FANSHAWE

INFO-6065

Ethical Hacking & Exploits

Lecture 04

FANSHAWE

Agenda

- Scanning Networks
- Types of Scanning
- More on Scanning Tools
- Lab 04 Overview

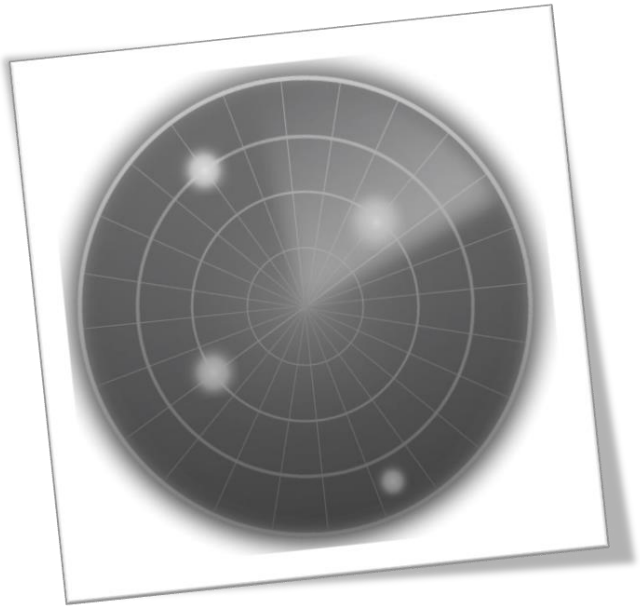
FANSHAWE

Warning

- This is course is **NOT** designed to teach you how to be a hacker
- You are **NOT** allowed to use the tools and techniques we will be covering outside of the isolated lab environment
- Use of these tools on the rest of the College's network would constitute an **Academic Offence**
- The College has full pack capture capabilities to track down illegal activity

Scanning

Scanning Networks



FANSHAWE

Types of Scanning

- Discovery Scanning
  - Identifying live hosts on the network
- Port Scanning
  - Determining what ports are open on the hosts
- Fingerprinting
  - Determining what services are running behind the ports
- Vulnerability Scanning
  - What services have vulnerabilities that can be exploited

FANSHAWE

Scanning Tools

There are many tools can scan at multiple layers of the OSI model and some work better than others at specific layers…

Tools available include:

Nmap Scapy, ARPing, NetDiscover, Metasploit, ICMP, fping, hping3, Dmitry, Netcat, Ncat, Amap xProbe2, Python sockets, Onsixtyone, SNMPwalk, Nessus, OpenVAS, MSF auxiliary modules, etc.

FANSHAWE

Scanning Tools

Different protocols run at different layers of the OSI model (some cross layers, sort of)

- We will go into why you might want to scan at one layer over another

FANSHAWE

OSI Layers

You should be familiar with the OSI model from previous courses:

- Layer 7 – Application
- Layer 6 – Presentation
- Layer 5 – Session
- Layer 4 – Transport
- Layer 3 – Network
- Layer 2 – Data Link
- Layer 1 – Physical

FANSHAWE

Layers / Protocols

Application Layer

- Layer 7

Protocols include:

- HTTP port 80
- FTP ports 20 & 21
- Telnet port 23
- SSH port 22
- DNS port 53
- DHCP ports 67 & 68

FANSHAWE

Layers / Protocols

Presentation Layer

- Layer 6
  - ASCII, PDF, PNG, XLSX, TLV, etc.

The presentation layer takes care of the syntax that controls how transferred data is displayed between connected systems (serialization)

