Penetration Testing

Edmund Whitehead
Rayce West

Introduction

- Definition of Penetration Testing
- Who needs Penetration Testing?
- Penetration Testing Viewpoints
- Phases of Penetration Testing
  - Reconnaissance and Information Gathering
  - Network Enumeration and Scanning
  - Vulnerability Testing and Exploitation
- Reporting
- How to become a Penetration Tester

Penetration Testing

Definition of Penetration Testing:

- A penetration test or pentest is a test evaluating the strengths of all security controls on the computer system. Penetration tests evaluate procedural and operational controls as well as technological controls.

Who needs Penetration Testing

- Banks/Financial Institutions, Government Organizations, Online Vendors, or any organization processing and storing private information

- Most certifications require or recommend that penetration tests be performed on a regular basis to ensure the security of the system.

- PCI Data Security Standard's Section 11.3 requires organizations to perform application and penetration tests at least once a year.

- HIPAA Security Rule's section 8 of the Administrative Safeguards requires security process audits, periodic vulnerability analysis and penetration testing.

Penetration Testing Viewpoints

-External vs. Internal

Penetration Testing can be performed from the viewpoint of an external attacker or a malicious employee.

- Overt vs. Covert

Penetration Testing can be performed with or without the knowledge of the IT department of the company being tested.

Phases of Penetration Testing

- Reconnaissance and Information Gathering
- Network Enumeration and Scanning
- Vulnerability Testing and Exploitation
- Reporting

Reconnaissance and Information Gathering

Purpose: To discover as much information about a target (individual or organization) as possible without actually making network contact with said target.

Methods:

- Organization info discovery via WHOIS
- Google search
- Website browsing

WHOIS Results for www.clemson.edu

Domain Name: CLEMSON.EDU
Registrant:
Clemson University
340 Computer Ct
Anderson, SC 29625
UNITED STATES
Administrative Contact:
Network Operations Center
Clemson University
340 Computer Court
Anderson, SC 29625
UNITED STATES
(864) 656-4634
noc@clemson.edu
Technical Contact:
Mike S. Marshall
DNS Admin
Clemson University
Clemson University
340 Computer Court
Anderson, SC 29625
UNITED STATES
(864) 247-5381
hubcap@clemson.edu
Name Servers:
EXTNS1.CLEMSON.EDU 130.127.255.252
EXTNS2.CLEMSON.EDU 130.127.255.253
EXTNS3.CLEMSON.EDU 192.42.3.5

Network Enumeration and Scanning

Purpose: To discover existing networks owned by a target as well as live hosts and services running on those hosts.

Methods:

- Scanning programs that identify live hosts, open ports, services, and other info (Nmap, autoscan)
- DNS Querying
- Route analysis (traceroute)

NMap Results

```
    nmap -sS 127.0.0.1
 1
 2
 3 Starting Nmap 4.01 at 2006-07-06 17:23 BST
 4 Interesting ports on chaos (127.0.0.1):
 5 (The 1668 ports scanned but not shown below are in state: closed)
 6 PORT     STATE SERVICE
 7 21/tcp   open  ftp
 8 22/tcp   open  ssh
 9 631/tcp  open  ipp
10 6000/tcp open  X11
11
12 Nmap finished: 1 IP address (1 host up) scanned in 0.207
13         seconds
```

Vulnerability Testing and Exploitation

Purpose: To check hosts for known vulnerabilities and to see if they are exploitable, as well as to assess the potential severity of said vulnerabilities.

Methods:

- Remote vulnerability scanning (Nessus, OpenVAS)
- Active exploitation testing
  - Login checking and bruteforcing
  - Vulnerability exploitation (Metasploit, Core Impact)
  - 0day and exploit discovery (Fuzzing, program analysis)
  - Post exploitation techniques to assess severity (permission levels, backdoors, rootkits, etc)

Reporting

Purpose: To organize and document information found during the reconnaissance, network scanning, and vulnerability testing phases of a pentest.

Methods:

- Documentation tools (Dradis)
  - Organizes information by hosts, services, identified hazards and risks, recommendations to fix problems

How to Become a Penetration Tester

- Stay up to date on recent developments in computer security, reading newsletters and security reports are a good way to do this.

- Becoming proficient with C/C++ and a scripting language such as PEARL

- Microsoft, Cisco, and Novell certifications

- Penetration Testing Certifications

  - Certified Ethical Hacker (CEH)

  -GIAC Certified Penetration Tester (GPEN)

Conclusion

Questions?