SEC 285 Course Project

SEC 285

In this course we explored the fundamentals of network security. Using various tools and techniques we were able to mitigate internal and external threats. Two IoT devices were developed, a program that remotely communicated with a microprocessor and a security system that detected motion.

Topics Covered:

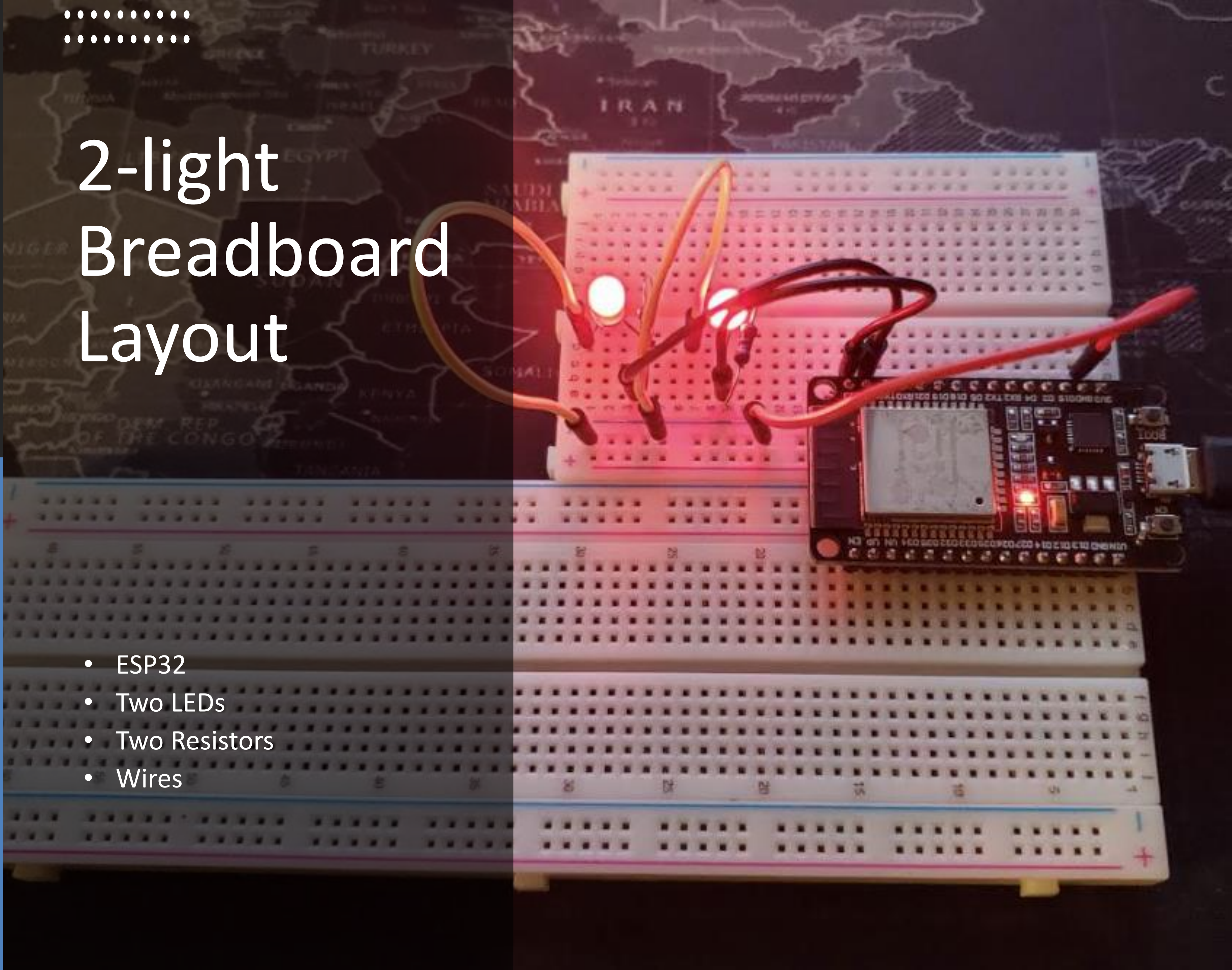
- Electrical circuits and an ESP32 microprocessor
- Python code and Hypertext implementation
- Stateful Firewall & Multi-Factor authentication
- Bring Your Own Device (BYOD) Security Policy
- Asymmetric Key Encryption and Password Enforcement

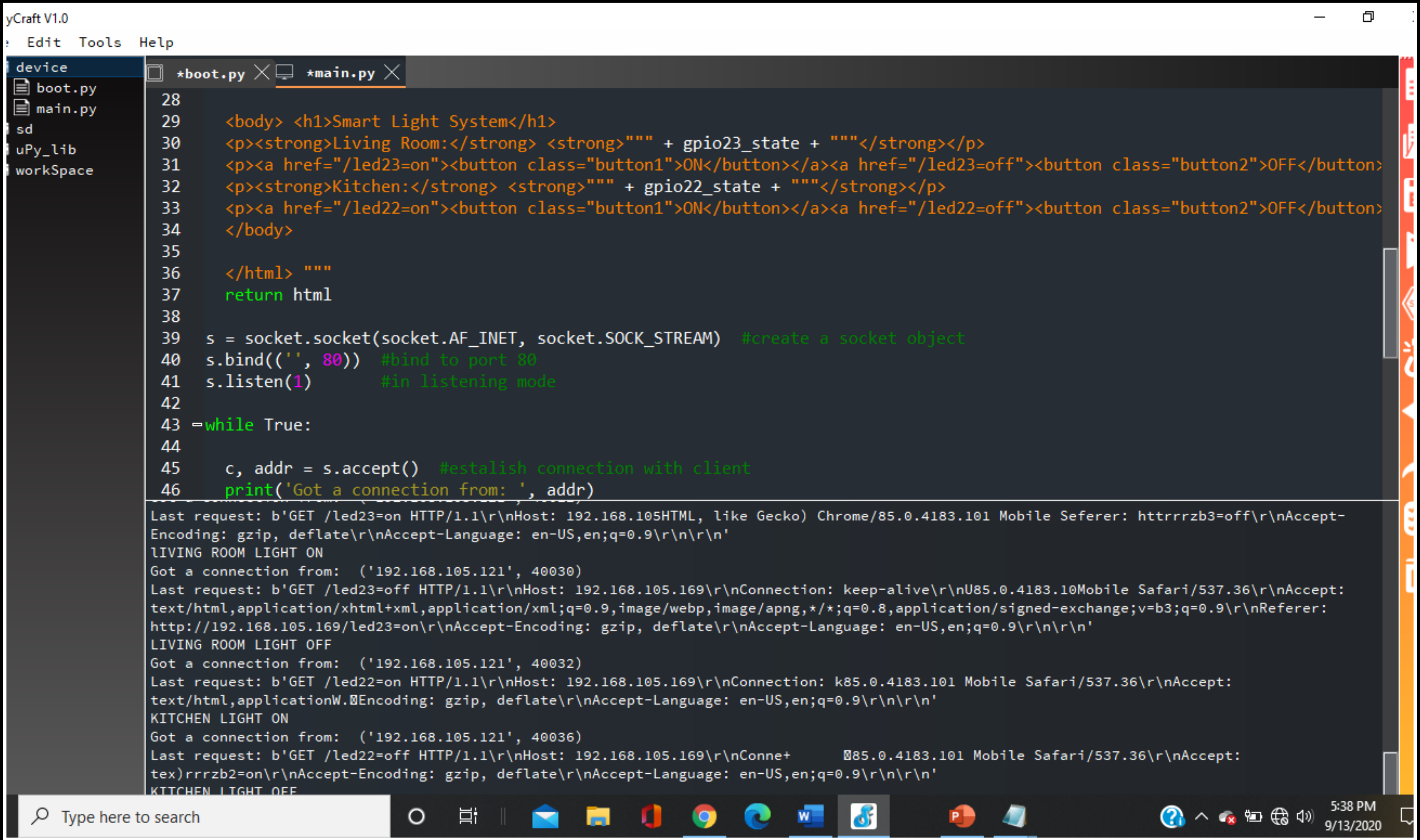
Light Control System

An ESP32 driven circuit that controls 2 LED lights via a Web Browser.

2-light Breadboard Layout

- ESP32
- Two LEDs
- Two Resistors
- Wires

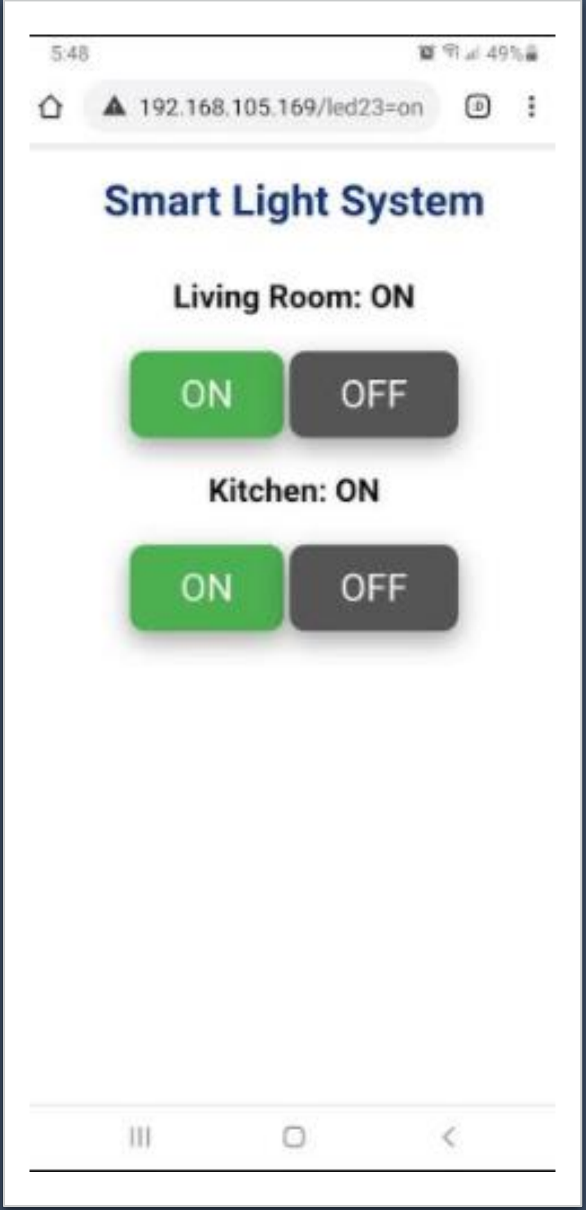




```

    <body> <h1>Smart Light System</h1>
    <p><strong>Living Room:</strong> <strong>""" + gpio23_state + """</strong></p>
    <p><a href="/led23=on"><button class="button1">ON</button></a><a href="/led23=off"><button class="button2">OFF</button>
    <p><strong>Kitchen:</strong> <strong>""" + gpio22_state + """</strong></p>
    <p><a href="/led22=on"><button class="button1">ON</button></a><a href="/led22=off"><button class="button2">OFF</button>
    </body>

    </html> """
    return html

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)  #create a socket object
s.bind(('', 80))  #bind to port 80
s.listen(1)       #in listening mode

while True:

    c, addr = s.accept()  #estalish connection with client
    print('Got a connection from: ', addr)
```

```
Last request: b'GET /led23=on HTTP/1.1\r\nHost: 192.168.105HTML, like Gecko) Chrome/85.0.4183.101 Mobile Seferer: httrrrzb3=off\r\nAccept-
Encoding: gzip, deflate\r\nAccept-Language: en-US,en;q=0.9\r\n\r\n'
lIVING ROOM LIGHT ON
Got a connection from:  ('192.168.105.121', 40030)
Last request: b'GET /led23=off HTTP/1.1\r\nHost: 192.168.105.169\r\nConnection: keep-alive\r\nU85.0.4183.10Mobile Safari/537.36\r\nAccept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\nReferer:
http://192.168.105.169/led23=on\r\nAccept-Encoding: gzip, deflate\r\nAccept-Language: en-US,en;q=0.9\r\n\r\n'
LIVING ROOM LIGHT OFF
Got a connection from:  ('192.168.105.121', 40032)
Last request: b'GET /led22=on HTTP/1.1\r\nHost: 192.168.105.169\r\nConnection: k85.0.4183.101 Mobile Safari/537.36\r\nAccept:
text/html,applicationW.Encoding: gzip, deflate\r\nAccept-Language: en-US,en;q=0.9\r\n\r\n'
KITCHEN LIGHT ON
Got a connection from:  ('192.168.105.121', 40036)
Last request: b'GET /led22=off HTTP/1.1\r\nHost: 192.168.105.169\r\nConne+      85.0.4183.101 Mobile Safari/537.36\r\nAccept:
tex)rrrzb2=on\r\nAccept-Encoding: gzip, deflate\r\nAccept-Language: en-US,en;q=0.9\r\n\r\n'
KITCHEN LIGHT OFF
```

