Vulnerability Assessment and Penetration Testing

CC Faculty

ALTTC, Ghaziabad

Need

Vulnerabilities

- Vulnerabilities are transpiring in different platforms and applications regularly.

Information Security evaluation

- The security situation of the organisation's network/systems need to be evaluated at regular intervals

How often do you evaluate the security situation of your network?

Risk Management

Risk ?

- Assets
- Vulnerabilities
- Threats
- Safeguards

- Risk Assessment

- Risk Management
  - Accept
  - Mitigate
  - Transfer

Pen Test v. VA v. Audit

- What are the differences between a Penetration Test, a Vulnerability Assessment and an Audit?
- Many people use this terms interchangeably.
- There are actually distinct differences.

Pen Test v. Vuln Assess v. Audit

Audits

- Auditing compares current practices against a set of standards.
- Industry groups or security institutions may create those standards.
- Organizational management is responsible for demonstrating that the standards they adopt are appropriate for their organization

Pen Test vs VA vs Audit

Assessments

- An assessment is a study to locate security vulnerabilities and identify corrective actions.
- An assessment differs from an audit by not having a set of standards to test against.
- It differs from a penetration test by providing the tester with full access to the systems being tested.

Pen Test v. VA v. Audit

	Pen Test	Vulnerability Assessment	Audit
Initial Info	Limited	Limited	Full
Outcome	Access to Internal Network	List of Vulnerabilities	Secure System
Location	Internal / External	Internal/External	On System
Time	Medium	Short	Long

Penetration Testing

- A set of procedures designed to bypass the security controls of a system or organization
- Real life test of the organization's exposure to known security threats
- Performed to uncover the security weakness of a system
- Focuses on exploiting network and systems vulnerabilities that an unauthorized user would exploit

A typical penetration

Phase 1:
Discover/ Map

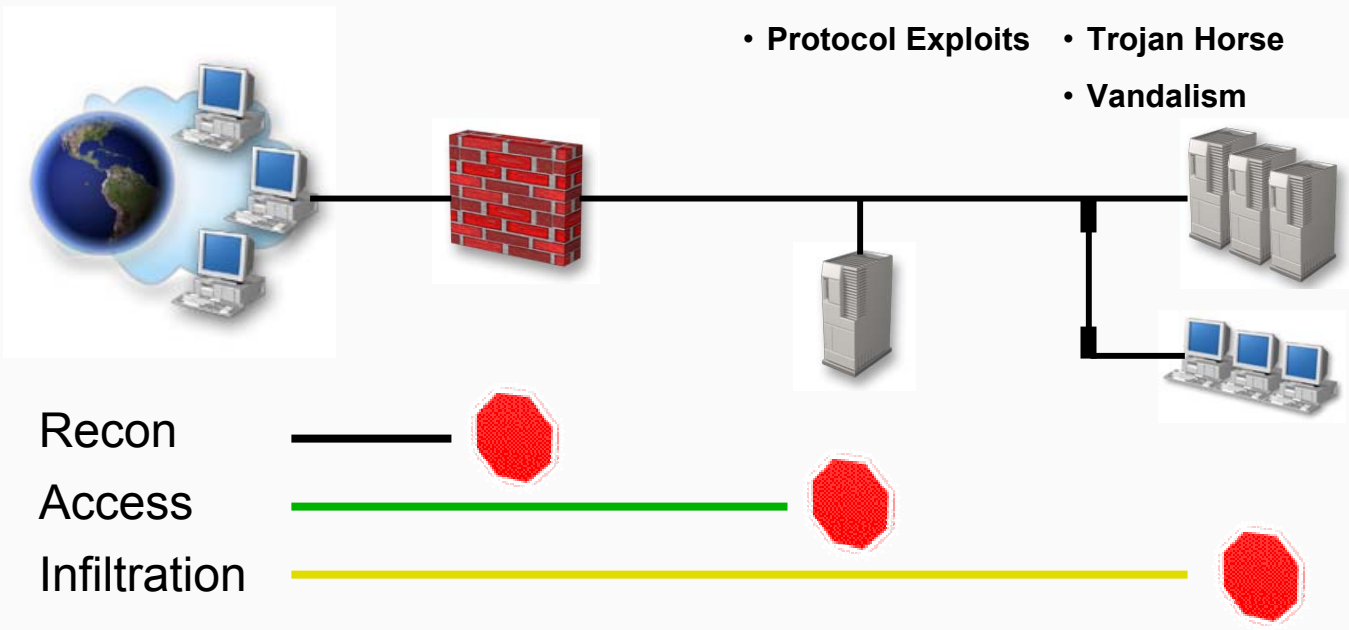
- Scanning & Probing

Phase 2:
Penetrate Perimeter

- Denial of Service
- Spoofing
- Protocol Exploits

Phase 3:
Attack Resources

- Password attacks
- Privilege grabbing
- Trojan Horse
- Vandalism
- Audit trail tampering
- Admin Changes
- Theft



