Cadre
information security

PENETRATION TESTING

Do's and Don't's

Paul E. Griggs
Assessment and Compliance Services Manager
CISSP, CISA, CISM, CRISC, PCI-QSA
Cadre Information Security

PAUL E. GRIGGS

Cadre Assessment Services Manager

- Payment Card Industry Qualified Security Assessor
  - DSS Validation and Gap Analysis
  - DSS Penetration Testing
- HIPAA Risk and Controls Analysis
- ISO 27001 Risk and Control Analysis
- Application Assessment
- Network Assessment
- Risk and Compliance Consulting
- Beer Brewer

Simplifying the business of security.

Cadre information security

PENETRATION TESTING

What is Penetration Testing?

- Simulation of an attack on a data system as one might experience from a malicious user.
- Used to establish the overall vulnerability of a data system
- Useful for evaluating the affect of many low risk vulnerabilities that can cascade into a high risk vulnerability.
- Tests the effectiveness of both preventative and detective controls.
- Helps determine the magnitude of exposure presented by control failure.
- Requirement of many compliance protocols (PCI-DSS, etc.)

PENETRATION TESTING

Who should perform penetration testing?

Penetration testing is a specialized skill. Effective penetration testing requires:

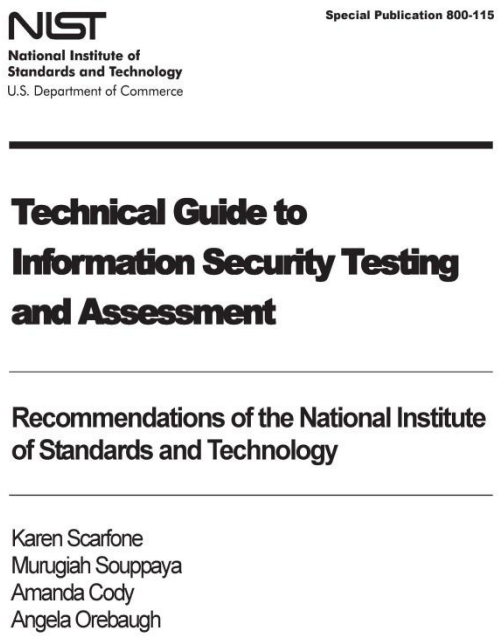
- Experience with the systems and technologies in use
- Understanding of low-level protocols and processes
- Managerial independence from system process owners
- Being methodical in practice, approach, execution, and reporting
- Tools and platforms suitable for pentesting
- Integrity and honesty!

PENETRATION TESTING

Resources

Guides and Methodologies:

National Institute of Standards and Technology Special Publication 800-115: http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf


NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-115

Technical Guide to Information Security Testing and Assessment

Recommendations of the National Institute of Standards and Technology

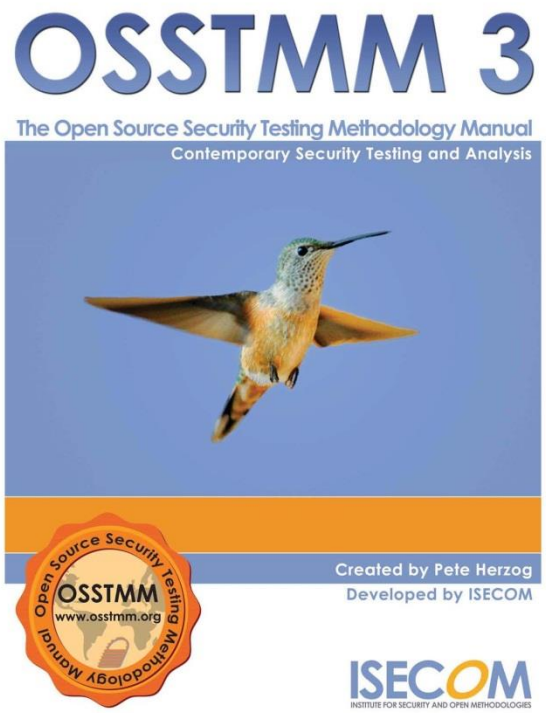
Karen Scarfone
Murugiah Souppaya
Amanda Cody
Angela Orebaugh

PENETRATION TESTING

Resources

Guides and Methodologies:

Institute for Security and Open Methodologies: http://www.isecom.org/



PENETRATION TESTING

Resources

Operating system distributions for Pen Testers:

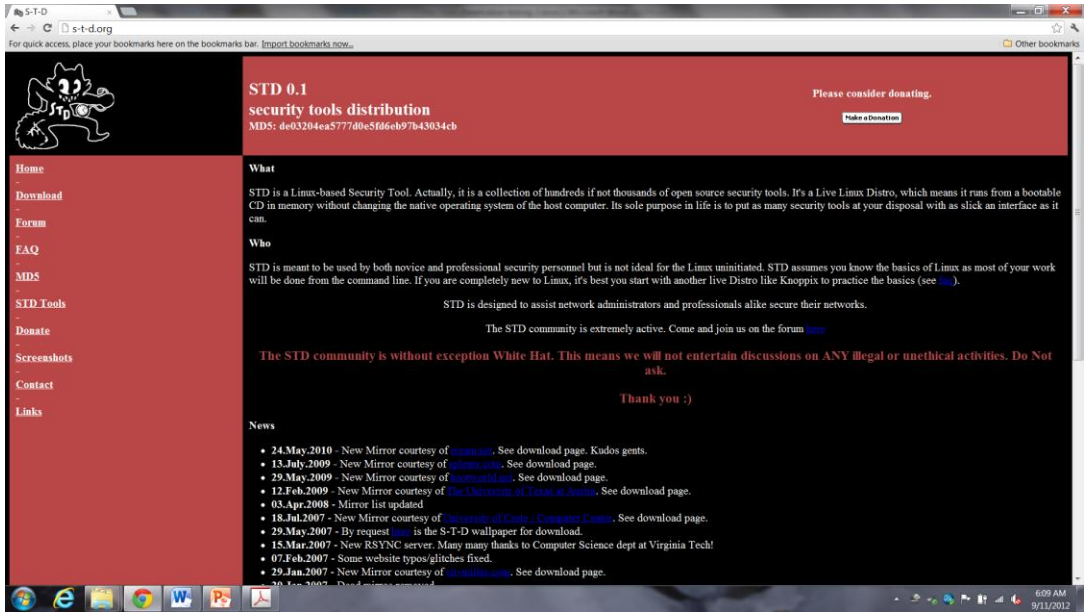
Kali: https://www.kali.org/

PENETRATION TESTING

Resources

Operating system distributions for Pen Testers:

Knoppix STD: http://s-t-d.org/ (No activity since 2010)



PENETRATION TESTING

Isn't a penetration test the same as a vulnerability scan?

- ***No!*** A vulnerability assessment (hopefully more than a scan) concentrates on a single application, operating system, host, or other well defined item or entity.
- A pentest offers the perspective of system security as a whole.
- Make sure everyone is aware of the scope of the pen test. Don't color outside the lines!

PENETRATION TESTING

Example:

A vulnerability assessment determines your publicly facing terminal Server has not been patched and is subject to a remote code execution flaw/DoS (MS12-020, CVE-2012-002).

A penetration test might exploit this vulnerability to gain access to the Terminal Server, then install malware, perhaps a keylogger to gain user account credentials.

PENETRATION TESTING

How to get started

- Pen testing is a higher risk activity than vulnerability assessment. Make sure the process owners understand the risk.
- Establish a strict scope to reduce risk. Make sure everyone agrees to what is “in-bounds” versus “out-of-bounds”.
- Agree on reasonable limits. Are users in-bounds? Phishing? ARP cache poisoning?
- Be aware that limits reduce risk while also potentially reducing the value of the pen test. Hackers generally are less thoughtful.
- Agree on times to begin and end.
- Is IT Ops informed?

PENETRATION TESTING: GEAR?

What do I need for a Pen Test?

What do your tools require?

- Generally, some form of Windows or Linux
- Virtual machines can be very helpful!
- Removable media booting (CD, USB flash) You will need a filesystem for your results!
- “Alternative” devices…

PENETRATION TESTING:

PenTesting with "Alternative Devices"

Android or iPhone/iPad

- Inconspicuous – Easy to use covertly
- Use as a terminal for another device (via ssh or RDP)
- Limited to wireless use
- Limited toolset – no Kali for Android (yet).

PENETRATION TESTING:

PenTesting with "Alternative Devices"

Old laptops

- Can dedicate hardware (no removable media boot needed)
- Generally support both Linux and Windows
- Small, easy to conceal
- Local filesystem for keeping log files and results
- Familiar (good and bad!)

PENETRATION TESTING:

PenTesting with "Alternative Devices"

Mini Linux devices

- GumStix – Very small, a bit expensive
- Ethernet and Compact Flash in a 1 3/8 by 4 1/8 form factor
- Very easy to conceal!

PENETRATION TESTING:

PenTesting with "Alternative Devices"

Mini Linux devices

- Raspberry Pi (Model B)
- Ethernet, SD Card, two USB, HDMI and composite video, sound
- Supports wireless, additional Ethernet, etc via USB
- 3 1/2 by 2 1/4 inch form factor.
- Very easy to conceal!
- Cheap! $35 plus SD card

PENETRATION TESTING:

Pen Test Types

Internal – Find and exploit vulnerabilities on the internal network Perspectives:

- Trusted internal user or “blind on a hot jack”?
- Internal users are much easier to discover and enumerate (typically Active Directory)
- “Blind on a hot jack” becomes internal user after an account is stolen.