IDE with Python code with Hypertext showing external communication with circuit


5:48

49%

192.168.105.169/led23=on

Smart Light System

Living Room: ON

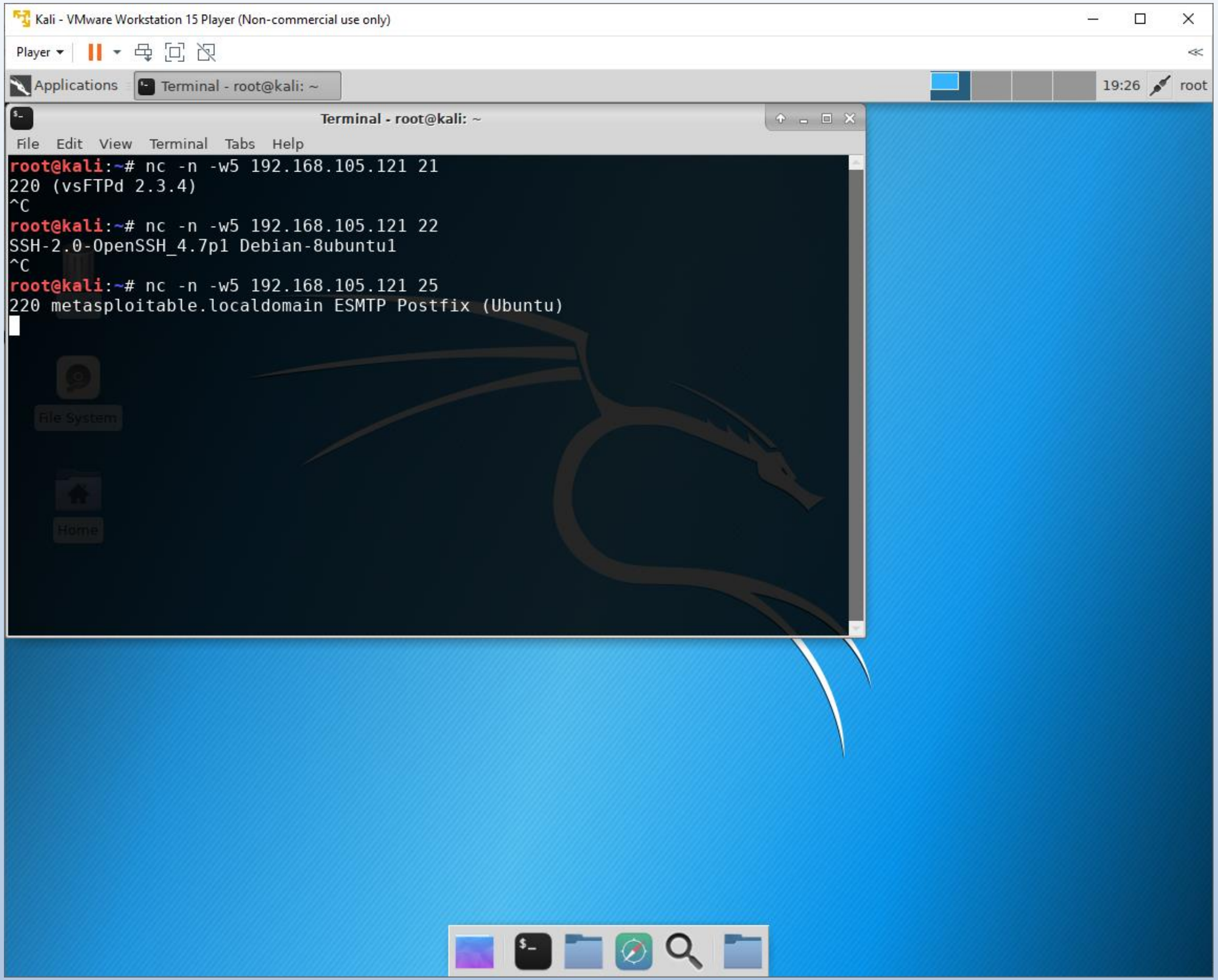
Kitchen: ON

2-light Control Web Interface

- Two buttons that remotely interact with lighting to control operation with unique URL to access this function.

Exploring Network Vulnerabilities

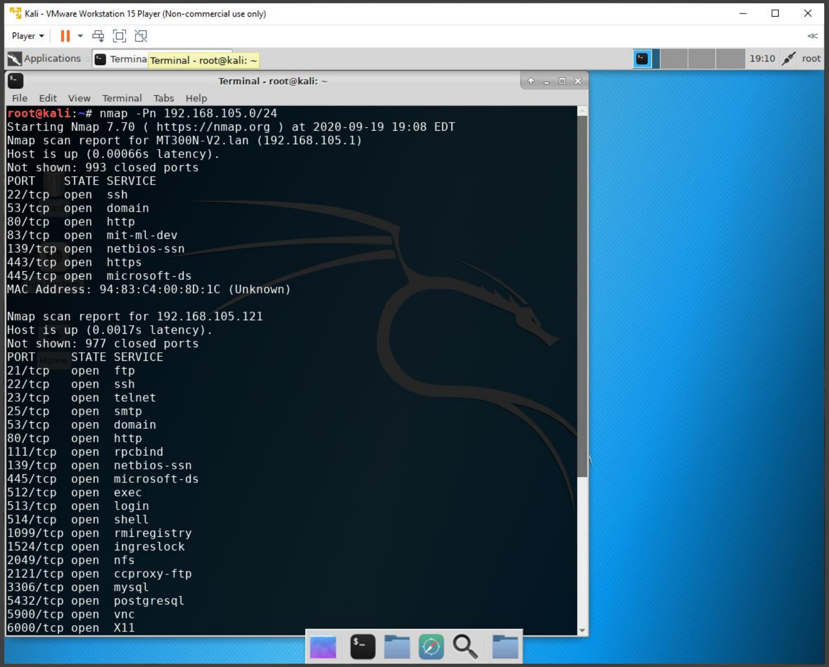
- Ranking vulnerabilities by their significance is important to allow IT professionals the ability to prioritize threats to protect company assets and reduce risk.



```
root@kali:~# nc -n -w5 192.168.105.121 21
220 (vsFTPd 2.3.4)
^C
root@kali:~# nc -n -w5 192.168.105.121 22
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
^C
root@kali:~# nc -n -w5 192.168.105.121 25
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
```

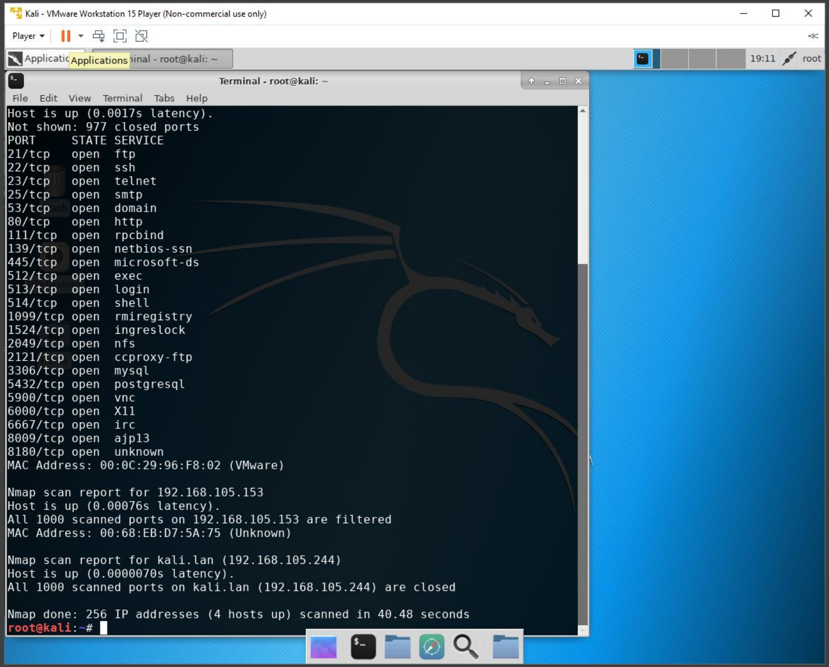
Reconnaissance was conducted to on my home network to determine host addresses and open ports and services.

These are the commands in Kali VM to grab the banner of the Linux Server FTP, SSH and SMTP applications.



Kali - VMware Workstation 15 Player (Non-commercial use only)
Player
Applications
Termina
Terminal - root@kali: ~
19:10
root
Terminal - root@kali: ~
File Edit View Terminal Tabs Help

```
root@kali:~# nmap -Pn 192.168.105.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2020-09-19 19:08 EDT
Nmap scan report for MT300N-V2.lan (192.168.105.1)
Host is up (0.00066s latency).
Not shown: 993 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
53/tcp  open  domain
80/tcp  open  http
83/tcp  open  mit-ml-dev
139/tcp open  netbios-ssn
443/tcp open  https
445/tcp open  microsoft-ds
MAC Address: 94:83:C4:00:8D:1C (Unknown)

Nmap scan report for 192.168.105.121
Host is up (0.0017s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
```



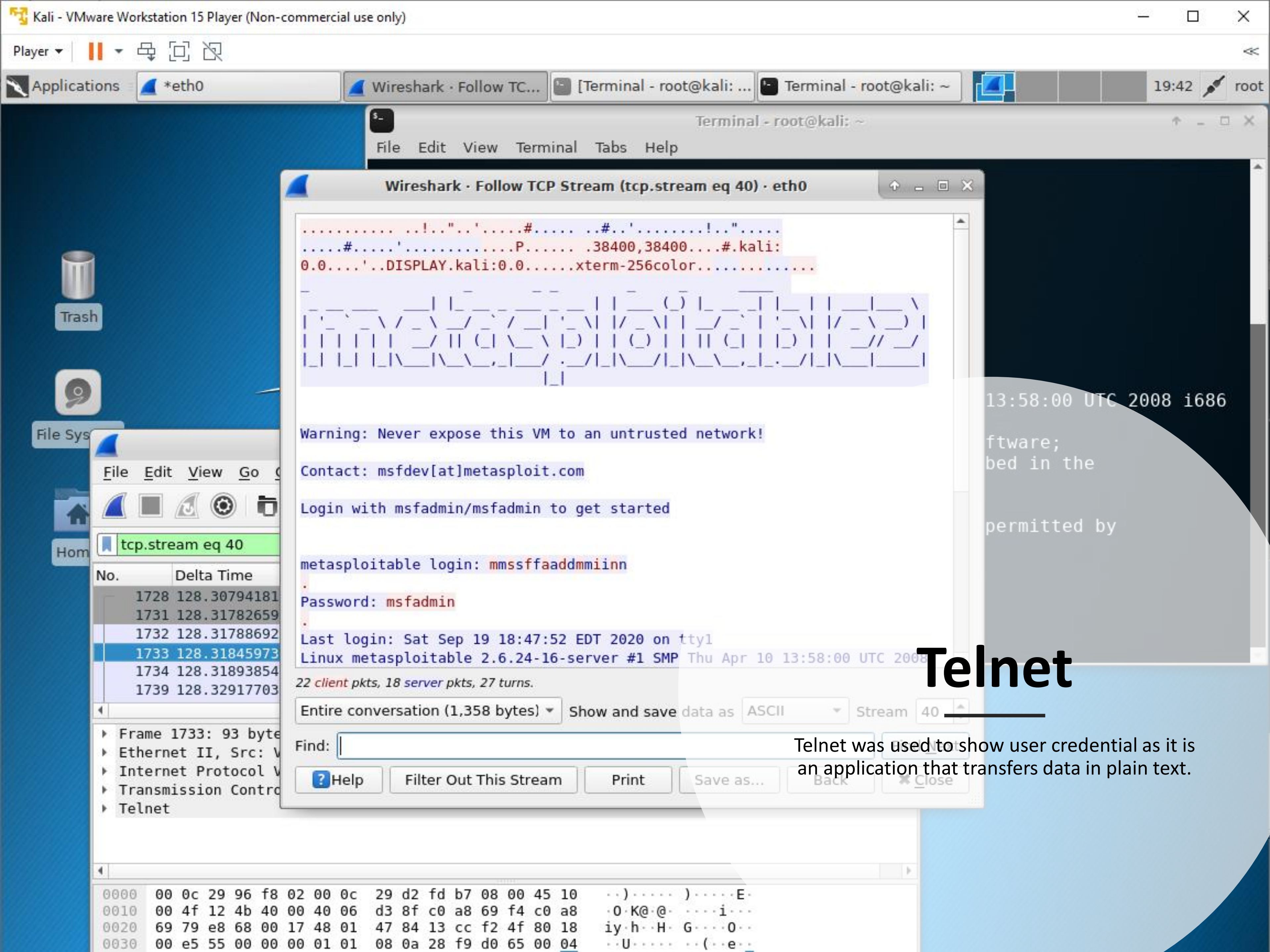
Kali - VMware Workstation 15 Player (Non-commercial use only)
Player
Applicatic
Applications
ninal - root@kali: ~
19:11
root
Terminal - root@kali: ~
File Edit View Terminal Tabs Help

```
Host is up (0.0017s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:96:F8:02 (VMware)

Nmap scan report for 192.168.105.153
Host is up (0.00076s latency).
All 1000 scanned ports on 192.168.105.153 are filtered
MAC Address: 00:68:EB:D7:5A:75 (Unknown)

Nmap scan report for kali.lan (192.168.105.244)
Host is up (0.0000070s latency).
All 1000 scanned ports on kali.lan (192.168.105.244) are closed

Nmap done: 256 IP addresses (4 hosts up) scanned in 40.48 seconds
root@kali:~# 
```