Knowledge Assumptions

- What kinds of test can be performed?
  - Test should address risks and illustrate:
    - zero knowledge: hacker from Internet
    - knowledgeable: former employee, no access, but understands organization
    - insider: current employee, has legitimate access to IT resources
    - knowledgeable insider: IT person, detailed systems knowledge

Penetration Testing - Prerequisites

- The persons conducting penetration testing should be skilled professionals
- Security Auditors
- CERT-In empanelled Security Auditors

Penetration Testing

overview

- Preparation
- Conducting
- Conclusion

Penetration Testing - Preparation

Rules of Engagement:

formal permission for conducting penetration testing prior to starting.

This may include:

- Specific IP addresses/ranges to be tested
- Any restricted hosts
- A list of acceptable testing techniques
- Identification of a finite period for testing
- IP addresses of the machines from which penetration testing will be conducted so that administrators can differentiate the legitimate penetration testing attacks from actual malicious attacks
- Points of contact for the penetration testing team, the targeted systems, and the networks
- Measures to prevent law enforcement being called with false alarms (created by the testing)
- Handling of information collected by penetration testing team.

Penetration Testing - Procedures

- Reconnaissance (Information Gathering)
  - Foot printing, scanning etc.
- Discovery
- Security Testing
  - Vulnerability Assessment
- Reports
- Cleanup

Penetration Testing - Methodology

Teams

- Red Team
  attempts to discover vulnerabilities

- Blue Team
  simulates normal administration
  detection of attacks
  respond to attacks

- White Team
  inject workload
  captures results

Note:

- The team system is only optional
- We are focusing on functions to be performed by Red Team here

Penetration Testing – Reconnaissance

- Objective

  To collect basic information about the organisation and their network

- Methodology

  - collect as much information as possible without actually scanning the target network.
  - study the webpage, search the Internet about the organisation mailing list archives
  - Whois queries, reverse DNS

- Tools

  Samspade, Smartwhois, Neotrace, traceroute etc.

Penetration Testing – Foot printing

- Objective

To determine

- the operating system – platform, version etc., running the webserver, mailserver, clients etc.
- applications running

- Methodology
  - Conduct various web based queries
  - TCP Fingerprinting
  - Target Acquisition

Penetration Testing – Foot printing

Penetration Testing > Foot printing > TCP finger printing

- Active finger printing – sending a crafter packet
- Passive finger printing – capturing packets and analysing

- probe the TCP/IP stack, because it varies with OSs
- this information is used to create a “fingerprint” to determine what type of machine is running

Tools

- Nmap
- Queso
- Cheops

Penetration Testing – Footprinting

Penetration Testing > Footprinting > Target acquisition

- Target Acquisition : Obtain as much information as possible about the target

- Tools

  - Netcraft
  - Internic database searches - whois queries
  - Dig
  - Route analysis
  - traceroute / http://www.visualroute.com

Penetration Testing - Scanning

- Objective

  - To find out the live hosts of target network,

  - determine details of operating systems, applications, ports, services running on target network, systems

- Methodology
  - Conduct various types of scans
  - Analyse the results of Target Acquisition
  - Host Discovery
  - Port Scanning
  - Banner Retrieval

Penetration Testing - Scanning

Penetration Testing > Scanning > Host Discovery

- Identify which machines to target
- to determine which machines are alive and responding
- Tools

Tools:

- fping, pinger, nmap, hostcount
- NetScan Tools
- WS_Ping ProPack

Penetration Testing - Scanning

Penetration Testing > Scanning > Port Scanning

- Port scans to determine which services are running
- To find out vulnerable services
- Port scans can be noisy
- stealth scanners do not make full TCP connections, making detection difficult
- Results of different types of scans viz. connect, SYN, FIN, ACK, XMAS, NULL etc are to be correlated

Tools

strobe, nmap, jakal, netcat, Asmodeus, Cybercop scanner, ISS, NetSonar, WS_Ping ProPack, NetScan Tools

Port Scanning Results of nmap

```
Starting nmap V. 2.53
by fyodor@insecure.org ( www.insecure.org/nmap/ )
Interesting ports on babbage (192.168.1.10):
(The 1515 ports scanned but not shown below are in
  state: closed)
Port State Service
22/tcp open ssh
25/tcp open smtp
80/tcp open http
111/tcp open sunrpc
443/tcp open https
662/tcp open unknown
1024/tcp open kdm
3128/tcp open squid-http
```