FANSHAWE

ASCII Table

Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char
0	0	[NULL]	32	20	[SPACE]	64	40	@	96	60	`
1	1	[START OF HEADING]	33	21	!	65	41	A	97	61	a
2	2	[START OF TEXT]	34	22	"	66	42	B	98	62	b
3	3	[END OF TEXT]	35	23	#	67	43	C	99	63	c
4	4	[END OF TRANSMISSION]	36	24	$	68	44	D	100	64	d
5	5	[ENQUIRY]	37	25	%	69	45	E	101	65	e
6	6	[ACKNOWLEDGE]	38	26	&	70	46	F	102	66	f
7	7	[BELL]	39	27	'	71	47	G	103	67	g
8	8	[BACKSPACE]	40	28	(	72	48	H	104	68	h
9	9	[HORIZONTAL TAB]	41	29	)	73	49	I	105	69	i
10	A	[LINE FEED]	42	2A	*	74	4A	J	106	6A	j
11	B	[VERTICAL TAB]	43	2B	+	75	4B	K	107	6B	k
12	C	[FORM FEED]	44	2C	,	76	4C	L	108	6C	l
13	D	[CARRIAGE RETURN]	45	2D	-	77	4D	M	109	6D	m
14	E	[SHIFT OUT]	46	2E	.	78	4E	N	110	6E	n
15	F	[SHIFT IN]	47	2F	/	79	4F	O	111	6F	o
16	10	[DATA LINK ESCAPE]	48	30	0	80	50	P	112	70	p
17	11	[DEVICE CONTROL 1]	49	31	1	81	51	Q	113	71	q
18	12	[DEVICE CONTROL 2]	50	32	2	82	52	R	114	72	r
19	13	[DEVICE CONTROL 3]	51	33	3	83	53	S	115	73	s
20	14	[DEVICE CONTROL 4]	52	34	4	84	54	T	116	74	t
21	15	[NEGATIVE ACKNOWLEDGE]	53	35	5	85	55	U	117	75	u
22	16	[SYNCHRONOUS IDLE]	54	36	6	86	56	V	118	76	v
23	17	[ENG OF TRANS. BLOCK]	55	37	7	87	57	W	119	77	w
24	18	[CANCEL]	56	38	8	88	58	X	120	78	x
25	19	[END OF MEDIUM]	57	39	9	89	59	Y	121	79	y
26	1A	[SUBSTITUTE]	58	3A	:	90	5A	Z	122	7A	z
27	1B	[ESCAPE]	59	3B	;	91	5B	[	123	7B	{
28	1C	[FILE SEPARATOR]	60	3C	<	92	5C	\	124	7C	|
29	1D	[GROUP SEPARATOR]	61	3D	=	93	5D	]	125	7D	}
30	1E	[RECORD SEPARATOR]	62	3E	>	94	5E	^	126	7E	~
31	1F	[UNIT SEPARATOR]	63	3F	?	95	5F	_	127	7F	[DEL]

FANSHAWE

Encoding

BINARY	DEC	HEX	ASCII
0100 0001 =	65	41	= A
0101 0010 =	82	52	= R
0101 0100 =	84	54	= T

BINARY
0100 0001 0101 0010 0101 0100

DECIMAL
65 82 84

HEX
41 52 54

FANSHAWE

Unicode Encoding

The Unicode Consortium (Unicode Inc.) coordinates the Unicode Standard

https://*en.wikipedia.org/wiki/Unicode_Consortium*

Members include:

- Adobe Systems
- Apple
- Facebook
- Google
- IBM
- Microsoft
- Netflix
- SAP SE
- Oman's Ministry of Endowments and Religious Affairs

FANSHAWE

Layers / Protocols

Session Layer

- Layer 5 – Responsible for communication synchronization

Protocols include:

- NetBIOS
- RPC
- SMB
- NFS
- SOCKS (port 1080)

FANSHAWE

Layers / Protocols

Transport Layer

- Layer 4

Protocols include:

- TCP
- UDP
- SCTP
- AH

FANSHAWE

Layers / Protocols

Network Layer

- Layer 3

Protocols include:

- IPv4
- IPv6
- IGMP
- ICMP
- ESP
- IPSec

FANSHAWE

Layers / Protocols

Data-link Layer

- Layer 2

Protocols include:

- ARP
- RARP
- ATM
- MPLS
- L2TP

```
┌──(root㉿artmack)-[/]
└─# macchanger -h
GNU MAC Changer
Usage: macchanger [options] device

  -h,   --help                  Print this help
  -V,   --version               Print version and exit
  -s,   --show                  Print the MAC address and exit
  -e,   --ending                Don't change the vendor bytes
  -a,   --another               Set random vendor MAC of the same kind
  -A                            Set random vendor MAC of any kind
  -p,   --permanent             Reset to original, permanent hardware MAC
  -r,   --random                Set fully random MAC
  -l,   --list[=keyword]        Print known vendors
  -b,   --bia                   Pretend to be a burned-in-address
  -m,   --mac=XX:XX:XX:XX:XX:XX
        --mac XX:XX:XX:XX:XX:XX  Set the MAC XX:XX:XX:XX:XX:XX
```

FANSHAWE

Layers / Protocols

Physical Layer

- Layer 1
  - The actual data on the wire, or other media

Protocols include:

- Digital Subscriber Line
- Infrared
- Bluetooth
- Ethernet

FANSHAWE

OSI Layers of Most Interest

- We have discussed in other courses that the Internet was initially designed to allow trusted end points to communicate
- Many of the lower layer protocols still exhibit behaviors based on the initial idea of trust
  - For example, many protocols are designed to send a response, regardless of whether a connection is allowed
  - This lets you determine what hosts are running on the network
- Layers 4, 3 and 2 are the most useful in terms of Scanning

FANSHAWE

OSI Layers of Most Interest

Layer 2 Scanning

- Advantages
  - Very fast and reliable scans
- Disadvantages
  - Limited to finding systems on the network segment you are connected to (non-routable)
  - Single broadcast domain
- At layer 2 we are primarily using ARP requests to find live hosts

FANSHAWE

OSI Layers of Most Interest

Layer 3 Scanning

- Advantages
  - Slower that layer 2 scanning, but still relatively fast
  - Can be used to discover systems on network segments other than the one your system is connected to (routable)
- Disadvantages
  - Layer 3 protocols are often discarded by firewalls
    - Both standalone appliances and host-based software
- At layer 3 we are primarily using ICMP (Internet Control Message Protocol) to discover hosts
  - ICMP echo requests and replies

FANSHAWE

OSI Layers of Most Interest

Layer 4 Scanning (TCP)

- Advantages
  - Like layer 3 scanning it can be used to discover remote systems (routable)
  - It is harder to filter than ICMP requests, so you get results more reliably
- Disadvantages
  - Stateful firewalls are effective at blocking TCP traffic
  - Layer 4 scans can be very time consuming
    - There are 65,536 ports after all

- A large variety of TCP scans are available

FANSHAWE

OSI Layers of Most Interest

Layer 4 Scanning (UDP)

- Advantages
  - Like layer 3 scanning it can be used to discover remote systems (routable)
  - Can be used to discover hosts when TCP is being filtered
- Disadvantages
  - Can produce inconsistent results based on the port and service you are scanning
    - UDP probe requests can get a ICMP port-unreachable response letting you know the system is live, or the service may simply reject the unsolicited traffic
  - As with TCP, layer 4 scans can be very time consuming

FANSHAWE

Why Teach Hacking?

- You need to know how attacks occur to be able to protect your organization from them
- Organizations often don't see the need to spend money on security until they have been compromised
  - Doing a penetration test can often show management where the holes are, and give them a reason to approve spending money on closing these holes

FANSHAWE

Are We Teaching Hacking?

- It is more technically accurate to say we are teaching Penetration Testing Methodologies or Ethical Hacking
- The term “Hacking” has developed a bad reputation over the years
  - It used to designate people who tried to find ways to get a product to do something it wasn’t intended to do
  - Over the years hacking has become associated with only the negative, and often illegal aspects

FANSHAWE

Types of Hackers

White Hat

- Breaks security for non-malicious purposes
- Often legally hacks their own environment, or the environment of others to test security

Black Hat

- Breaks security for malicious purposes
- Many/most of their activities are illegal

Grey Hat

- Breaks security for less easily definable reasons
  - Finding flaws, then notifying companies
    - May be trying to get a bounty for the hack, or the fix
  - Hacktivism

FANSHAWE

Dual Nature of Tools

- Most tools can be used for good or bad
- Password Cracking Tools
  - It is obviously wrong to use a password cracking tool to break into a privileged account.
  - If you use the same tool to check the strength of your password policies, you are protecting the organization
    - Always ensure you have permission
- "Hacking" tools can be used to test for a wide variety of problems
  - Firewall Policies, SQL Server configuration, etc.

FANSHAWE

Recognizing Attacks

- Knowing what it looks like when you are under attack helps you protect the organization
  - If you see a ping sweep one day, followed by some targeted port scans later in the week, you are probably going to see an attack in the near future
- The more tools and techniques you have used, the greater the chance you will recognize an attack when it is happening
  - Even if you are simply interpreting the results of an automated tool such as an IPS

FANSHAWE

Legal Concerns

- You need to be very careful when doing any pen-testing or ethical hacking activities
- Laws change depending on where you are performing the activities and whether you are working in the public, or private sector
- You need to make sure you are authorized to perform a pen-test or ethical hacking before you begin

FANSHAWE

Personal Lab Setup

FANSHAWE

Reasons to Build a Lab

- I have mentioned numerous times that you need to be very careful where you use pen-testing tools
- Creating an isolated lab environment gives you the ability to practice, research and learn how to use the tools without worrying about breaking any laws
  - If the lab is completely isolated, you also don't need to be in G Building to use these tools