Nmap scan

Nmap is a powerful free and open source network scanning tool

- The IP addresses of the host, Linux-Server VM, Kali VM, and Home Light Control System.
- NMAP is a great tool to identify on systems



Kali - VMware Workstation 15 Player (Non-commercial use only)
Player
Applications
*eth0
Wireshark · Follow TC...
[Terminal - root@kali: ...
Terminal - root@kali: ~
19:42
root
Terminal - root@kali: ~
File Edit View Terminal Tabs Help
Trash
File Sys
Hom
File Edit View Go
Wireshark · Follow TCP Stream (tcp.stream eq 40) · 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: mmssffaaddmmiinn
.
Password: msfadmin
.
Last login: Sat Sep 19 18:47:52 EDT 2020 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008
```

22 client pkts, 18 server pkts, 27 turns.

```
1728 128.30794181
1731 128.31782659
1732 128.31788692
1733 128.31845973
1734 128.31893854
1739 128.32917703
```

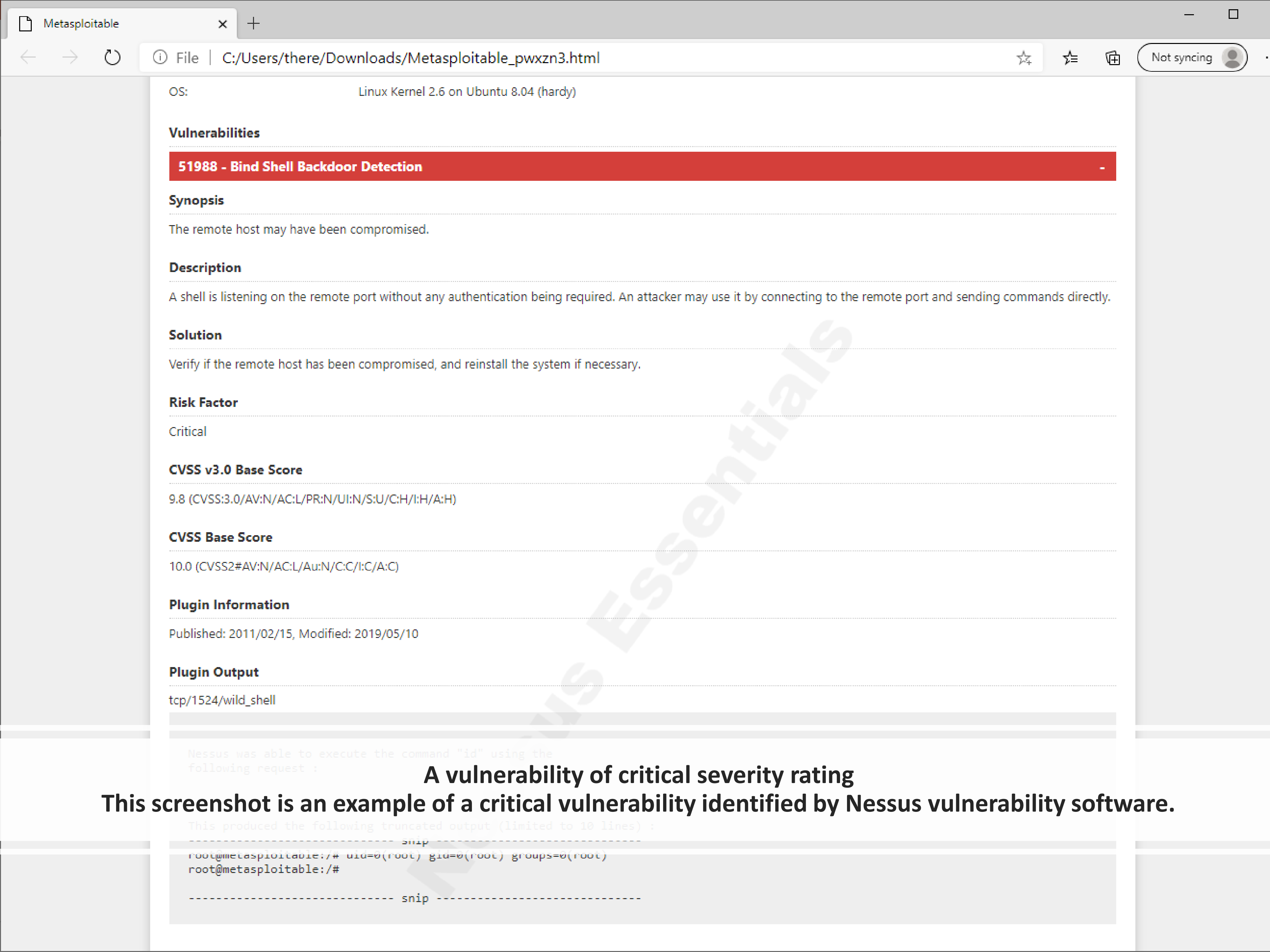
```
Frame 1733: 93 byte
Ethernet II, Src: V
Internet Protocol V
Transmission Contro
Telnet
```

```
0000  00 0c 29 96 f8 02 00 0c  29 d2 fd b7 08 00 45 10   ··)·····)·····E·
0010  00 4f 12 4b 40 00 40 06  d3 8f c0 a8 69 f4 c0 a8   ·O·K@·@·····i···
0020  69 79 e8 68 00 17 48 01  47 84 13 cc f2 4f 80 18   iy·h··H·G····O··
0030  00 e5 55 00 00 00 01 01  08 0a 28 f9 d0 65 00 04   ··U·······(··e··
```

```
13:58:00 UTC 2008 i686

ftware;
bed in the


permitted by
```

Telnet

Telnet was used to show user credential as it is an application that transfers data in plain text.



OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Vulnerabilities

51988 - Bind Shell Backdoor Detection

Synopsis

The remote host may have been compromised.

Description

A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

Solution

Verify if the remote host has been compromised, and reinstall the system if necessary.

Risk Factor

Critical

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Plugin Information

Published: 2011/02/15, Modified: 2019/05/10

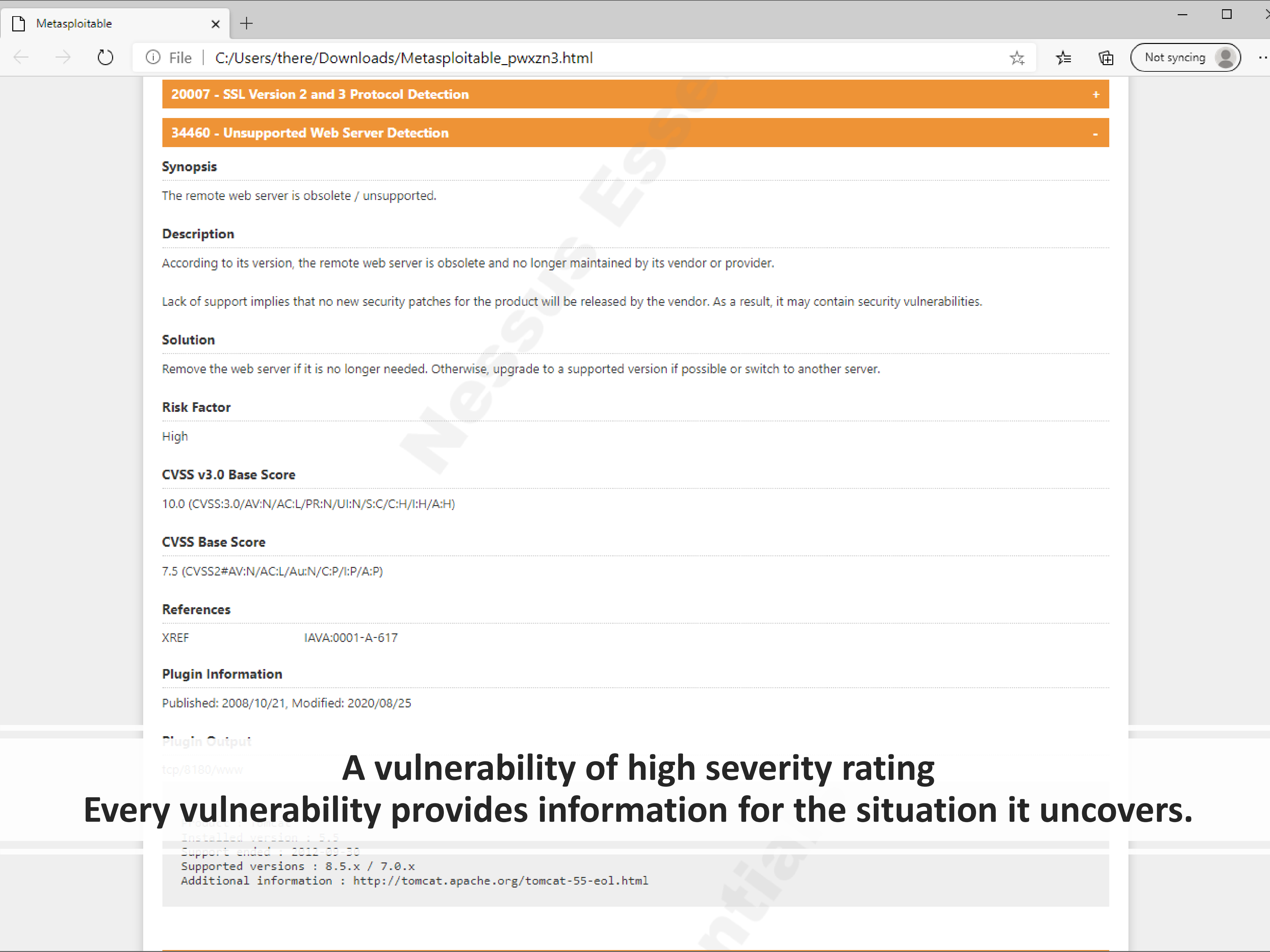
Plugin Output

tcp/1524/wild_shell

```
Nessus was able to execute the command "id" using the
following request :

This produced the following truncated output (limited to 10 lines) :
------------------------------ snip ------------------------------
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/#

