Managing Enterprise Cybersecurity MIS 4596

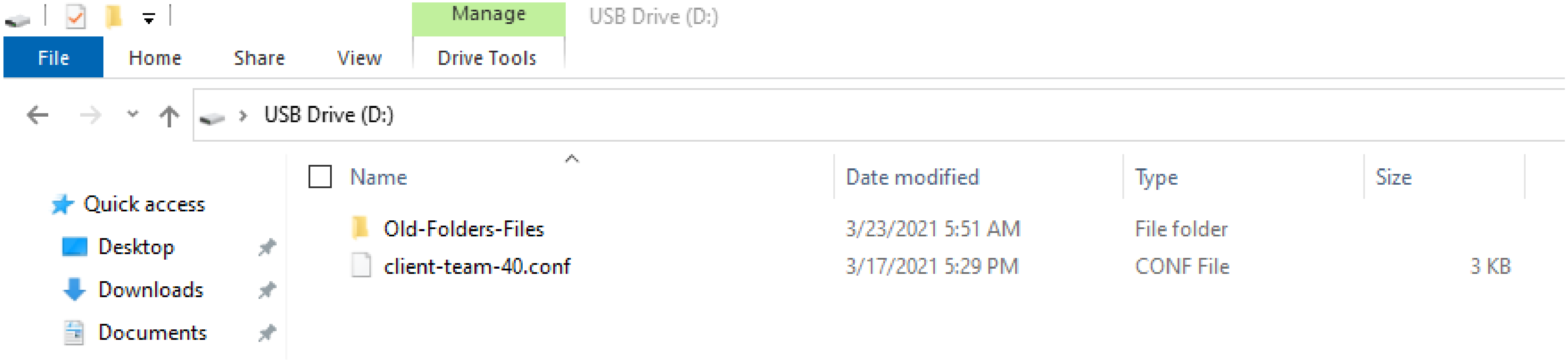
Physical Security

Unit #19

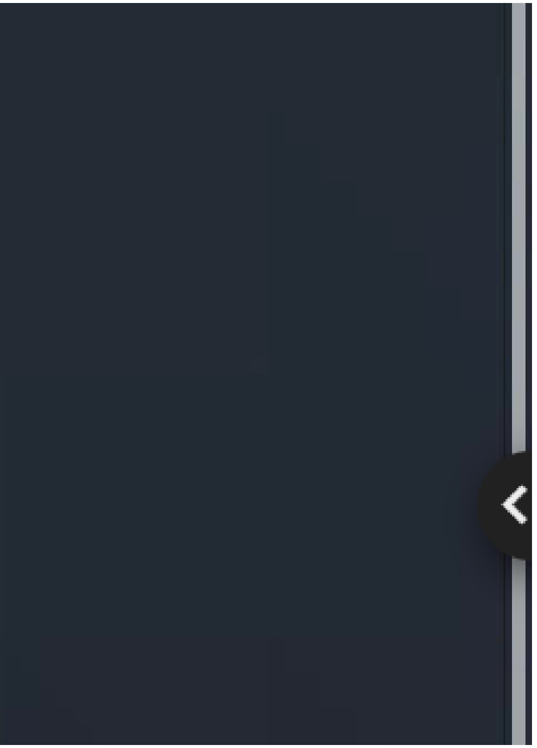
Agenda

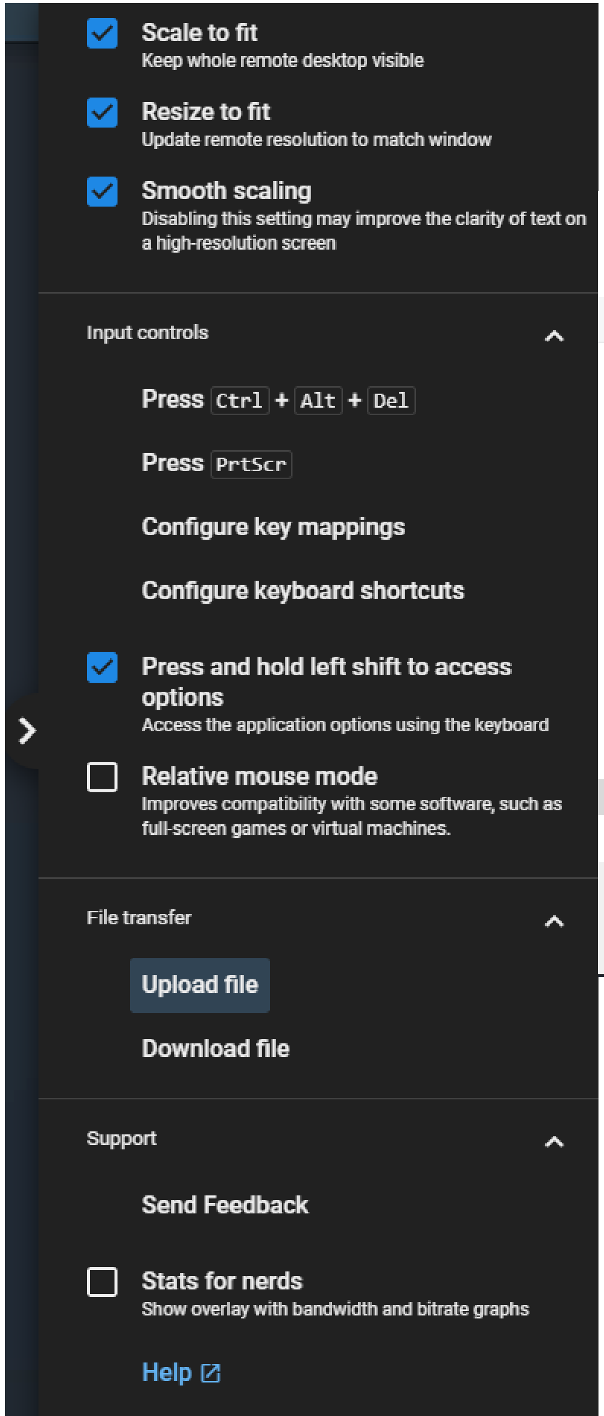
- Milestone 3 – Accessing your server
- Vulnerabilities and sources of threats
- Physical control inventory baselines
- Perimeter security
- Media protection
- Media sanitization

After you download your client.conf file



Name	Date modified	Type	Size
Old-Folders-Files	3/23/2021 5:51 AM	File folder	
client-team-40.conf	3/17/2021 5:29 PM	CONF File	3 KB





☑ **Scale to fit**
Keep whole remote desktop visible

☑ **Resize to fit**
Update remote resolution to match window

☑ **Smooth scaling**
Disabling this setting may improve the clarity of text on a high-resolution screen

Input controls

Press `Ctrl` + `Alt` + `Del`

Press `PrtScr`

Configure key mappings

Configure keyboard shortcuts

☑ **Press and hold left shift to access options**
Access the application options using the keyboard

☐ **Relative mouse mode**
Improves compatibility with some software, such as full-screen games or virtual machines.

File transfer

Upload file

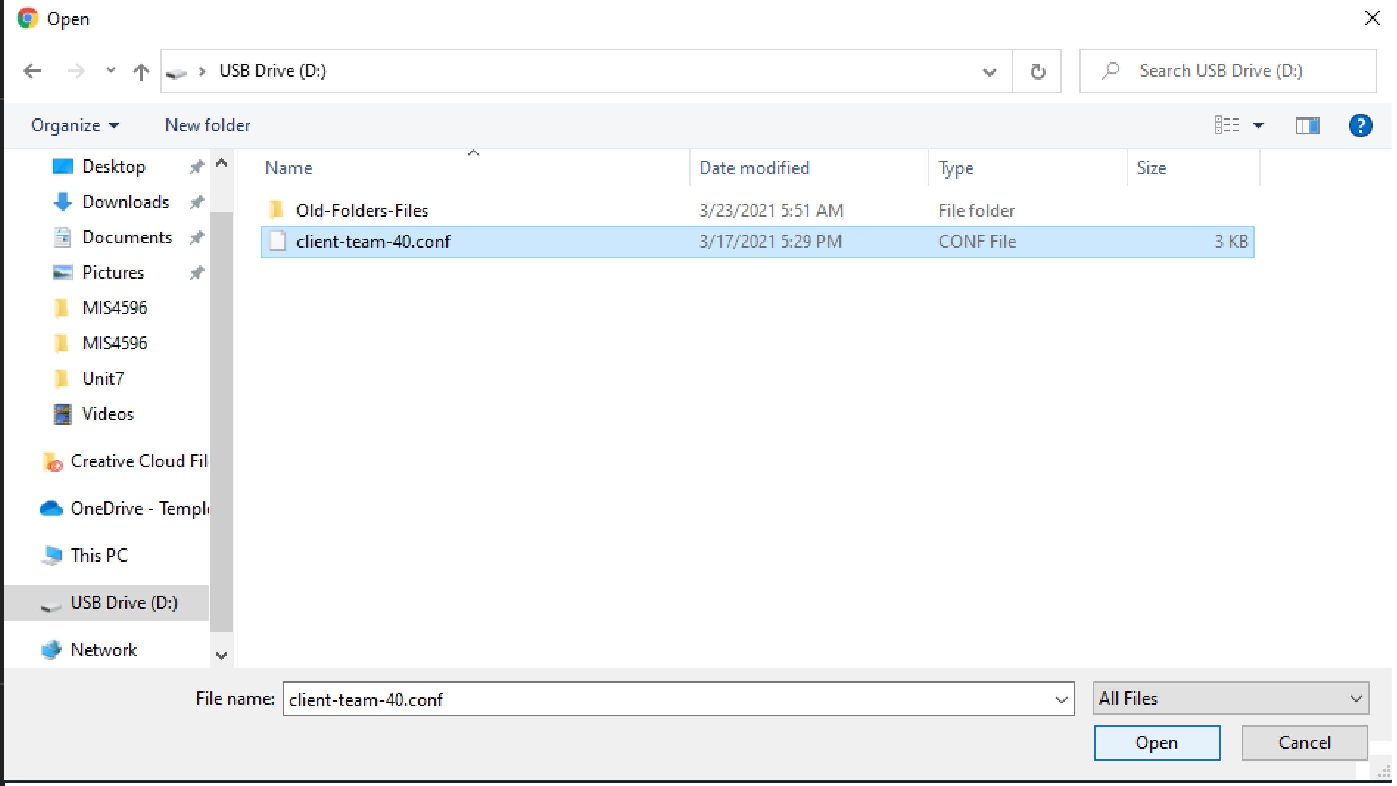
Download file

Support

Send Feedback

☐ **Stats for nerds**
Show overlay with bandwidth and bitrate graphs

Help



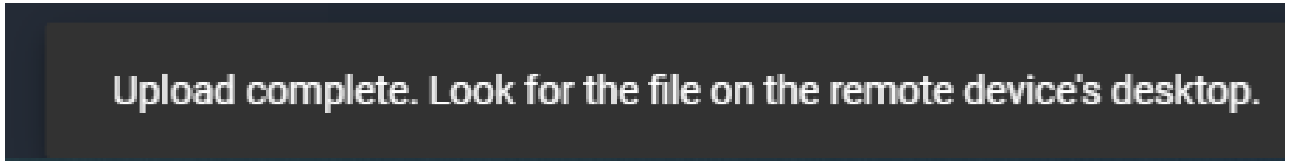
Open

USB Drive (D:)

Name	Date modified	Type	Size
Old-Folders-Files	3/23/2021 5:51 AM	File folder	
client-team-40.conf	3/17/2021 5:29 PM	CONF File	3 KB

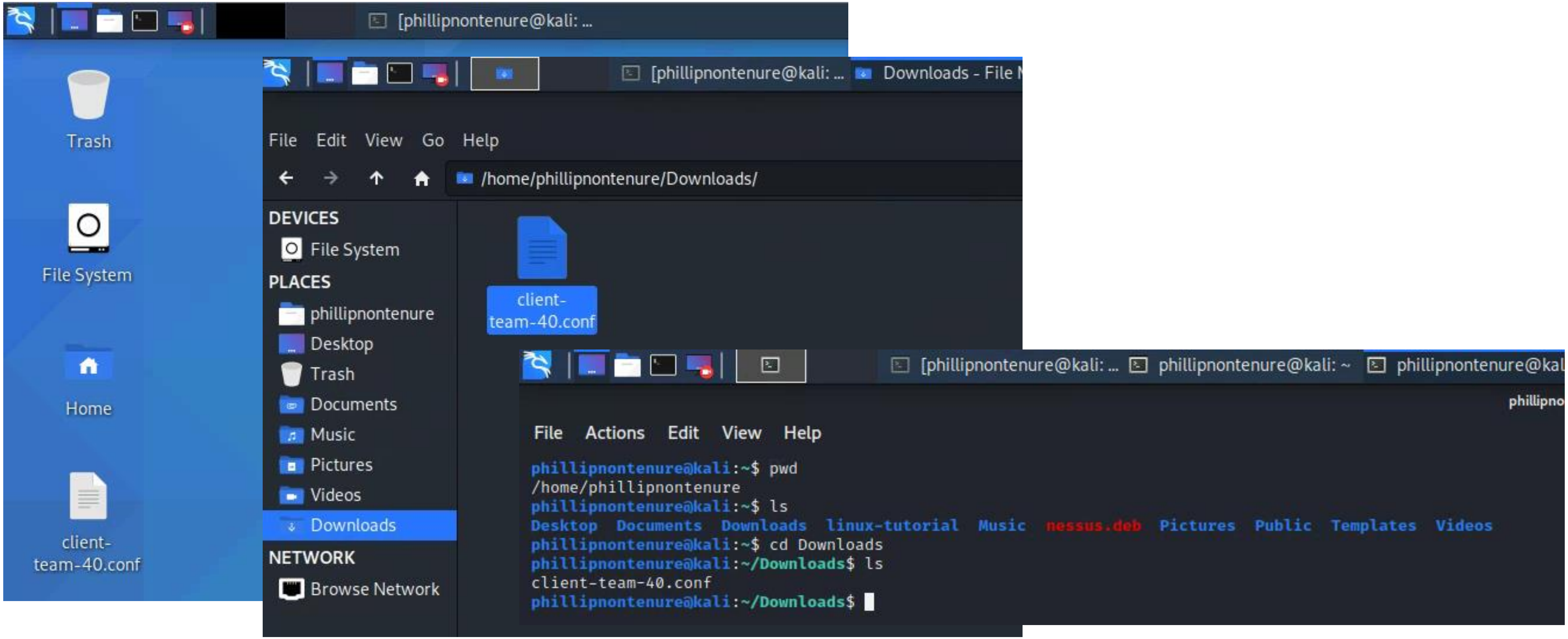
File name: client-team-40.conf

All Files

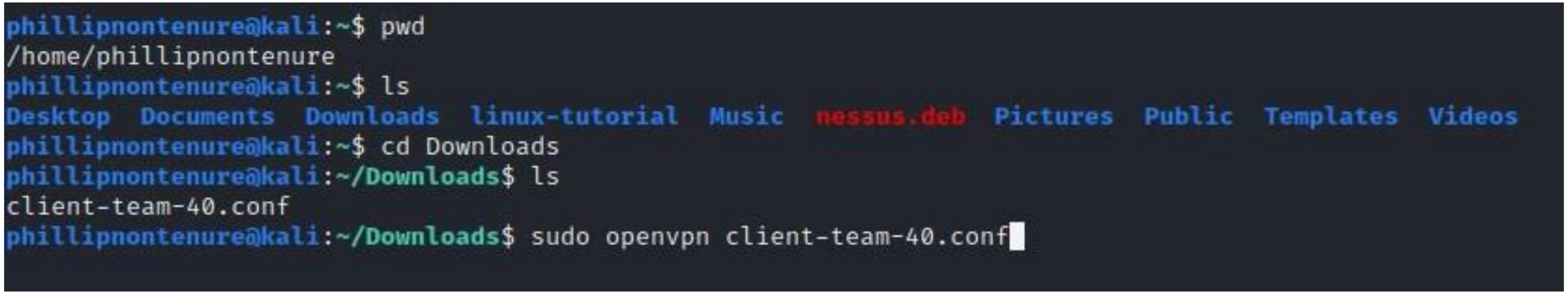


Upload complete. Look for the file on the remote device's desktop.

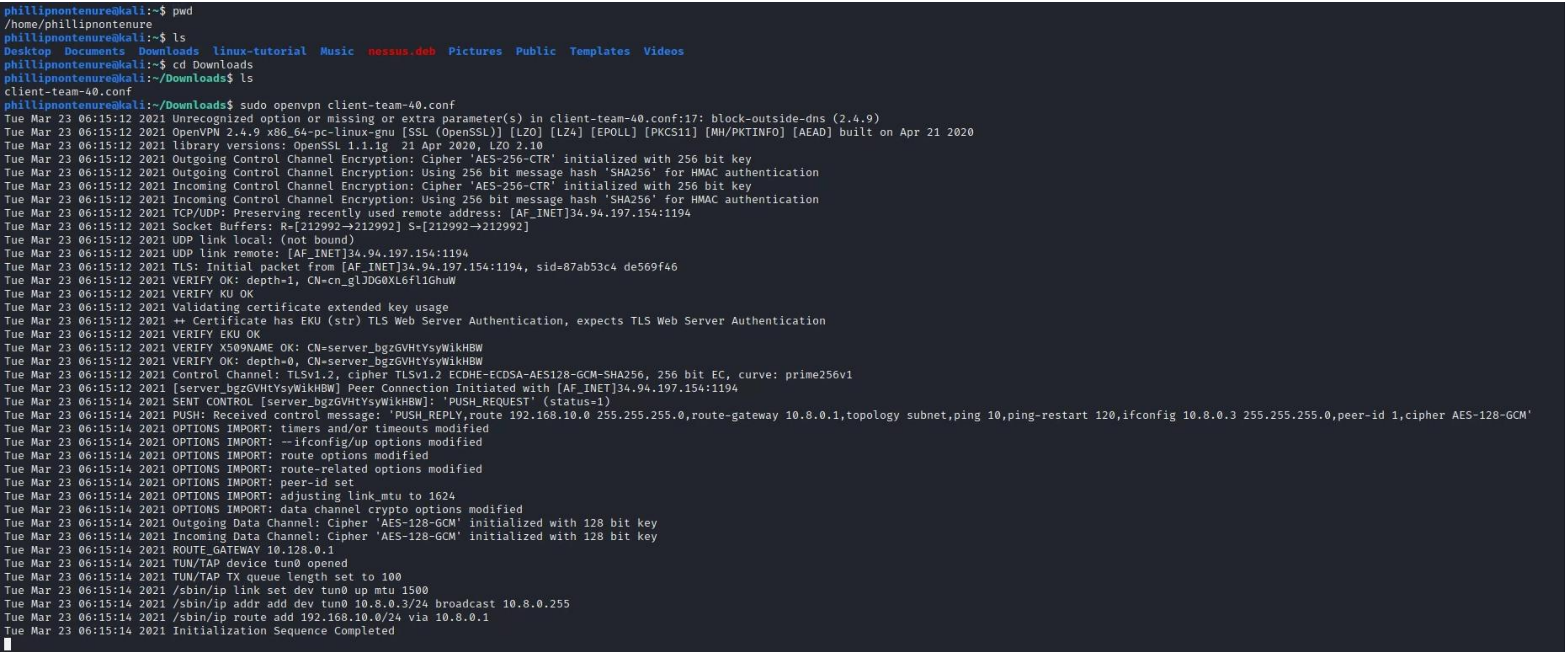
Copy/Paste



```
phillipnontenure@kali:~$ pwd
/home/phillipnontenure
phillipnontenure@kali:~$ ls
Desktop  Documents  Downloads  linux-tutorial  Music  nessus.deb  Pictures  Public  Templates  Videos
phillipnontenure@kali:~$ cd Downloads
phillipnontenure@kali:~/Downloads$ ls
client-team-40.conf
phillipnontenure@kali:~/Downloads$ 
```

