FIST Conference 2004 Frankfurt
February Edition

Information System Security Testing Framework
Draft

Balwant Rathore, CISSP

balwant@segress.com

Founder Open Information System Security Group

www.oissg.org

Information System Security Testing Framework

- About ISSTF
  - Licensing
  - What is ISSTF?
  - What is the Goal/Objective of ISSTF?
  - Target Audience
- Project Management
  - Authorization
  - Scope of Work and Out of Scope of Work
  - Milestone and Timelines
  - Team Composition
  - Commercials
  - Documentation
  - Access Points
  - Test Infrastructure

Information System Security Testing Framework

Information System Security Testing Framework...

- Network and Telecom, System, Application and Database Security Testing
- Process Security Testing
- Physical Security
- Social Engineering

Network and Telecom, System, Application and Database Security

- Methodology
  - Step 1: Information Gathering
  - Step 2: Network Mapping
  - Step 3: Vulnerability Identification
  - Step 4: Penetration
  - Step 5: Gaining Access & Privilege Escalation
  - Step 6: Enumerate Further
  - Step 7: Maintaining Access
  - Step 8: Delude thy Presence (Covering The Tracks)
  - Step 9: Reporting
  - Step 10: Clean up and Destroy Artifacts

Information Gathering

- Locate the target Web Presence
- Examine target using "Search Engines"
- Search Web Groups
- Search employee's Personal Web Sites
- Mirror Target Web Site
- Search Security & Exchange Commission and Finance sites
- Search Uptime Statistics Sites
- Search System/Network Survey Sites
- Search on P2P networks
- Search on Internet Relay Chat
- Search Job databases

Information Gathering...

- Search newsgroups (NNTP)
- Gain information from Domain Registrar
  - Check for Reverse DNS lookup presence
  - Check more DNS information
  - Check Spam database lookup
  - Check to change whois information
- Interrogate DNS
  - Zone Transfer with nslookup/host/axfr
    - ls –d target.com
  - Bruteforce on DNS Server

Information Gathering...

- Perform BGP Query
  - telnet <target>
  - show ip bgp <regexp_ASN$>
  - show ip bgp regexp_46$
- Collect all information and build a map

Network Mapping

- Scanning with Passive Fingerprinting
- Find Live Hosts
  - Using Passive Fingerprinting
  - Using ICMP
  - Using Stack Based scanning
- Perform Banner Grabbing
- Determine Running Services
  - Find open ports
    - using Active & Passive Scanning
    - Scan for TCP & UDP Ports
  - Identify Services

Network Mapping...

- Operating System Fingerprinting
  - Active Fingerprinting
    - TCP/IP stacked based fingerprinting
    - ICMP
    - HTTP
    - Telnet Handshake Analysis
  - Passive Fingerprinting
  - Identifying routes using Management Information Base (MIB)
- Identify Perimeter Network
  - Perform Tracerouting (TCP, UDP, ICMP)
  - Identify Routing Devices
  - Identify Firewall
  - Identify IDS/IPS
- Identifying Critical Services

Network Mapping

- Perform WarDialing
  - Find Listening Modems/RAS Servers
  - Find EPABX
  - Brute Force them
- Put All Information in map

Vulnerability Identification

- Identifying vulnerable services using service banners
- Perform Vulnerability Scan
- Perform False Positives Verification
- Perform False Negative Verification
- Make list of all found vulnerabilities

Target Penetration

- Find out Proof of Concept Code/Tool
- Test Proof of Concept Code/Tool
  - Customize Proof of Concept Code/Tool
  - Test Proof of Concept Code/Tool in isolated environment
- Use Proof of Concept Code/Tool against target

Gaining Access and Privilege Escalation

- Gaining Access
  - Gain Least Privileges
  - Gain Intermediate Privilege
  - Compromise
  - Final Compromise (Game Over)
- Privilege Escalation
  - If access is gained follow all steps again.

Enumerate Further

- Password Cracking
- Emails Gathering
- Identifying Routes and Networks
- Mapping Internal Networks

Maintain Access

- Backdoors
  - BACKDOORING A WEB SERVER WITH REVERSE WWW SHELL
  - BACKDOORING WITH INTERNET SUPER SERVER (IDENT)
  - BACKDOORING WITH REVERSE TELNETS
  - SHOOTING BACK XTERMS
  - BACKDOORING SSHD
  - VIRUS, WORM AND TROJANS
- Root-Kits
  - Application Level
    - Lrk5
    - T0rnkit
  - Kernel Level
    - Knark
    - Adore
    - Solaris LKM

Covering The Tracks

- Hide Files
  - Unix System
  - Windows System
- Clear Logs
  - Unix System
  - Windows System
- Root-Kits
- Defeat Integrity Checking
- Account Entry Editing

Reporting

Clean up and Destroy Artifacts

Unix Security – Enumeration Attack

- Identify Users
  - Finger
    - #finger -l @target.com
    - #finger -l root@target.com
    - #finger -l 'a b c d e f g h'@target.com (Solaris Vulnerability)
  - rwho

    #rwho -a wally becky smith

    becky cygnus:pts0 Jan 17 11:20 :12

    smith aquila:ttyp0 Jan 15 09:52 :22

    wally lyra:pts7 Jan 17 13:15 1:32

    wally lyra:pts8 Jan 17 14:15 1:01
  - ruser

    #rusers -a

    #rusers -h

Identify Users...

- SMTP
  - EXPN, VRFY Command
  - telnet <target> 25 → *vrfy user*
- rpcinfo
  - *#rpcinfo -p target*
- TFTP
  - *tftp> connect target*

Enumeration Attack

- NFS Shares
  - #showmount -e target
  - #mount -t nfs target:/share /mnt
- SNMP
- Password Sniffing

Windows Systems

- Identify Browser Masters
- Identify Domains on the Network
- Identify Hosts within a Domain
- Identify Domain Controllers
- View Domain Membership
  - C:\> netdom query \\host_name
- List Remote machine's name table

Web Application Security Testing

Database Security Testing

- MS SQL Server
- Oracle Database Server

Anti-Virus Security Testing

- ANTI VIRUS TEST FILE
- ZIP-OF-DEATH TEST
- SENDING MAILS WITH WORDINGS LIKE *MIDDLESEX*
- MAIL BOMBING TEST
- VIRUS TESTING
- ROOT-KITS TESTING
- SPYWARE TESTING

VPN Security

- VPN Discovery and Fingerprinting
- VPN Discovery
- VPN Fingerprinting
- IKE Aggressive Mode Hack
- PPTP/Security Flaw
- Split Tunneling Hack
- Vulnerability Identification, Exploit Research and Proof of Concept

Other Areas

- Router and Routing Protocol Testing
- Firewall Security Testing
- Switch Security Testing
- Storage Area Network Security Testing
- Web Server Security Testing
  - IIS
  - Apache
- Wireless Security Testing
- Password Testing

Security Process Testing

- Disaster Recovery Planning
- Business Continuity Planning
- Access Control Testing
- Security Observation

Physical Security

Reporting

- Report Format
- Template