------------------------------ snip ------------------------------
```

A vulnerability of critical severity rating

This screenshot is an example of a critical vulnerability identified by Nessus vulnerability software.



20007 - SSL Version 2 and 3 Protocol Detection +

34460 - Unsupported Web Server Detection -

Synopsis

The remote web server is obsolete / unsupported.

Description

According to its version, the remote web server is obsolete and no longer maintained by its vendor or provider.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

Solution

Remove the web server if it is no longer needed. Otherwise, upgrade to a supported version if possible or switch to another server.

Risk Factor

High

CVSS v3.0 Base Score

10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

References

XREF	IAVA:0001-A-617

Plugin Information

Published: 2008/10/21, Modified: 2020/08/25

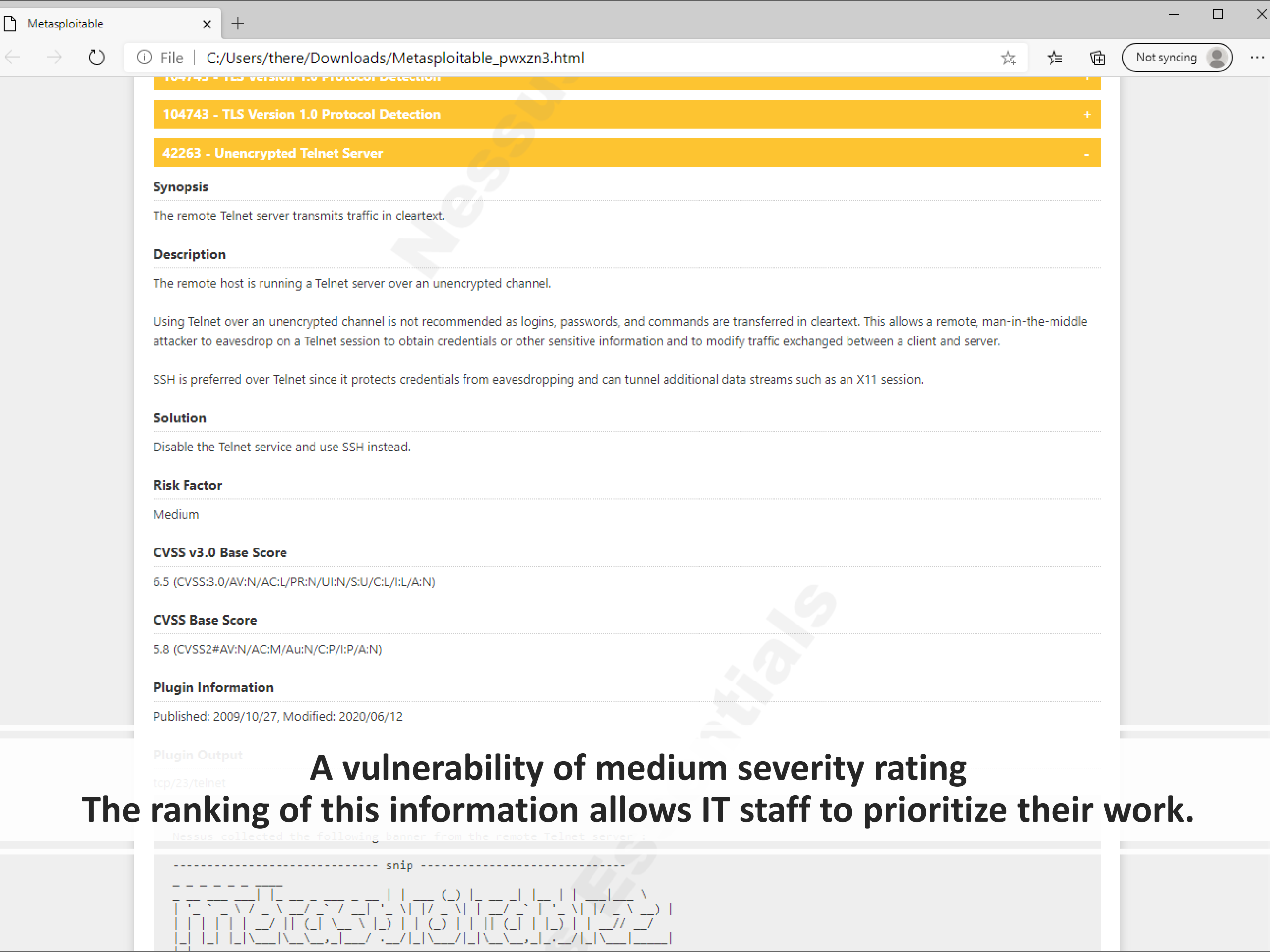
Plugin Output

tcp/8180/www

```
  Product : Tomcat
  Installed version : 5.5
  Support ended : 2012-09-30
  Supported versions : 8.5.x / 7.0.x
  Additional information : http://tomcat.apache.org/tomcat-55-eol.html
```

A vulnerability of high severity rating

Every vulnerability provides information for the situation it uncovers.



104743 - TLS Version 1.0 Protocol Detection +

104743 - TLS Version 1.0 Protocol Detection +

42263 - Unencrypted Telnet Server -

Synopsis

The remote Telnet server transmits traffic in cleartext.

Description

The remote host is running a Telnet server over an unencrypted channel.

Using Telnet over an unencrypted channel is not recommended as logins, passwords, and commands are transferred in cleartext. This allows a remote, man-in-the-middle attacker to eavesdrop on a Telnet session to obtain credentials or other sensitive information and to modify traffic exchanged between a client and server.

SSH is preferred over Telnet since it protects credentials from eavesdropping and can tunnel additional data streams such as an X11 session.

Solution

Disable the Telnet service and use SSH instead.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS Base Score

5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N)

Plugin Information

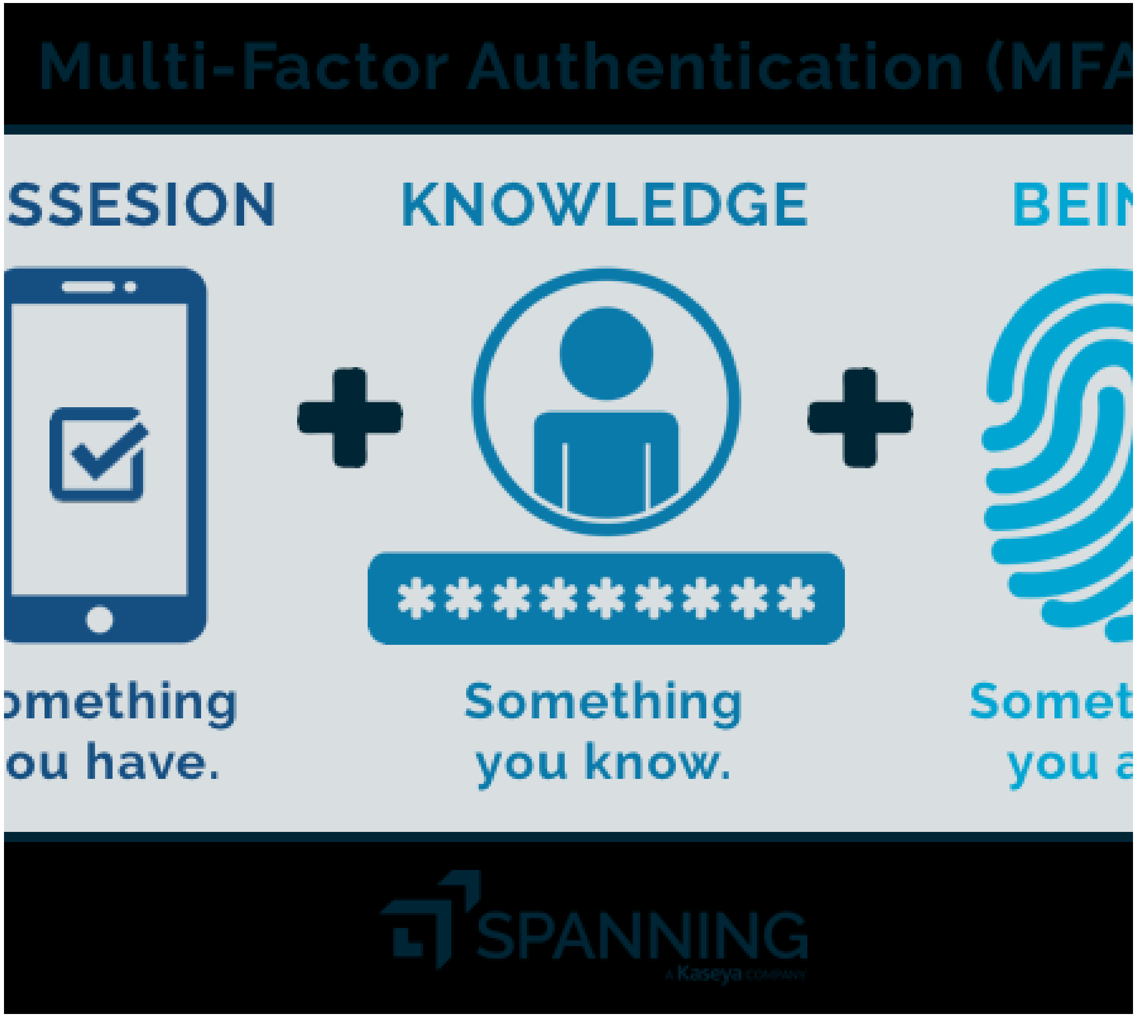
Published: 2009/10/27, Modified: 2020/06/12

Plugin Output

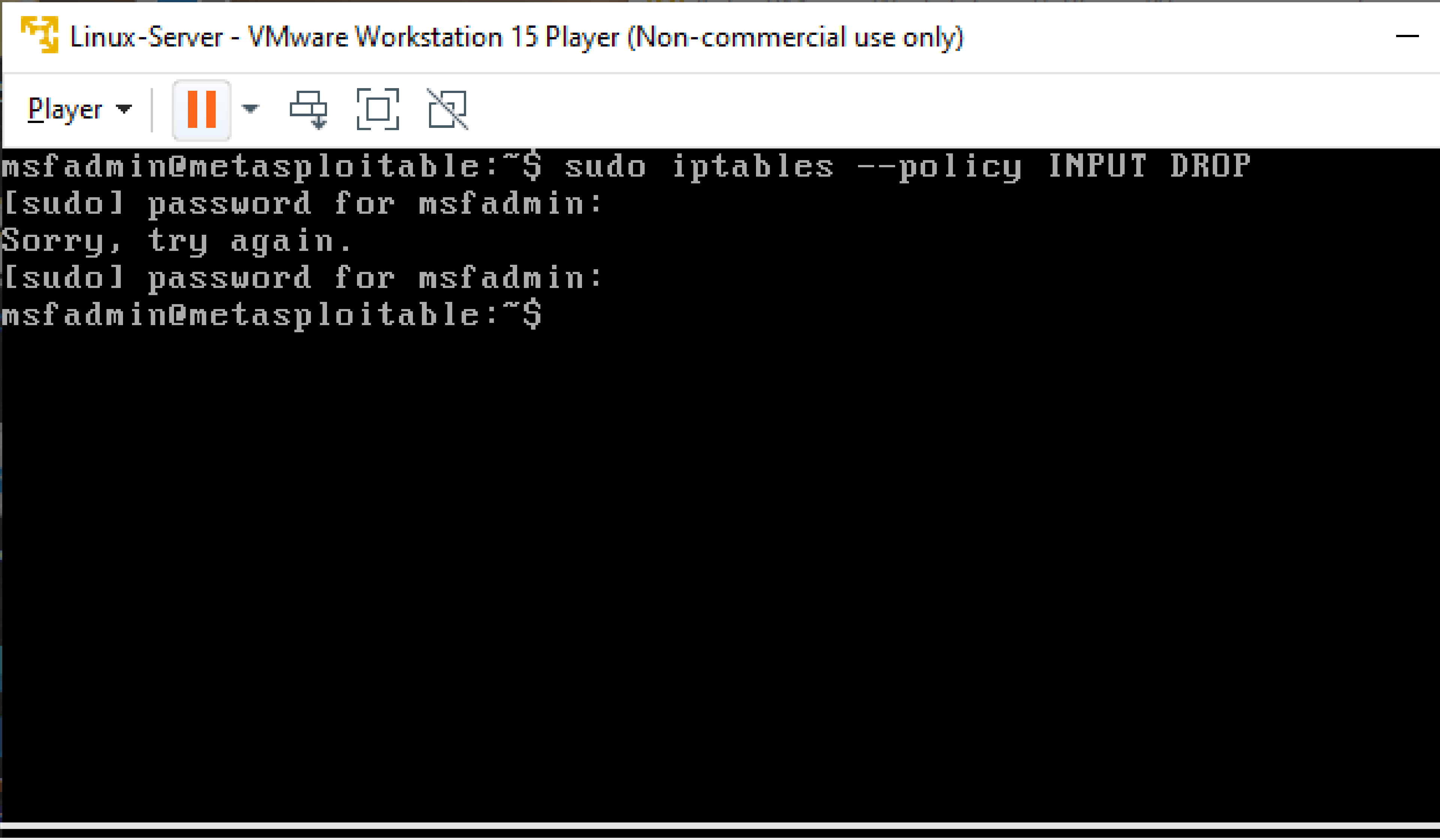
tcp/23/telnet