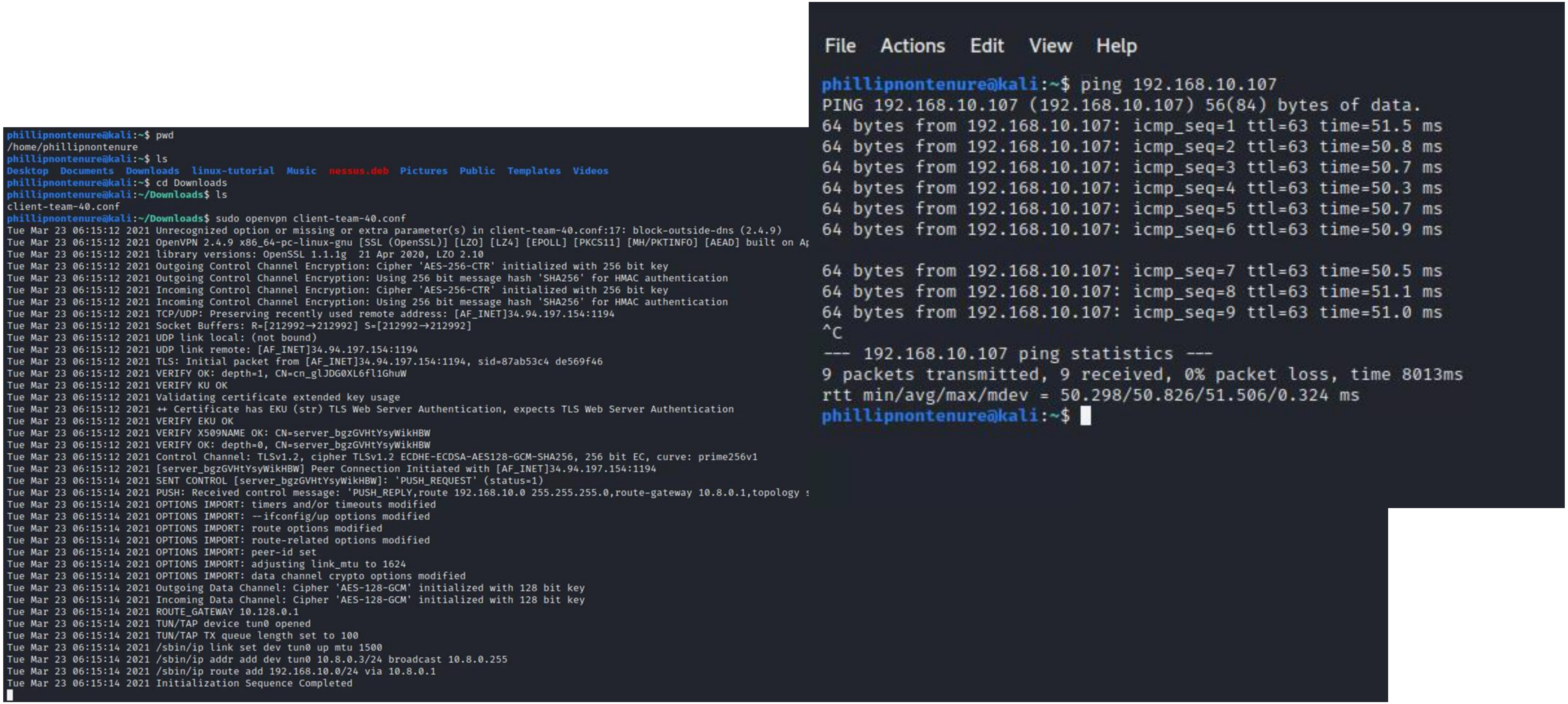


```
phillipnontenure@kali:~$ pwd
/home/phillipnontenure
phillipnontenure@kali:~$ ls
Desktop  Documents  Downloads  linux-tutorial  Music  nessus.deb  Pictures  Public  Templates  Videos
phillipnontenure@kali:~$ cd Downloads
phillipnontenure@kali:~/Downloads$ ls
client-team-40.conf
phillipnontenure@kali:~/Downloads$ sudo openvpn client-team-40.conf
```



```
phillipnontenure@kali:~$ pwd
/home/phillipnontenure
phillipnontenure@kali:~$ ls
Desktop  Documents  Downloads  linux-tutorial  Music  nessus.deb  Pictures  Public  Templates  Videos
phillipnontenure@kali:~$ cd Downloads
phillipnontenure@kali:~/Downloads$ ls
client-team-40.conf
phillipnontenure@kali:~/Downloads$ sudo openvpn client-team-40.conf
Tue Mar 23 06:15:12 2021 Unrecognized option or missing or extra parameter(s) in client-team-40.conf:17: block-outside-dns (2.4.9)
Tue Mar 23 06:15:12 2021 OpenVPN 2.4.9 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Apr 21 2020
Tue Mar 23 06:15:12 2021 library versions: OpenSSL 1.1.1g  21 Apr 2020, LZO 2.10
Tue Mar 23 06:15:12 2021 Outgoing Control Channel Encryption: Cipher 'AES-256-CTR' initialized with 256 bit key
Tue Mar 23 06:15:12 2021 Outgoing Control Channel Encryption: Using 256 bit message hash 'SHA256' for HMAC authentication
Tue Mar 23 06:15:12 2021 Incoming Control Channel Encryption: Cipher 'AES-256-CTR' initialized with 256 bit key
Tue Mar 23 06:15:12 2021 Incoming Control Channel Encryption: Using 256 bit message hash 'SHA256' for HMAC authentication
Tue Mar 23 06:15:12 2021 TCP/UDP: Preserving recently used remote address: [AF_INET]34.94.197.154:1194
Tue Mar 23 06:15:12 2021 Socket Buffers: R=[212992→212992] S=[212992→212992]
Tue Mar 23 06:15:12 2021 UDP link local: (not bound)
Tue Mar 23 06:15:12 2021 UDP link remote: [AF_INET]34.94.197.154:1194
Tue Mar 23 06:15:12 2021 TLS: Initial packet from [AF_INET]34.94.197.154:1194, sid=87ab53c4 de569f46
Tue Mar 23 06:15:12 2021 VERIFY OK: depth=1, CN=cn_glJDG0XL6fl1GhuW
Tue Mar 23 06:15:12 2021 VERIFY KU OK
Tue Mar 23 06:15:12 2021 Validating certificate extended key usage
Tue Mar 23 06:15:12 2021 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
Tue Mar 23 06:15:12 2021 VERIFY EKU OK
Tue Mar 23 06:15:12 2021 VERIFY X509NAME OK: CN=server_bgzGVHtYsyWikHBW
Tue Mar 23 06:15:12 2021 VERIFY OK: depth=0, CN=server_bgzGVHtYsyWikHBW
Tue Mar 23 06:15:12 2021 Control Channel: TLSv1.2, cipher TLSv1.2 ECDHE-ECDSA-AES128-GCM-SHA256, 256 bit EC, curve: prime256v1
Tue Mar 23 06:15:12 2021 [server_bgzGVHtYsyWikHBW] Peer Connection Initiated with [AF_INET]34.94.197.154:1194
Tue Mar 23 06:15:14 2021 SENT CONTROL [server_bgzGVHtYsyWikHBW]: 'PUSH_REQUEST' (status=1)
Tue Mar 23 06:15:14 2021 PUSH: Received control message: 'PUSH_REPLY,route 192.168.10.0 255.255.255.0,route-gateway 10.8.0.1,topology subnet,ping 10,ping-restart 120,ifconfig 10.8.0.3 255.255.255.0,peer-id 1,cipher AES-128-GCM'
Tue Mar 23 06:15:14 2021 OPTIONS IMPORT: timers and/or timeouts modified
Tue Mar 23 06:15:14 2021 OPTIONS IMPORT: --ifconfig/up options modified
Tue Mar 23 06:15:14 2021 OPTIONS IMPORT: route options modified
Tue Mar 23 06:15:14 2021 OPTIONS IMPORT: route-related options modified
Tue Mar 23 06:15:14 2021 OPTIONS IMPORT: peer-id set
Tue Mar 23 06:15:14 2021 OPTIONS IMPORT: adjusting link_mtu to 1624
Tue Mar 23 06:15:14 2021 OPTIONS IMPORT: data channel crypto options modified
Tue Mar 23 06:15:14 2021 Outgoing Data Channel: Cipher 'AES-128-GCM' initialized with 128 bit key
Tue Mar 23 06:15:14 2021 Incoming Data Channel: Cipher 'AES-128-GCM' initialized with 128 bit key
Tue Mar 23 06:15:14 2021 ROUTE_GATEWAY 10.128.0.1
Tue Mar 23 06:15:14 2021 TUN/TAP device tun0 opened
Tue Mar 23 06:15:14 2021 TUN/TAP TX queue length set to 100
Tue Mar 23 06:15:14 2021 /sbin/ip link set dev tun0 up mtu 1500
Tue Mar 23 06:15:14 2021 /sbin/ip addr add dev tun0 10.8.0.3/24 broadcast 10.8.0.255
Tue Mar 23 06:15:14 2021 /sbin/ip route add 192.168.10.0/24 via 10.8.0.1
Tue Mar 23 06:15:14 2021 Initialization Sequence Completed
```

Leave your VPN configuration process running in 1 terminal and open another to do your work…



```
phillipnontenure@kali:~$ pwd
/home/phillipnontenure
phillipnontenure@kali:~$ ls
Desktop  Documents  Downloads  linux-tutorial  Music  nessus.deb  Pictures  Public  Templates  Videos
phillipnontenure@kali:~$ cd Downloads
phillipnontenure@kali:~/Downloads$ ls
client-team-40.conf
phillipnontenure@kali:~/Downloads$ sudo openvpn client-team-40.conf
Tue Mar 23 06:15:12 2021 Unrecognized option or missing or extra parameter(s) in client-team-40.conf:17: block-outside-dns (2.4.9)
Tue Mar 23 06:15:12 2021 OpenVPN 2.4.9 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Ap
Tue Mar 23 06:15:12 2021 library versions: OpenSSL 1.1.1g  21 Apr 2020, LZO 2.10
Tue Mar 23 06:15:12 2021 Outgoing Control Channel Encryption: Cipher 'AES-256-CTR' initialized with 256 bit key
Tue Mar 23 06:15:12 2021 Outgoing Control Channel Encryption: Using 256 bit message hash 'SHA256' for HMAC authentication
Tue Mar 23 06:15:12 2021 Incoming Control Channel Encryption: Cipher 'AES-256-CTR' initialized with 256 bit key
Tue Mar 23 06:15:12 2021 Incoming Control Channel Encryption: Using 256 bit message hash 'SHA256' for HMAC authentication
Tue Mar 23 06:15:12 2021 TCP/UDP: Preserving recently used remote address: [AF_INET]34.94.197.154:1194
Tue Mar 23 06:15:12 2021 Socket Buffers: R=[212992→212992] S=[212992→212992]
Tue Mar 23 06:15:12 2021 UDP link local: (not bound)
Tue Mar 23 06:15:12 2021 UDP link remote: [AF_INET]34.94.197.154:1194
Tue Mar 23 06:15:12 2021 TLS: Initial packet from [AF_INET]34.94.197.154:1194, sid=87ab53c4 de569f46
Tue Mar 23 06:15:12 2021 VERIFY OK: depth=1, CN=cn_glJDG0XL6fl1GhuW
Tue Mar 23 06:15:12 2021 VERIFY KU OK
Tue Mar 23 06:15:12 2021 Validating certificate extended key usage
Tue Mar 23 06:15:12 2021 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
Tue Mar 23 06:15:12 2021 VERIFY EKU OK
Tue Mar 23 06:15:12 2021 VERIFY X509NAME OK: CN=server_bgzGVHtYsyWikHBW
Tue Mar 23 06:15:12 2021 VERIFY OK: depth=0, CN=server_bgzGVHtYsyWikHBW
Tue Mar 23 06:15:12 2021 Control Channel: TLSv1.2, cipher TLSv1.2 ECDHE-ECDSA-AES128-GCM-SHA256, 256 bit EC, curve: prime256v1
Tue Mar 23 06:15:12 2021 [server_bgzGVHtYsyWikHBW] Peer Connection Initiated with [AF_INET]34.94.197.154:1194
Tue Mar 23 06:15:14 2021 SENT CONTROL [server_bgzGVHtYsyWikHBW]: 'PUSH_REQUEST' (status=1)
Tue Mar 23 06:15:14 2021 PUSH: Received control message: 'PUSH_REPLY,route 192.168.10.0 255.255.255.0,route-gateway 10.8.0.1,topology s
Tue Mar 23 06:15:14 2021 OPTIONS IMPORT: timers and/or timeouts modified
Tue Mar 23 06:15:14 2021 OPTIONS IMPORT: --ifconfig/up options modified
Tue Mar 23 06:15:14 2021 OPTIONS IMPORT: route options modified
Tue Mar 23 06:15:14 2021 OPTIONS IMPORT: route-related options modified
Tue Mar 23 06:15:14 2021 OPTIONS IMPORT: peer-id set
Tue Mar 23 06:15:14 2021 OPTIONS IMPORT: adjusting link_mtu to 1624
Tue Mar 23 06:15:14 2021 OPTIONS IMPORT: data channel crypto options modified
Tue Mar 23 06:15:14 2021 Outgoing Data Channel: Cipher 'AES-128-GCM' initialized with 128 bit key
Tue Mar 23 06:15:14 2021 Incoming Data Channel: Cipher 'AES-128-GCM' initialized with 128 bit key
Tue Mar 23 06:15:14 2021 ROUTE_GATEWAY 10.128.0.1
Tue Mar 23 06:15:14 2021 TUN/TAP device tun0 opened
Tue Mar 23 06:15:14 2021 TUN/TAP TX queue length set to 100
Tue Mar 23 06:15:14 2021 /sbin/ip link set dev tun0 up mtu 1500
Tue Mar 23 06:15:14 2021 /sbin/ip addr add dev tun0 10.8.0.3/24 broadcast 10.8.0.255
Tue Mar 23 06:15:14 2021 /sbin/ip route add 192.168.10.0/24 via 10.8.0.1
Tue Mar 23 06:15:14 2021 Initialization Sequence Completed
```

```
phillipnontenure@kali:~$ ping 192.168.10.107
PING 192.168.10.107 (192.168.10.107) 56(84) bytes of data.
64 bytes from 192.168.10.107: icmp_seq=1 ttl=63 time=51.5 ms
64 bytes from 192.168.10.107: icmp_seq=2 ttl=63 time=50.8 ms
64 bytes from 192.168.10.107: icmp_seq=3 ttl=63 time=50.7 ms
64 bytes from 192.168.10.107: icmp_seq=4 ttl=63 time=50.3 ms
64 bytes from 192.168.10.107: icmp_seq=5 ttl=63 time=50.7 ms
64 bytes from 192.168.10.107: icmp_seq=6 ttl=63 time=50.9 ms

64 bytes from 192.168.10.107: icmp_seq=7 ttl=63 time=50.5 ms
64 bytes from 192.168.10.107: icmp_seq=8 ttl=63 time=51.1 ms
64 bytes from 192.168.10.107: icmp_seq=9 ttl=63 time=51.0 ms
^C
--- 192.168.10.107 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8013ms
rtt min/avg/max/mdev = 50.298/50.826/51.506/0.324 ms
phillipnontenure@kali:~$ 
```

