



**HORNE** CYBER

# Secure Penetration Testing Operations

Demonstrated Weaknesses in  
Learning Material and Tools

Wesley McGrew, Ph.D.

Director of Cyber Operations

wesley.mcgreg@hornecyber.com

@McGrewSecurity

# Bio

- Co-Founder of HORNE Cyber, previously Halberd Group
- Directs and participates
  - Penetration testing engagements
  - Research and development
- Adjunct professor at Mississippi State University
  - NSA-CAE Cyber Operations program
  - Information Security & Reverse Engineering

# The Situation at a Glance

**Insecure practices used on penetration tests put clients and penetration testers alike at risk.**

**Penetration testers and clients during/between engagements are attractive soft targets.**

**The root cause of this problem is a lack of awareness, and learning materials that teach insecure practices.**

**This has to change.**

# What are we covering today?

- Previous and Current Work
- The Threat
- Role of Learning and Reference Materials
- Analysis of Currently-Available Materials
- Recommended Best Practices
- Demonstration and Tool Release
  - Snagterpreter – Hijack meterpreter sessions
- Conclusions
- Call to Action

# Where are we?

Two previous papers & presentations, DEF CON 21 and 23

**Pwn the Pwn Plug:**

Analyzing and Counter-Attacking  
Attacker-Implanted Devices

**I HUNT  
PENETRATION  
TESTERS!**

More Weaknesses in Tools and Procedures

This work – a paper and talk studying the root causes of these issues, recommending change.

# The Threat

Why is the compromise of a penetration tester attractive?

## **As a Target**

Tools, tactics, procedures. Intellectual property.

## **Operational Cover For Compromising Clients**

Testers are expected to break rules, attack, elevate privilege, exfiltrate.

# Cause and Effect

## **No Standard**

Dependent on experience, intuition, pattern recognition,  
and complex ad-hoc processes

Tradeoff: Flexibility vs. Rigor

## **We operate as we learn**

## **Lowest Common Denominator = Profit**

No formal requirements for education

Few prerequisites

No testing requirements

# Cause and Effect

## **Testing Processes Follow Training**

Convenience and Expediency

## **Lower Depth & Breadth of Technical Knowledge**

## **Lack of Situational Awareness in Secure Operation/Communication**

Re-applying procedures learned in reading/training to  
more complex operational environments



## The Study – The Goal

**How are secure practices in penetration testing covered (or not covered) in learning and reference materials?**

Books, Training, Standards  
Documents

# The Study – The Material

## **Books: 16**

Top Amazon results, well-known and popular books

## **Training: 3**

Publicly available material, limited (NDAs, cost)

## **Standards: 4**

Well known

# The Study – Disclosure

## Disclosure:

You'll see from the results: the lack of coverage of secure practices, and the promotion of vulnerable practices, is the norm, not an outlier.

Titles, author names, sources, are not stated. The purpose is to demonstrate an industry-wide need to move forward.

Examples are provided, if you're well-read, you may recognize them.

## The Study – The Questions

# Host Security, Penetration Tester

Does the work address precautions for preventing penetration testers' systems from being compromised?

# The Study – The Questions

## Host Security, Client

Does the work address precautions for maintaining the security of client systems during the test?

# The Study – The Questions

## COMSEC

Does the work address establishing secure means of communicating with the client about the engagement?

# Client Data in Transit

Does the work address issues surrounding the transmission of sensitive client data between targets and penetration testers' systems in the course of the engagement?

# Client Data at Rest

Does the work discuss procedures for securing client data at rest, during, and/or after the engagement?



# The Study – The Questions

## OSINT OPSEC

Does the work address operational security during intelligence gathering phases?

# Potential Threats

Does the work address issues with conducting tests against systems over hostile networks, such as the public Internet or unencrypted wireless?

## The Study – The Questions

# Insecure Practices

Does the work demonstrate or teach at least one example of an insecure practice without describing how it might leave the tester or client vulnerable?

