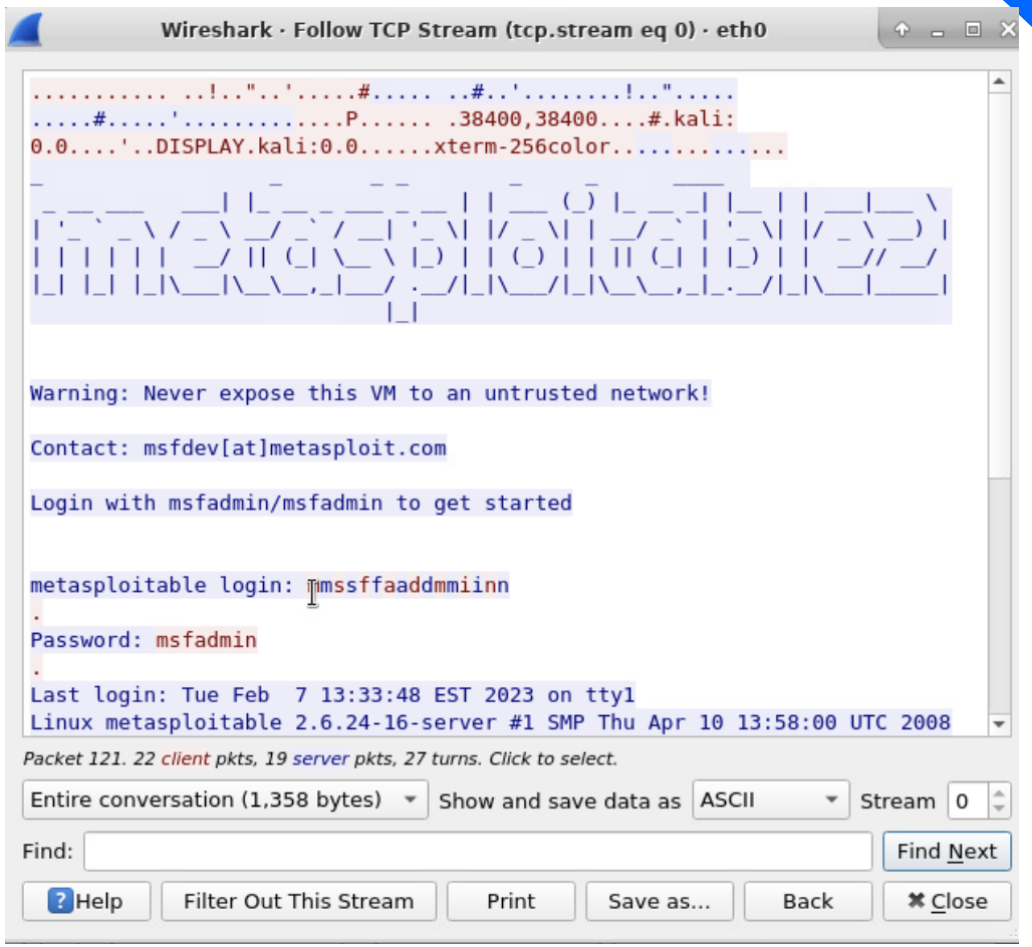

user1@Ubuntu-S: ~/Desktop
GNU nano 4.8 /etc/pam.d/common-auth
#
/etc/pam.d/common-auth - authentication settings common to all services
#
This file is included from other service-specific PAM config files,
and should contain a list of the authentication modules that define
the central authentication scheme for use on the system
(e.g., /etc/shadow, LDAP, Kerberos, etc.). The default is to use the
traditional Unix authentication mechanisms.
#
As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
To take advantage of this, it is recommended that you configure any
local modules either before or after the default block, and use
pam-auth-update to manage selection of other modules. See
pam-auth-update(8) for details.
here are the per-package modules (the "Primary" block)
auth [success=1 default=ignore] pam_unix.so nullok_secure
here's the fallback if no module succeeds
auth requisite pam_deny.so
prime the stack with a positive return value if there isn't one already;
this avoids us returning an error just because nothing sets a success code
since the modules above will each just jump around
auth required pam_permit.so
and here are more per-package modules (the "Additional" block)
auth optional pam_cap.so
end of pam-auth-update config
auth required pam_google_authenticator.so nullok
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos M-U Undo
^X Exit ^R Read File ^\ Replace ^U Paste Text ^T To Spell ^_ Go To Line M-E Redo


Ubuntu on WIN-6JNN6RLT6IL
user1
Verification code
ubuntu

Vulnerability Assessment

I used various tools to test for vulnerabilities such as Wireshark to capture packets to intercept information between two networks, and nessus to scan for vulnerabilities on the network.


nessus
Report generated by Nessus™
Linux Server
Thu, 09 Feb 2023 14:11:24 EST
TABLE OF CONTENTS
Vulnerabilities by Host
192.168.105.55
Remediations
Suggested Remediations
Vulnerabilities by Host
Collapse All | Expand All
192.168.105.55
6
CRITICAL
3
HIGH
15
MEDIUM
3
LOW
112
INFO
Scan Information
Start time: Thu Feb 9 14:03:40 2023
End time: Thu Feb 9 14:11:24 2023
Host Information
Netbios Name: METASPLOITABLE
IP: 192.168.105.55
MAC Address: 00:15:5D:00:BA:06
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Vulnerabilities
Nessus Essentials


Wireshark · Follow TCP Stream (tcp.stream eq 0) · eth0
.....#.....'.....P..... .38400,38400....#.kali:
0.0....'..DISPLAY.kali:0.0.....xterm-256color.....
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
metasploitable login: msfadmin
Password: msfadmin
Last login: Tue Feb 7 13:33:48 EST 2023 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008
Packet 121. 22 client pkts, 19 server pkts, 27 turns. Click to select.
Entire conversation (1,358 bytes)
Show and save data as
ASCII
Stream
0
Find:
Find Next
Help
Filter Out This Stream
Print
Save as...
Back
Close

Career Skills learned

- Encrypting files with password
- Configuring a firewall with policies to filter traffic
- BYOD policy/ creating a security policy
- Setting up 2FA
- Running vulnerability assessments on a system and network.

Conclusion

I enjoyed getting to learn about how to practice efficient security on a network and an insight on vulnerabilities so that I can secure them and prevent a threat actor from stealing data when possible.