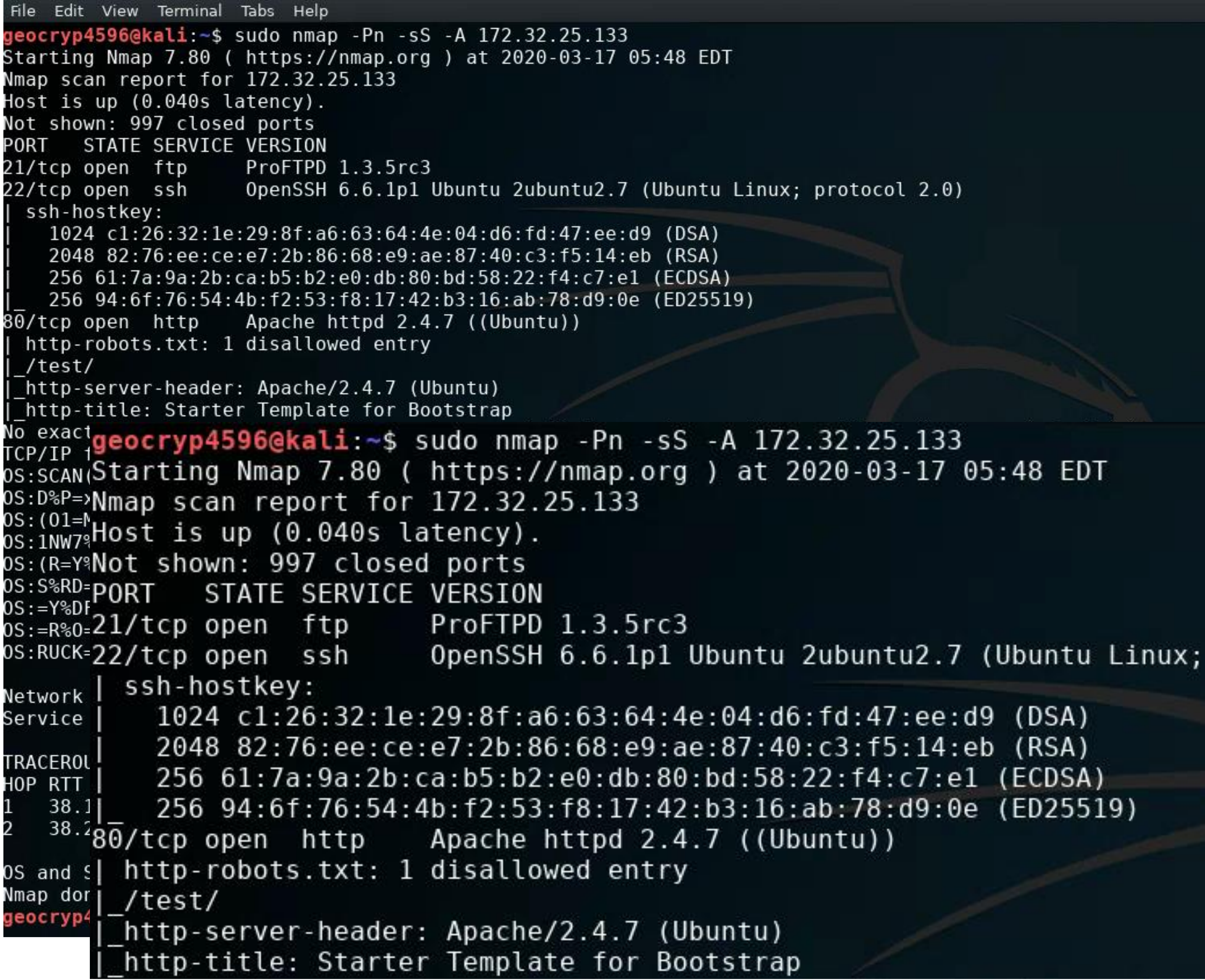
Vulnerability Analysis

Let’s scan for open ports on the target machine and see what we can learn…

-sS look for open TCP ports

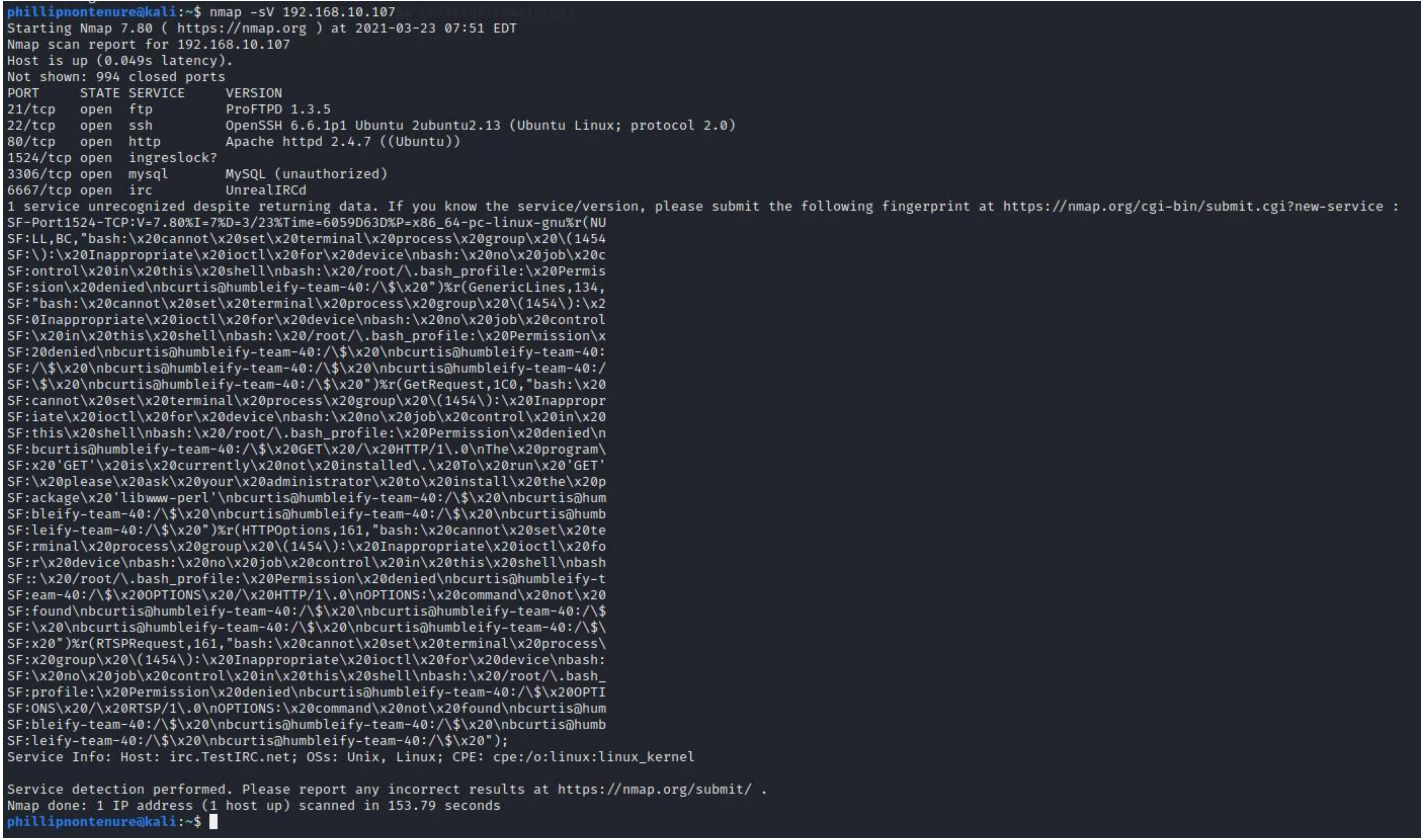
-A detect OS and versions

-Pn do not use Ping

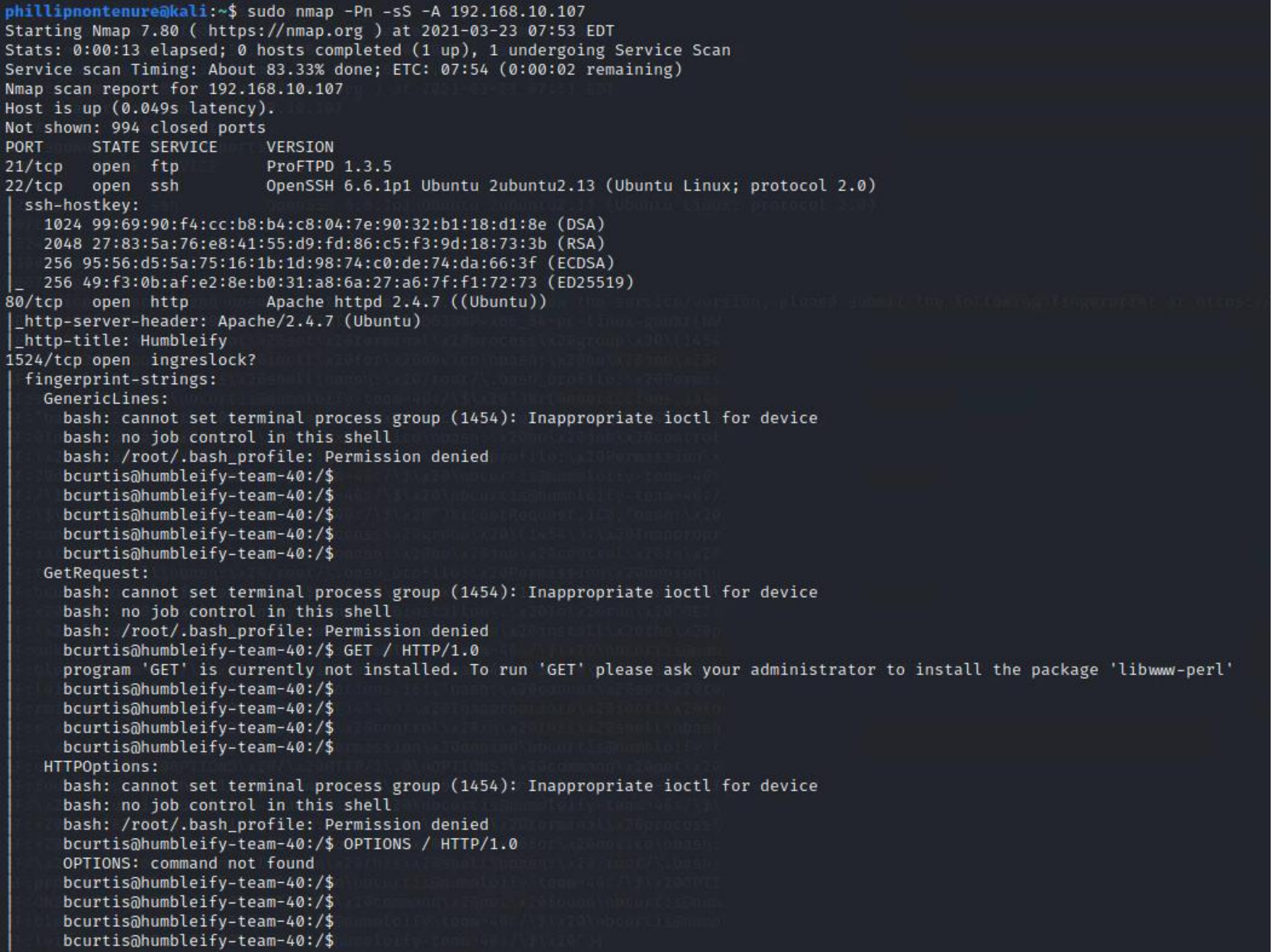


```
geocryp4596@kali:~$ sudo nmap -Pn -sS -A 172.32.25.133
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-17 05:48 EDT
Nmap scan report for 172.32.25.133
Host is up (0.040s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.5rc3
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 c1:26:32:1e:29:8f:a6:63:64:4e:04:d6:fd:47:ee:d9 (DSA)
|   2048 82:76:ee:ce:e7:2b:86:68:e9:ae:87:40:c3:f5:14:eb (RSA)
|   256 61:7a:9a:2b:ca:b5:b2:e0:db:80:bd:58:22:f4:c7:e1 (ECDSA)
|_  256 94:6f:76:54:4b:f2:53:f8:17:42:b3:16:ab:78:d9:0e (ED25519)
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
| http-robots.txt: 1 disallowed entry
|_/test/
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Starter Template for Bootstrap
No exact
TCP/IP f
OS:SCAN(
OS:D%P=x
OS:(O1=M
OS:1NW7%
OS:(R=Y%
OS:S%RD=
OS:=Y%DF
OS:=R%O=
OS:RUCK=

Network
Service

TRACEROU
HOP RTT
1   38.1
2   38.2

OS and S
Nmap don
geocryp4
```

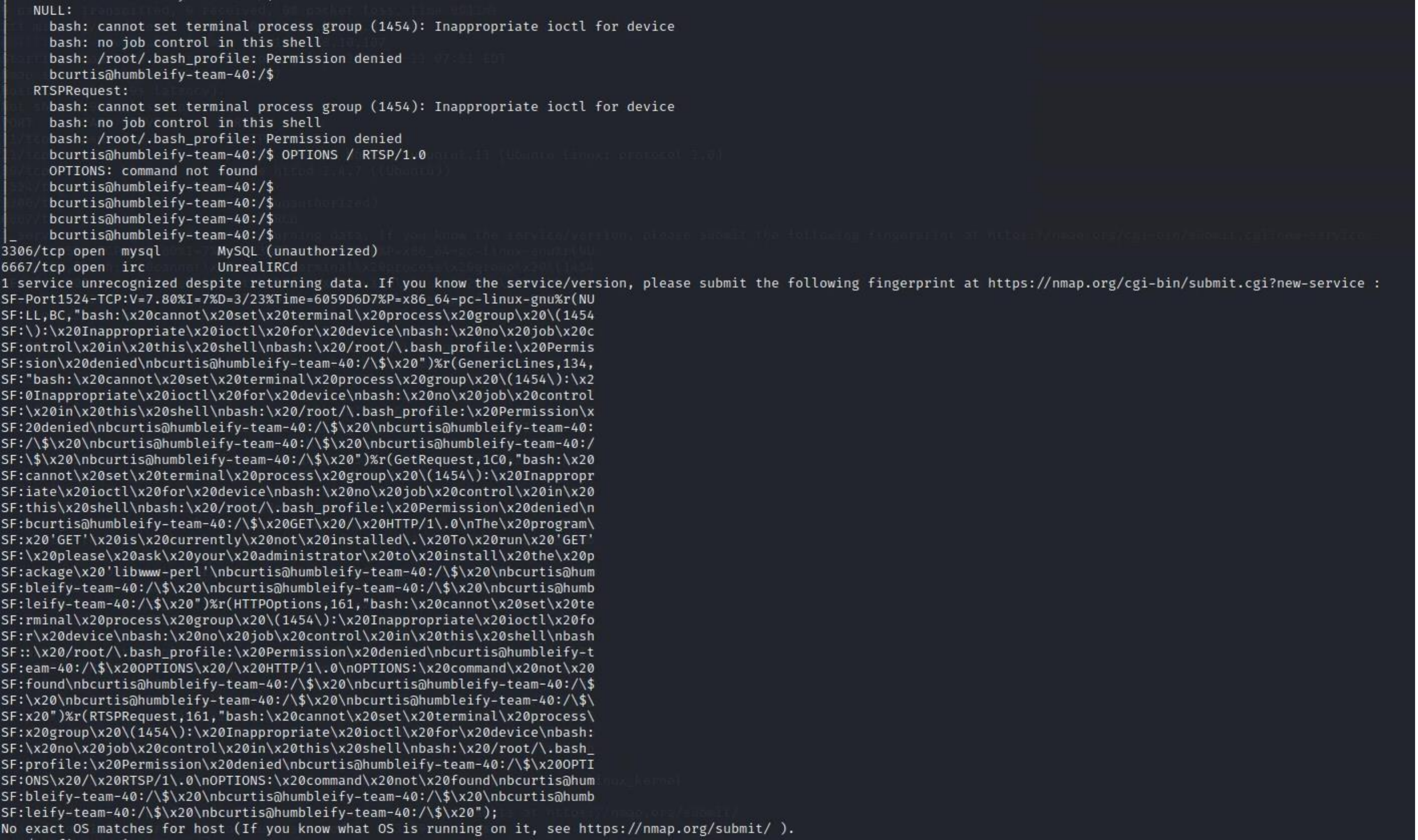
```
geocryp4596@kali:~$ sudo nmap -Pn -sS -A 172.32.25.133
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-17 05:48 EDT
Nmap scan report for 172.32.25.133
Host is up (0.040s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.5rc3
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.7 (Ubuntu Linux;
| ssh-hostkey:
|   1024 c1:26:32:1e:29:8f:a6:63:64:4e:04:d6:fd:47:ee:d9 (DSA)
|   2048 82:76:ee:ce:e7:2b:86:68:e9:ae:87:40:c3:f5:14:eb (RSA)
|   256 61:7a:9a:2b:ca:b5:b2:e0:db:80:bd:58:22:f4:c7:e1 (ECDSA)
|_  256 94:6f:76:54:4b:f2:53:f8:17:42:b3:16:ab:78:d9:0e (ED25519)
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
| http-robots.txt: 1 disallowed entry
|_/test/
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Starter Template for Bootstrap
```



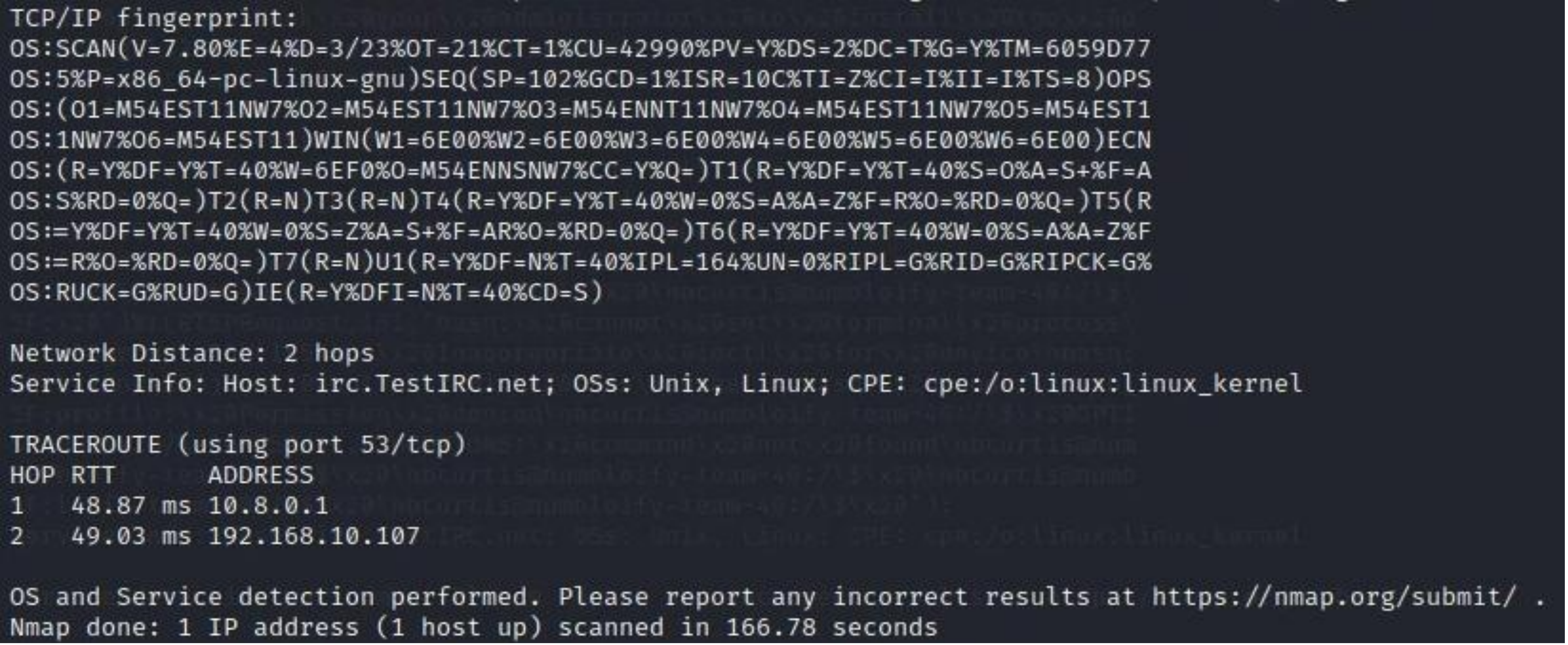
```
phillipnontenure@kali:~$ nmap -sV 192.168.10.107
Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-23 07:51 EDT
Nmap scan report for 192.168.10.107
Host is up (0.049s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         ProFTPD 1.3.5
22/tcp   open  ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http        Apache httpd 2.4.7 ((Ubuntu))
1524/tcp open  ingreslock?
3306/tcp open  mysql       MySQL (unauthorized)
6667/tcp open  irc         UnrealIRCd
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port1524-TCP:V=7.80%I=7%D=3/23%Time=6059D63D%P=x86_64-pc-linux-gnu%r(NU
SF:LL,BC,"bash:\x20cannot\x20set\x20terminal\x20process\x20group\x20\(1454
SF:\):\x20Inappropriate\x20ioctl\x20for\x20device\nbash:\x20no\x20job\x20c
SF:ontrol\x20in\x20this\x20shell\nbash:\x20/root/\.bash_profile:\x20Permis
SF:sion\x20denied\nbcurtis@humbleify-team-40:/\$\x20")%r(GenericLines,134,
SF:"bash:\x20cannot\x20set\x20terminal\x20process\x20group\x20\(1454\):\x2
SF:0Inappropriate\x20ioctl\x20for\x20device\nbash:\x20no\x20job\x20control
SF:\x20in\x20this\x20shell\nbash:\x20/root/\.bash_profile:\x20Permission\x
SF:20denied\nbcurtis@humbleify-team-40:/\$\x20\nbcurtis@humbleify-team-40:
SF:/\$\x20\nbcurtis@humbleify-team-40:/\$\x20\nbcurtis@humbleify-team-40:/
SF:\$\x20\nbcurtis@humbleify-team-40:/\$\x20")%r(GetRequest,1C0,"bash:\x20
SF:cannot\x20set\x20terminal\x20process\x20group\x20\(1454\):\x20Inappropr
SF:iate\x20ioctl\x20for\x20device\nbash:\x20no\x20job\x20control\x20in\x20
SF:this\x20shell\nbash:\x20/root/\.bash_profile:\x20Permission\x20denied\n
SF:bcurtis@humbleify-team-40:/\$\x20GET\x20/\x20HTTP/1\.0\nThe\x20program\
SF:x20'GET'\x20is\x20currently\x20not\x20installed\.\x20To\x20run\x20'GET'
SF:\x20please\x20ask\x20your\x20administrator\x20to\x20install\x20the\x20p
SF:ackage\x20'libwww-perl'\nbcurtis@humbleify-team-40:/\$\x20\nbcurtis@hum
SF:bleify-team-40:/\$\x20\nbcurtis@humbleify-team-40:/\$\x20\nbcurtis@humb
SF:leify-team-40:/\$\x20")%r(HTTPOptions,161,"bash:\x20cannot\x20set\x20te
SF:rminal\x20process\x20group\x20\(1454\):\x20Inappropriate\x20ioctl\x20fo
SF:r\x20device\nbash:\x20no\x20job\x20control\x20in\x20this\x20shell\nbash
SF::\x20/root/\.bash_profile:\x20Permission\x20denied\nbcurtis@humbleify-t
SF:eam-40:/\$\x20OPTIONS\x20/\x20HTTP/1\.0\nOPTIONS:\x20command\x20not\x20
SF:found\nbcurtis@humbleify-team-40:/\$\x20\nbcurtis@humbleify-team-40:/\$
SF:\x20\nbcurtis@humbleify-team-40:/\$\x20\nbcurtis@humbleify-team-40:/\$\
SF:x20")%r(RTSPRequest,161,"bash:\x20cannot\x20set\x20terminal\x20process\
SF:x20group\x20\(1454\):\x20Inappropriate\x20ioctl\x20for\x20device\nbash:
SF:\x20no\x20job\x20control\x20in\x20this\x20shell\nbash:\x20/root/\.bash_
SF:profile:\x20Permission\x20denied\nbcurtis@humbleify-team-40:/\$\x20OPTI
SF:ONS\x20/\x20RTSP/1\.0\nOPTIONS:\x20command\x20not\x20found\nbcurtis@hum
SF:bleify-team-40:/\$\x20\nbcurtis@humbleify-team-40:/\$\x20\nbcurtis@humb
SF:leify-team-40:/\$\x20\nbcurtis@humbleify-team-40:/\$\x20");
Service Info: Host: irc.TestIRC.net; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 153.79 seconds
phillipnontenure@kali:~$ 
```



```
phillipnontenure@kali:~$ sudo nmap -Pn -sS -A 192.168.10.107
Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-23 07:53 EDT
Stats: 0:00:13 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 83.33% done; ETC: 07:54 (0:00:02 remaining)
Nmap scan report for 192.168.10.107
Host is up (0.049s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE      VERSION
21/tcp   open  ftp          ProFTPD 1.3.5
22/tcp   open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 99:69:90:f4:cc:b8:b4:c8:04:7e:90:32:b1:18:d1:8e (DSA)
|   2048 27:83:5a:76:e8:41:55:d9:fd:86:c5:f3:9d:18:73:3b (RSA)
|   256 95:56:d5:5a:75:16:1b:1d:98:74:c0:de:74:da:66:3f (ECDSA)
|_  256 49:f3:0b:af:e2:8e:b0:31:a8:6a:27:a6:7f:f1:72:73 (ED25519)
80/tcp   open  http         Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Humbleify
1524/tcp open  ingreslock?
| fingerprint-strings:
|   GenericLines:
|     bash: cannot set terminal process group (1454): Inappropriate ioctl for device
|     bash: no job control in this shell
|     bash: /root/.bash_profile: Permission denied
|     bcurtis@humbleify-team-40:/$
|     bcurtis@humbleify-team-40:/$
|     bcurtis@humbleify-team-40:/$
|     bcurtis@humbleify-team-40:/$
|     bcurtis@humbleify-team-40:/$
|   GetRequest:
|     bash: cannot set terminal process group (1454): Inappropriate ioctl for device
|     bash: no job control in this shell
|     bash: /root/.bash_profile: Permission denied
|     bcurtis@humbleify-team-40:/$ GET / HTTP/1.0
|     program 'GET' is currently not installed. To run 'GET' please ask your administrator to install the package 'libwww-perl'
|     bcurtis@humbleify-team-40:/$
|     bcurtis@humbleify-team-40:/$
|     bcurtis@humbleify-team-40:/$
|     bcurtis@humbleify-team-40:/$
|   HTTPOptions:
|     bash: cannot set terminal process group (1454): Inappropriate ioctl for device
|     bash: no job control in this shell
|     bash: /root/.bash_profile: Permission denied
|     bcurtis@humbleify-team-40:/$ OPTIONS / HTTP/1.0
|     OPTIONS: command not found
|     bcurtis@humbleify-team-40:/$
|     bcurtis@humbleify-team-40:/$
|     bcurtis@humbleify-team-40:/$
|     bcurtis@humbleify-team-40:/$
```



```
|   NULL:
|     bash: cannot set terminal process group (1454): Inappropriate ioctl for device
|     bash: no job control in this shell
|     bash: /root/.bash_profile: Permission denied
|     bcurtis@humbleify-team-40:/$
|   RTSPRequest:
|     bash: cannot set terminal process group (1454): Inappropriate ioctl for device
|     bash: no job control in this shell
|     bash: /root/.bash_profile: Permission denied
|     bcurtis@humbleify-team-40:/$ OPTIONS / RTSP/1.0
|     OPTIONS: command not found
|     bcurtis@humbleify-team-40:/$
|     bcurtis@humbleify-team-40:/$
|     bcurtis@humbleify-team-40:/$
|_    bcurtis@humbleify-team-40:/$
3306/tcp open  mysql       MySQL (unauthorized)
6667/tcp open  irc         UnrealIRCd
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port1524-TCP:V=7.80%I=7%D=3/23%Time=6059D6D7%P=x86_64-pc-linux-gnu%r(NU
SF:LL,BC,"bash:\x20cannot\x20set\x20terminal\x20process\x20group\x20\(1454
SF:\):\x20Inappropriate\x20ioctl\x20for\x20device\nbash:\x20no\x20job\x20c
SF:ontrol\x20in\x20this\x20shell\nbash:\x20/root/\.bash_profile:\x20Permis
SF:sion\x20denied\nbcurtis@humbleify-team-40:/\$\x20")%r(GenericLines,134,
SF:"bash:\x20cannot\x20set\x20terminal\x20process\x20group\x20\(1454\):\x2
SF:0Inappropriate\x20ioctl\x20for\x20device\nbash:\x20no\x20job\x20control
SF:\x20in\x20this\x20shell\nbash:\x20/root/\.bash_profile:\x20Permission\x
SF:20denied\nbcurtis@humbleify-team-40:/\$\x20\nbcurtis@humbleify-team-40:
SF:/\$\x20\nbcurtis@humbleify-team-40:/\$\x20\nbcurtis@humbleify-team-40:/
SF:\$\x20\nbcurtis@humbleify-team-40:/\$\x20")%r(GetRequest,1C0,"bash:\x20
SF:cannot\x20set\x20terminal\x20process\x20group\x20\(1454\):\x20Inappropr
SF:iate\x20ioctl\x20for\x20device\nbash:\x20no\x20job\x20control\x20in\x20
SF:this\x20shell\nbash:\x20/root/\.bash_profile:\x20Permission\x20denied\n
SF:bcurtis@humbleify-team-40:/\$\x20GET\x20/\x20HTTP/1\.0\nThe\x20program\
SF:x20'GET'\x20is\x20currently\x20not\x20installed\.\x20To\x20run\x20'GET'
SF:\x20please\x20ask\x20your\x20administrator\x20to\x20install\x20the\x20p
SF:ackage\x20'libwww-perl'\nbcurtis@humbleify-team-40:/\$\x20\nbcurtis@hum
SF:bleify-team-40:/\$\x20\nbcurtis@humbleify-team-40:/\$\x20\nbcurtis@humb
SF:leify-team-40:/\$\x20")%r(HTTPOptions,161,"bash:\x20cannot\x20set\x20te
SF:rminal\x20process\x20group\x20\(1454\):\x20Inappropriate\x20ioctl\x20fo
SF:r\x20device\nbash:\x20no\x20job\x20control\x20in\x20this\x20shell\nbash
SF::\x20/root/\.bash_profile:\x20Permission\x20denied\nbcurtis@humbleify-t
SF:eam-40:/\$\x20OPTIONS\x20/\x20HTTP/1\.0\nOPTIONS:\x20command\x20not\x20
SF:found\nbcurtis@humbleify-team-40:/\$\x20\nbcurtis@humbleify-team-40:/\$
SF:\x20\nbcurtis@humbleify-team-40:/\$\x20\nbcurtis@humbleify-team-40:/\$\
SF:x20")%r(RTSPRequest,161,"bash:\x20cannot\x20set\x20terminal\x20process\
SF:x20group\x20\(1454\):\x20Inappropriate\x20ioctl\x20for\x20device\nbash:
SF:\x20no\x20job\x20control\x20in\x20this\x20shell\nbash:\x20/root/\.bash_
SF:profile:\x20Permission\x20denied\nbcurtis@humbleify-team-40:/\$\x20OPTI
SF:ONS\x20/\x20RTSP/1\.0\nOPTIONS:\x20command\x20not\x20found\nbcurtis@hum
SF:bleify-team-40:/\$\x20\nbcurtis@humbleify-team-40:/\$\x20\nbcurtis@humb
SF:leify-team-40:/\$\x20\nbcurtis@humbleify-team-40:/\$\x20");
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```