```
Nessus collected the following banner from the remote Telnet server :

------------------------------- snip -------------------------------
_ _ _ _ _ _ ___
_ __ ___ ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | | __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | | __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
| |
```

A vulnerability of medium severity rating
The ranking of this information allows IT staff to prioritize their work.



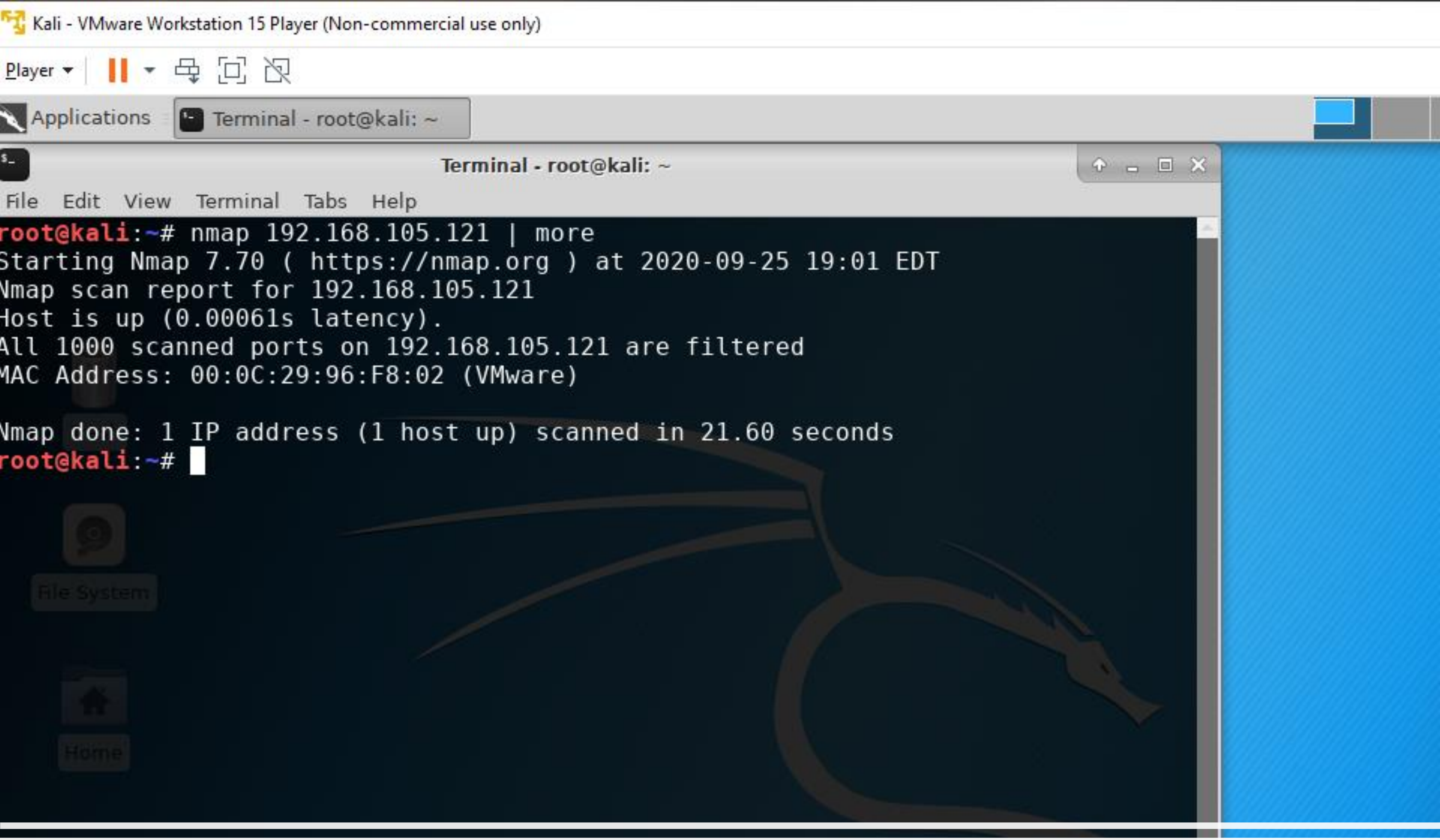
Understanding Stateful Firewalls using iptables and exploring multifactor Authentication using Google Multifactor Authenticator



Linux-Server - VMware Workstation 15 Player (Non-commercial use only)
Player

```
msfadmin@metasploitable:~$ sudo iptables --policy INPUT DROP
[sudo] password for msfadmin:
Sorry, try again.
[sudo] password for msfadmin:
msfadmin@metasploitable:~$
```

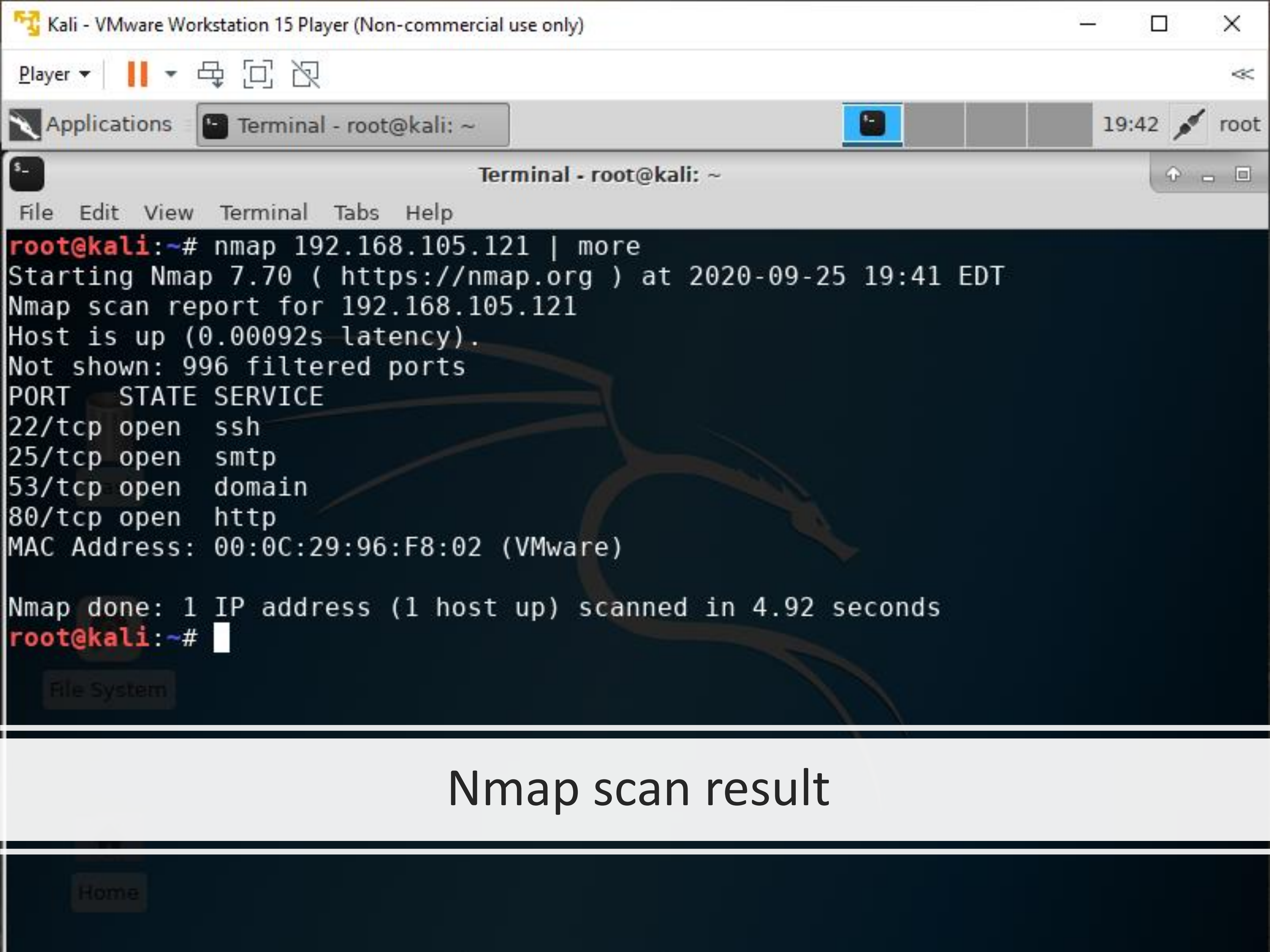
Command on Linux Server to close all ports



Kali - VMware Workstation 15 Player (Non-commercial use only)
Player
Applications
Terminal - root@kali: ~
Terminal - root@kali: ~
File Edit View Terminal Tabs Help

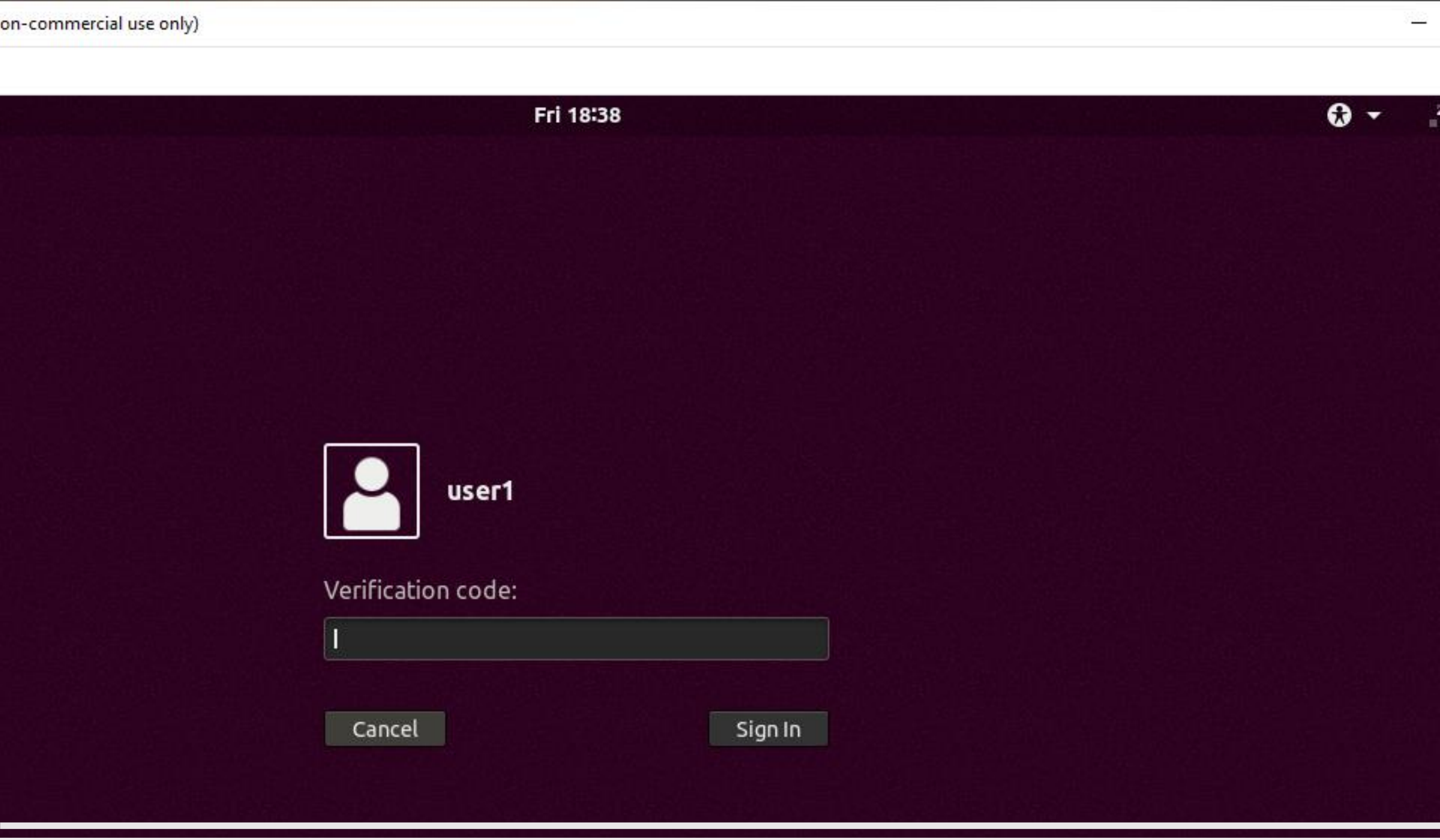
```
root@kali:~# nmap 192.168.105.121 | more
Starting Nmap 7.70 ( https://nmap.org ) at 2020-09-25 19:01 EDT
Nmap scan report for 192.168.105.121
Host is up (0.00061s latency).
All 1000 scanned ports on 192.168.105.121 are filtered
MAC Address: 00:0C:29:96:F8:02 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 21.60 seconds
root@kali:~#
```

Kali command to verify Linux Server ports are closed



