Penetration Testing

Overview of PTES

Information Gathering

What Is Penetration Testing?

- Help Defense by doing Offense
- Search for vulnerabilities, and exploit them.
  - Bypass security controls
  - Expose weaknesses
  - Demonstrate
    - Severity of issues
    - How an attacker would get in

Different Types of Pentests

- Black Box
  - Penetration tester has no knowledge of the system
- White Box
  - Penetration tester has full knowledge of the system
- Overt
  - They know you're there
  - White box
- Covert
  - They don't know you're there
  - Black box

Within the Federal Government

- Director, Operational Test and Evaluation (DOT&E)
  - Adviser to the US Secretary of Defense
  - Develops DoD OT&E policy and procedures

Procedures for OT&E of Cybersecurity in Acquisition Programs

- "All systems capable of sending or receiving digital information are required to conduct cybersecurity testing."
  - Includes systems that transfer data with USB devices
  - Systems with two-way communications must undergo both phases of testing
    - CVPA
    - AA
- http://www.dote.osd.mil/pub/policies/2014/8-1-14_Procs_for_OTE_of_Cybersec_in_Acq_Progs(7994).pdf

Cooperative Vulnerability and Penetration Assessment (CVPA)

- "…provide a comprehensive characterization of the cybersecurity status of a system in a fully operational context…"
- "…overt and cooperative examination…"
- "…identify all significant vulnerabilities and the risk of exploitation of those vulnerabilities."
- "…document reviews, physical inspection, personnel interviews, the use of automated scanning, password tests, and applicable exploitation tools"

Adversarial Assessment (AA)

- "…assess the ability of a unit equipped with a system to support its missions while withstanding validated and representative cyber threat activity…"
- "…evaluate the ability to protect the system/data, detect threat activity, react to threat activity, and restore mission capability degraded or lost due to threat activity."

Cybersecurity Compliance Metrics

- Account Management
- Least Privilege
- Identification and Authentication
- Content of Audit Records
- Audit Review, Analysis and Reporting
- Continuous Monitoring
- Configuration Settings

- Backup, Recovery, and Restoration
- Device Identification and Authentication
- Authenticator Management
- Default Authenticators
- Physical Access Control
- Boundary Protection
- Secure Network Communications
- Update Management
- Malicious Code Prevention

Core System Protection Data and Metrics

- Vulnerabilities
- Intrusion/Privilege Escalation/Exploitation Techniques
- Password Strength
- Protect
- Detect
- React
- Restore/Continuity of Operations
- Mission Effects

As You Conduct a Test…

- Document
- Document
- Document
- Document
- Document
- Document
- Document
- Document
- Document
- Document
- Document
- Document
- Document
- Document
- Document
- Document
- Document
- Document
- Document
- Document
- Document
- Document
- Document
- Document
- Document
- Document
- Document
- Document
- Document
- Document
- Document
- Document
- Document
- Document
- Document
- Document
- Document
- Document
- Document
- Document
- Document
- Document
- Document
- Document
- Document
- Document
- Document
- Document
- Document
- Document
- Document
- Document
- Document
- Document

Penetration Testing Execution Standard (PTES)

1. Pre-engagement Interactions
2. Intelligence Gathering / Reconnaissance
3. Threat Modeling
4. Vulnerability Analysis
5. Exploitation
6. Post-Exploitation
7. Reporting

www.pentest-standard.org

Penetration Testing Execution Standard (PTES)

1. **Pre-engagement Interactions**
2. Intelligence Gathering / Reconnaissance
3. Threat Modeling
4. Vulnerability Analysis
5. Exploitation
6. Post-Exploitation
7. Reporting

www.pentest-standard.org

Pre-Engagement Interactions

- Scoping
- Goals
- Testing Terms and Definitions
- Establishing Lines of Communication
- Rules of Engagement
- Protect Yourself

Scoping

- You must know what needs to be tested
  - Systems
  - Applications
  - Processes
  - Etc.
- Verify Bounds
  - Locally hosted vs. Hosting Providers

Scoping Meeting

- Often occurs after the contract has been signed
- Establish explicitly what IP ranges are in scope
  - Sometimes customers might want to make the attack more real, and not provide addresses or any information.
- Verify the customer owns all target equipment
  - Many companies often outsource the management of some devices.
    - DNS
    - Email
    - Hardware that servers run on
    - Firewall/IDS/IPS
- Discuss local laws

Scoping Questions

- Why does the customer want the penetration test?
  - Is it required for a specific compliance requirement?
- When should the active portions be conducted? Business hours? After business hours? Weekends?
- How many IP addresses are being tested?
- Any devices in place that may affect the test, such as a firewall or IDS/IPS?
- If a system is penetrated, how should the team proceed?
  - Perform a local vulnerability assessment?
  - Attempt to elevate privileges?
  - Perform password attacks against local password hashes?