```
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=3/23%OT=21%CT=1%CU=42990%PV=Y%DS=2%DC=T%G=Y%TM=6059D77
OS:5%P=x86_64-pc-linux-gnu)SEQ(SP=102%GCD=1%ISR=10C%TI=Z%CI=I%II=I%TS=8)OPS
OS:(O1=M54EST11NW7%O2=M54EST11NW7%O3=M54ENNT11NW7%O4=M54EST11NW7%O5=M54EST1
OS:1NW7%O6=M54EST11)WIN(W1=6E00%W2=6E00%W3=6E00%W4=6E00%W5=6E00%W6=6E00)ECN
OS:(R=Y%DF=Y%T=40%W=6EF0%O=M54ENNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=A
OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R
OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F
OS:=R%O=%RD=0%Q=)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%
OS:RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: Host: irc.TestIRC.net; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 53/tcp)
HOP RTT      ADDRESS
1   48.87 ms 10.8.0.1
2   49.03 ms 192.168.10.107

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 166.78 seconds
```

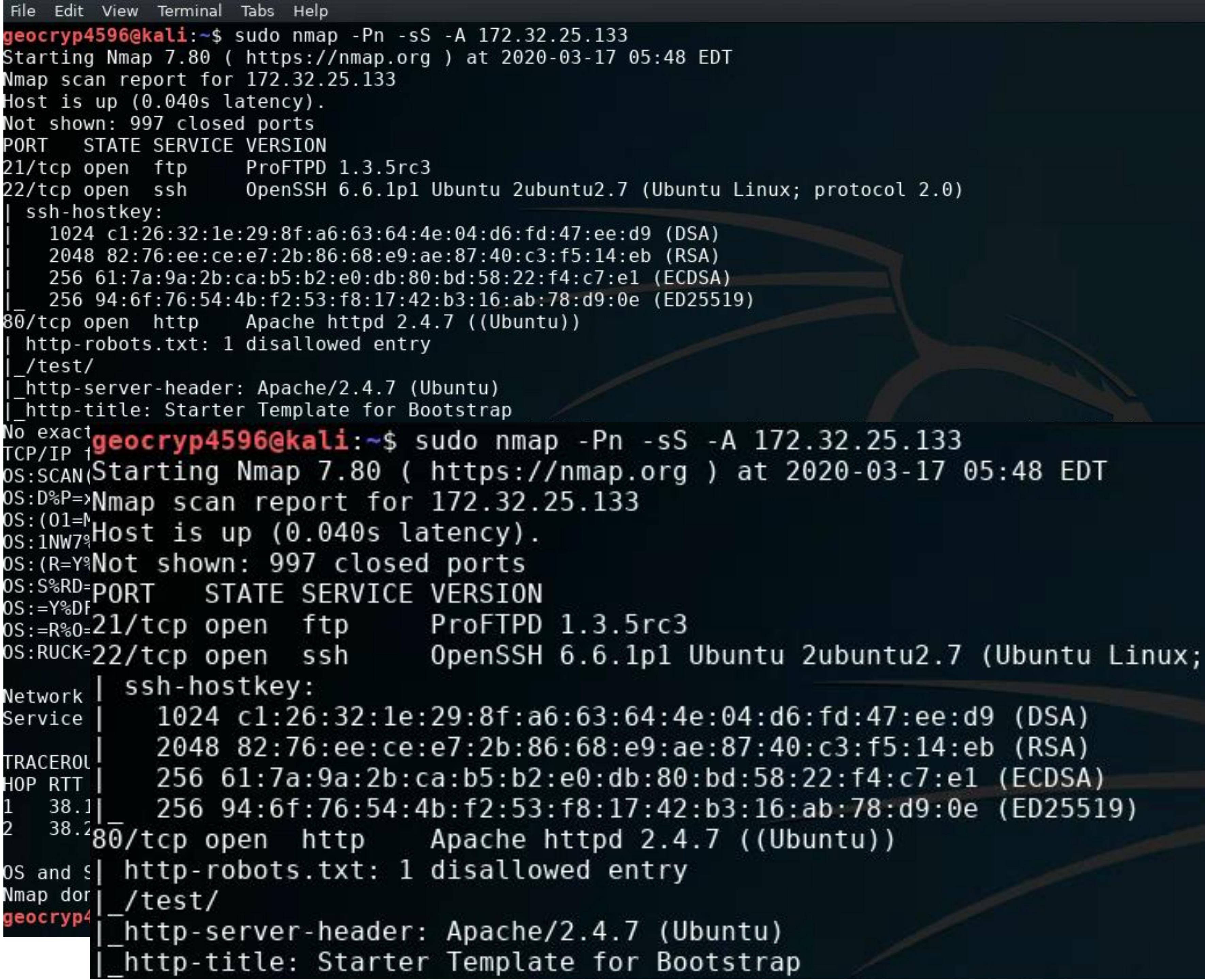
Vulnerability Analysis

Let’s scan for open ports on the target machine and see what we can learn…

-sS look for open TCP ports

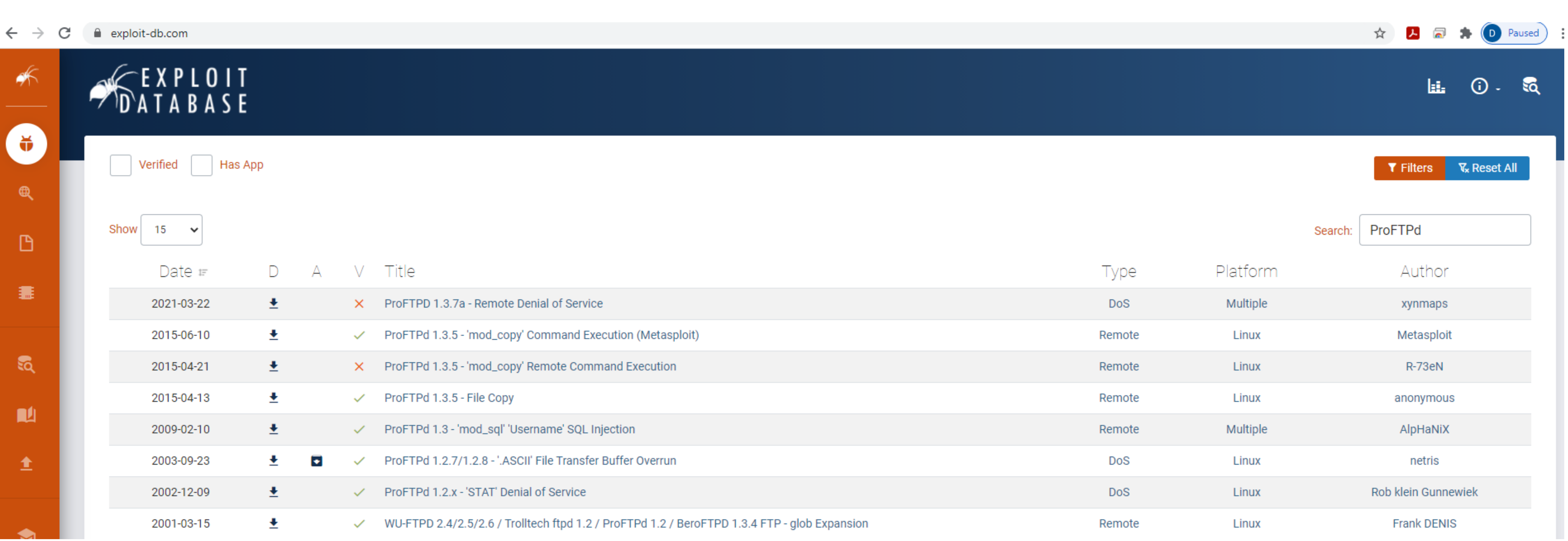
-A detect OS and versions

-Pn do not use Ping



```
geocryp4596@kali:~$ sudo nmap -Pn -sS -A 172.32.25.133
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-17 05:48 EDT
Nmap scan report for 172.32.25.133
Host is up (0.040s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.5rc3
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 c1:26:32:1e:29:8f:a6:63:64:4e:04:d6:fd:47:ee:d9 (DSA)
|   2048 82:76:ee:ce:e7:2b:86:68:e9:ae:87:40:c3:f5:14:eb (RSA)
|   256 61:7a:9a:2b:ca:b5:b2:e0:db:80:bd:58:22:f4:c7:e1 (ECDSA)
|_  256 94:6f:76:54:4b:f2:53:f8:17:42:b3:16:ab:78:d9:0e (ED25519)
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
| http-robots.txt: 1 disallowed entry
|_/test/
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Starter Template for Bootstrap
No exact
TCP/IP f
OS:SCAN(
OS:D%P=x
OS:(O1=M
OS:1NW7%
OS:(R=Y%
OS:S%RD=
OS:=Y%DF
OS:=R%O=
OS:RUCK=

Network
Service

TRACEROU
HOP RTT
1   38.1
2   38.2

OS and S
Nmap don
geocryp4
```

```
geocryp4596@kali:~$ sudo nmap -Pn -sS -A 172.32.25.133
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-17 05:48 EDT
Nmap scan report for 172.32.25.133
Host is up (0.040s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.5rc3
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.7 (Ubuntu Linux;
| ssh-hostkey:
|   1024 c1:26:32:1e:29:8f:a6:63:64:4e:04:d6:fd:47:ee:d9 (DSA)
|   2048 82:76:ee:ce:e7:2b:86:68:e9:ae:87:40:c3:f5:14:eb (RSA)
|   256 61:7a:9a:2b:ca:b5:b2:e0:db:80:bd:58:22:f4:c7:e1 (ECDSA)
|_  256 94:6f:76:54:4b:f2:53:f8:17:42:b3:16:ab:78:d9:0e (ED25519)
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
| http-robots.txt: 1 disallowed entry
|_/test/
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Starter Template for Bootstrap
```

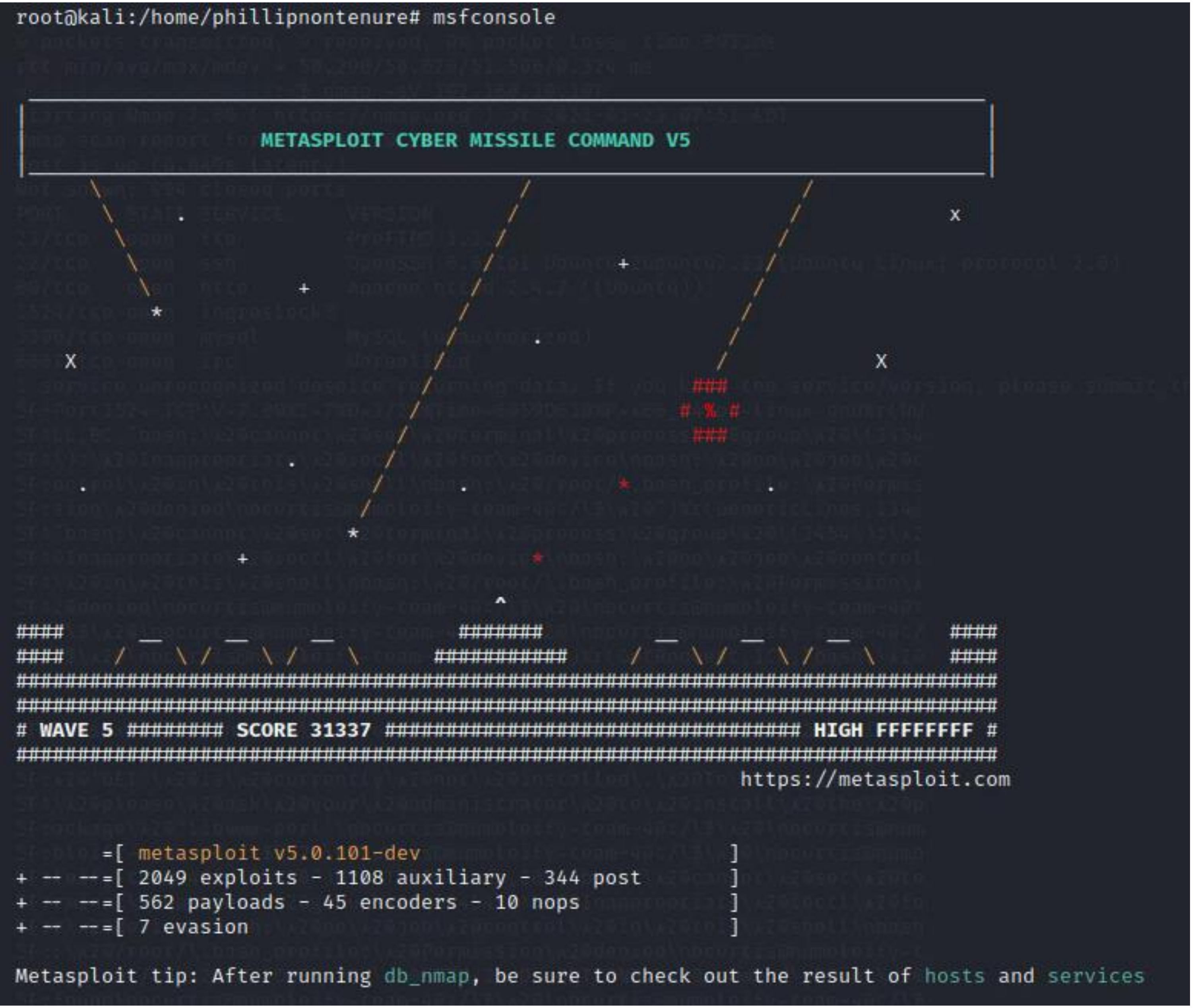


□ Verified □ Has App

Show 15

Search: ProFTPd

Date	D	A	V	Title	Type	Platform	Author
2021-03-22	⬇		✗	ProFTPD 1.3.7a - Remote Denial of Service	DoS	Multiple	xynmaps
2015-06-10	⬇		✓	ProFTPd 1.3.5 - 'mod_copy' Command Execution (Metasploit)	Remote	Linux	Metasploit
2015-04-21	⬇		✗	ProFTPd 1.3.5 - 'mod_copy' Remote Command Execution	Remote	Linux	R-73eN
2015-04-13	⬇		✓	ProFTPd 1.3.5 - File Copy	Remote	Linux	anonymous
2009-02-10	⬇		✓	ProFTPd 1.3 - 'mod_sql' 'Username' SQL Injection	Remote	Multiple	AlpHaNiX
2003-09-23	⬇	▣	✓	ProFTPd 1.2.7/1.2.8 - '.ASCII' File Transfer Buffer Overrun	DoS	Linux	netris
2002-12-09	⬇		✓	ProFTPd 1.2.x - 'STAT' Denial of Service	DoS	Linux	Rob klein Gunnewiek
2001-03-15	⬇		✓	WU-FTPD 2.4/2.5/2.6 / Trolltech ftpd 1.2 / ProFTPd 1.2 / BeroFTPD 1.3.4 FTP - glob Expansion	Remote	Linux	Frank DENIS



```
root@kali:/home/phillipnontenure# msfconsole

 ______________________________________________________________________________
|                                                                              |
|                   METASPLOIT CYBER MISSILE COMMAND V5                        |
|______________________________________________________________________________|
      \                                  /                      /
       \     .                          /                      /            x
        \                              /                      /
         \                            /          +           /
          \            +             /                      /
           *                        /                      /
                                   /      .               /
    X                             /                      /            X
                                 /                     ###
                                /                     # % #
                               /                       ###
                      .       /
     .                       /      .            *           .
                            /
                           *
                  +                       *

                                       ^
####      __     __     __          #######         __     __     __        ####
####    /    \ /    \ /    \      ###########     /    \ /    \ /    \      ####
################################################################################
################################################################################
# WAVE 5 ######## SCORE 31337 ################################## HIGH FFFFFFFF #
################################################################################
                                                           https://metasploit.com