```
root@kali:~# nmap 192.168.105.121 | more
Starting Nmap 7.70 ( https://nmap.org ) at 2020-09-25 19:41 EDT
Nmap scan report for 192.168.105.121
Host is up (0.00092s latency).
Not shown: 996 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh
25/tcp open  smtp
53/tcp open  domain
80/tcp open  http
MAC Address: 00:0C:29:96:F8:02 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.92 seconds
root@kali:~# 
```

Nmap scan result

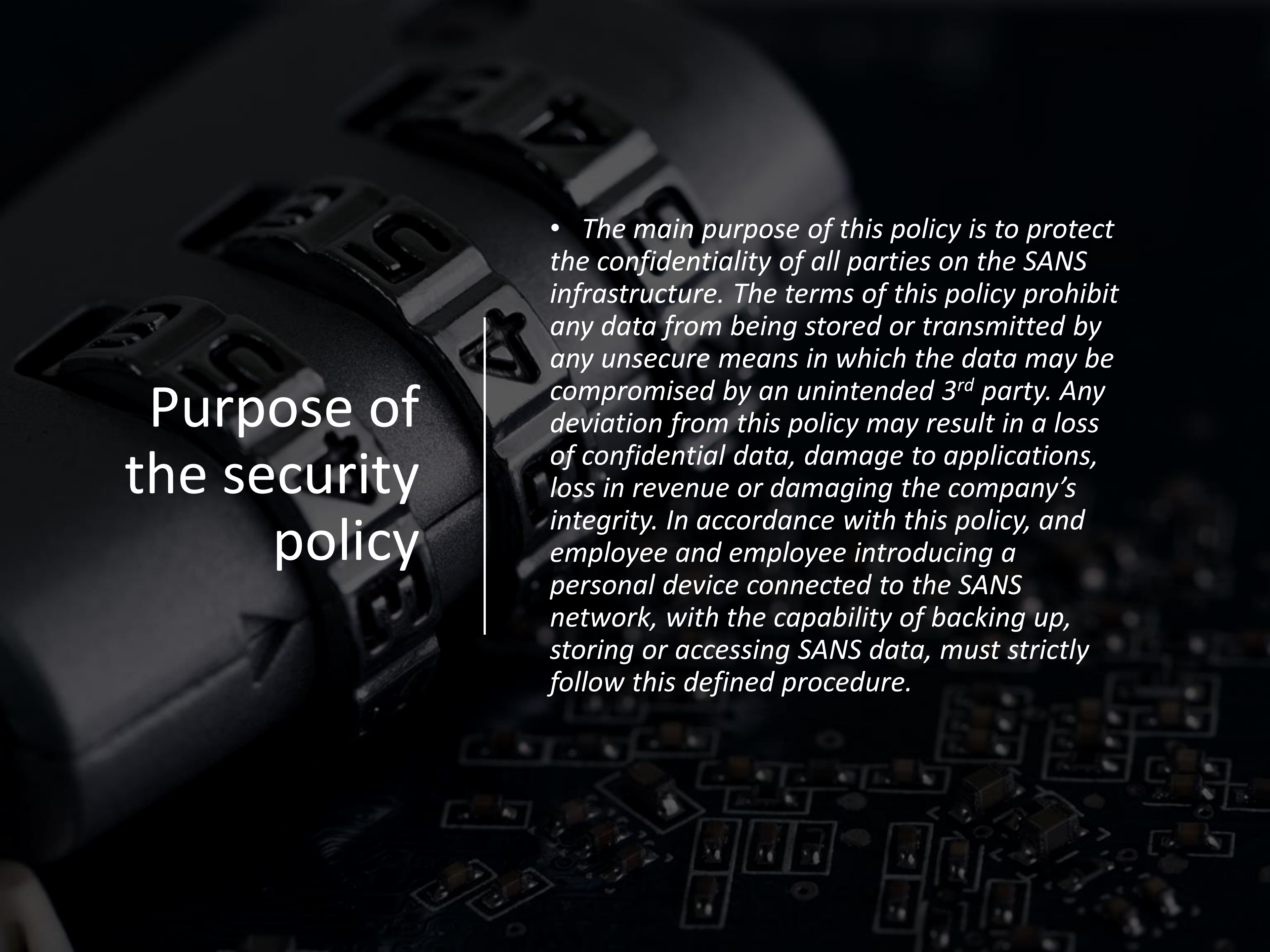


User1 logon screen with 2 factor authentication

Bring Your Own Device (BYOD) Security Policy

Overview of the security policy

- Now that roughly 75% of the modern workforce is remote, it’s time for many organizations to implement a cost-effective and user-friendly bring your own device (BYOD) strategy. SANS reserves the right to revoke a user’s clearance if the security policies of our organization are not followed. This policy protects the security of our organization’s data and infrastructure. Some exceptions may be provided due to certain devices or Operating Systems. Onboarding includes agreeance to the terms and conditions set forth in this policy to be able to connect to the company network.



Purpose of the security policy

- *The main purpose of this policy is to protect the confidentiality of all parties on the SANS infrastructure. The terms of this policy prohibit any data from being stored or transmitted by any unsecure means in which the data may be compromised by an unintended 3rd party. Any deviation from this policy may result in a loss of confidential data, damage to applications, loss in revenue or damaging the company's integrity. In accordance with this policy, and employee and employee introducing a personal device connected to the SANS network, with the capability of backing up, storing or accessing SANS data, must strictly follow this defined procedure.*

Scope of the security policy

- *This policy includes, but not limited to:*
  - *Smartphones(not “jailbroken” or “rooted” unless expressly authorized).*
  - *Tablets*
  - *Portable media devices(USB thumb drives or external hard drives)*
  - *PDAs*
  - *Laptop/Notebook computers*
  - *Any personal device with storage capabilities that can access the company network.*
  - *Any hardware or software this is not company owned or supplied.*

Policy section of the security policy

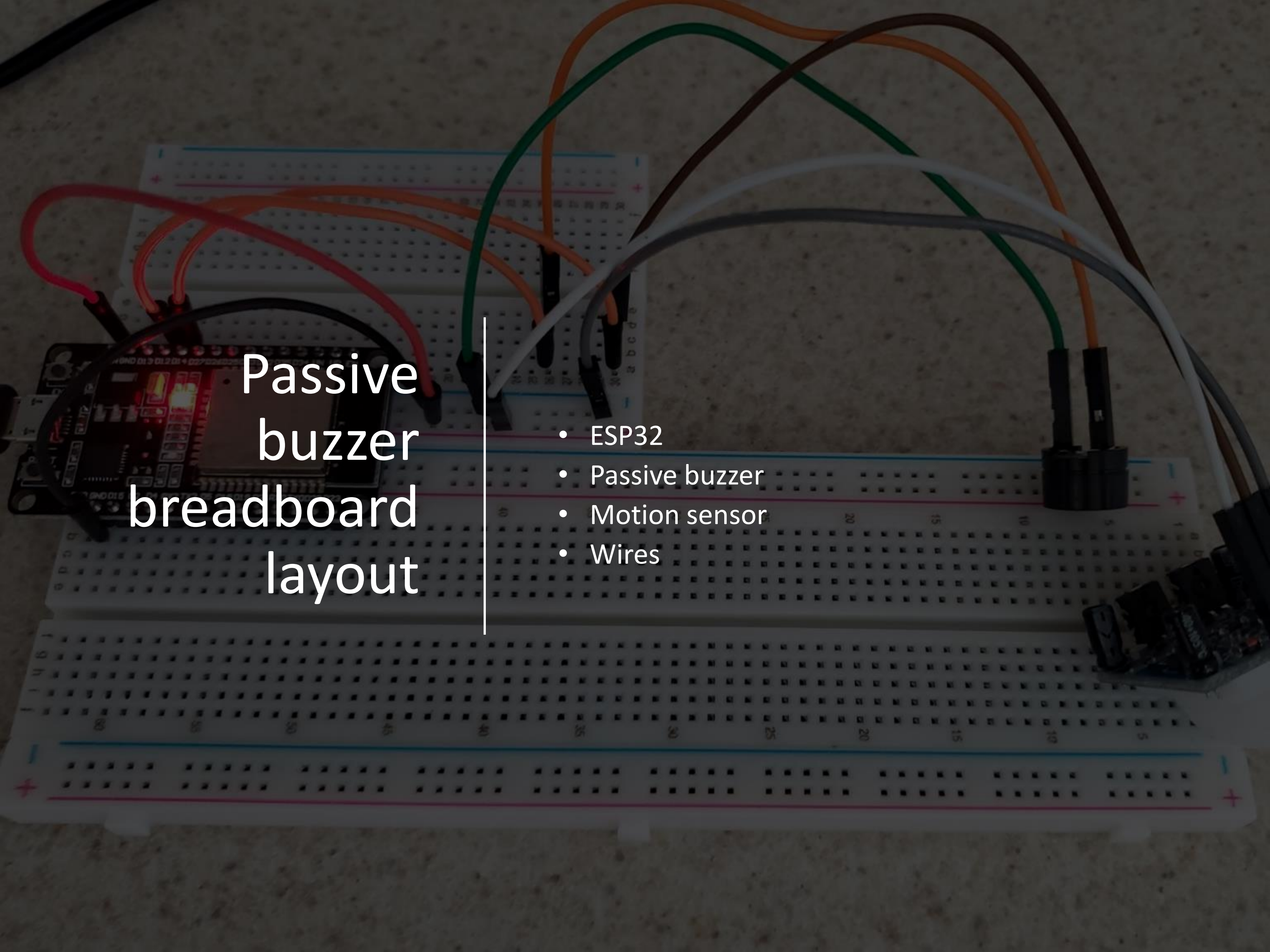
- To establish a connection on the company network all users must agree to the terms and conditions contained in this policy.
- Acceptable personal use is defined by reasonable personal communication or recreation such as, surfing social media or game playing.
- Users are prohibited from accessing certain websites during scheduled work hours while connected to the company's network. Such blocking of these websites will be determined by the company.

- These websites include, but not limited to:
  - Social media sites
  - Shopping sites
  - 3rd party email sites

- Devices are strictly prohibited from:
  - Storing or transmitting company data
  - Storing or transmitting information belonging to another company.
  - Harass others
  - Pursuit outside business activities

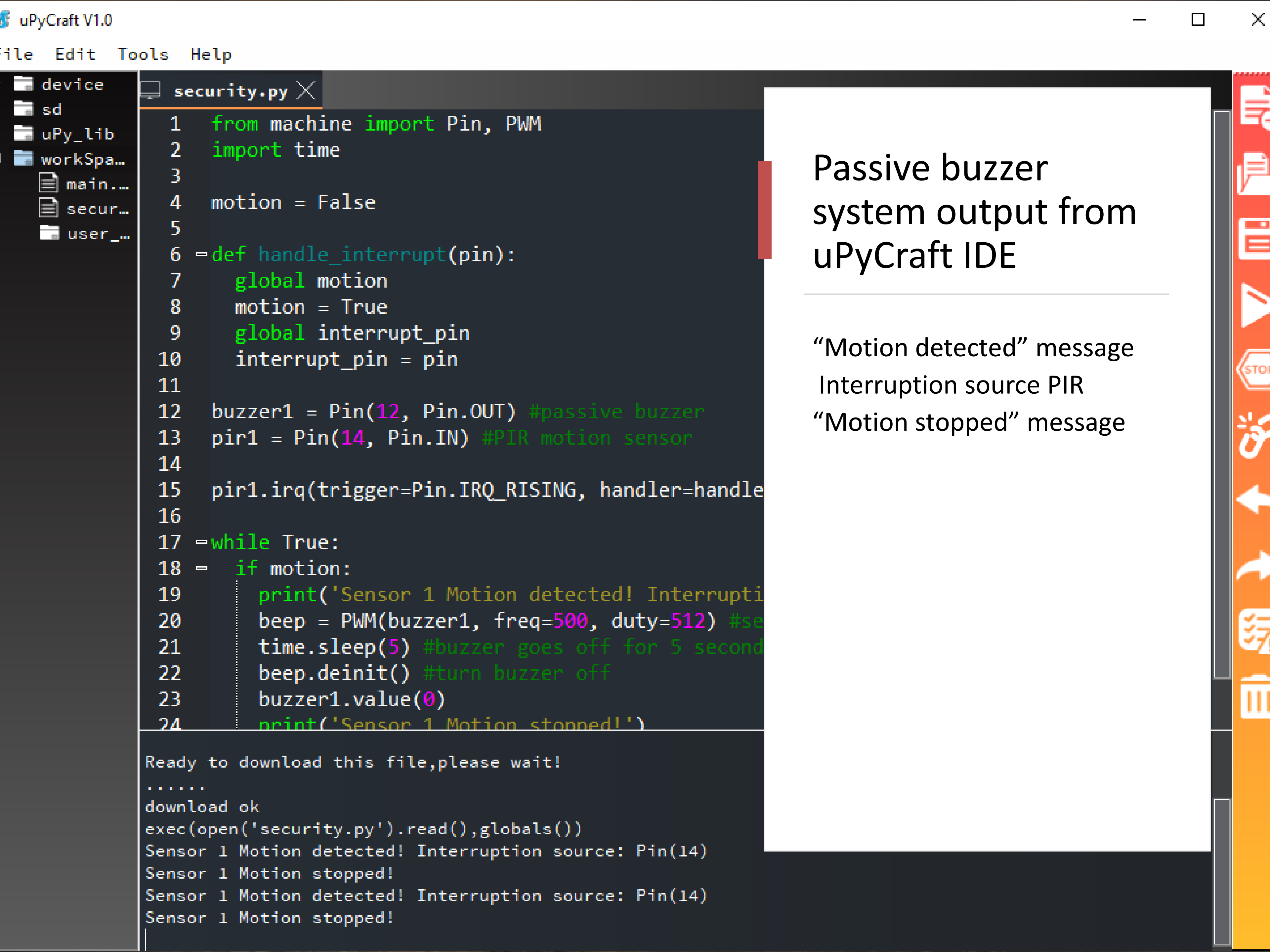
- The following applications are allowed:
  - Weather Channel
  - News/RSS feeds
  - Office 365
  - Productivity applications
-
- The following applications are not allowed:
  - Any downloads from sources other than iTunes or Google Play
  - Social Media
-
- This company has a zero-tolerance for non-compliance. If you feel that you may be in violation, please see your department manager.

The ESP32 driven circuit is used to detect motion with a proximity sensor making a centralized home security system.



Passive buzzer breadboard layout

- ESP32
- Passive buzzer
- Motion sensor
- Wires