FANSHAWE

Network Level Isolation

- LAN segments give you the highest degree of isolation
  - No virtual NIC on the host machine
  - VMs can only communicate with other VMs on the LAN segment
  - Packet captures will only see the traffic on the LAN segment, not your host machine
    - Reduces the background noise and lets you see what is actually happening

Note: You may periodically require a NAT connection for Kali to do upgrades or add packages

FANSHAWE

VMWare Network Types

FANSHAWE

Virtual Network Details

Bridged

- Connected to your laptops physical NIC
- No isolation
- VMware doesn't provide DHCP

Host Only

- Connected to virtual NIC on laptop
- Isolated from the Internet
- VMware provides DHCP
- VMs on network can talk to each other and host computer

FANSHAWE

Virtual Network Details

Custom vmnet (most similar to host-only)

- Connected to virtual NIC on laptop
  - Created when you create the custom vmnet
- Isolated from the Internet
- VMware provides DHCP
- VMs on network can talk to each other and host computer

LAN Segment

- No virtual NIC on laptop
- Completed isolated from laptop
- VMware doesn't provide DHCP

FANSHAWE

Virtual Network Details

NAT

- Connected to a virtual NIC on laptop
- Internet connectivity
- VMware provides DHCP
- VMs on network can talk to each other, host computer and the Internet

FANSHAWE

Configuration Notes

When you are working with VMs you should power the VM down before changing the network type

- Moving from NAT to Bridged for example
- It may work without powering off, but it is better to power the VM off

Always confirm network connectivity before proceeding to more advanced steps

- ipconfig
- ifconfig
- ping

FANSHAWE

Setting Hostnames in Linux

When you are changing the hostname on a Linux machine you need to edit a specific file:

- /etc/hostname
- This is the name of the file that holds the value for the hostname

You can use a variety of tools to edit the file

- VI (command line)
- Nano (command line)
- Gedit (GUI tool)
- Leafpad (GUI tool)

I don't mind which tool you use during the labs as long as you manage to make the appropriate change