       =[ metasploit v5.0.101-dev                         ]
+ -- --=[ 2049 exploits - 1108 auxiliary - 344 post       ]
+ -- --=[ 562 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: After running db_nmap, be sure to check out the result of hosts and services
```

Follow instructions for Milestone 3 found in Canvas, follow instructions for Accessing the Asset in:

https://anthonyvance.com/security-assignments/projects/pen-test.html

Agenda

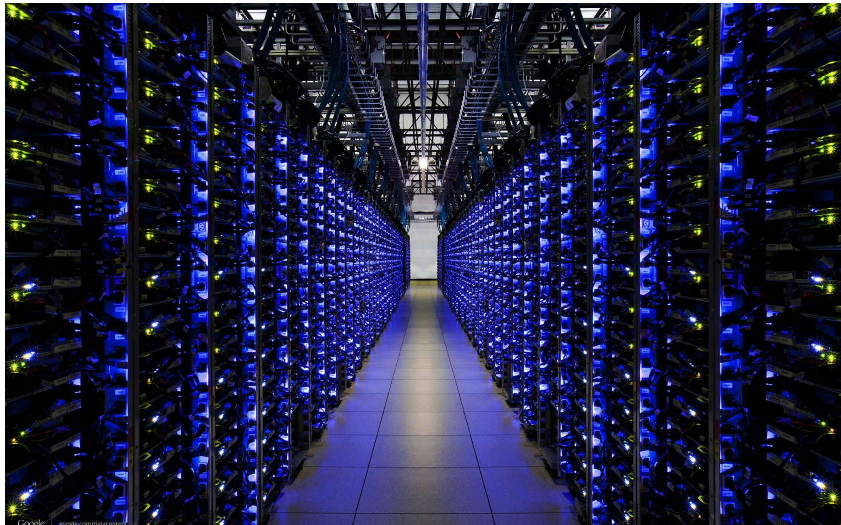
- Milestone 3 – Accessing your server
- Vulnerabilities and sources of threats
- Physical control inventory baselines
- Perimeter security
- Media protection
- Media sanitization

Physical and Environmental (PE) Security

…encompasses protection of physical assets from damage, misuse, or theft

- **Physical security addresses**
  - **…mechanisms used to create secure areas around hardware**

- **Environmental security addresses**
  - **…safety of assets from damage from environmental concerns**



Sources of threats…

Human *– vandalism, sabotage, theft, terrorism, war*

Materials

- ***Water*** *– floods, leaks*
- ***Chemicals and particulates -*** *smoke, toxic materials, industrial pollution*
- ***Organism*** *- virus, bacteria, animal, insect*
- *…*

Energy

- ***Fire***
- ***Explosion***
- ***Electricity****,* ***magnetism, radio wave*** *anomalies*
- *…*

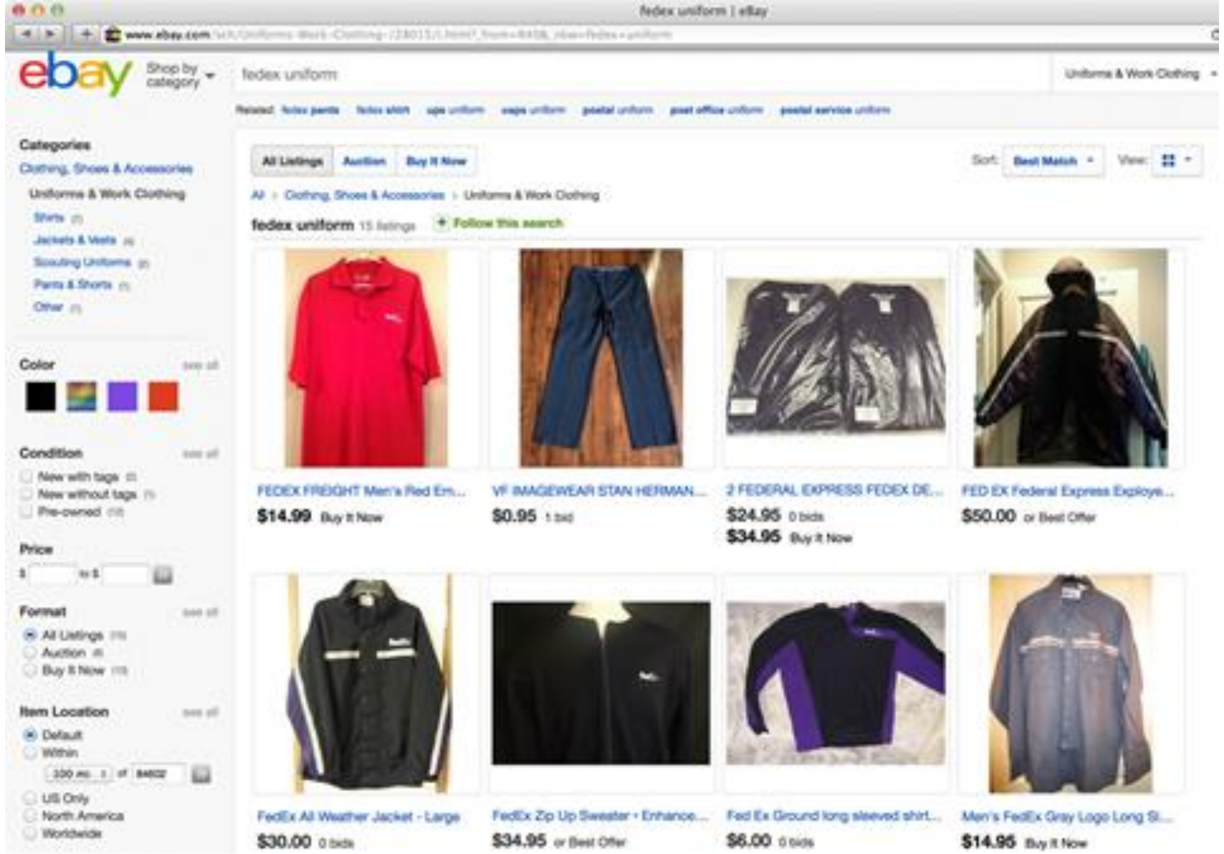
NO
HOWARE YOU

“Tailgating”, “Piggybacking” and Social Engineering

Social engineering

Are receptionists good at preventative security?

- **No,** their job is to help people feel welcome and guide them through the organization in an efficient way
- But intruders can get past guards with social engineering…



FEDEX FREIGHT Men's Red Em... $14.99 Buy It Now

VF IMAGEWEAR STAN HERMAN... $0.95 1 bid

2 FEDERAL EXPRESS FEDEX DE... $24.95 0 bids $34.95 Buy It Now

FED EX Federal Express Exploye... $50.00 or Best Offer

FedEx All Weather Jacket - Large $30.00 0 bids

FedEx Zip Up Sweater + Enhance... $34.95 or Best Offer

Fed Ex Ground long sleeved shirt... $6.00 0 bids

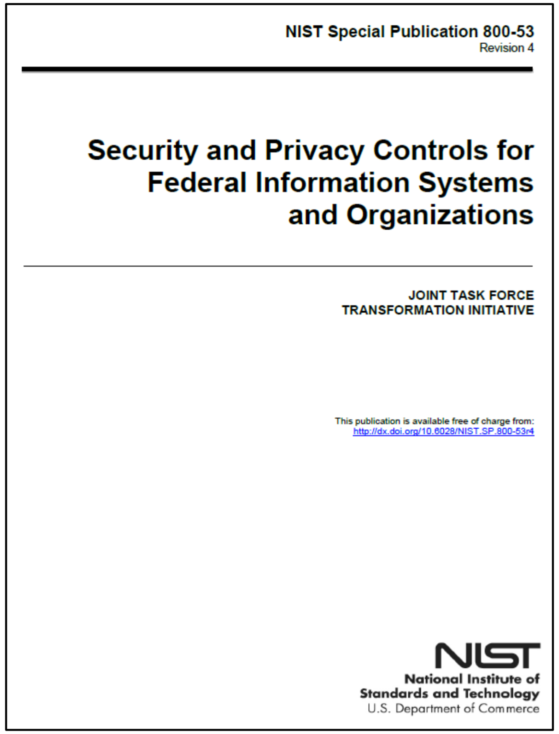
Men's FedEx Gray Logo Long Sl... $14.95 Buy It Now

Google | google.com/datacenters

What could a hacker do, once in a server room?

Physical access to an unlocked, running system usually means “game over!”

Control inventory baselines



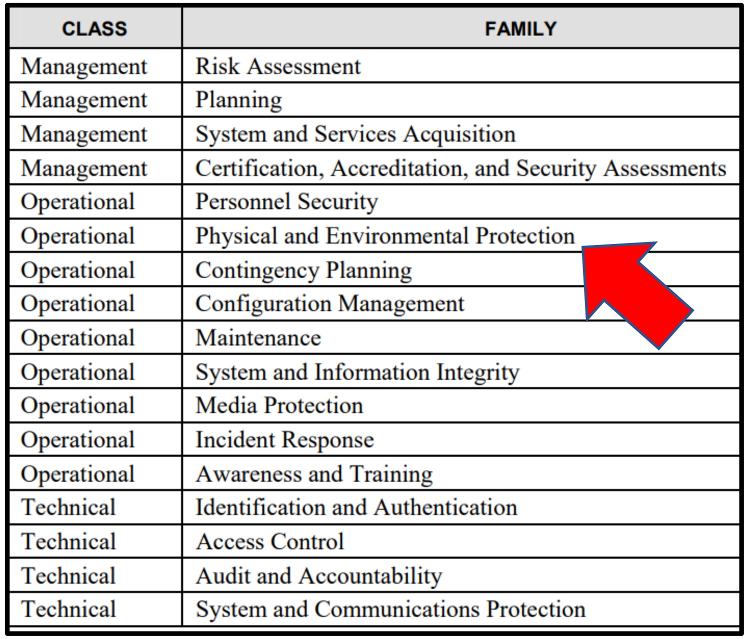
NIST Special Publication 800-53
Revision 4

Security and Privacy Controls for Federal Information Systems and Organizations

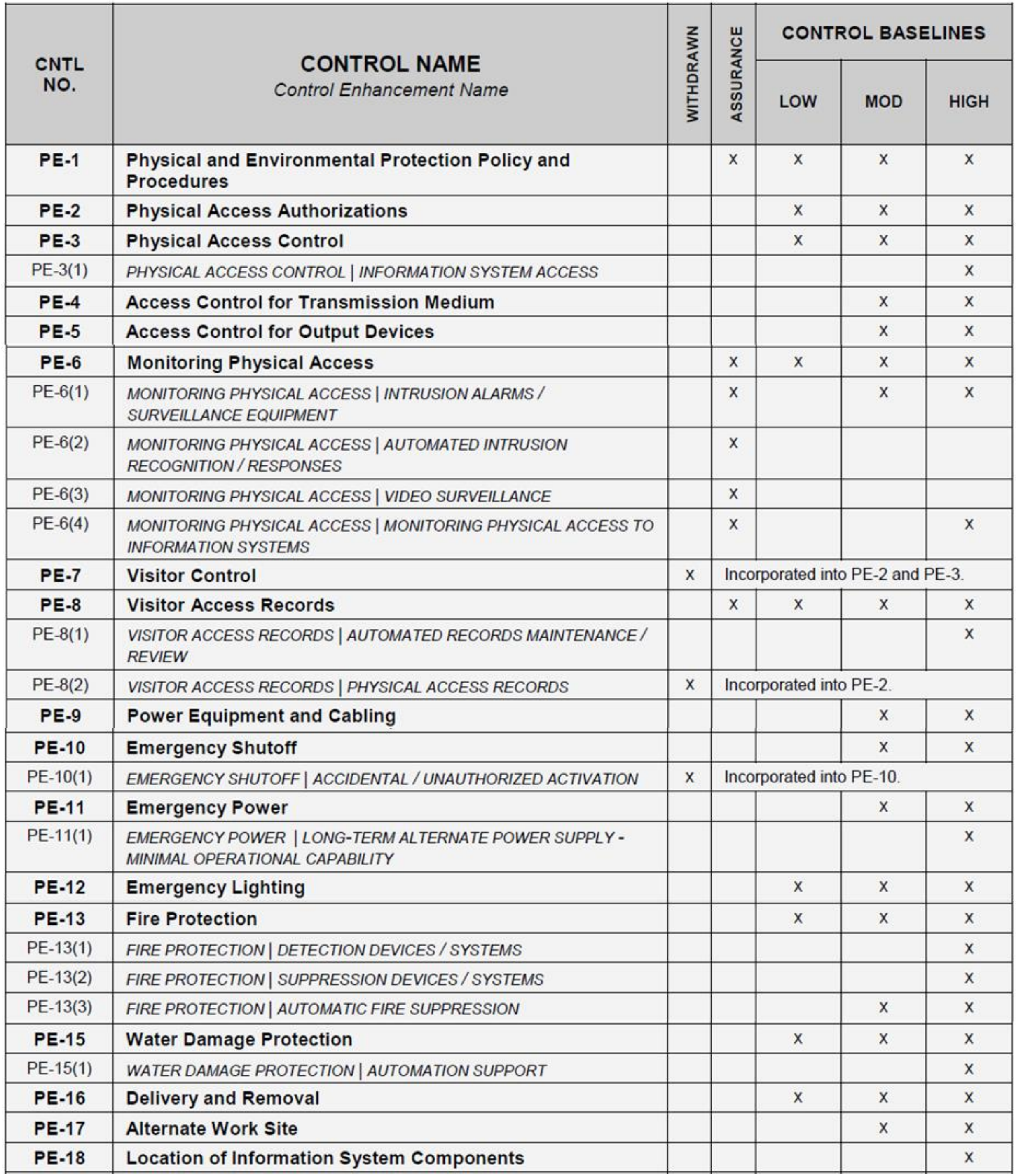
JOINT TASK FORCE
TRANSFORMATION INITIATIVE

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-53r4

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

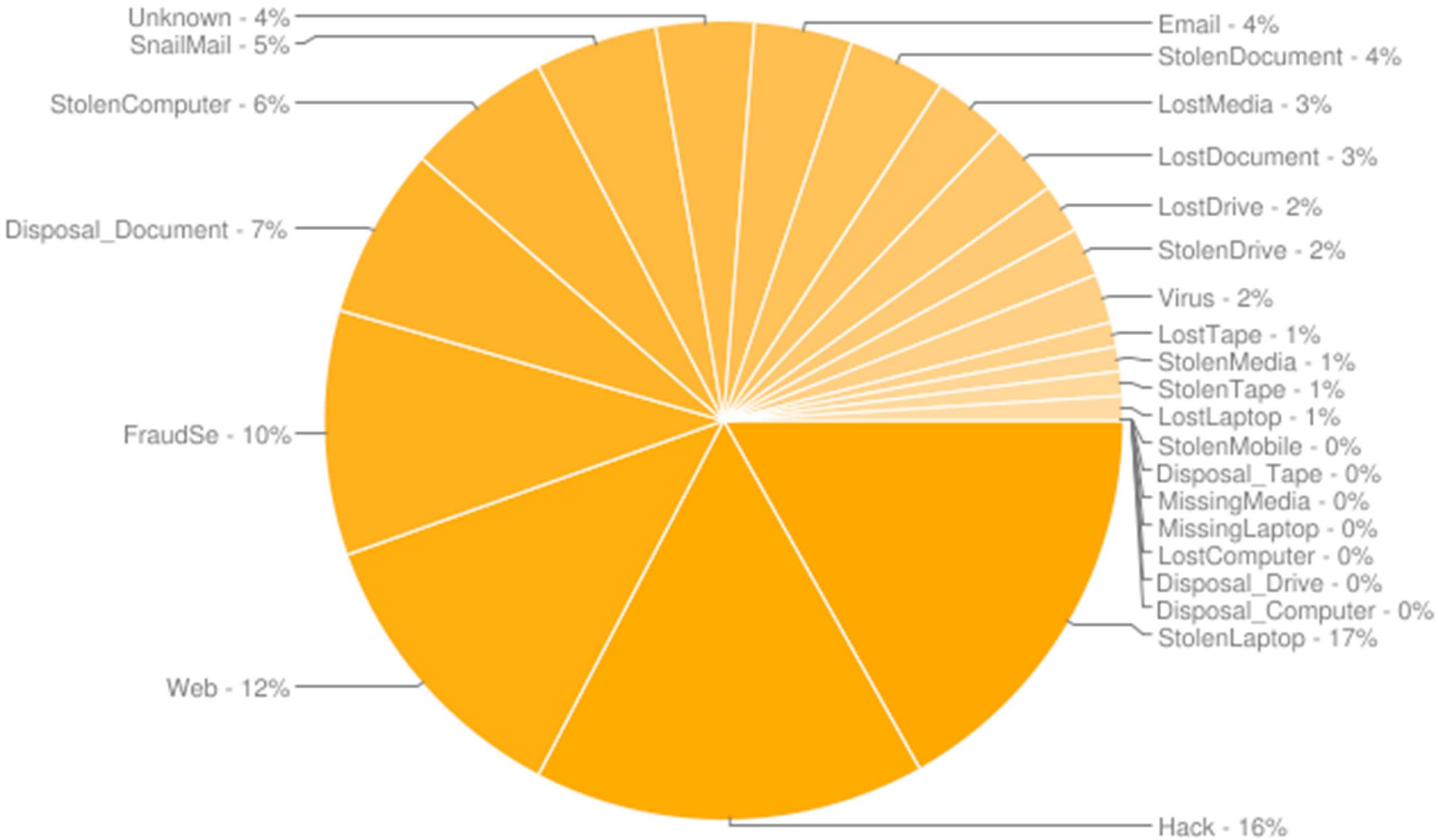


CLASS	FAMILY
Management	Risk Assessment
Management	Planning
Management	System and Services Acquisition
Management	Certification, Accreditation, and Security Assessments
Operational	Personnel Security
Operational	Physical and Environmental Protection
Operational	Contingency Planning
Operational	Configuration Management
Operational	Maintenance
Operational	System and Information Integrity
Operational	Media Protection
Operational	Incident Response
Operational	Awareness and Training
Technical	Identification and Authentication
Technical	Access Control
Technical	Audit and Accountability
Technical	System and Communications Protection

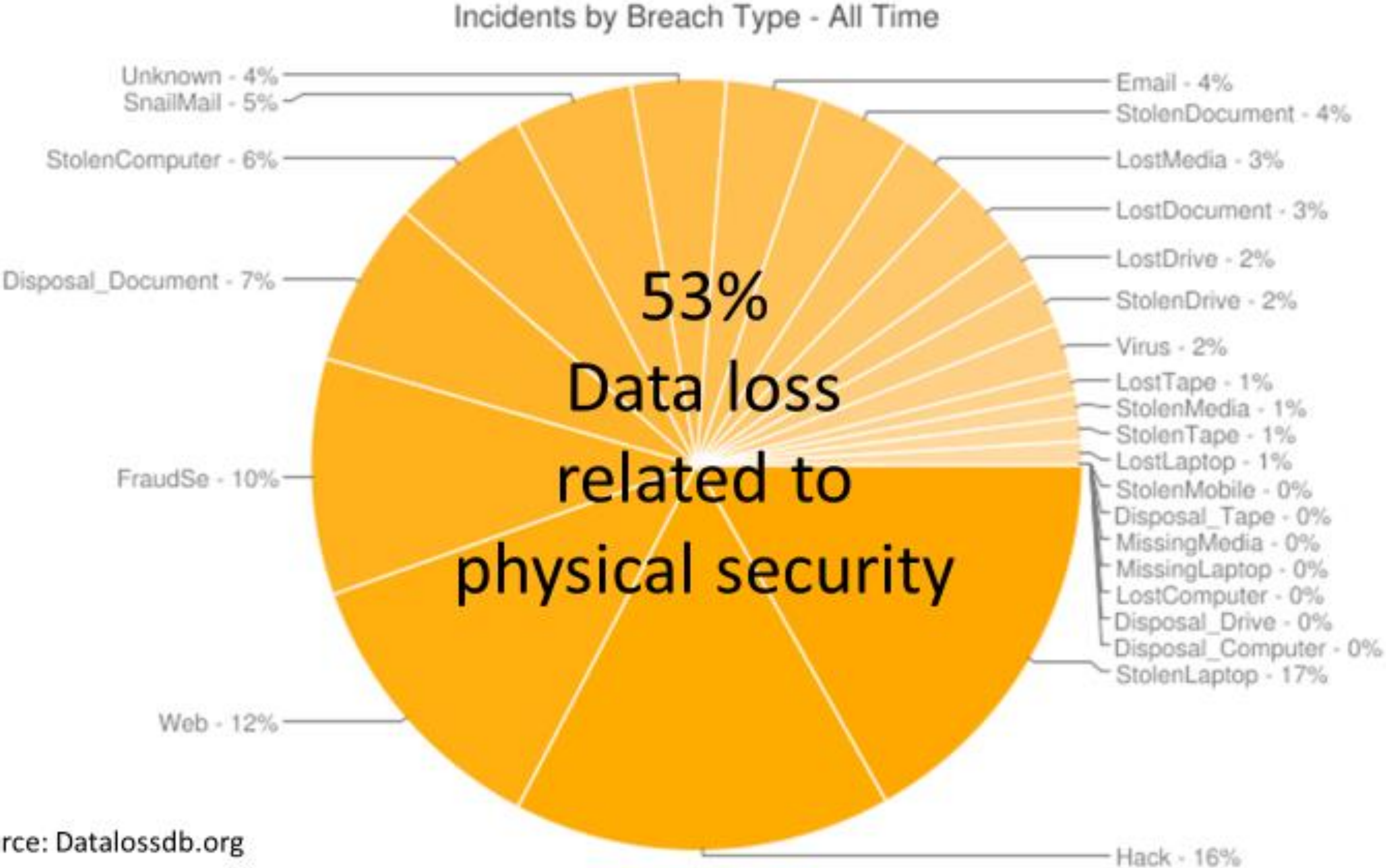


CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
PE-1	**Physical and Environmental Protection Policy and Procedures**		X	X	X	X
PE-2	**Physical Access Authorizations**			X	X	X
PE-3	**Physical Access Control**			X	X	X
PE-3(1)	*PHYSICAL ACCESS CONTROL | INFORMATION SYSTEM ACCESS*					X
