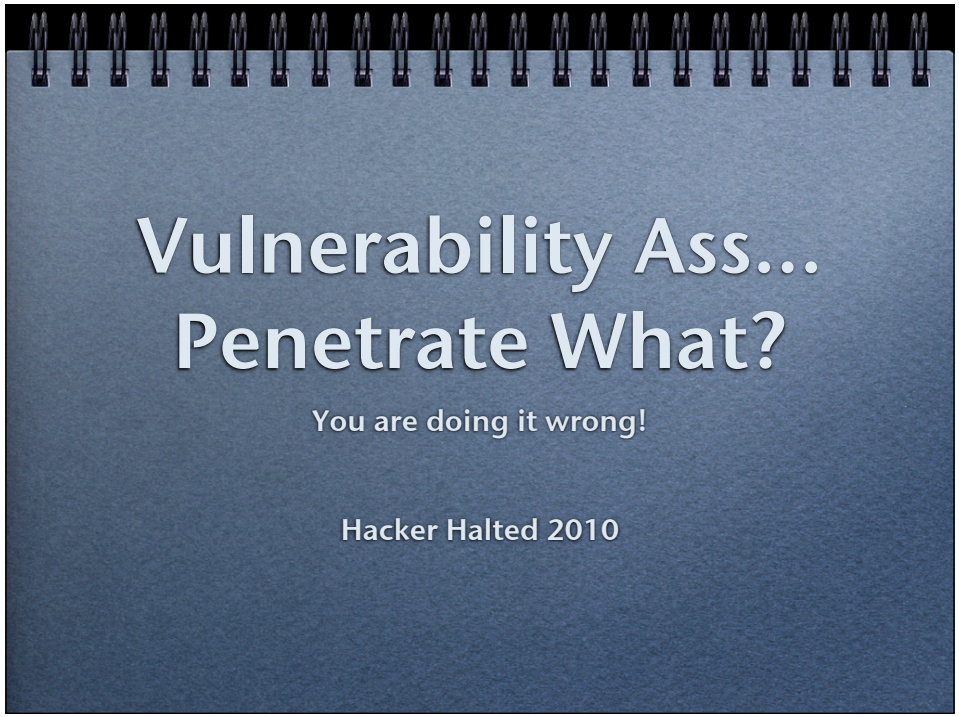
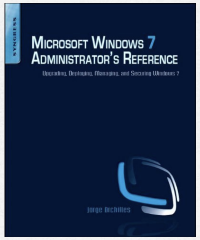

Vulnerability Ass...
Penetrate What?
You are doing it wrong!
Hacker Halted 2010

Jorge Orchilles is a South Florida Information Security Professional

- Information * field for over 8 years
- Security Analyst for Fortune 10 company (not speaking on their behalf, LinkedIn.com for more ;)
- Consultant by night - Orchilles Consulting
- BBA and MS in MIS - Florida International University
- Author - Microsoft Windows 7 Administrator's Reference (Syngress)
- Certs - CEH, GCIH, CICP, CCDA, CSSDA, MCTS, MCP, Security+
- Organizations - VP of SFISSA, OWASP, Hack Miami, InfraGard, MECTF




We will be discussing how to perform a vulnerability assessment (VA) or penetration test (PenTest) to provide the most value to the target business
Audience Feedback
Terminology
Planning (scope)
Testing
Reporting

What does the audience know about VA and/or PenTesting and/or Ethical Hacking

- Does your company have a VA or PenTest policy or had an assessment performed against your organization?
  - Internal or third-party testing?
- Have you ever performed a VA or PenTest?
  - Internal or for another organization?

VA and/or PenTests are performed to bring business value

- Measure the organizations business risk
- What is the business trying to accomplish or get out of the test?
  - Identify vulnerabilities
  - Add realism to threats
  - Test defenses (IDS, IPS, Firewall, AV, etc)
  - Compliance :(

Terminology

- Vulnerability – a flaw or weakness in system security procedures, design, implementation, or internal controls that may be exploited
- Threat – any potential danger to information or an information system
- Attack – an effort by a threat agent to launch a threat by exploiting a vulnerability
- Risk – compromised of the factors of threats, vulnerabilities, and current value of assets

