HORNE CYBER

PROTECTING PENTESTS: RECOMMENDATIONS FOR PERFORMING MORE SECURE TESTS

July 28, 2017

Wesley McGrew, Ph.D.
Director of Cyber Operations
wesley.mcgrew@hornecyber.com

Purpose:

In light of vulnerable tools, practices, and training

...and hostile network environments:

Comprehensive recommendations for conducting secure offense-oriented engagements
(penetration tests, red teaming, etc.)

My Background – How did I get interested in this?

- Education – Computer Science @ Mississippi State
- Academia
  - Helped build cybersecurity program at MSU
  - Research
    - NSA CAE – Research
    - SCADA HMI Vulnerabilities – My Ph.D. dissertation, and more importantly, my DEF CON 20 talk ☺
    - GhostExodus Incident
    - Malware attribution/grouping with machine learning
  - Education
    - Professor – Computer Security, developed course on Reverse Engineering
    - NSA CAE – Education, and *Cyber Ops*
- Private: Freelance > Startup > Acquisition > Growth
    - "Director of Cyber Operations" @ HORNE Cyber

My Background – How did I get interested in this?

DEF CON

DC19 & BHUSA 2011: Post-Exploitation Forensics with Metasploit

DC20: SCADA HMI and Microsoft Bob

DC21: Pwn the Pwn Plug

DC22: Instrumenting Point-of-Sale Malware
(and a little extracurricular pineapple hunting)

DC23: I Hunt Penetration Testers

DC24 & BHUSA 2016: Secure Penetration Testing: Flawed Practices Taught in Training, Books

Motivation

- Penetration testers are…
  - …attractive targets
    - Level of access
    - Information
      - Tester
      - Client
  - …highly vulnerable
    - Tools
    - Procedures
    - Training

Attacker Capabilities

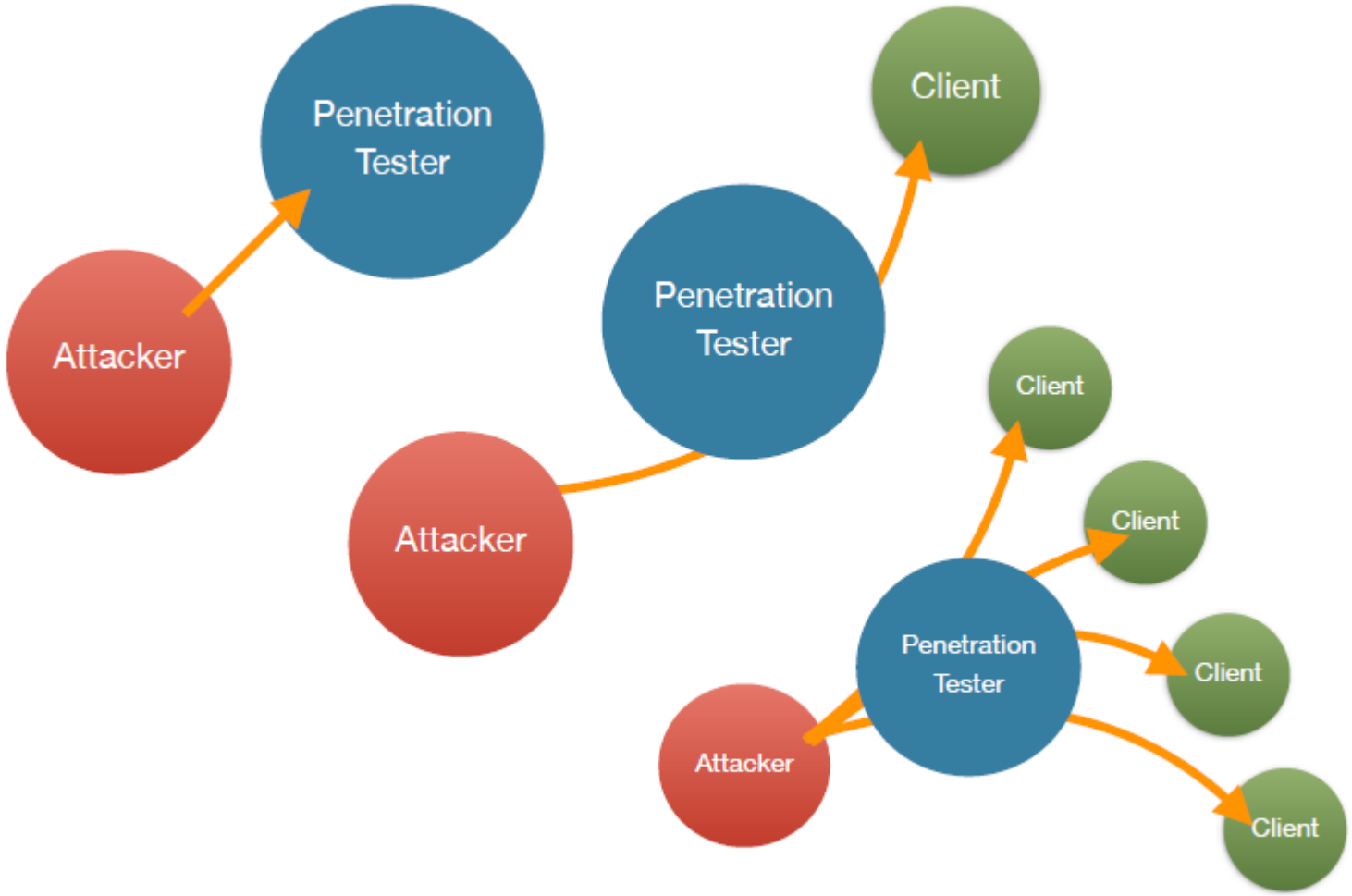
An unencrypted protocol would get man-in-the-middle'd
and reported as a finding on any one of our tests