```python
from machine import Pin, PWM
import time

motion = False

def handle_interrupt(pin):
  global motion
  motion = True
  global interrupt_pin
  interrupt_pin = pin

buzzer1 = Pin(12, Pin.OUT) #passive buzzer
pir1 = Pin(14, Pin.IN) #PIR motion sensor

pir1.irq(trigger=Pin.IRQ_RISING, handler=handle

while True:
  if motion:
    print('Sensor 1 Motion detected! Interrupti
    beep = PWM(buzzer1, freq=500, duty=512) #se
    time.sleep(5) #buzzer goes off for 5 second
    beep.deinit() #turn buzzer off
    buzzer1.value(0)
    print('Sensor 1 Motion stopped!')
```

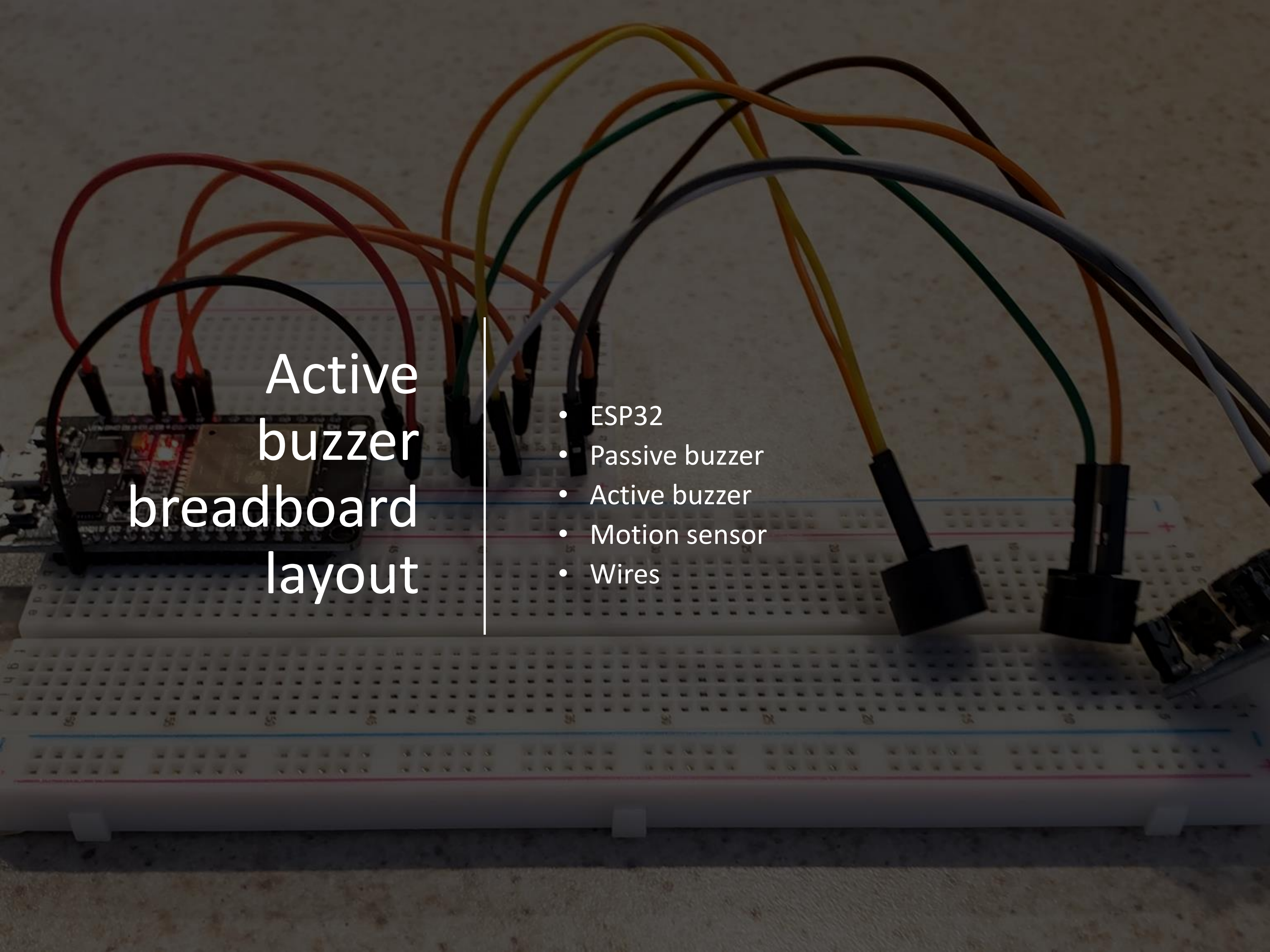
```
Ready to download this file,please wait!
......
download ok
exec(open('security.py').read(),globals())
Sensor 1 Motion detected! Interruption source: Pin(14)
Sensor 1 Motion stopped!
Sensor 1 Motion detected! Interruption source: Pin(14)
Sensor 1 Motion stopped!
```

Passive buzzer system output from uPyCraft IDE

“Motion detected” message

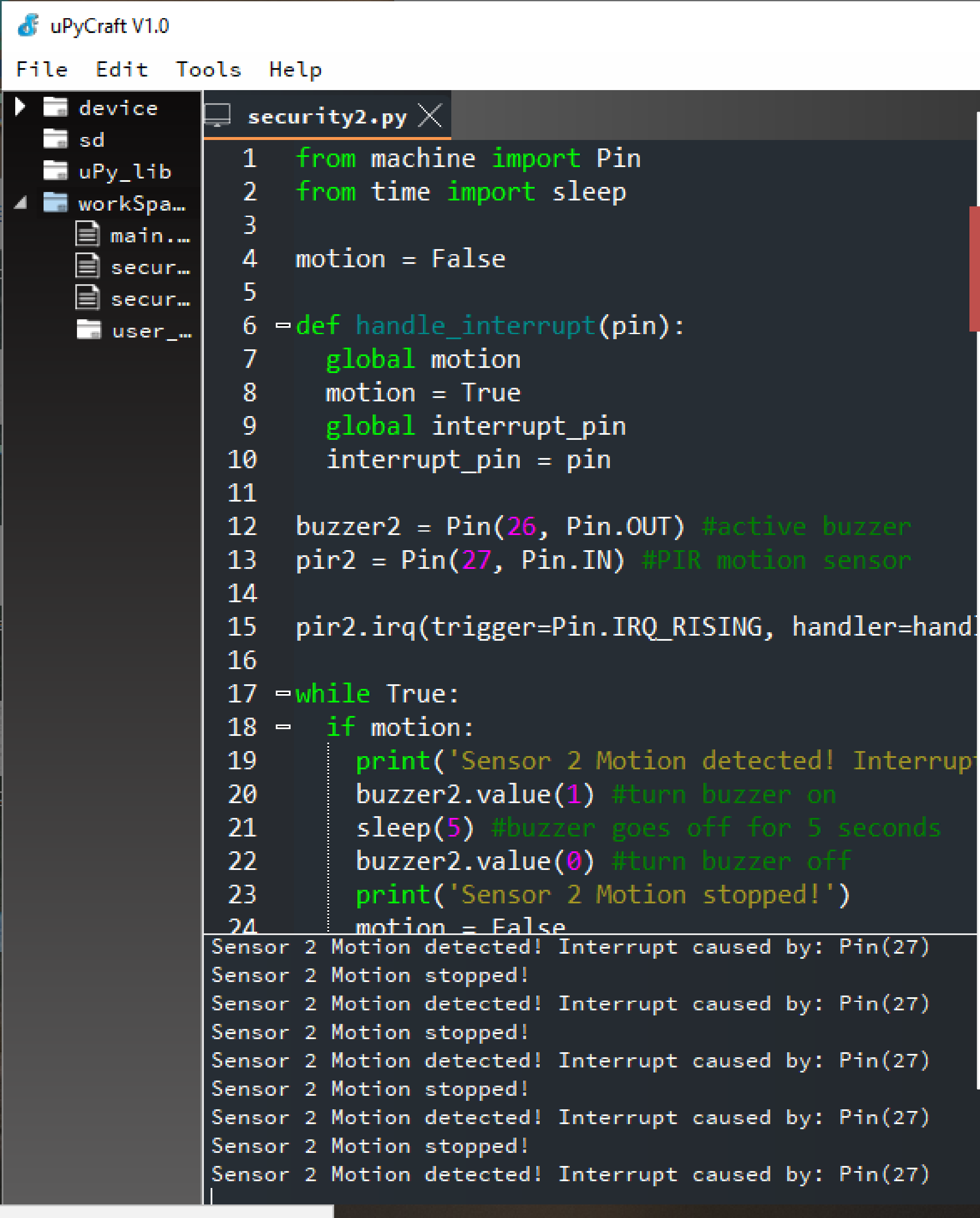
Interruption source PIR

“Motion stopped” message



Active buzzer breadboard layout

- ESP32
- Passive buzzer
- Active buzzer
- Motion sensor
- Wires



```
from machine import Pin
from time import sleep

motion = False

def handle_interrupt(pin):
  global motion
  motion = True
  global interrupt_pin
  interrupt_pin = pin

buzzer2 = Pin(26, Pin.OUT) #active buzzer
pir2 = Pin(27, Pin.IN) #PIR motion sensor

pir2.irq(trigger=Pin.IRQ_RISING, handler=hand

while True:
  if motion:
    print('Sensor 2 Motion detected! Interrup
    buzzer2.value(1) #turn buzzer on
    sleep(5) #buzzer goes off for 5 seconds
    buzzer2.value(0) #turn buzzer off
    print('Sensor 2 Motion stopped!')
    motion = False
```

