ANATOMY OF A PEN TEST

Understanding the [Mindset | Toolset] of Penetration Testers
ANATOMY OF A PEN TEST
Poppin' Boxes Like a Pro
Alijohn Ghassemlouei

- Handle == [ PushPin | Revolver ]
- DEF CON Attendee - DC15 - Present
- U.S. Department of Energy Contractor - A few years
- Co authored “The Hacker's Guide to OS X” - Kinda neat
- U.S. Department of State Contractor - For a bit
- Sony PlayStation - Now
Hacking in movies != Reality
Running scripts != [ Hacker | Pentester | Programmer ]
Understanding core technologies are crucial
Overnight penetration tester? Hell no.
Developing and refining your skill set takes time
Documentation & boring stuff? Unfortunately, yes
Set expectations and common terminology early
What is your definition of a penetration test?
A penetration test is a method of evaluating the security controls of an asset, system, or network through the emulation of malicious or unauthorized actors with limited knowledge.

This is achieved by demonstrating the execution of the objective at a technical level which should improve the effectiveness and efficiency of the existing security controls in place.¹
Considerations | Penetration Testing

security is not a state, nor a product, it is an ongoing process
a snapshot of an asset in a specific state at a specific time
Assessment Types | General Information

• Vulnerability Assessment - [ 2 to 4 weeks ]
  • Complete stakeholder assistance, credentialed scans, interviews, in-depth review, narrow scope

• Penetration Test - [ 2 to 6 weeks ]
  • Partial stakeholder assistance via trusted agent, partial site notification, larger scope

• Red Team Assessment - [ 4 - 24 months ]
  • Limited stakeholder assistance, no site information, largest scope
IN HOUSE or EXTERNAL
INDEPENDENT OVERSIGHT / THIRD PARTY / EXTERNAL ENT-TITTY

Placement | Penetration Testing

CISO
CYBER SECURITY
MONITORING
INCIDENT RESPONSE

CIO
SYSTEMS
NETWORK
HELP DESK

COO
HUMAN RESOURCES
ACCOUNTING
MAINTENANCE

DIRECTOR

PENETRATION TESTING TEAM
Placement | Penetration Testing

IN-HOUSE

- DIRECTOR
  - CISO
  - CIO
  - COO
- SYSTEMS
- NETWORK
- INCIDENT RESPONSE
- HELP DESK
- HUMAN RESOURCES
- ACCOUNTING
- MAINTENANCE

PENETRATION TESTING
intelligent assholes

or

somewhat slightly less skilled but personable
<table>
<thead>
<tr>
<th>Knowledge</th>
<th>Mindset</th>
<th>Personality</th>
<th>Presentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Past Experience</td>
<td>Identification of true vulnerabilities</td>
<td>Detail Oriented</td>
<td>Communication</td>
</tr>
<tr>
<td>Tool Usage</td>
<td>Prioritization of identified vulnerabilities</td>
<td>Driven</td>
<td>Attire</td>
</tr>
<tr>
<td>Methodologies</td>
<td>Creativity</td>
<td>Lazy</td>
<td>Writing Ability</td>
</tr>
<tr>
<td>General Technical Knowledge</td>
<td>Observant</td>
<td>Cheeky</td>
<td></td>
</tr>
<tr>
<td>Credentials</td>
<td>Meticulous</td>
<td>Always willing to learn</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Knowing when to quit</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
To enhance and improve the state of security throughout the organization through high profile and impactful assessments.