Why assume any different of the parties interested in attacking us?

What does this (along with the value of the target) mean for:

- Sophistication?
- Skill?
- Resources?

Victimology



Defining OPSEC

- Operational Security (OPSEC)
- In the context of information security?
  - It's all @theGrugq and people just saying what he's saying ☺
  - Security of the "operation" – the pentest engagement
    - The information involved
    - The parties involved
  - How do we address? What does NSA IAD have to say?
    - Five steps:
      - Identify Critical Information
      - Analyze the Threat
      - Analyze Vulnerabilities
      - Assess Risk
      - Apply Countermeasures
- Much of this is also COMSEC

Team Qualifications

- Qualification as a hacker – “Script Kiddie” < “l33t”
- As a professional – Alphabet Soup < ???
- The current state is not good enough
  - There is no natural tendency towards good engagement OPSEC
  - There is no training that covers it
  - Foundational knowledge is skipped
    - “for dummies”
    - “101”
    - “boot camp”
- You wind up with testers who can’t build
  - This hurts you on capability
  - Also hurts your security awareness

Team Qualifications

- How do we raise the bar?
- Saying **NO** to skipping fundamentals, background.
- Automated “pentesting” is easy, hacking is *hard*
- Qualifications
- Skills crisis

The Magic Box

- Everyone winds up stopping at some layer of abstraction, below which the computer is a magical box.
- Unfortunately, all the bugs are either:
  - ...due to not understanding how the magic box works
  - ...or in the magic box itself

Skill Set

- Must
  - Understand published vulnerability information, to include that of pentesting tools
  - Evaluate software for trust
  - Understand impact of tools on client systems
- Proficiency
  - Programming
  - Platforms
  - Networking
- Education must go beyond brief training courses

Recommendation:

Building a secure penetration test requires a team with higher qualifications. Team members with a fluency in programming, platforms, and networking will have the fundamental skills needed to implement this set of recommendations.

In-shop vulnerability analysis

Why do it yourself?

Security researcher interest, or “eyes on”

Mainstream IT Software

Vs.

Penetration Testing Software

Recommendation:

Vulnerability analysis must be undertaken to identify vulnerabilities in the software and processes you use to conduct tests. New tools and exploits that are to be used on engagements should be adequately vetted.

Impact Estimation

The potential impact of exploitation on a system

For confidentiality, integrity, and availability, ask:

- Does the exploitation process leave the system being attacked more vulnerable immediately?
  - Are security features being disabled system-wide?
- Does the continuous process of C2 leave the system, or its data, vulnerable?
  - Listeners vs connect-back
  - Encryption
- Can changes that impact security be reverted by the tester?
  - *Can* you clean it up yourself?

Recommendation:

Team members should have the capability to assess and test the impact of exploitation tools and procedures on the security of the target systems before executing them against client organization systems. This will help the team determine what changes need to be made to the operational use of tools on engagements.

Layering Security

Technical and non-technical

- Tunneling securely
- Best practices and standard operating procedures that are practical
- Ability analyze one’s own toolchain
    - Better decision making
- Human oversight
- Client communication

Recommendation:

Security of the penetration testing process, like most aspects of information security, benefits from defense in depth. Security measures should be taken that enhance the effectiveness of other measures. Fail safe.

Client Data/Tester Intellectual Property

- At Rest
- In Transit
- Retention: After the engagement?

Recommendation:

Sensitive data about the client and the penetration testing team's activities should be encrypted in transit and at rest. Communication between representatives of the team and the client should be secure. Data retention policies should be clearly communicated to the client organization.

Client Involvement

Your job is to illustrate risk, explicitly.

Threat, Vulnerability, Impact

Communicate the risks of testing and your measures put in place to reduce it.