PE-4	**Access Control for Transmission Medium**				X	X
PE-5	**Access Control for Output Devices**				X	X
PE-6	**Monitoring Physical Access**		X	X	X	X
PE-6(1)	*MONITORING PHYSICAL ACCESS | INTRUSION ALARMS / SURVEILLANCE EQUIPMENT*		X		X	X
PE-6(2)	*MONITORING PHYSICAL ACCESS | AUTOMATED INTRUSION RECOGNITION / RESPONSES*		X			
PE-6(3)	*MONITORING PHYSICAL ACCESS | VIDEO SURVEILLANCE*		X			
PE-6(4)	*MONITORING PHYSICAL ACCESS | MONITORING PHYSICAL ACCESS TO INFORMATION SYSTEMS*		X			X
PE-7	**Visitor Control**	X	Incorporated into PE-2 and PE-3.			
PE-8	**Visitor Access Records**		X	X	X	X
PE-8(1)	*VISITOR ACCESS RECORDS | AUTOMATED RECORDS MAINTENANCE / REVIEW*					X
PE-8(2)	*VISITOR ACCESS RECORDS | PHYSICAL ACCESS RECORDS*	X	Incorporated into PE-2.			
PE-9	**Power Equipment and Cabling**				X	X
PE-10	**Emergency Shutoff**				X	X
PE-10(1)	*EMERGENCY SHUTOFF | ACCIDENTAL / UNAUTHORIZED ACTIVATION*	X	Incorporated into PE-10.			
PE-11	**Emergency Power**				X	X
PE-11(1)	*EMERGENCY POWER | LONG-TERM ALTERNATE POWER SUPPLY - MINIMAL OPERATIONAL CAPABILITY*					X
PE-12	**Emergency Lighting**			X	X	X
PE-13	**Fire Protection**			X	X	X
PE-13(1)	*FIRE PROTECTION | DETECTION DEVICES / SYSTEMS*					X
PE-13(2)	*FIRE PROTECTION | SUPPRESSION DEVICES / SYSTEMS*					X
PE-13(3)	*FIRE PROTECTION | AUTOMATIC FIRE SUPPRESSION*				X	X
PE-15	**Water Damage Protection**			X	X	X
PE-15(1)	*WATER DAMAGE PROTECTION | AUTOMATION SUPPORT*					X
PE-16	**Delivery and Removal**			X	X	X
PE-17	**Alternate Work Site**				X	X
PE-18	**Location of Information System Components**					X

Incidents by Breach Type - All Time



Media theft

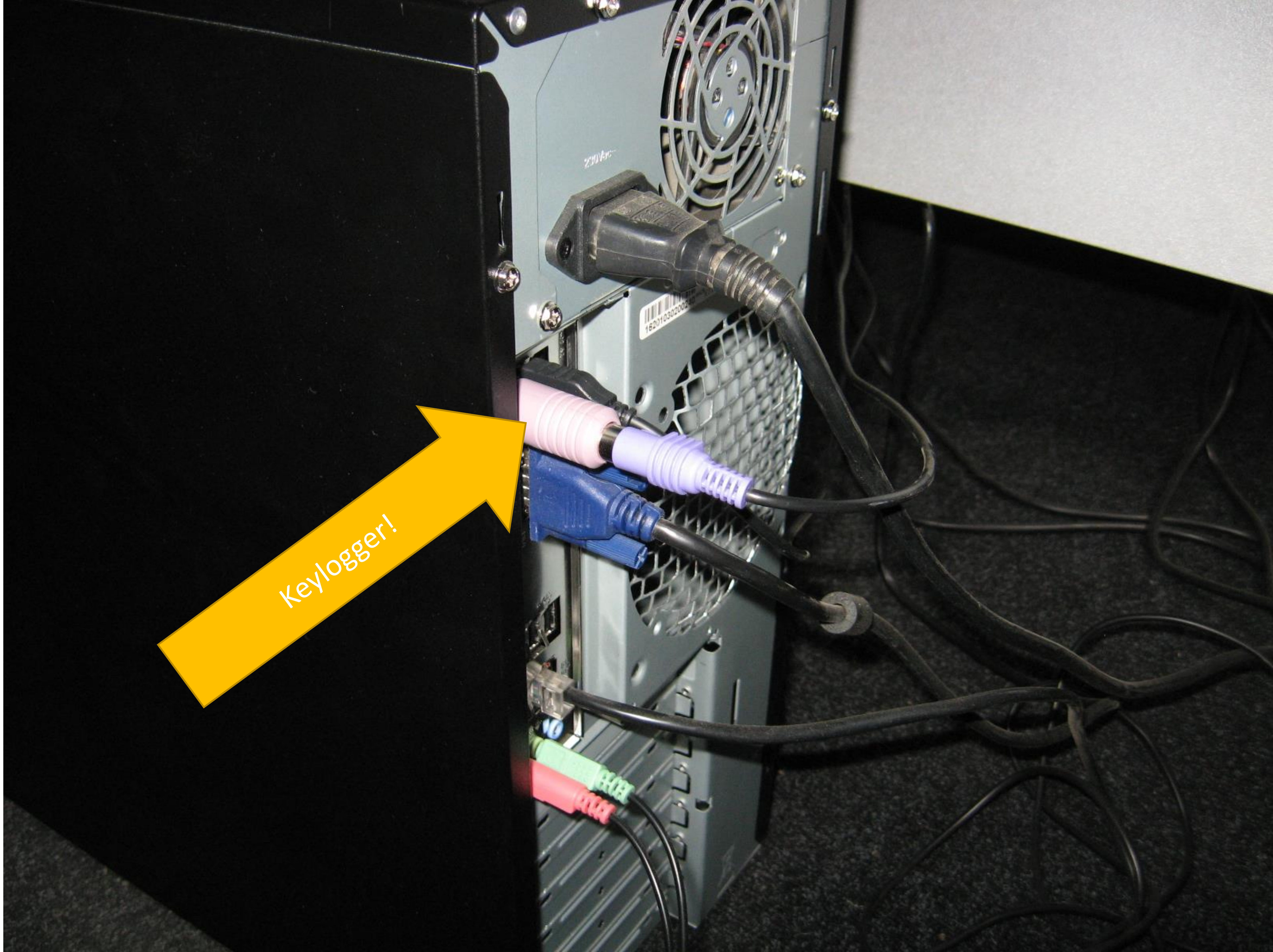


53%
Data loss
related to
physical security

Source: Datalossdb.org

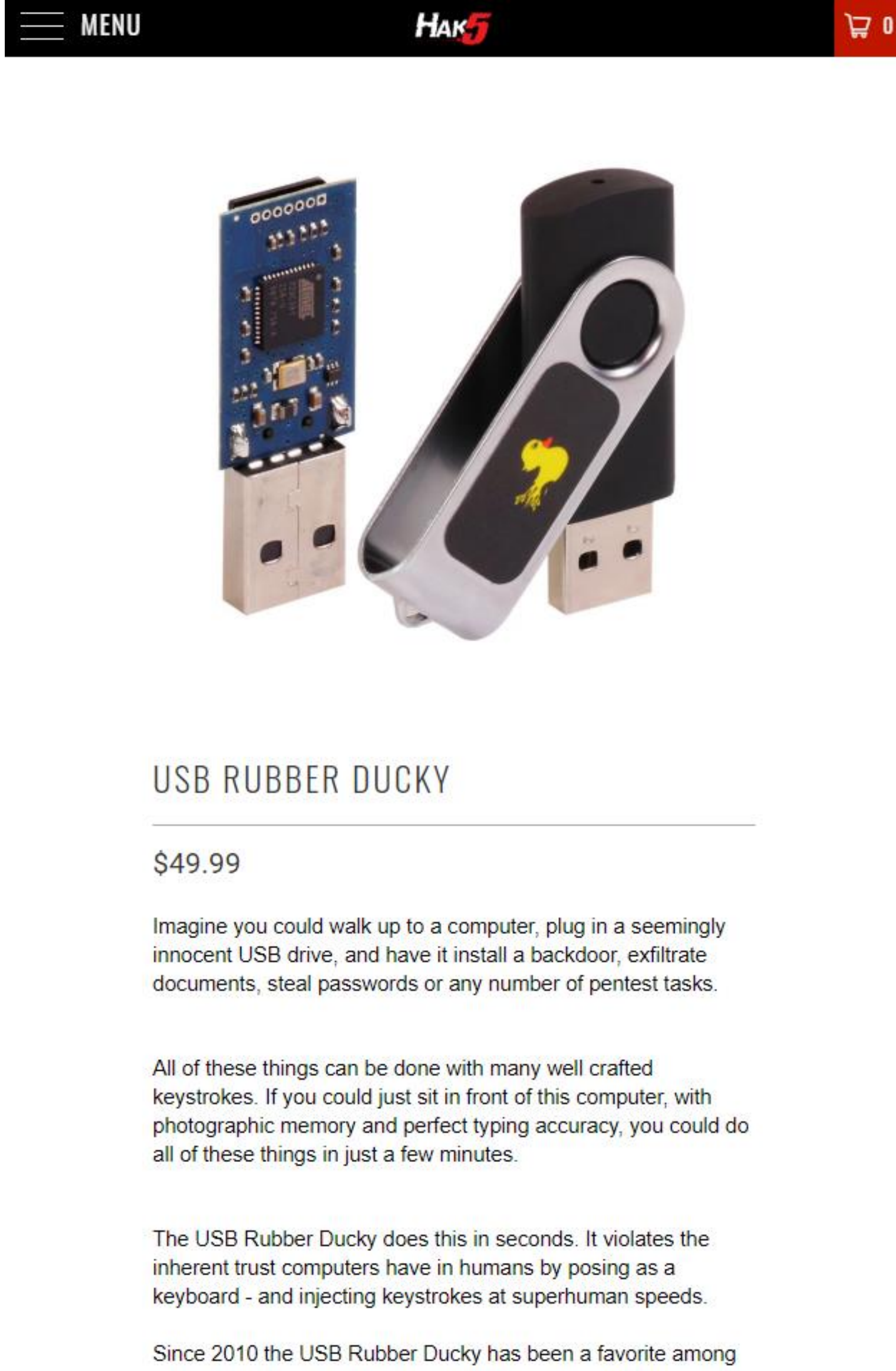
Key loggers

What's wrong in this photo?



Keyloggers violate federal wiretapping laws

Key loggers



USB RUBBER DUCKY

$49.99

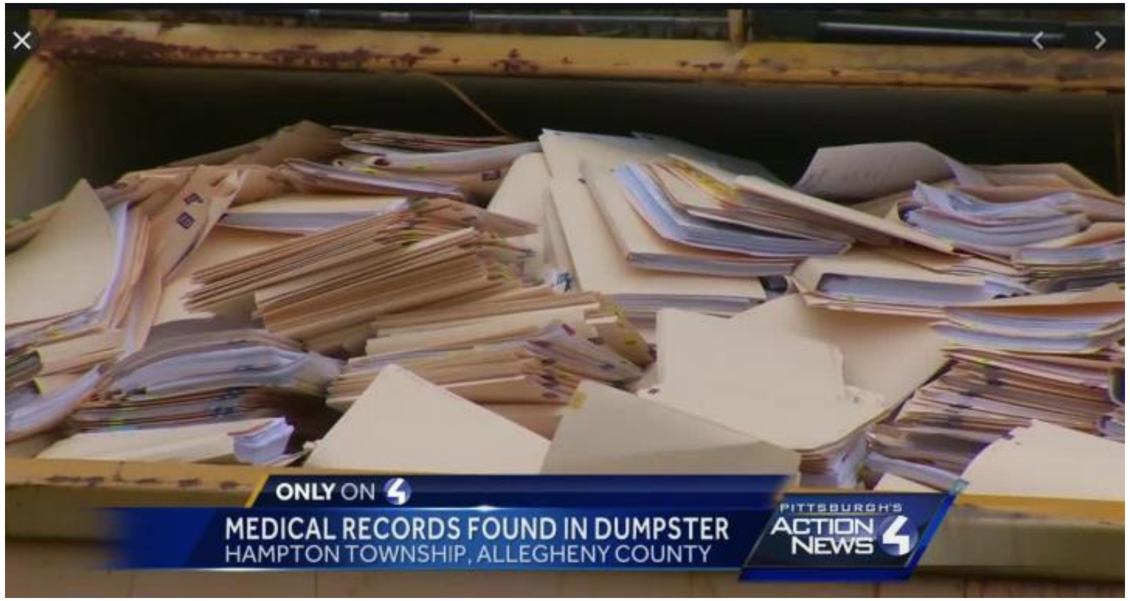
Imagine you could walk up to a computer, plug in a seemingly innocent USB drive, and have it install a backdoor, exfiltrate documents, steal passwords or any number of pentest tasks.

All of these things can be done with many well crafted keystrokes. If you could just sit in front of this computer, with photographic memory and perfect typing accuracy, you could do all of these things in just a few minutes.

The USB Rubber Ducky does this in seconds. It violates the inherent trust computers have in humans by posing as a keyboard - and injecting keystrokes at superhuman speeds.

Since 2010 the USB Rubber Ducky has been a favorite among

“Dumpster diving”


ONLY ON 4
MEDICAL RECORDS FOUND IN DUMPSTER
HAMPTON TOWNSHIP, ALLEGHENY COUNTY
PITTSBURGH'S ACTION NEWS 4

PAPER

The Philadelphia Inquirer

Walgreens tells Philly customers their prescription info may have been stolen during May looting

by Christian Hetrick, Posted: July 28, 2020

Physical Security Control Types

Physical Controls

Perimeter security, fences, lighting, facility construction, keys and locks, access card and readers, …

Administrative Controls

Facility selection, facility construction and management, personnel identity badges and controls, evacuation procedures, system shutdown procedures, fire suppression procedures, hardware failure procedures, bomb threat and lock down procedures,…

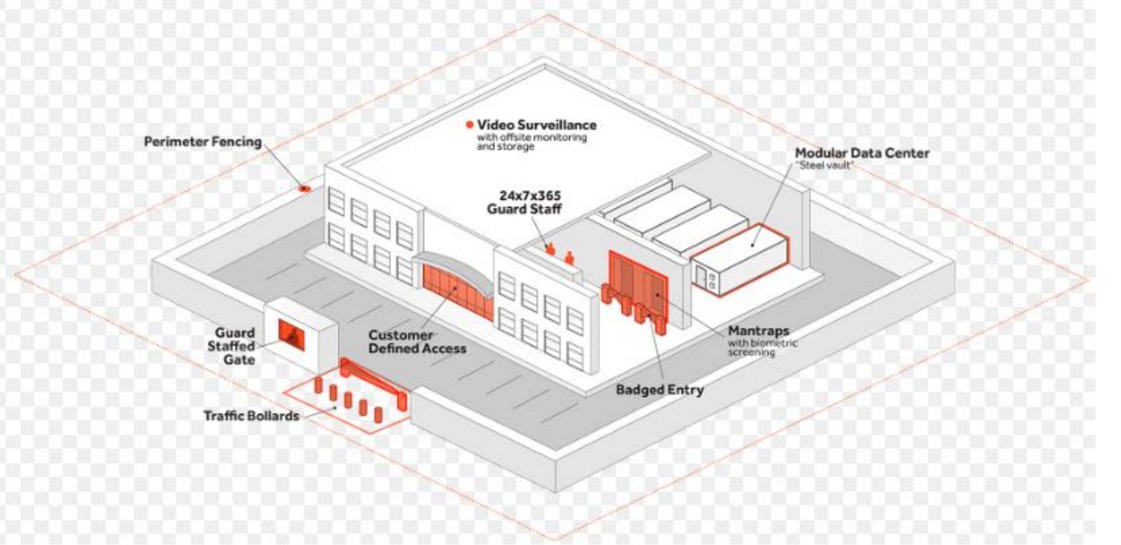
Technical Controls

Physical access control and monitoring system, intrusion detection and alarm system, fire detection and suppression system, uninterrupted power supply, heating / ventilation / air conditioning system (HVAC), disk mirroring, data backup,…

Perimeter Security

Perimeter security controls are used to prevent, detect and respond to unauthorized access to a facility

Perimeter Control