Vulnerability Assessments and Penetration Testing are different

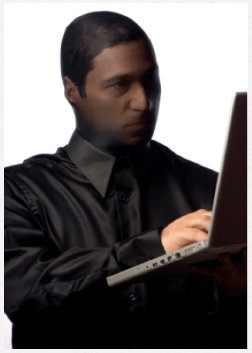
- Vulnerability Assessment (VA)- process of identifying, quantifying, and prioritizing the vulnerabilities in a system
- Penetration Testing (PenTest)- simulating an actual attack. May not identify all vulnerabilities.
- Difference is in the scope (is exploitation allowed; how far can you go)

Defining the scope is critical

- What does the business want?
- External or Internal:
  - External testing is more realistic of an external attacker
  - Internal testing is more realistic to an insider threat or once an external attacker has breached the perimeter. Easier to identify vulnerabilities
- Type of testing:
  - Black Box testing - no authentication
  - White Box testing - authenticated testing
- Who will be notified?
- What systems will be tested?
- When may they be tested (green zones)?
- What systems may be exploited?
- Social Engineering allowed?
- Physical, Wireless, Web App, Network testing?

Attackers do not have these boundaries

- Attackers don't have a scope or testing times
- Attackers don't stop once they get root
- Attackers don't have portions of the test removed from scope



Manage the VA or Pentest

- Sales Engineer - understands technical and business
- Project Manager
- Primary Tester
- Secondary Tester
- Specialized testers?
- Communication is key!

The kick off call is very important for everyone

- This is the conference that must occur before the testing begins
- It is mainly to confirm the scope
- A great time and opportunity for the testers to understand the business and processes (reason for the systems in the first place)
- Notify business where you will be attacking from (if in scope)

Different Methodologies

- Information System Security Assessment Framework (ISSAF)
- Open Source Security Testing Methodology Manual (OSSTM)
- Project Management Body of Knowledge
- Combination of these and some of your own

The testing process may vary depending on scope

- Step 1: Information Gathering
- Step 2: Scanning
- Step 3: Identify and Validate Vulnerabilities
- Step 4: Exploitation, Post-Exploitation, and clean-up (Pen Testing)
- Step 5: Reporting

Information Gathering is VERY important

- Understand and learn the network
- Learn about your target
- Develop your attack for this specific target
- This will ensure the other steps don't fail

Gathering Information is time consuming but worth it

- Google Hacking (Dorks)
- Social Networks
- Mailing Lists
- DNS (whois, host)

Scanning

"One machine can do the work of fifty ordinary men. No machine can do the work of an extraordinary man." – Elbert Hubbard

- Automated Scanning
  - nmap - identify hosts, OS, services
  - Nessus - based on nmap (Nmap NASL) and intel configure the scan
- Manual Testing
  - Difference between you and others

Vulnerability Identification & Verification

- Go through the automated and manual scan output
  - http://cve.mitre.org
  - http://osvdb.org/
- Must verify all identified vulnerabilities as they may be false positive

Exploitation

- Frameworks
  - Metasploit
  - Core Impact
  - Immunity Canvas
- Manual
  - http://www.exploit-db.com/
  - http://inj3ct0r.com/

OMG! I g0t r00t!

- So what?
- This brings no business value!
- Dig deeper - find:
  - Intellectual property
  - Future projections
  - Confidential or Secret documents

Clean-up your mess!

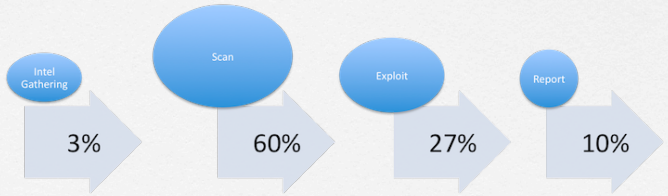
- After exploitation and digging deeper, clean up your mess!
- Very important to document what you did.
- If this step fails we as an industry look bad!

The report is the most important to the business

- Who will get the report?
  - SysAdmins get technical
  - Management gets summary
- Spend time writing the report! Make sure it is understandable and brings value!

Most organizations and service providers are not doing it right

- Lack of talent and focus
- Many cheap providers of VA and PenTests
- Reason for testing = Compliance



How it should be done

Remediation & Retesting

- The report alone doesn't bring value if the issues are not fixed.
- Assist the business in fixing. Provide recommendations to issues on the report.
- Retest once the business thinks they fixed the issue

Thank you

- Email: jorge@orchilles.com
- Blog: http://www.orchilles.com/
- Twitter: jorgeorchilles