Make them ask *have previous firms taken this much care?*

Educate them.

Client Involvement

Addressing

- “Knocking over” systems – availability
- Exfiltration

Keep open lines of immediate communication, encourage hair-trigger “sanity checks”. Respond and resolve quickly.

Some situations require notification of the client during the engagement

How do you securely communicate with your client?

Secret Squirrel vs Reality

During the engagement…

Report Delivery…

Recommendation:

Open communication should flow both ways between the client organization and the penetration testing team leader. Anomalies identified by the client should be verified with the team, and risks of high and immediate concern should be communicated back to the client in timely fashion.

Scoping Concessions

How closely do you emulate a real attacker?

- Best to do so with high fidelity.
- …but
  - Fragile systems?
    - Helping your client define fragility ☺
  - Scheduling:
    - Emergency contact availability
    - Acceptable downtime
  - Avoiding DoS – Common
  - Meeting
    - Client requirements

Recommendation:

The breadth, depth, and rules of engagement for a penetration test should consider the security of performing the test on the client organization’s systems.

Standard Operating Procedures

(sounds mad boring)

Checks and balances

Too rigid: Negative impact on agility, detriment to the value of the test.

Needed: Consistency

- In the quality of testing by each team member, across multiple hosts on multiple engagements
- In the secure procedures followed

Standard Operating Procedures

EXAMPLE: Managing pentester-created accounts

- Secure username/password pairs
  - Resisting temptation of “admin/admin”, password reuse
- Documentation and secure storage of credentials
  - Team leader awareness
- Client notification of “forced” password changes
  - First-logins, timed-out passwords, etc.
  - Minimize disruption
- Defined “cleanup” phase – get rid of as many created accounts as you can
- Coordinate with IT staff for the stubborn ones.

Recommendation:

Standard operating procedures should be developed to ensure that safety-critical processes are being followed consistently by all team members on every engagement. These defined procedures should have a mechanism for having peers and team leaders review situationally-appropriate exceptions.

Post-Mortems

Add these to the post-mortem:

- Discussion by team members who reviewed team logs for signs of intrusion (or nosy client sysadmins ☺)
- Review of exceptions to standard operating procedure
    - Where was it needed?
    - How did we minimize risk?
    - Is there a more secure alternative - light research
    - More intense R&D needed on better tooling/process?
- What do we need to take back to the lab for vulnerability analysis?
    - Replicate real-world testing situations
    - Test impact on confidentiality, integrity, availability
    - Peer review

Recommendation:

Engaging team members on the development of secure best practices will help them retain ownership of their tools, tactics, and procedures. Continuous improvement and self-testing are necessary to keep “ahead of the curve” in potential risks posed by testing.

The Nature of Exploitation

- Exploitation is a “destructive” process
- Exploits in theory of computation: Functionality that is…
  - …additional,
  - …unintended,
  - …and often unrestricted
- There is no guarantee that an exploit, in this sense, will
  - …establish secure communication before revealing its secrets
  - …leave the system in a stable and secure state
- Many exploits are unreliable, making the opposite true.

Ongoing Challenge:

The nature of exploitation will always result in the development of testing tools and practices that are a challenge to deploy in a secure way.

Ongoing Challenge:

The unknown density of vulnerabilities makes improving the security of penetration testing tools difficult to measure.

My take: Enough can be found and mitigated to “raise the bar”, and reduce attack surface.

Agility

- Pentesters are loath to make changes that slow them down or restrict their ability to improvise
- A more secure penetration process must not degrade existing agility that results in identifying exploitable vulnerabilities
- To accomplish this:
  - Standard operating procedures can keep things moving, with fewer questions of “how do I do this securely?”
  - Team and client understanding of the balance of security and time
  - A process must be in place to evaluate exceptions to the standard operating procedure and identify risks associated with a potentially vulnerable process

Ongoing Challenge:

It will always be hard to balance the benefits of agile and improvised testing with the need to maintain secure testing.

Only by having a flexible process to sanely evaluate the risks of proposed techniques, can there be a balance.

Conclusions

- Established the need for better
  - Tools
  - Practices
  - Training
- Recommendations in nine categories
  - Team Qualifications
  - Vulnerability Analysis
  - Impact Estimation
  - Layering Protection
  - Client Involvement
  - Data Protection
  - Scoping Concessions
  - Standard Operating Procedures
  - Continuous Improvement

- Challenges Exist
  - Nature of Exploitation
  - Vulnerability Density
  - Agility
  - Standardization

Q&A, Discussion

Contact information:

Wesley McGrew, Ph.D.
Director of Cyber Operations
@mcgrewsecurity
wesley.mcgrew@hornecyber.com
http//hornecyber.com

HORNE CYBER