Fencing – different heights serve different purposes:

- 3 – 4 feet – deter casual trespassers
- 6 – 7 feet – deter general intruders
- 8 feet with barbed wire slanted at a 45º angle – deter more determined intruders

PIDAS – Perimeter Intrusion and Detection Assessment System

- Fencing system with mesh wire and passive cable vibration sensors
- Detects intruder approaching and damaging the fence (may generate many false alarms)

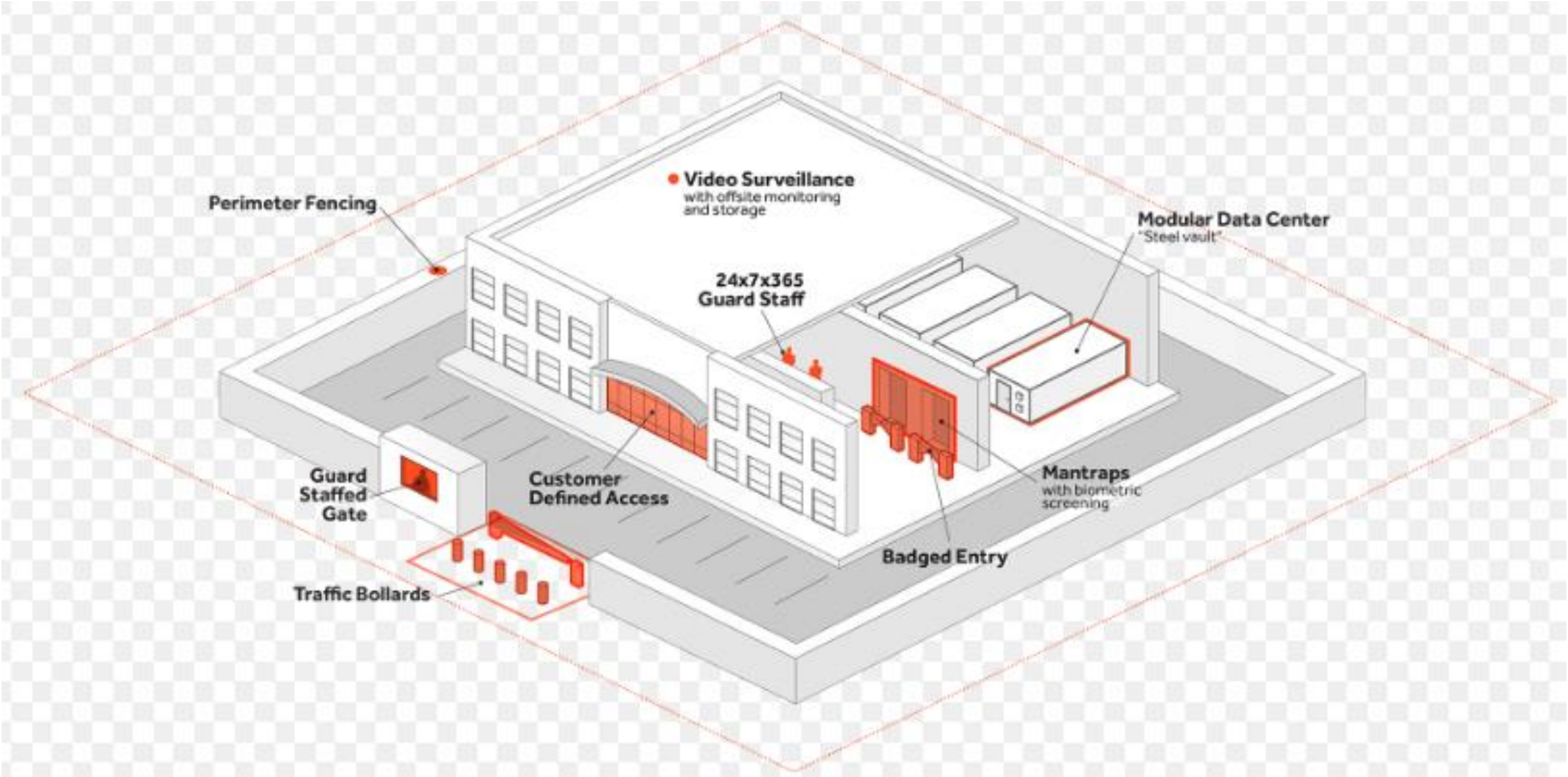
Bollards – Small round concrete pillars placed around a building

- Protects from damage by someone running a vehicle into the side of the building or getting too close for car-bomb

Lighting – Streetlights, floodlights or searchlights

- Good deterrents for unauthorized access and personnel safety
- National Institute of Standards and Technology (NIST) standard requires critical areas to be illuminated 8 feet in height with 2-foot candle power

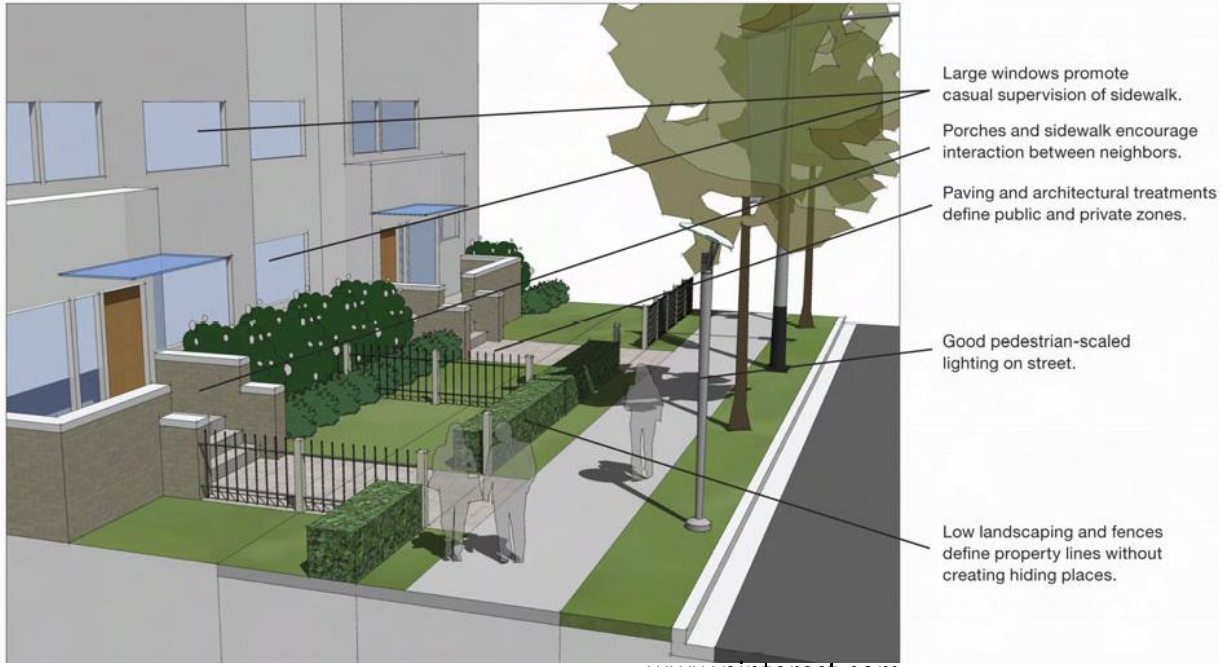
Perimeter Control example…



Perimeter Security - *physical control for facilities*

Natural access control to limit opportunities for crime

- Uses security zones to restrict movement and differentiate between areas
- Requiring different levels of protection
  - Public areas
  - Semi-private area
  - Private areas
- Limiting points of entry into a building, using structures (e.g. sidewalks & lights) to guide visitors to main entrances and reception areas


Large windows promote casual supervision of sidewalk.
Porches and sidewalk encourage interaction between neighbors.
Paving and architectural treatments define public and private zones.
Good pedestrian-scaled lighting on street.
Low landscaping and fences define property lines without creating hiding places.

www.pinterest.com

Target Hardening

Complements natural access controls by using mechanical and/or operational controls:

- alarms, guards and receptionists
- visitor sign-in/sign-out procedures
- picture identification requirements,…

Restricted and work area security often

receive additional physical security controls beyond:

- ***Key card access control systems***
- ***Video surveillance***

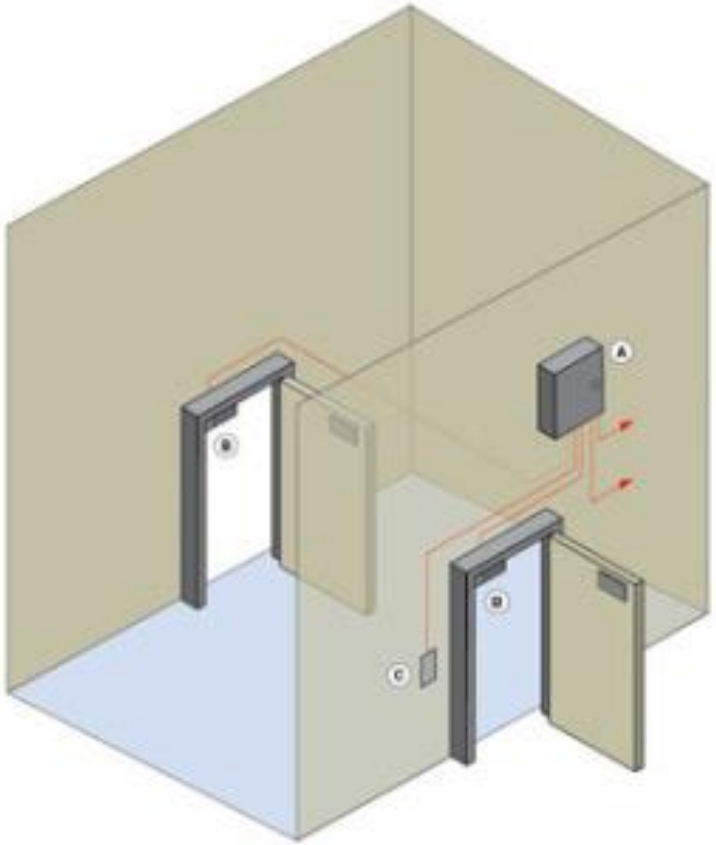
<u>Physical security controls</u> for secure locations may also include:

- **Multi-factor key card entry**
  - Bi-factor (or tri-factor): Key cards + PIN pad or biometric
- **Security guards (and guard dogs)**
  - At ingress/egress points to prevent unauthorized access, roaming facility alert for unauthorized personnel or activities, involved in capture of unauthorized personnel in a facility
- ***Security wall and fences***
  - 1 or more to keep authorized personnel away from facilities
- ***Security cameras and lighting***
  - Additional lighting to expose and deter would-be intruders
- ***Security gates, crash gates, and bollards***
  - Limit the movement of vehicles near a facility to reduce vehicle-borne threats

<u>Physical security controls </u>for secure locations may also include:

Mantrap

- Made of two doors, one for entry, one for exit from the booth/ mantrap
  - When the first door is open, the second remains locked until the first one is closed and the individual inside the booth is cleared by a security operator monitoring this interlocking system



DexID

Media protection

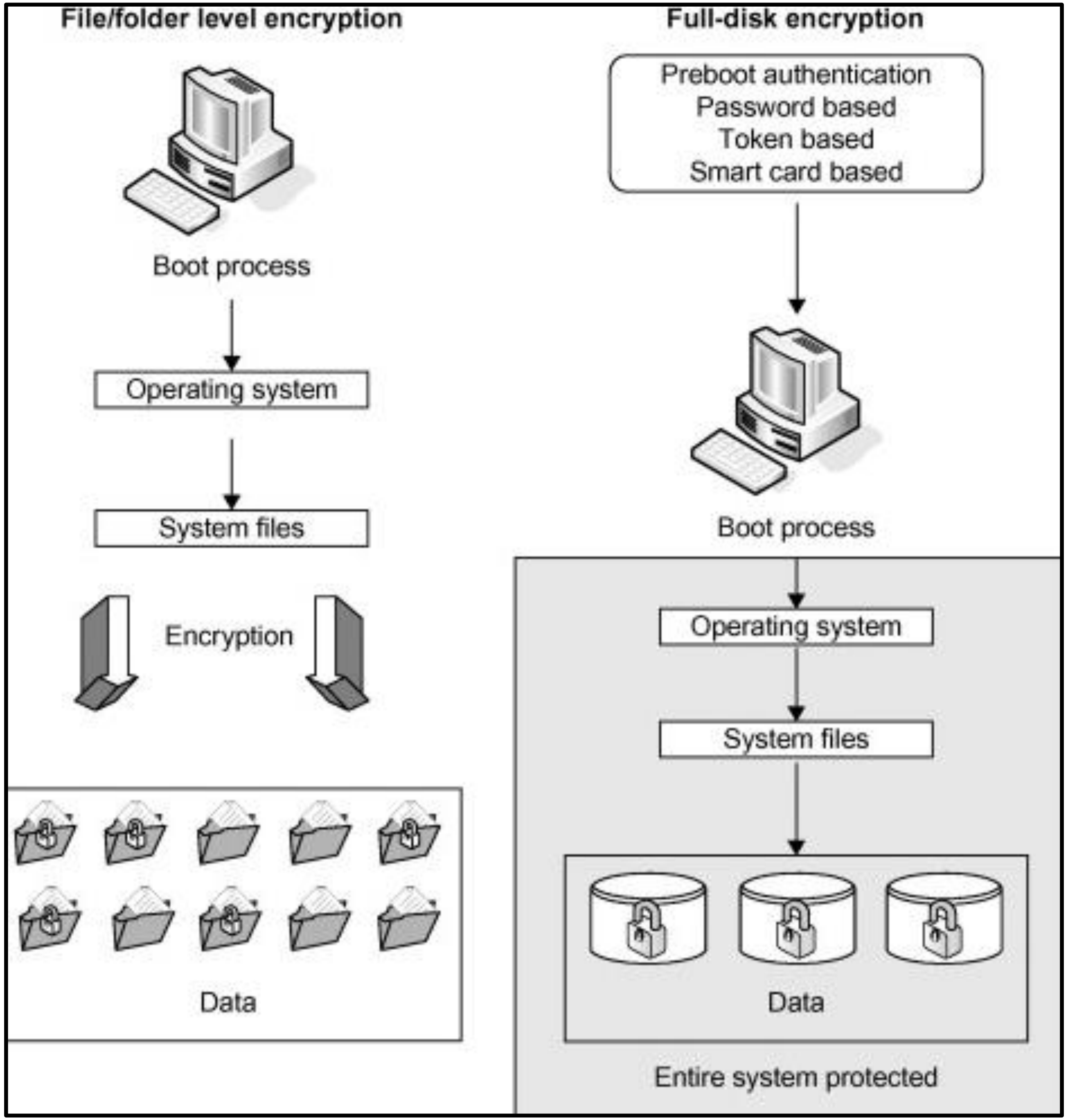
Bitlocker

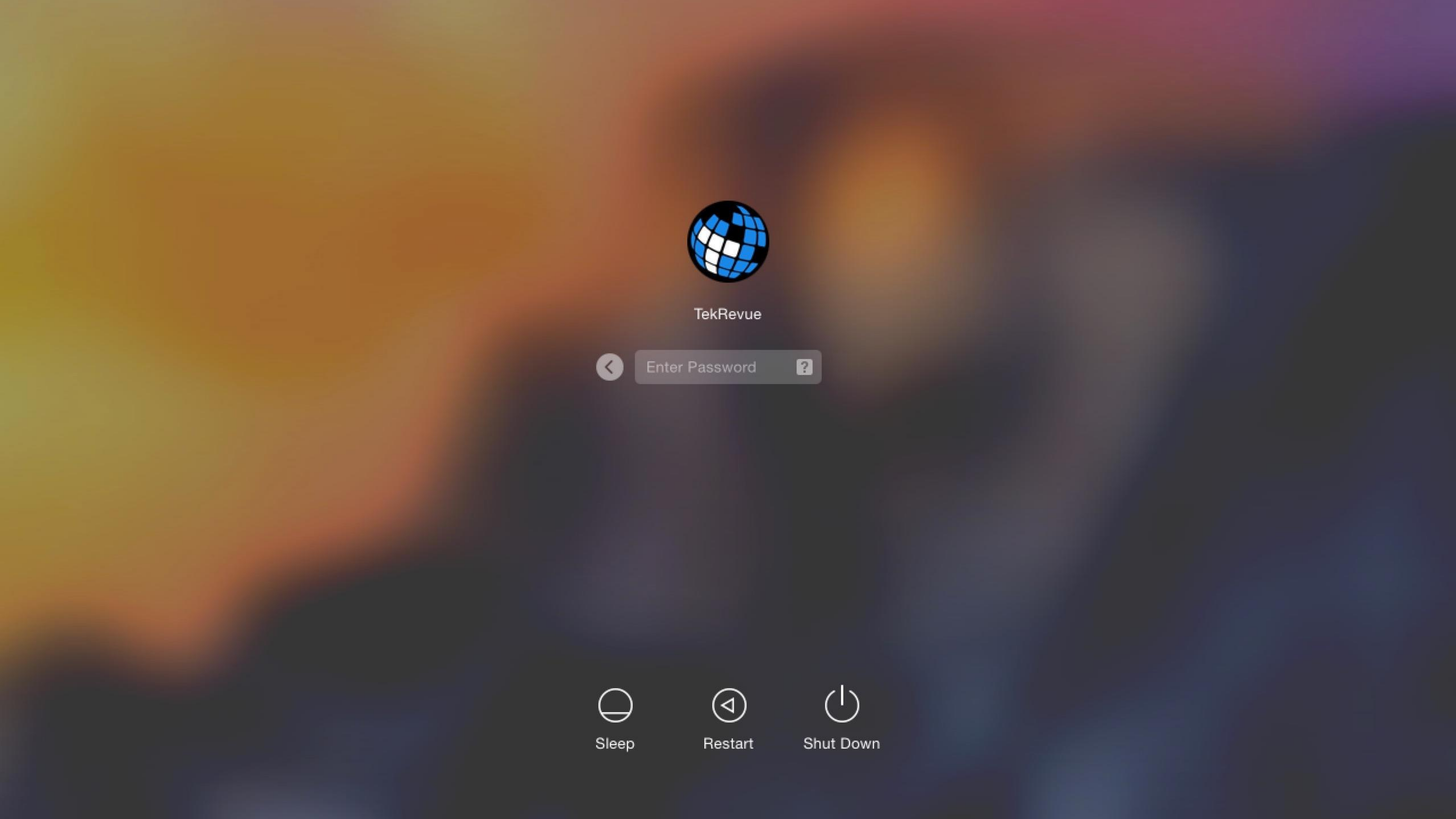
FileVault

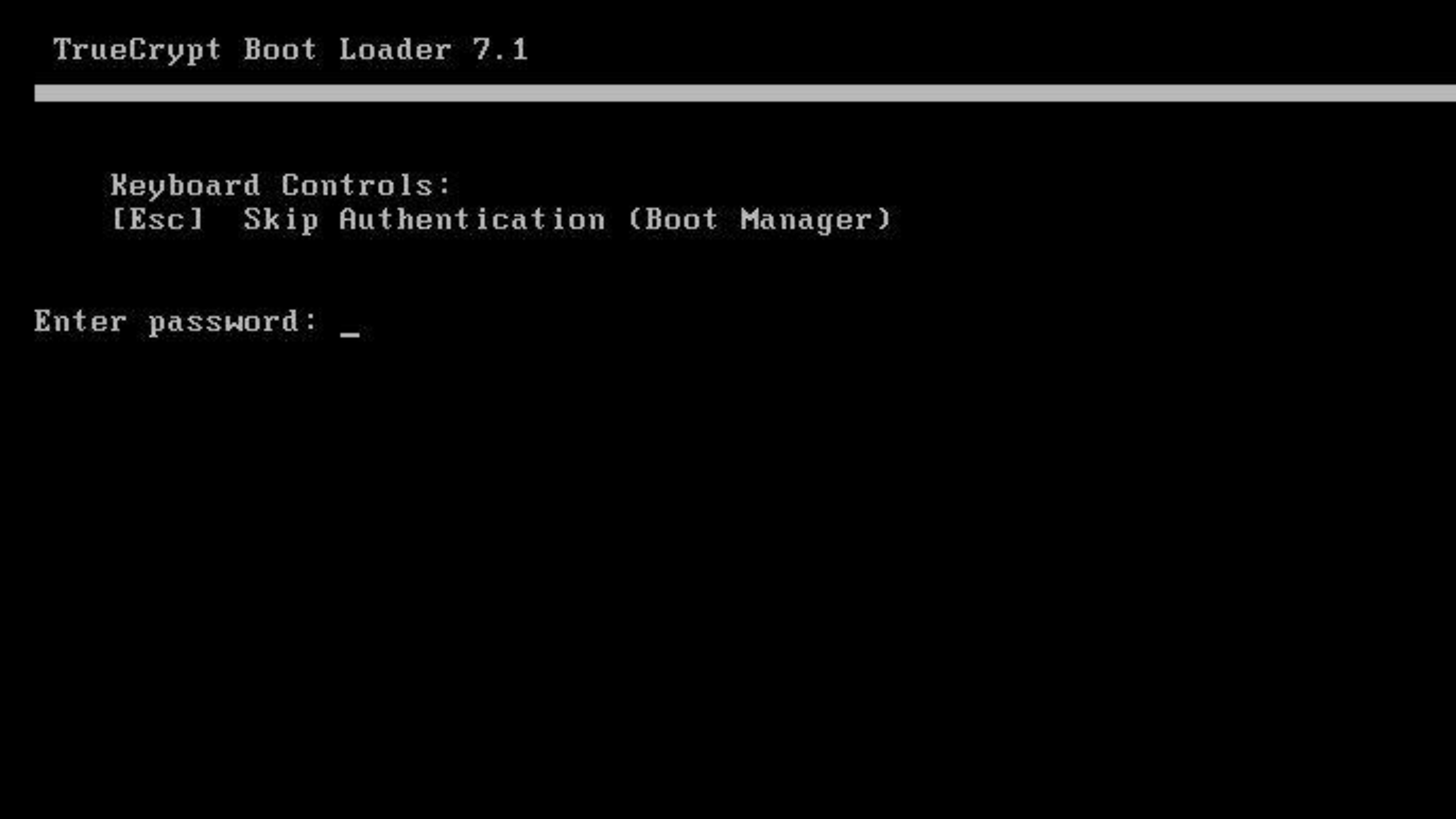
LUKS

Full disk encryption

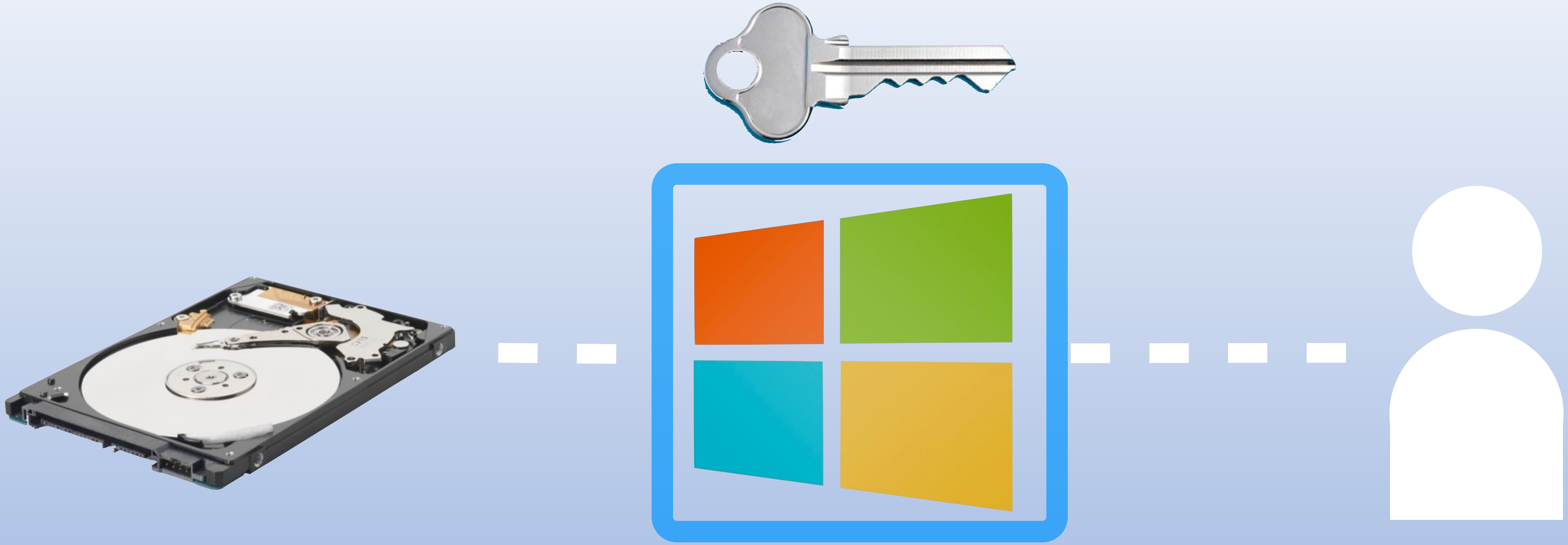
Uses disk encryption software or hardware to encrypt all data that goes on a disk or disk volume

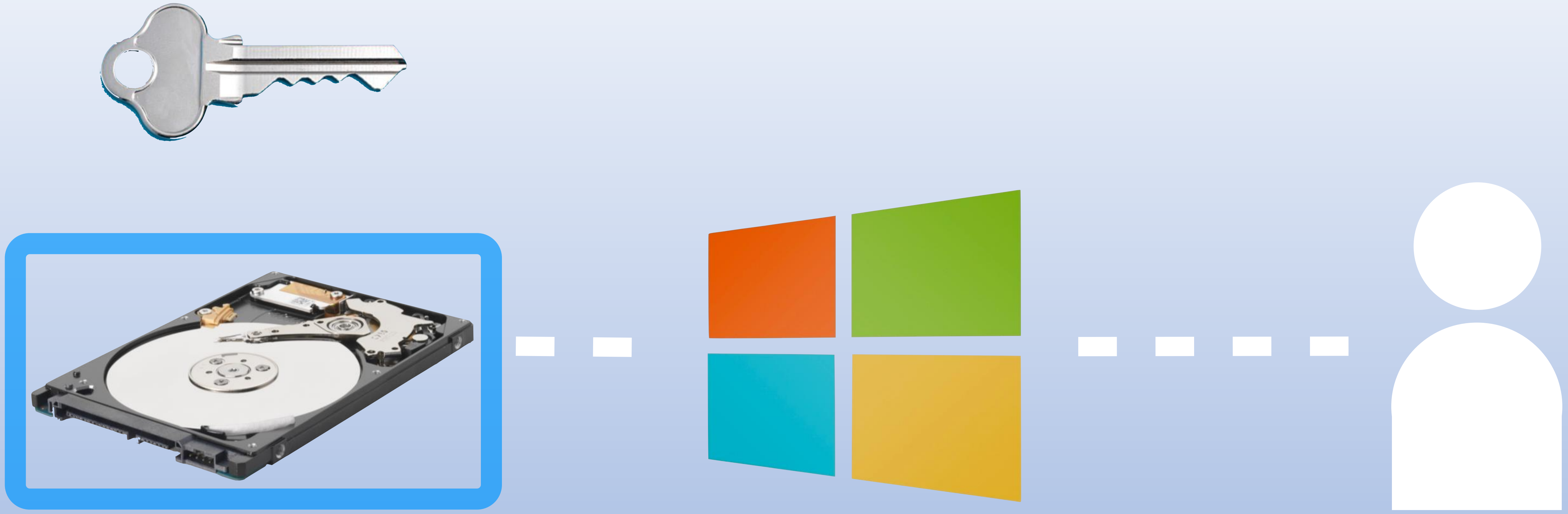



TekRevue
Enter Password
?
Sleep
Restart
Shut Down

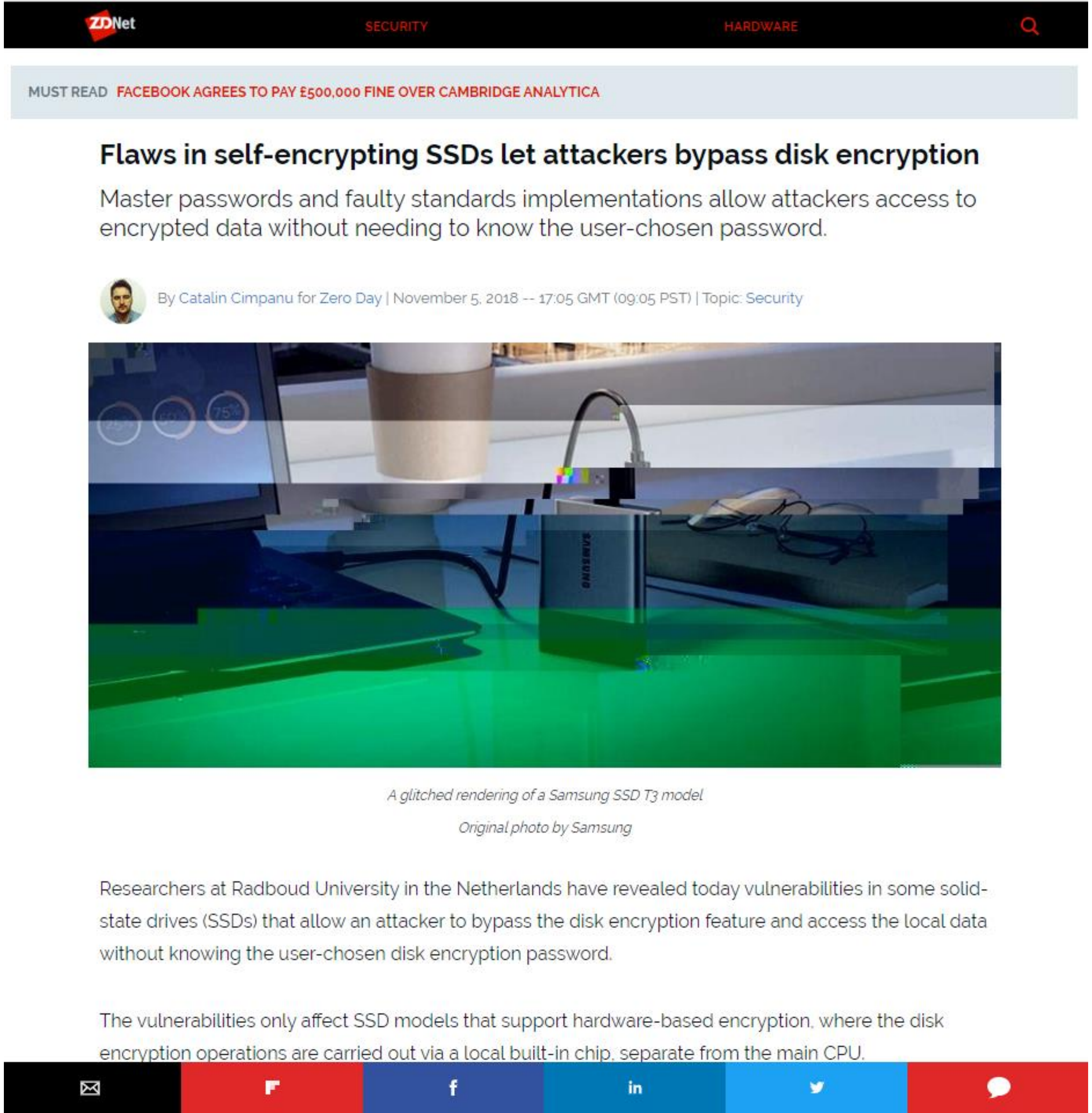