Penetration Testing - Scanning

Penetration Testing > Scanning > Banner Retrieval

- collect prompts
- provides clues: system types, platforms, vendors, version numbers, dates, etc.
- mail, http, ftp, telnet
- finger @www.abc.com

Tools

Cybercop Scanner, ISS, NetSonar, strobe, netcat, SATAN

telnet <ip> 25 (smtp port)

Penetration Testing - Enumeration

- Objective

  To determine various user groups, user accounts and their privileges

- Methodology

  Analyse the results of scanning phase, select a server/client system

- Tools

  NAT,, Enum, GetAdmin, user2sid

Penetration Testing - VA

Objective

To find out the vulnerabilities existing in the target network/systems

Methodology

- Analyse the results of previous phases
- Assess the vulnerabilities in the target network/systems
- Automated Vulnerability scanners

Tools

Retina, Nessus, ISS

Penetration Testing - VA

Automated Vulnerability Scanning Tools

- run against target systems
- scans a range of IP addresses only looking for known vulnerabilities
- up to date(?) vulnerability checking
- can be configured for specific tests
  - Windows modules
  - web server modules
  - UNIX module
  - denial of service modules

Tools

Retina, Nessus, ISS

Vulnerability Scanning

- Other considerations
  - **false positives** - verification of scan results
  - some scanners are free
  - scans are “noisy”, leaving large footprints
  - denial of service attacks may bring down scan target
  - some tests require root/administrator access
  - password grinding may lock accounts

Types of tools

- Port Scanners
- Single purpose scanners
- Banner Scan
- Vulnerability Assessment Suites
  - Nessus
  - SAINT
  - ISS Internet security scanner
  - Others , Retina, Shadow, etc.

Types of tools

- Port Scanners
  - Give a good initial picture of what a host/network looks like
  - Easily bogged down by personal firewalls
  - Most popular: nmap, xprobe2

Types of tools

Single purpose scanners

- Tools written to test a specific vulnerability
- Extremely useful when they are timely
- The type of scan opportunistic attackers use

Types of tools

- Vulnerability Assessment Suites - Nessus
- Nessus
  - Open source
  - Quick to add new signatures
  - Used by many consultants
  - Various report formats
  - Allows custom scan checks

Types of tools:

- Vulnerability Assessment Suites - SAINT
- SAINT
  - One of the first
  - Less complex than Nessus to setup
  - SAINT runs exclusively on UNIX
  - Saint used to be free and open source, but is now a commercial product.

Types of tools

Vulnerability Assessment Suites – ISS

- ISS Internet security scanner
  - Reasonably up to date
  - Understands different reporting audiences
  - May be priced out of most IT budgets

Types of tools

Vulnerability Assessment Suites - Others

- Other Commercial Products
  - Cisco Scanner
  - Network Associates' CyberCop
  - Core Impact

Actual Penetration - Hacking

Perimeter penetration

- Router vulnerabilities
  - SNMP – Solarwinds
- Firewall vulnerabilities
  - Fragmentation, Spoofing
- IDS
  - Spoofing, Timing of Scans etc.

Actual Penetration - Hacking

System hacking

- Privilege escalation
- Password cracking
- DoS

Actual Penetration - Hacking

Password guessing methods

- Dictionary attack
- Brute force attack
- Hybrid attack
- Social engineering

Hacking : Covering the tracks

To see whether the evidence of hacking could be erased

Tools:

- elSave
- WinZapper

Penetration Testing - Conclusion

- Preparation of Reports
- Report format
  - illustrates each step of Pentest carried out
  - Tools used
  - Vulnerabilities found
  - audit trails
  - Recommended solutions

Penetration Testing - Cleanup

Follow up on Reports of Penetration Testing

- Information Security Policy
- Standards
- Guidelines
- Procedures

Security Testing Standard

OSSTMM –

Open-Source Security Testing Methodology Manual

Version 2.1 at www.osstmm.org

Report format templates: (page 93 to 120)

Version 3.0 (to be released)

- Developed by Pete Herzog, it is a living document on how to perform a penetration test.
- Defines how to go about performing a pen test, but does not go into the actual tools.

References

- Information Security - Chris Clifton
- NIST Special Publication 800-42: Guideline on Network Security Testing
- www.osstmm.org
- www.cert.org
- www.foundstone.com
- www.cert-in.org.in

Thank You