Using Penetration Testing to Assessment

Penetration Testing

Penetration testing can be defined as a legal and authorized attempt to locate and successfully exploit computer systems for the purpose of making those sys-tems more secure. the process includes probing for vulnerabilities as well as providing proof of concept (Poc) attacks to demonstrate the vulnerabilities are real. Proper penetration testing always ends with specific recommendations for addressing and fixing the issues that were discovered during the test. on the whole, this process is used to help secure computers and networks against future attacks.

Types of Penetration Testing

Black-box testing

- The black-box approach is also known as external testing. While applying this approach, the security auditor will be assessing the network infrastructure from a remote location and will not be aware of any internal technologies deployed by the concerning organization.

Types of Penetration Testing

White-box testing

- The white-box approach is also referred to as internal testing. An auditor involved in this kind of penetration testing process should be aware of all the internal and underlying technologies used by the target environment.

Tools of the Trade

- Nmap
  - Host discovery and port enumerating

- Wireshark
  - Protocol analyzer
- Aircrack-ng
  - Capture wireless traffic
- Nessus
  - Vulnerability Mapping
- OpenVAS
  - Vulnerability Mapping

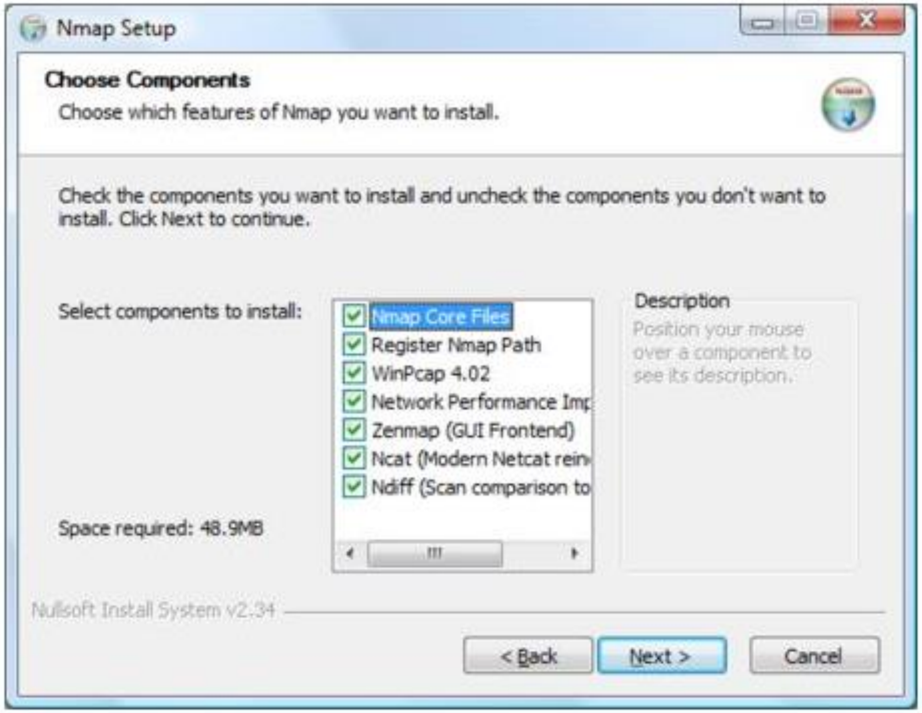
- Dsniff
  - Capture network traffic

Introduction BackTrack 5-R3

- http://www.backtrack-linux.org/backtrack/backtrack-5-r3-released/
- Linux base image both ISO and VMware live image.
- Burn to CD or USB
- Run In Wmware player

NMAP

- www.nmap.com



Nmap Setup

Choose Components

Choose which features of Nmap you want to install.

Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

Select components to install:

- ☑ Nmap Core Files
- ☑ Register Nmap Path
- ☑ WinPcap 4.02
- ☑ Network Performance Imp
- ☑ Zenmap (GUI Frontend)
- ☑ Ncat (Modern Netcat rein
- ☑ Ndiff (Scan comparison to

Space required: 48.9MB

Description

Position your mouse over a component to see its description.

Nullsoft Install System v2.34

NMAP

```
C:\Users>nmap scanme.insecure.org

Starting Nmap 5.21 ( http://nmap.org ) at 2013-04-24 14:22 SA Western Standard T
Nmap scan report for scanme.insecure.org (74.207.244.221)
Host is up (0.15s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 19.53 seconds

C:\Users>
```

Linux/Unix OS

- For Debian and Ubuntu based systems
- # apt-get install nmap
- For Red Hat and Fedora based systems
- # yum install nmap For Gentoo Linux based systems
- # emerge nmap

Nmap

- **Scan a Single Target**
- Executing Nmap with no command line options will perform a basic scan on the specified target.
- A target can be specified as an IP address or host name (which Nmap will try to resolve).
- Usage syntax: *nmap [target]*
- $ nmap 192.168.10.1

Multiple Target

- Usage syntax: nmap [target1 target2 etc]
- $ nmap 192.168.10.1 192.168.10.100 192.168.10.101
- $ nmap 192.168.10.1-100
- $ nmap 192.168.1-100.*
- Nmap –A 192.168..1.105
- nmap --traceroute scanme.insecure.org

Advanced Scanning

- -sS
- TCP SYN Scan
- -sT TCP Connect Scan
- -sU UDP Scan
- -sN TCP NULL Scan
- -sF TCP FIN Scan

Advanced Scanning

- -sX
- Xmas Scan
- -sA
- TCP ACK Scan
- --scanflags
- Custom TCP Scan
- -sO IP Protocol Scan
- --send-eth
- Send Raw Ethernet Packets
- --send-ip
- Send IP Packets

TCP SYN Scan

- The -sS option performs a TCP SYN scan.
- Usage syntax: nmap -sS [target]
- # nmap -sS 10.10.1.48
- Starting Nmap 5.00 (http://nmap.org) at 2009-08-25 11:01 CDT Interesting ports on 10.10.1.48:
- Not shown: 994 closed ports
- PORT   STATE SERVICE
- 21/tcp   open ftp
- 22/tcp   open ssh
- 25/tcp   open smtp
- 80/tcp   open http
- 111/tcp open rpcbind
- 2049/tcp open nfs
- MAC Address: 00:0C:29:D5:38:F4 (VMware)
- Nmap done: 1 IP address (1 host up) scanned in 1.73 seconds

Using Aircrack

- Ubuntu 12.10
- Vmware Player
- Backtrack 5 r3
- ALFA wireless card

Aircrack

- Ifconfig wlan0 up
- Airmon-ng start wlan0
  - Create mon0
  - Iwconfig
- airodump-ng mon0

Aircrack

- airodump-ng –bssid 00:21:91:D2:8E:25 --channel 11 --write WEPCrackingDemo mon0
- Aireplay-ng -3 –b -h   mon0
- aircrack-ng WEBCrackingDemo-01.cap