```
 TrueCrypt Boot Loader 7.1


    Keyboard Controls:
    [Esc]  Skip Authentication (Boot Manager)


Enter password: _
```





Some disks have built-in encryption



Flaws in self-encrypting SSDs let attackers bypass disk encryption

Master passwords and faulty standards implementations allow attackers access to encrypted data without needing to know the user-chosen password.

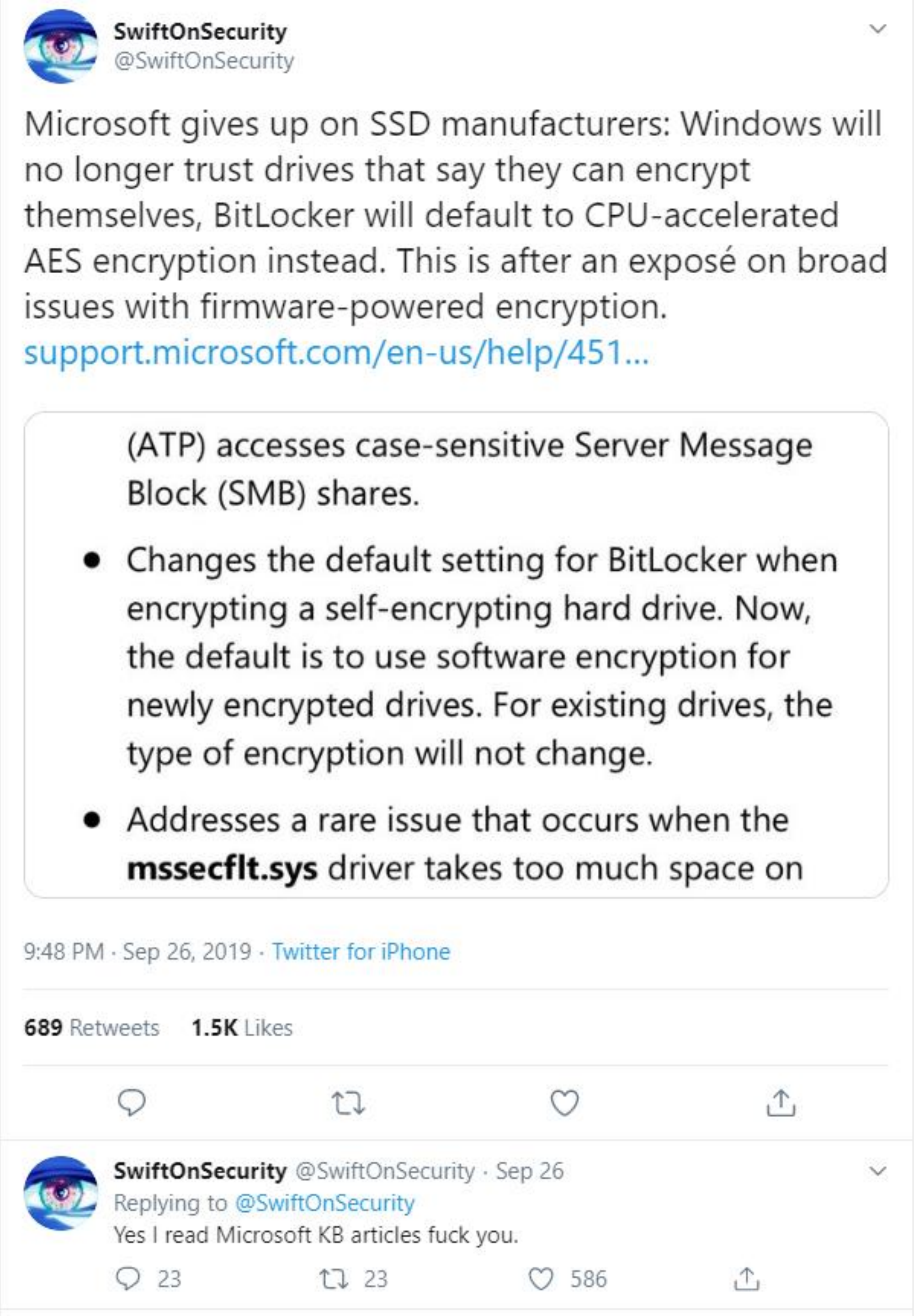
By Catalin Cimpanu for Zero Day | November 5, 2018 -- 17:05 GMT (09:05 PST) | Topic: Security

A glitched rendering of a Samsung SSD T3 model

Original photo by Samsung

Researchers at Radboud University in the Netherlands have revealed today vulnerabilities in some solid-state drives (SSDs) that allow an attacker to bypass the disk encryption feature and access the local data without knowing the user-chosen disk encryption password.

The vulnerabilities only affect SSD models that support hardware-based encryption, where the disk encryption operations are carried out via a local built-in chip, separate from the main CPU.



SwiftOnSecurity
@SwiftOnSecurity

Microsoft gives up on SSD manufacturers: Windows will no longer trust drives that say they can encrypt themselves, BitLocker will default to CPU-accelerated AES encryption instead. This is after an exposé on broad issues with firmware-powered encryption. support.microsoft.com/en-us/help/451...

(ATP) accesses case-sensitive Server Message Block (SMB) shares.

- Changes the default setting for BitLocker when encrypting a self-encrypting hard drive. Now, the default is to use software encryption for newly encrypted drives. For existing drives, the type of encryption will not change.
- Addresses a rare issue that occurs when the **mssecflt.sys** driver takes too much space on

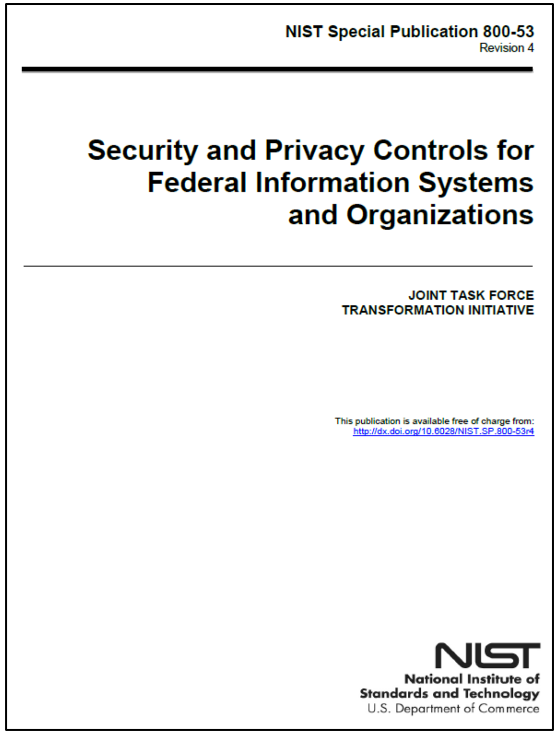
9:48 PM · Sep 26, 2019 · Twitter for iPhone

689 Retweets **1.5K** Likes

SwiftOnSecurity @SwiftOnSecurity · Sep 26
Replying to @SwiftOnSecurity
Yes I read Microsoft KB articles fuck you.

ENERPAC

Control inventory baselines



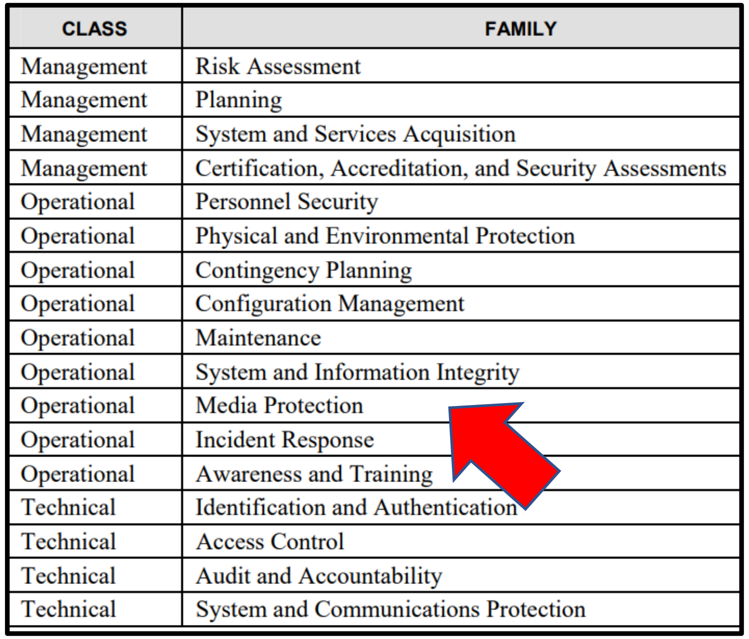
NIST Special Publication 800-53
Revision 4

Security and Privacy Controls for Federal Information Systems and Organizations

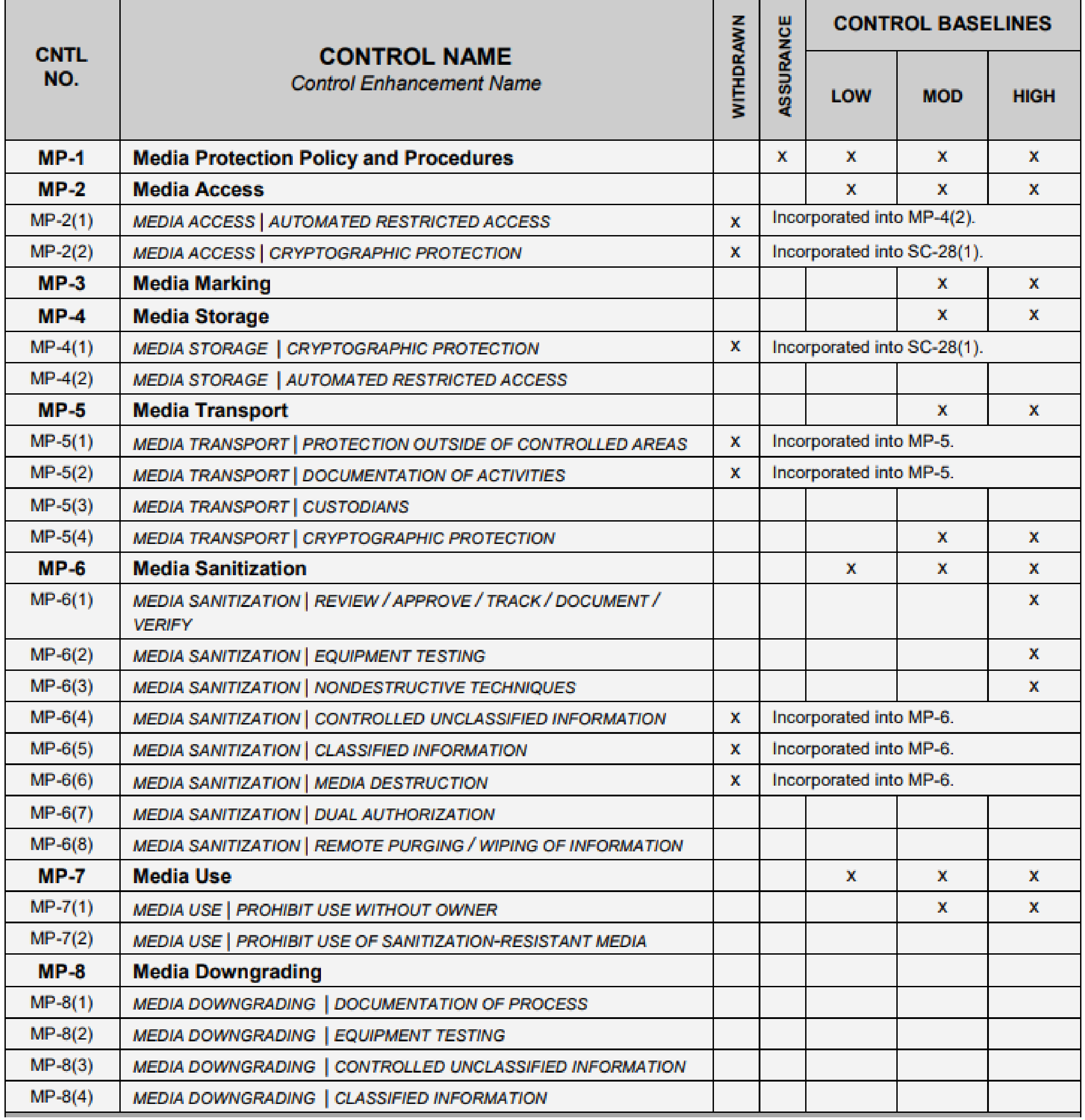
JOINT TASK FORCE
TRANSFORMATION INITIATIVE

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-53r4

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

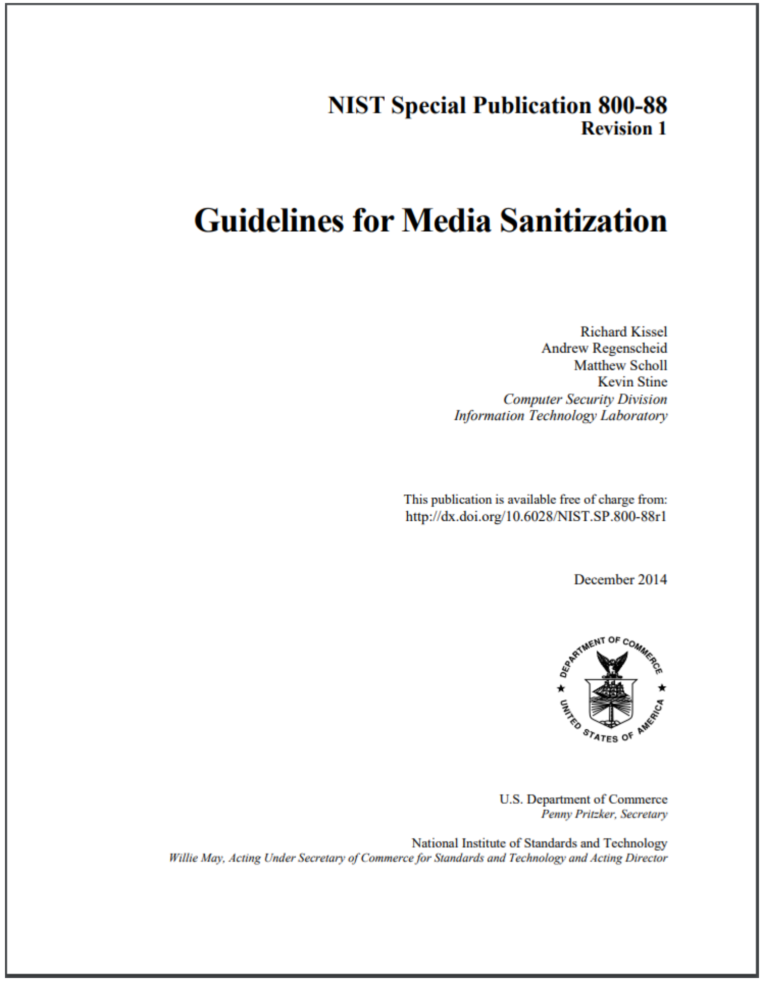


CLASS	FAMILY
Management	Risk Assessment
Management	Planning
Management	System and Services Acquisition
Management	Certification, Accreditation, and Security Assessments
Operational	Personnel Security
Operational	Physical and Environmental Protection
Operational	Contingency Planning
Operational	Configuration Management
Operational	Maintenance
Operational	System and Information Integrity
Operational	Media Protection
Operational	Incident Response
Operational	Awareness and Training
Technical	Identification and Authentication
Technical	Access Control
Technical	Audit and Accountability
Technical	System and Communications Protection



CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
MP-1	**Media Protection Policy and Procedures**		x	x	x	x
MP-2	**Media Access**			x	x	x
MP-2(1)	*MEDIA ACCESS | AUTOMATED RESTRICTED ACCESS*	x	Incorporated into MP-4(2).			
MP-2(2)	*MEDIA ACCESS | CRYPTOGRAPHIC PROTECTION*	x	Incorporated into SC-28(1).			
MP-3	**Media Marking**				x	x
MP-4	**Media Storage**				x	x
MP-4(1)	*MEDIA STORAGE | CRYPTOGRAPHIC PROTECTION*	x	Incorporated into SC-28(1).			
MP-4(2)	*MEDIA STORAGE | AUTOMATED RESTRICTED ACCESS*					
MP-5	**Media Transport**				x	x
MP-5(1)	*MEDIA TRANSPORT | PROTECTION OUTSIDE OF CONTROLLED AREAS*	x	Incorporated into MP-5.			
MP-5(2)	*MEDIA TRANSPORT | DOCUMENTATION OF ACTIVITIES*	x	Incorporated into MP-5.			
MP-5(3)	*MEDIA TRANSPORT | CUSTODIANS*					
MP-5(4)	*MEDIA TRANSPORT | CRYPTOGRAPHIC PROTECTION*				x	x
MP-6	**Media Sanitization**			x	x	x
MP-6(1)	*MEDIA SANITIZATION | REVIEW / APPROVE / TRACK / DOCUMENT / VERIFY*					x
MP-6(2)	*MEDIA SANITIZATION | EQUIPMENT TESTING*					x
MP-6(3)	*MEDIA SANITIZATION | NONDESTRUCTIVE TECHNIQUES*					x
MP-6(4)	*MEDIA SANITIZATION | CONTROLLED UNCLASSIFIED INFORMATION*	x	Incorporated into MP-6.			
MP-6(5)	*MEDIA SANITIZATION | CLASSIFIED INFORMATION*	x	Incorporated into MP-6.			
MP-6(6)	*MEDIA SANITIZATION | MEDIA DESTRUCTION*	x	Incorporated into MP-6.			
MP-6(7)	*MEDIA SANITIZATION | DUAL AUTHORIZATION*					
MP-6(8)	*MEDIA SANITIZATION | REMOTE PURGING / WIPING OF INFORMATION*					
MP-7	**Media Use**			x	x	x
MP-7(1)	*MEDIA USE | PROHIBIT USE WITHOUT OWNER*				x	x
MP-7(2)	*MEDIA USE | PROHIBIT USE OF SANITIZATION-RESISTANT MEDIA*					
MP-8	**Media Downgrading**					
MP-8(1)	*MEDIA DOWNGRADING | DOCUMENTATION OF PROCESS*					
MP-8(2)	*MEDIA DOWNGRADING | EQUIPMENT TESTING*					
MP-8(3)	*MEDIA DOWNGRADING | CONTROLLED UNCLASSIFIED INFORMATION*					
MP-8(4)	*MEDIA DOWNGRADING | CLASSIFIED INFORMATION*					

Media sanitization



NIST Special Publication 800-88
Revision 1

Guidelines for Media Sanitization

Richard Kissel
Andrew Regenscheid
Matthew Scholl
Kevin Stine
Computer Security Division
Information Technology Laboratory

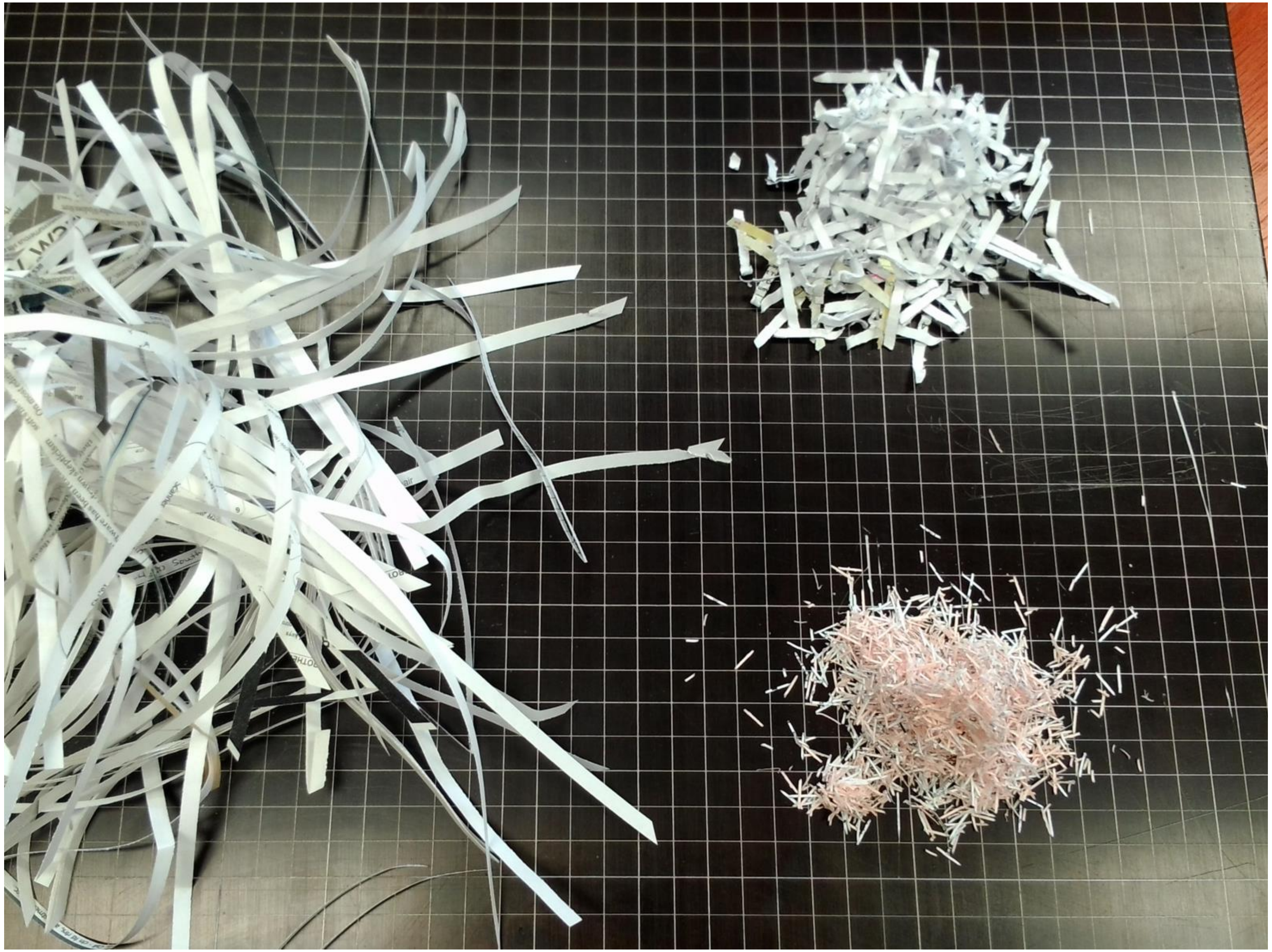
This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-88r1

December 2014

DEPARTMENT OF COMMERCE
UNITED STATES OF AMERICA

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Acting Under Secretary of Commerce for Standards and Technology and Acting Director



Paper shredders have different levels of security, above:
Levels 1, 3, 6

Agenda

✓Milestone 2 – some thought on the workflow

✓Vulnerabilities and sources of threats

✓Physical control inventory baselines

✓Perimeter security

✓Media protection

✓Media sanitization