Goals

- What is the customer trying to do by having the test?
  - Compliance requirement?
  - Testing a new product?
  - System accreditation?
  - Testing security controls/responders?
- Tell the client what to expect from the testers
- Have someone technical in these discussions

Testing Terms and Definitions

- The client is rarely a penetration tester and can speak the same speak you do.
- Make sure everyone understands common terms and expectations
- Think about your likely audience
  - CTO
  - IT teams
  - Board of Directors

Establishing Lines of Communication

- Document a communication plan
  - POCs within the organization
  - Share your contact information to be used during the test
  - After-hours testing and communication

Rules of Engagement

- An agreed approach to the penetration test.
- Timeframe
- Scope
- How far the tester can go with a target
- Allowed Methodologies

Protect Yourself

- “Get out of jail free” card
- Document with written permission to perform the test
- Must be signed by a senior officer of the client
- Protect the tester from liability, in case there are adverse effects

Penetration Testing Execution Standard (PTES)

1. Pre-engagement Interactions
2. **Intelligence Gathering / Reconnaissance**
3. Threat Modeling
4. Vulnerability Analysis
5. Exploitation
6. Post-Exploitation
7. Reporting

www.pentest-standard.org

Active vs. Passive Recon

- Passive Recon
  - Never touching the customer
  - Customer should have no idea you're gathering info on them
- Active Recon
  - Touching the customer/equipment
  - Customer could (should) know you're gathering info on them.

Active vs. Passive Recon

- Passive Recon
  - Never touching the customer
  - Customer should have no idea you're gathering info on them
- Active Recon
  - Touching the customer/equipment
  - Customer could (should) know you're gathering info on them.

Target Selection

- White box – All targets are known
- Black box – No targets are known
  - Will need to find assets to target
- This is a continual process – Need to continually re-evaluate as the test progresses
- Not all targets are valuable

Open Source Intelligence (OSINT)

- Gathering information from publically available sources
- The Internet!!
  - Search engines
  - Financial reporting
  - Job postings
- Public information the company puts out may reveal a lot about them, and their weaknesses
- OSINT sources may not always be correct, relevant, or timely

Gathering Technical Information on Hosts

- Passive – Difficult to gather anything technical about a host without touching it
- Semi-passive – Gathering information through normal means
  - Sending normal web traffic to a web server
  - Target probably doesn't know it's being "tested"
- Active – Typically looks suspicious
  - Port Scans
  - Vulnerability Scans

Corporate Information

- Locations
  - Physical
  - Cyber
- Relationships
  - Business Partners
  - Business Clients
  - Competitors
- Product line
- Job Openings
- Charity Affiliations

- Court Records
- Org Chart
- Document Metadata
- Network Blocks
- Email Addresses
- Purchase Agreements
- Remote Access
- Defense Technologies
- Market Analysis

Individual Information - Employees

- Court Records
- Political Donations
- Professional Licenses
- Social Media
  - Location things?
- Internet Presence
  - Email addresses
  - Handles/Nicknames
  - Domain Names
- Mobile Phone

Senior Manager of Solution Delivery, Custom Development at Schwan's Company.

Covert Gathering

- Physical security inspections
- Wireless scanning
- Employee behavior
- Shared spaces
- Dumpster diving
- Types of equipment in use
- Data center locations

HUMINT

- Social Engineering
- Ex: call in response to a job posting, learn more about the internal workings of the company.
- Want to know what AV is running? Just ask.
- Present yourself as not you.
- Leverage OSINT

Footprinting

- Interacting with the target in order to gain information from an external perspective
- Identify hosts that are in scope.
  - DNS Lookups
  - DNS Bruting
  - WHOIS

Passive Footprinting

- WHOIS Lookups
  - Obtain registrant information from the registrar.
  - ICANN/ IANA
- BGP Autonomous System Number

Active Footprinting

- Port Scanning
- Banner Grabbing
- SNMP Sweeps
- Zone Transfers
- SMTP Bounce Back
- DNS Bruteforce

Internal Active Footprinting

- Directory Services (Active Directory)
- Intranet sites providing business functionality
- Enterprise applications
- Sensitive network segments
- VoIP Infrastructure
- Authentication provisioning

Security Mechanisms

- Network Based Protections
  - DLP Systems
  - Traffic Shaping
  - Encryption/Tunneling
  - IDS/IPS
- Host Based Protections
  - DLP Systems
  - Antivirus
  - Application Whitelisting
- Application Level Protections
  - Whitelisted Pages
  - Encoding Options
  - Bypass Avenues
- Storage Protections
  - Storage Controller
  - LUN Masking
- User Protections
  - Spam filters
  - Antivirus

So, let’s search for some stuff

- Things about Cody Welu on DSU’s website

Google Search Operators

- Usage
  - Directive:Term
- site:dsu.edu
- allintitle:index of
- inurl:admin
- filetype:pdf

- Logon
- Signin
- Signon
- Forgotpassword
- Forgot
- Reeset

Exploit-DB.com

Shodan

- Search Engine
- Shodan scans the internet for stuff.
  - 4.2 billion IP addresses in IPv4
  - 65,535 ports
  - 275,000,000,000,000 potential targets

Before You Use It…

- Shodan requires an account
- Free for students
- Use your .edu email address

How?

- Search by…
  - Keywords
    - Default password
  - Location
    - country:us city:madison state:sd
  - Network Traits
    - hostname:dsu.edu port:80
    - net:138.247.0.0/16
  - Operating System
  - Organization

theharvester

- Simple Python script
- Collects e-mail addresses and subdomains related to our target
- -d specify domain
- -l limit results
- -b data source
  - Google, googleCSE, bing, bingapi, pgp, linkedin, google-profiles, jigsaw, twitter, googleplus, all

recon-ng