PENETRATION TESTING:

Pen Test Types

External – Find and exploit vulnerabilities of hosts facing the Internet

- Typically web applications/Intranet
- Potential for data base access (!)
- Email
- Customers/Cardholder data
- DNS naughtiness

PENETRATION TESTING:

Pen Test Process

1) Discovery – Find your hosts
2) Enumeration – What are they running
3) Vulnerability detection – What vulnerabilities exist
4) Exploitation – What can I do with the vulnerabilities
5) Post-exploitation – Clean up and reporting

PENETRATION TESTING:

Step One: Discovery

Wireshark: http://www.wireshark.org/

- Protocol Analyzer
- Supports Windows and Linux
- Supports standard packet capture formats
- Free! (and Open Source)
- Useful for “testing the waters” when you are “blind on a hot jack”

PENETRATION TESTING:

Step Two: Enumeration

Easy: nmap. http://www.insecure.org

- Nmap is the port scanning tool that has no equal
- Included in all PenTest OS distributions
- Included in most Linux software depositories
- Supports Windows
- Scripting engine includes many vulnerability checks
- Free! (and Open Source)

PENETRATION TESTING:

Step Three: Vulnerability Detection

OpenVAS: http://www.openvas.org/

- Fork of the Nessus scanner when Nessus went commercial
- The Nasl scripting engine uses the same syntax as Nessus
- Linux only, but there is a client for Windows
- Free! (and Open Source)

PENETRATION TESTING:

Step Four: Exploitation

MetaSploit Framework: http://www.metasploit.com/

- Began in 2003 as a portable exploit tool in PERL
- Later rewritten in Ruby, gathers many contributors
- Commercialized by Rapid7 in 2009
- Is the reference platform for security researchers
- Free and open source! (Commercial version available from Rapid7)

PENETRATION TESTING:

Step One: Discovery

Wireshark

- Use Wireshark to analyze network broadcast traffic.
- Examine ARP and DHCP traffic to determine the local subnet and default router.
- By monitoring ARP and DHCP, you can determine your “network neighbors”, presumably “authorized network users”.
- Capturing MAC addresses and associated IP addresses may tell you “interesting things”, such as the vendors of the ethernet interfaces on the wire (e.g. SUN, IBM, Dell, HP, Cisco, Juniper, Apple,etc)

PENETRATION TESTING:

Step One: Discovery

- **Problem:** Bogus IP addresses and/or unauthorized DHCP requests/responses can be detected on the wire and can cause alerts.
- **Solution:** Throwing Star LAN tap. http://greatscottgadgets.com/throwingstar/

PENETRATION TESTING:

Step One: Discovery

Solution: Throwing Star LAN tap

- The Throwing Star LAN tap allows you to receive network traffic but does not allow you to transmit. If you do not transmit, you are undetectable on the wire.
- Record authorized MAC addresses. Wait until that MAC address is no longer present. Change your MAC address to one observed, remove the LAN tap, and now you are an authorized user (at layer 2).

PENETRATION TESTING:

Step One: Discovery

Problem: An authorized MAC on an unauthorized port can be detected and can cause alerts.

- Life is not without risk…
- Clone a printer MAC address and commandeer a printer Ethernet jack. While the activity will not be attributable to a printer, an IPS would have to be well configured to differentiate the traffic as from a device that should only receive print jobs.

PENETRATION TESTING:

Step Two: Enumeration

Nmap

- If your external, you should already have an idea of your targets. Use the spoof option to hide the real scanner if needed. (-D decoy list)
- Most organizations do not consider a port scan an attack, and while it may raise suspicions, it may not result in a “red alert”

PENETRATION TESTING:

Step Two: Enumeration

Nmap

- Consider, low-and-slow may make it past IPS and avoid attention.
- Scan out-of-order. Consecutive hosts are obvious in the logs (--randomize-hosts)
- UDP is painful. Use --top-ports “-sU --top-ports 15094” is less than a quarter of all possible ports, yet 99% as effective.

PENETRATION TESTING:

Step Two: Enumeration

Nmap

- Internally, an nmap scan might light up the IPS. The fewer ports you hit, especially consecutively, the less attention you will get.
- Use the --top-ports parameter to limit nmap to only the top *n* most popular ports, less than 100.
- Scan once and get the most. Use –A to get service info (TCP).

PENETRATION TESTING:

Step Three: Vulnerability Detection

OpenVAS: http://www.openvas.org/

- Externally, limit the scan to detected services. The less noise you throw, the better.
- Pick out vulnerabilities from the nmap scan. If you see a vulnerable version of Apache, don't risk running the OpenVAS scan to tell you what you already know.