- You do need to be comfortable with VI though

FANSHAWE

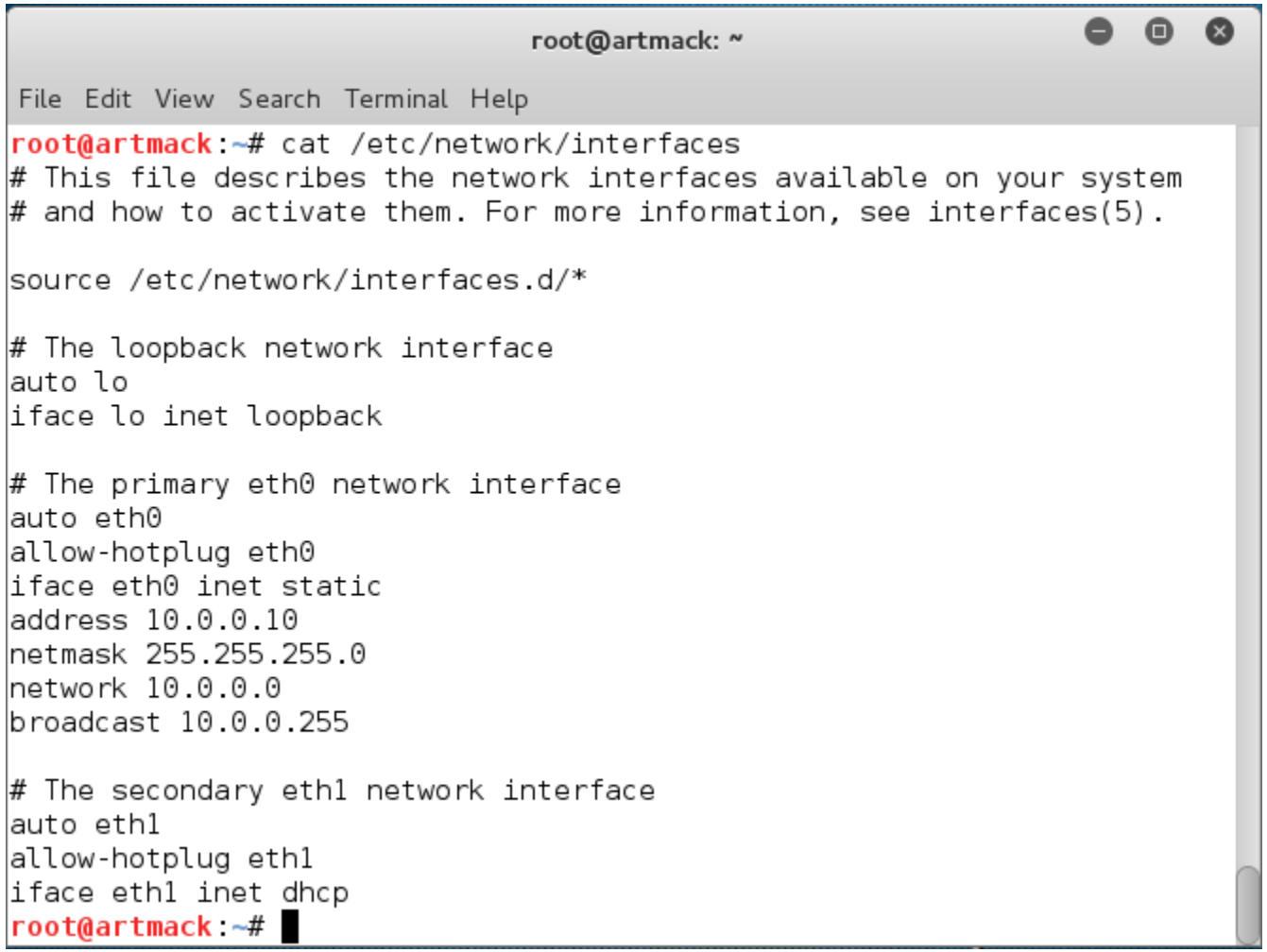
Changing IPs in Linux

Temporary and permanent methods to change your IP:

- Temporary Method: (not recommended)
  - ifconfig eth? 10.0.0.10 netmask 255.255.255.0
    - You will notice the question mark, this means you need to provide this value
    - You can use ifconfig alone to determine this value
- Permanent Method: (recommended)
  - edit /etc/network/interfaces
  - save
  - reboot

FANSHAWE

/etc/network/interfaces



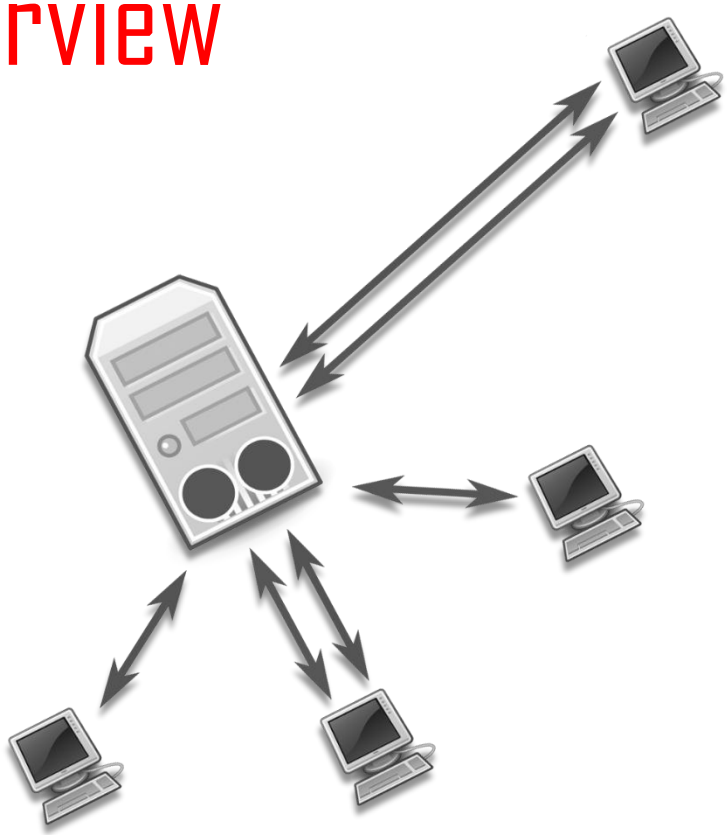
FANSHAWE

Metasploitable2

- Created by Rapid7, the same people who created Metasploit
- Ubuntu Linux distribution that has vulnerabilities built into it
- Great tool for demonstrating common vulnerabilities
- Much easier to get repeatable results with a tool like metasploitable2
- We will talk more about metasploitable2 when we start doing some specific exploits

FANSHAWE

Lab 04 Overview



FANSHAWE

Lab 04 Overview

- Comparing nmap results
- Angry IP Scanner
- Wireshark
- Netdiscover
- Bash Scripting
- Challenge Script