```
Sensor 2 Motion detected! Interrupt caused by: Pin(27)
Sensor 2 Motion stopped!
Sensor 2 Motion detected! Interrupt caused by: Pin(27)
Sensor 2 Motion stopped!
Sensor 2 Motion detected! Interrupt caused by: Pin(27)
Sensor 2 Motion stopped!
Sensor 2 Motion detected! Interrupt caused by: Pin(27)
Sensor 2 Motion stopped!
Sensor 2 Motion detected! Interrupt caused by: Pin(27)
```

Active buzzer system output from uPyCraft IDE

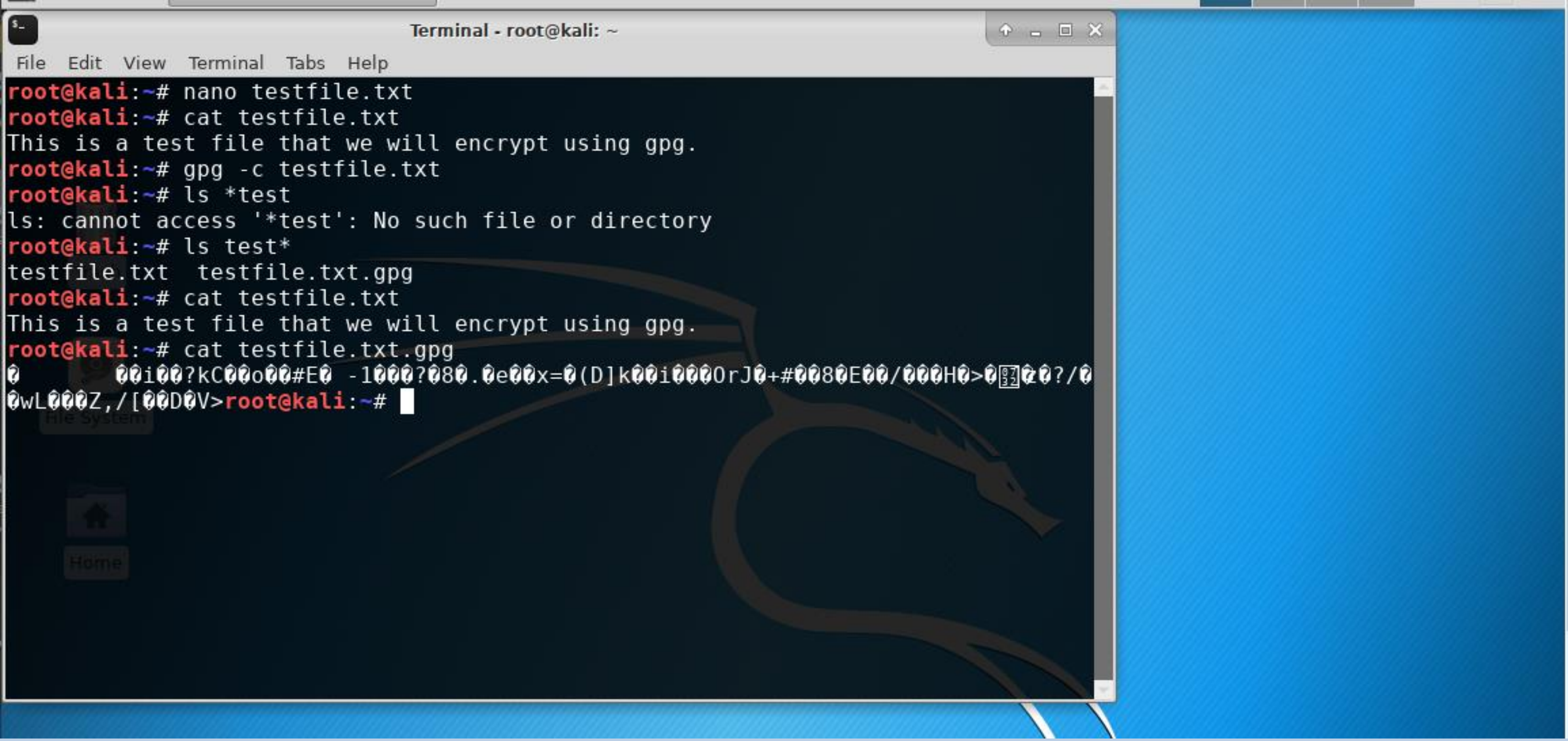
“Motion detected” message

Interruption source

“Motion stopped” message

Asymmetric Key Encryption and Password Policy Enforcement

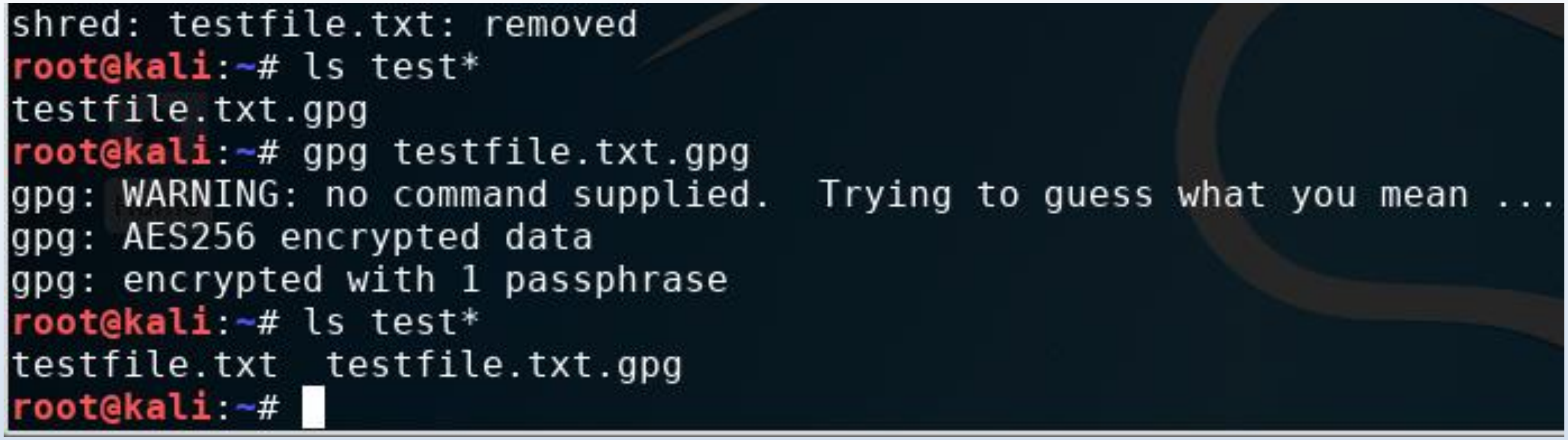
To implement secure file management and password policies using encryption and password administrative controls



```
root@kali:~# nano testfile.txt
root@kali:~# cat testfile.txt
This is a test file that we will encrypt using gpg.
root@kali:~# gpg -c testfile.txt
root@kali:~# ls *test
ls: cannot access '*test': No such file or directory
root@kali:~# ls test*
testfile.txt  testfile.txt.gpg
root@kali:~# cat testfile.txt
This is a test file that we will encrypt using gpg.
root@kali:~# cat testfile.txt.gpg
�       ��i��?kC��o��#E� -1���?�8�.�e��x=�(D]k��i���OrJ�+#��8�E��/���H�>��̒�?/�
�wL���Z,/[��D�V>root@kali:~# 
```

File encryption

- content of the plaintext file
- content of the encrypted file

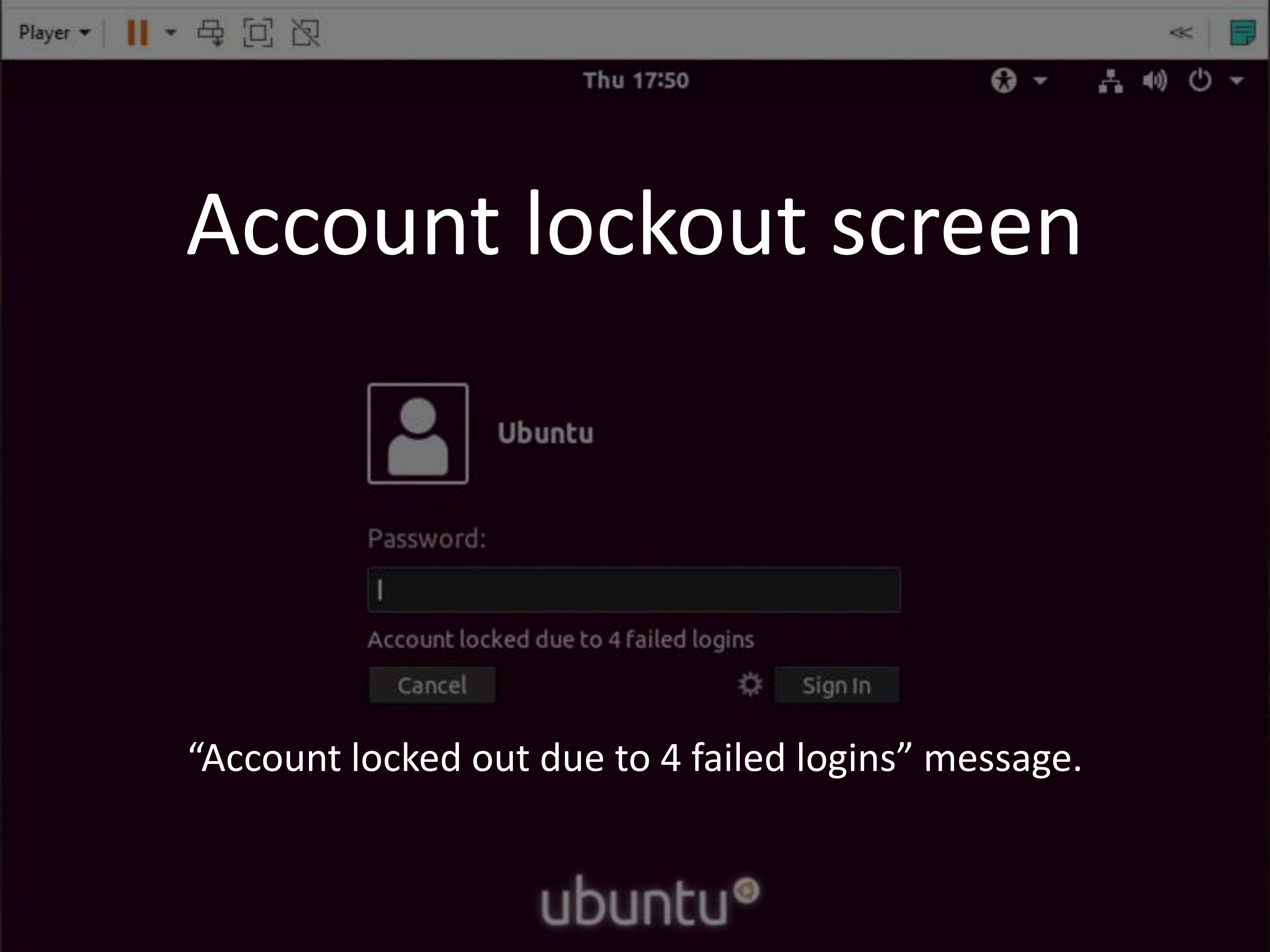


```
shred: testfile.txt: removed
root@kali:~# ls test*
testfile.txt.gpg
root@kali:~# gpg testfile.txt.gpg
gpg: WARNING: no command supplied.  Trying to guess what you mean ...
gpg: AES256 encrypted data
gpg: encrypted with 1 passphrase
root@kali:~# ls test*
testfile.txt  testfile.txt.gpg
root@kali:~# 
```

File decryption

- The single encrypted file
- The decrypting process
- Both the encrypted file and the original plaintext file

Account lockout screen



Password:

Account locked due to 4 failed logins

“Account locked out due to 4 failed logins” message.

Project Conclusion

- Risk assessment impacts the development of a program’s security policy. A security policy is crucial as threat, vulnerability and impact assessments should be made to mitigate exposure of secure data to unwarranted third parties. Technology is rapidly developing so it is important that the policies governing the use of these technologies is being updated.