PENETRATION TESTING:

Step Three: Vulnerability Detection

OpenVAS: http://www.openvas.org/

- Internally, a full blown top-to-bottom scan is going to get some attention. Try to avoid it.
- Hit different tests for different hosts. If one workstation hasn't been patched recently, there are likely others.

PENETRATION TESTING:

Step Four: Exploitation

MetaSploit Framework

- No, MetaSploit Framework is not a point-and-click exploit tool. *(I'm sure Rapid7 would love to sell you one, though.)*
- MetaSploit Framework is highly effective, however.
- There are some very good tutorials on-line: http://www.offensive-security.com/metasploit-\unleashed/Main_Page

PENETRATION TESTING:

Step Four: Exploitation

You got exploitable vulnerabilities, you've got exploits — time to smash those servers, right?

- No! Servers are on the alter in the datacenter. Admins are watching them closely, especially critical hosts.
- At least on your first round of exploits, do not target servers!

PENETRATION TESTING:

Step Four: Exploitation

You got exploitable vulnerabilities, you've got exploits — time to smash those servers, right?

- No! Servers are on the alter in the datacenter. Admins are watching them closely, especially critical hosts.
- At least on your first round of exploits, do not target servers!

(Target admins… ;)

PENETRATION TESTING:

Step Four: Exploitation

Target the Admins

- Admins have the keys to the kingdom. You want the keys to the kingdom. Don’t settle for some gold when you can have the kingdom.
- Finding the admins can be difficult. Some strategies for finding them…

PENETRATION TESTING:

Step Four: Exploitation

Finding the Admins

Is there a department or room for admins?

- They might notice you fussing around with their machines! Work the control panel of a network printer in their area to get subnet info.
- Look at the network config, or just get the printer to print a status page.

PENETRATION TESTING:

Step Four: Exploitation

Know the Enemy

- Phish the admins. Walk through their cubes to note their interests. Formulate an appropriate enticement to your server with a payload (MetaSploit). Java, Adobe Reader, and Adobe Flash are great payload targets.

- Get friendly with them. Do they smoke? Can't smoke in the building. Step outside and chat them up. (Read the sports page in the morning.)

PENETRATION TESTING:

Step Four: Exploitation

You've exploited an admin. What's the goal?

- You want their credentials.
- Keylogger (MetaSploit). Remote VNC desktop (MetaSploit). Remote registry access.

PENETRATION TESTING:

Step Four: Exploitation

You've got admin credentials. Now what?

- It's not fair going through life with someone else's identity. So make your own.
- When making a new admin account, be careful. A new Domain Admin with the name "l33tHax0r" might draw undue attention.
- Find a respected admin and mimic their account. If Bsmith is an admin, make an account Bsmith2. "Oh, that's just Bill. He must be testing something."

PENETRATION TESTING:

Step Four: Exploitation

Look at the Domain Admin group.

I bet there are some service accounts in there because someone was too lazy to figure out what privileges the service account really needed. (Service accounts are good targets for credential stealing as well. They're admins, right?)

PENETRATION TESTING:

Step Four: Exploitation

Look at the Domain Admin group.

I bet there are some service accounts in there because someone was too lazy to figure out what privileges the service account really needed. (Service accounts are good targets for credential stealing as well. They're admins, right?)

> *"PSYS_Backup" Great, a service account. Make a new account "PSYSDEV_Backup". Put in the account description, "Service account for PSYSDEV per Bsmith." Bill said it was OK, must be OK! ;)*

PENETRATION TESTING:

Step Five: Post Exploitation

The two most important portions of a pen test:

1. You must be able to articulate the particular vulnerabilities exploited, down to host, vulnerability, the exploit, date, and time.
2. You must absolutely be able to provide enough information to clean up your mess.
    - Did you push down a keylogger?
    - Did you make a new admin account?
    - Did you introduce a new GRE tunnel in the core router?
    - The organization must be able to roll back to a known condition.

PENETRATION TESTING:

Final Thoughts

- **A pen tester uses criminal tools and techniques for a legitimate purpose.** Some folks find pen testers untrustworthy because of this. It is absolutely imperative for a pen tester to avoid any circumstance that may call his or her ethics into question.
- **Be sure to treat the confidential data of others securely.** If you downloaded the HR database, protect it, and don't go rummaging through it unless it supports the pen test objectives.
- **Treat people with respect.** Admins don't like to have their systems compromised. Be helpful, not condescending.

PENETRATION TESTING:

Question & Answer Session

Thanks again!

Paul E. Griggs, CISA, CISM, CISSP, CRISC, PCI-QSA
Assessment and Compliance Services Manager
Cadre Information Security