Yes, seriously.
Why is it important to scope your assessments properly?
Scoping | Super Important General Information

Overall significance of system / site / asset
Impact analysis [ political, economic ]
Ability to determine target value [ crown jewels ]
Scoping | Super Important General Information

Location & size
Access
Difficulty
Available Resources
Expectations
Timeline
Broad strategy*
Scoping | Super Important General Information

Location & size

5270F

Scope

Broad strategy*
<table>
<thead>
<tr>
<th></th>
<th>Reconnaissance</th>
<th>Attack</th>
<th>Reporting</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>S1</strong></td>
<td>Scanning, site profile generation, and service detection with manual verification of potential vulnerabilities via exploitation.</td>
<td>Manual exploitation, establish foothold, migrate laterally, and complete objective.</td>
<td>Vulnerability scanning begins, web application scans begin. Collect team notes and begin writing report.</td>
</tr>
<tr>
<td><strong>S2</strong></td>
<td>Review network layout, firewall configs, and gpo’s.</td>
<td>see above</td>
<td>see above</td>
</tr>
<tr>
<td><strong>S3</strong></td>
<td>Interview administrators and responsible parties.</td>
<td>Continue exercise if objective has not been completed, otherwise begin testing site response capability.</td>
<td>Begin writing up findings and opportunities for improvement.</td>
</tr>
<tr>
<td><strong>S4</strong></td>
<td></td>
<td></td>
<td>Allow team lead to review notes, generate report, and send to management.</td>
</tr>
</tbody>
</table>
Rhetorical Question  [ STFU ]  | Query
How do we ensure that we are consistent with our assessments?

Should we just have a checklist?

Why not just script out the entire engagement?
Process | Assessment Tips

• Resource Allocation*
  • Two to four warm bodies for penetration testing and vulnerability assessment
  • Five to six somewhat warm bodies for red team assessments

• Communication
  • Store data centrally
  • Communicate often [ speaking | irc | private messaging ]
  • Shared space for improved cohesion¹
  • Take notes as assessment occurs with daily synopsis¹¹
  • Team member rotation to improve shared skillset / methodologies
  • Rules of Engagement
• General Unix/Linux/Windows Binaries
  • nc, sed, awk, wc, vi,
  • tcpdump, grep, cut
  • net, dig, cat
• Nmap
• Nessus Professional Feed
• Metasploit Framework
• Netsparker
• Solar Winds Engineers Toolkit
• VMWare Fusion
• IDA Pro
• AppDetective
Virtual Machines | General Information

• Host Operating System
• OS X - General Unix Tools & Some Attack Software
• VMware Fusion
• Ubuntu VM - General Linux Use Image
• Windows VM - General Windows Use & Attack Image
• Kali VM - Linux Attack Image
Hardware Tools | General Information

- Macbook Pro Notebook
- External HDD
- Alfa Wireless Card
- Mac Minis
- Gigabit Switch
- Legitimate Hub/Tap
- Beefy Notebook
- Spare Hard Drive
Understanding how to use a tool does not make you a skilled penetration tester
a hacker mindset is required
10,000 ft, oral, technical walkthrough of an attack
clear, condensed, overarching strategy/methodology
Potential Attack Avenues

Social Engineering
Web Drive By
Misconfiguration
Remote Exploitation
Lateral Migration
Zero Day
Custom Malware
Goals

Locate & exfiltrate sensitive organization information

0 - Reconnaissance
1 - Phishing
2 - Exploitation
3 - Privilege Escalation
4 - Lateral Migration
5 - Data Exfiltration
6 - Tasteful Communication of Findings
How do you exfiltrate all your hard work?
Exfiltration* | Possibilities

SCP / FTP / HTTPS
DNS
CUSTOM
Technical demonstration of findings are crucial
Walkthrough | Disappointing Example

Allowed Use of Ingress Email with HTML Formatting

Lack of User Training

Shared Local Admin Credentials

Misconfigured Windows System

Lack of Network Restriction & Segmentation

Lack of Antivirus or HIDS
• Re-identify system/site value
• Access / Data / Services Provided
• Outline the assessment and findings as the week progressed
• Identify issues and elaborate as to why it is important and relevant
• Recommend realistic potential mitigations and why it is important
• Do not suggest tools
This community is incredible and without the wisdom, guidance, and support of these individuals I would not be where I am today.
Noteworthy Individuals | Thank You

Russr
Wiseacre
Highwiz
Xaphan

0x58
Mexican Machine
Roamer
Family & Mom