Network Penetration Testing and Ethical Hacking

Scanning/Penetration Testing

SANS Security 560.2

Sans Mentor: Daryl Fallin

http://www.sans.org/info/55868

Scan Types

- Network sweeping:
  - Send a series of probe packets to identify live hosts at IP addresses in the target network
- Network tracing:
  - Determine network topology and draw a map
- Port scanning:
  - Determine listening TCP and UDP ports on target systems
- OS fingerprinting:
  - Determine target operating system type based on network behavior
- Version scanning:
  - Determine the version of services and protocols spoken by open TCP and UDP ports
- Vulnerability scanning:
  - Determine a list of potential vulnerabilities (misconfigurations, unpatched services, etc.) in the target environment

Nmap Port Scanning

- Nmap doesn't check all ports by default
  - This is very important to note… it's not a comprehensive scan by default
- By default, Nmap checks only the top 1,000 most used ports for TCP and/or UDP
  - The **nmap-services** file indicates the ranking of the most common ports, based on widespread scanning research by Fyodor
  - Nmap *does not* check all ports less than 1024 by default anymore
- The –F option (which stands for "Fast") says to scan the top 100 ports
- The --top-ports [N] option tells Nmap to scan for the N most popular ports
- For a comprehensive or targeted scan, use the –p option

`-p 0-65535` will scan all ports

`-p 22,23,25,80,445` will check only those ports

  - The flag T: and U: can be included in the list to specify TCP or UDP
- Ports are scanned in random order, but –r makes them not randomized

Version Scanning

- When Nmap identifies an open port, it displays the default service commonly associated with that port
  - Based on nmap-services file, which lists about 2,200 services
  - Additional services are searchable at the Internet Assigned Numbers Authority (IANA) port assignments at http://www.iana.org/assignments/port-numbers
- But, what services are on ports not in that list?
- And, what about an admin who configures a service to listen on an unexpected port?
  - Example: Web server on TCP 90 or sshd on TCP 3322
- And, what service and protocol version is the target listening service using?
- Nmap version scanning has the answer

Version Scanning Example

```
[root@fedora13 nmap-5.21]# ./nmap -n -sV -p 1-200 192.168.0.31

Starting Nmap 5.21 ( http://nmap.org ) at 2010-10-15 14:11 CDT
Nmap scan report for 192.168.0.31
Host is up (0.0022s latency).
Not shown: 197 closed ports
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 4.5 (protocol 2.0)
80/tcp  open  http?

Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 86.11 seconds
[root@fedora13 nmap-5.21]#
```

Nmap Scripting Engine

- Goals of the Nmap Scripting Engine (NSE)
  - Allow for arbitrary messages to be sent or received by Nmap to multiple targets, running scripts in parallel
  - Be easily extendable with community-developed scripts
  - Support extended network discovery (whois, DNS, etc.)
  - Perform more sophisticated version detection
  - Conduct vulnerability scanning
  - Detect infected or backdoored systems
  - Exploit discovered vulnerabilities
- May someday rival Nessus and NASL as a general-purpose, free, open source vulnerability scanner

Nmap Scripting Engine Scripts

- Written in the Lua programming language
  - Often used in games, Lua is fast, flexible, and free, with a small interpreter that works across platforms and is easily embedded inside of other applications
  - Described in detail at www.lua.org
- To invoke NSE:
  - To run all scripts in the category of 'default':

```
# nmap -sC [target] -p [ports]
```

  - To run an individual script:

```
# nmap --script=[all,category,dir,script…] [target] -p [ports]
```

  - Add "--script-trace" for detailed output from each script

Nexpose Vulnerability Scanner

- Nexpose Community Edition
  - No Roles, can only scan 32 IP's, support through community
- Nexpose Consultant Edition
  - No Roles, can only scan 128 IP's, limited Support
- Nexpose Enterprise Edition
  - Includes the full set of tools, unlimited IP's, Role definitions, LDAP/AD and Kerberos Authentication

Nexpose Vulnerability Scanner

- Built in Set of Scan Templates
  - In Community Edition the Scan Templates cannot be modified and you cannot add new Scan Templates
  - Templates:
    - PCI, HIPAA, Pen Testing, Audit, Discovery, SOX, Microsoft Hotfix, etc
- Built in identification of Vulnerabilities that are exploitable by Metasploit and known exploits found at www.exploit-db.com (with limits)

Exploitation

What is Exploitation?

- Exploit: Code or technique that a threat uses to take advantage of a vulnerability
  - For a penetration tester exploitation often involves gaining access to a machine to run commands on it
  - Possibly with limited privileges
  - Perhaps with superuser privileges
- Some examples:
  - Move files to a target machine
  - Take files from a target machine
  - Sniff packets at the target
  - Reconfigure the target machine
  - Install software on a target machine

Especially Dangerous!

Categories of Exploits

- Exploit: a piece of code that makes a target machine do something on behalf of an attacker
- Generally speaking, most exploits fall into one of three categories:
  - Service-side exploit
  - Client-side exploit
  - Local privilege escalation
- A penetration tester may need to use any one, or more likely, a combination of each of these kinds of attacks

Metasploit Exploitation Framework

- Metasploit is a free, open-source exploitation framework
- What's an exploitation framework?
  - An environment for running numerous different exploits in a flexible fashion
  - An environment for creating new exploits, using interchangeable piece parts
  - Simplifies the creation of new exploits
  - Standardizes the usage of new exploits
- Runs on Linux, Mac OS X, and Windows
  - Although, according to documentation for some versions, "The Metasploit Framework is only partially supported on the Windows platform. If you would like to access most of the Framework features from Windows, we recommend using a virtualization environment, such as VMware, with a supported Linux distribution…"

Metasploit Framework Components

```
Directorys under /opt/msfe (or your installed location of metasploit)


/msf3/ -  Various framework ways of usage: msfconsole, msfgui, msfweb, msfcli
          Encoding tools:  msfencode

/etc/msf3/documentation/ - Documentation

/etc/msf3/modules/ - exploits/ - exploits for various systems: unix/windows/etc
                     payloads/ - a stage and stager to implement a function such
                                 as a reverse shell
                     encoders/ - used to obuscate code

/etc/msf3/plugins/ - provide additional funcationality like intergration with
                     Nexpose.

/etc/msf3/tools/ - various tools like lm2ntcrack.rb used to crack NTLM hashes
```

Questions?
Ready for the Demo?

- Live Demonstaration
  - Use Nexpose to Scan Targets
  - Use Nmap to Scan Targets
  - Use Metasploit to exploit Targets
- Time Permitting - Scan a live host (that I own) using nmap and TOR Exit Nodes
- Videos of todays Demonstration will be posted online: http://www.liberterra.com
- Sign up for the Mentored SANS 560 here in KC - starting October 7, 2010 - http://www.sans.org/info/55868