# Results

Resource	1 - Host Security - Penetration Tester	2 - Host Security - Client	3 - COMSEC	4 - Client Data - In Transit	5 - Client Data - At Rest	6 - OSINT OPSEC	7 - Potential Threats	8 - Insecure Practices
1	Y	N	N	N	Y	N	N	N
2	N	N	N	N	N	N	N	Y
3	N	N	N	N	N	N	N	Y
4	N	N	N	N	N	N	N	Y
5	Y	Y	Y	Y	Y	Y	Y	N
6	N	N	N	Y	Y	N	N	Y
7	N	N	N	N	N	N	N	Y
8	N	N	N	N	N	N	N	Y
9	N	Y	N	N	Y	N	N	Y
10	N	N	N	N	N	N	N	Y
11	N	N	N	N	N	N	N	Y
12	N	N	N	N	N	N	N	N
13	N	Y	Y	Y	Y	Y	N	Y
14	N	N	N	N	N	N	N	Y
15	N	N	N	N	N	N	N	Y
16	N	N	N	N	N	N	N	Y
17	N	N	N	N	N	N	N	Y
18	N	N	Y	Y	N	N	N	Y
19	N	Y	N	Y	Y	N	N	Y
20	N	N	N	N	Y	N	N	Y
21	N	N	N	N	N	N	N	Y
22	N	N	N	N	N	N	N	Y
23	Y	N	N	Y	Y	N	N	Y

Mostly red!

Almost every one specifically teaches insecure practice.

## Out of 24 works...

**14** did not address basic issues.

**4** addressed more than two issues.

**Every work that actually covered technical practices described actions that were potentially dangerous/insecure.**

**2** did not cover technical practices

**1** Warned about unencrypted networks

## Analysis – Most Common Flaw

# Unencrypted command and control

netcat, web shells, default  
meterpreter, etc.

## “Greatest Hits”

You'll have to attend or watch the talk itself to hear specific (an humorous) examples of the most insecure practices presented in the works studied.

# Recommendations

**Client Communication Security**

**OSINT OPSEC**

**Awareness**

**Host Security – Client and Pentester**

**Data at Rest**



# Demonstration

*Snagterpreter*

Hijacking HTTP/HTTPS meterpreter sessions.

# What's going on in this demo?

- Metasploit's Meterpreter – Most commonly used and documented penetration testing implant/post-exploitation tool.
- Easy to use, more fully featured than a shell, therefore popular
- Operational use – Often traversing hostile networks, such as the public Internet.
- Protocols
  - Type-Length-Value – Commands & Responses
  - Transport – TCP, or HTTP/HTTPS for stateless resilience
- Default encryption is for **evasion**, not **security**!
- The developers know this, have implemented **paranoid** mode to validate server & client certificates
  - Nobody teaches anyone how to use this apart from official docs
- Let's demonstrate non-paranoid-mode hijacking...

**Penetration tester,  
test thyself!**

# Conclusions

- In this work:
  - Explained threats
  - Demonstrated vulnerabilities
- You cannot have it both ways
  - You can't report on vulnerabilities in situations involving malicious actors intercepting and modifying traffic.
  - ...while ignoring that threat model in your own operations
- We must improve
  - Tools
  - Techniques
  - Processes
  - It all has to be integrated into learning material

# Take-Away Points

- Penetration testers put their selves and clients at risk with insecure practices. Third-party malicious attackers can take advantage of this.
- The root cause: Learning material available teach insecure practices and do not address security issues. This leads to lack of rigor in penetration testing practices.
- Direct and mindful action must be taken by penetration testers, tool developers, and learning material authors to remedy this problem.

## Materials

White paper, slides, code

<https://hornecyber.com/> *<precise URL provided in final slides>*

## Contact

Wesley McGrew

wesley.mcgrew@hornecyber.com

@McGrewSecurity