I Hunt Penetration Testers!

More Weaknesses in Tools and Procedures

Wesley McGrew, Ph.D.
Distributed Analytics and Security Institute
Mississippi State University

http://mcgrewsecurity.com   @mcgrewsecurity
wesley@mcgrewsecurity.com

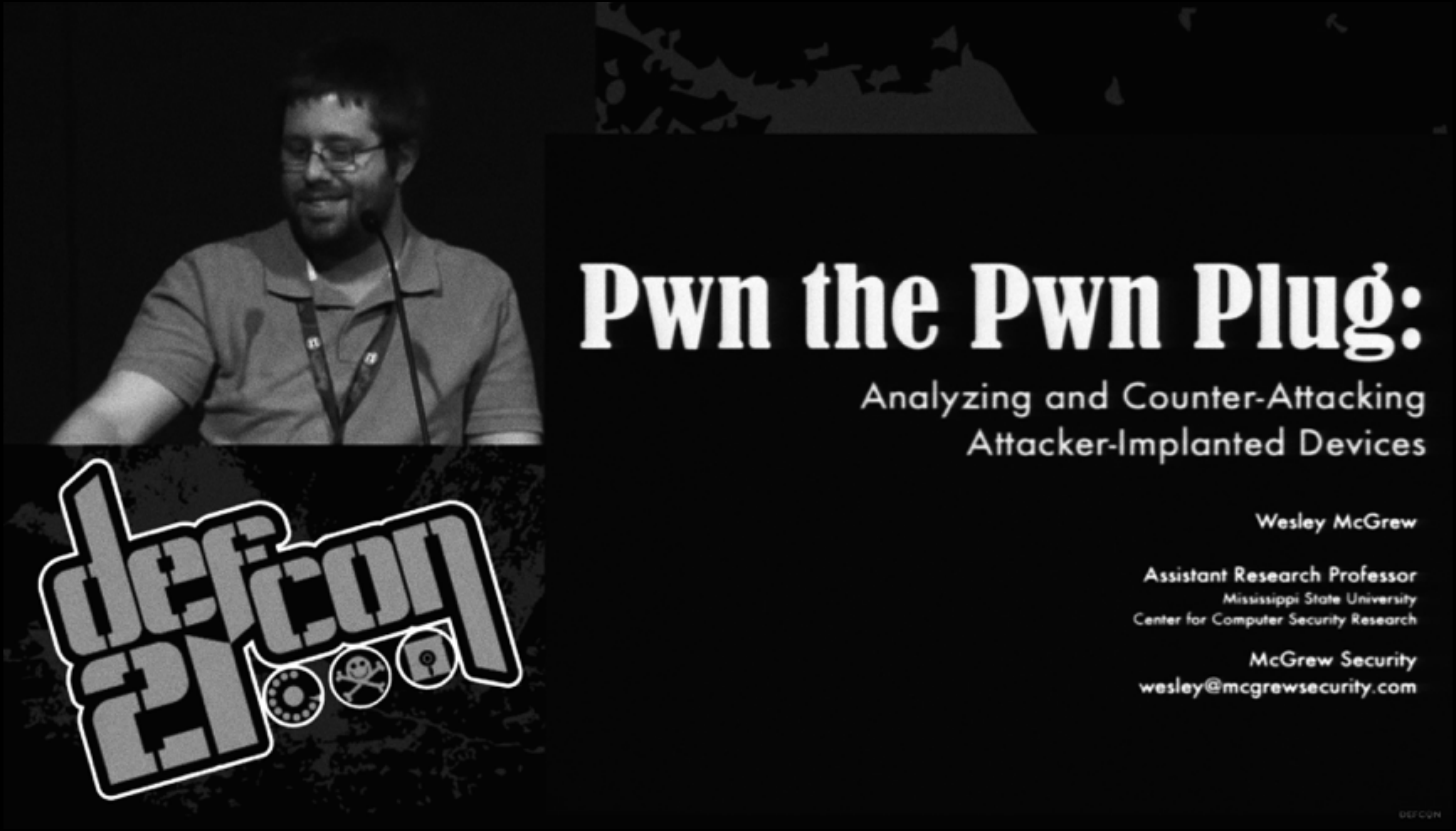
Introduction

- Wesley McGrew
  - Distributed Analytics & Security Institute, Mississippi State University
  - Halberd Group
- Vulnerabilities, Reverse Engineering, Forensics, Cyber Operations
- @McGrewSecurity wesley@mcgrewsecurity.com

What we're talking about today...

- Operational Security for Penetration Testers
  (whilst trying to not rip off The Grugq)
- Communication and Data Security Issues
  (not just "bugs")
- Illustrating and Classifying Risks Posed by Your Tools
- Recommendations
- For penetration testers and those who hunt them…

Previously . . .



Pwn the Pwn Plug:

Analyzing and Counter-Attacking
Attacker-Implanted Devices

Wesley McGrew

Assistant Research Professor
Mississippi State University
Center for Computer Security Research

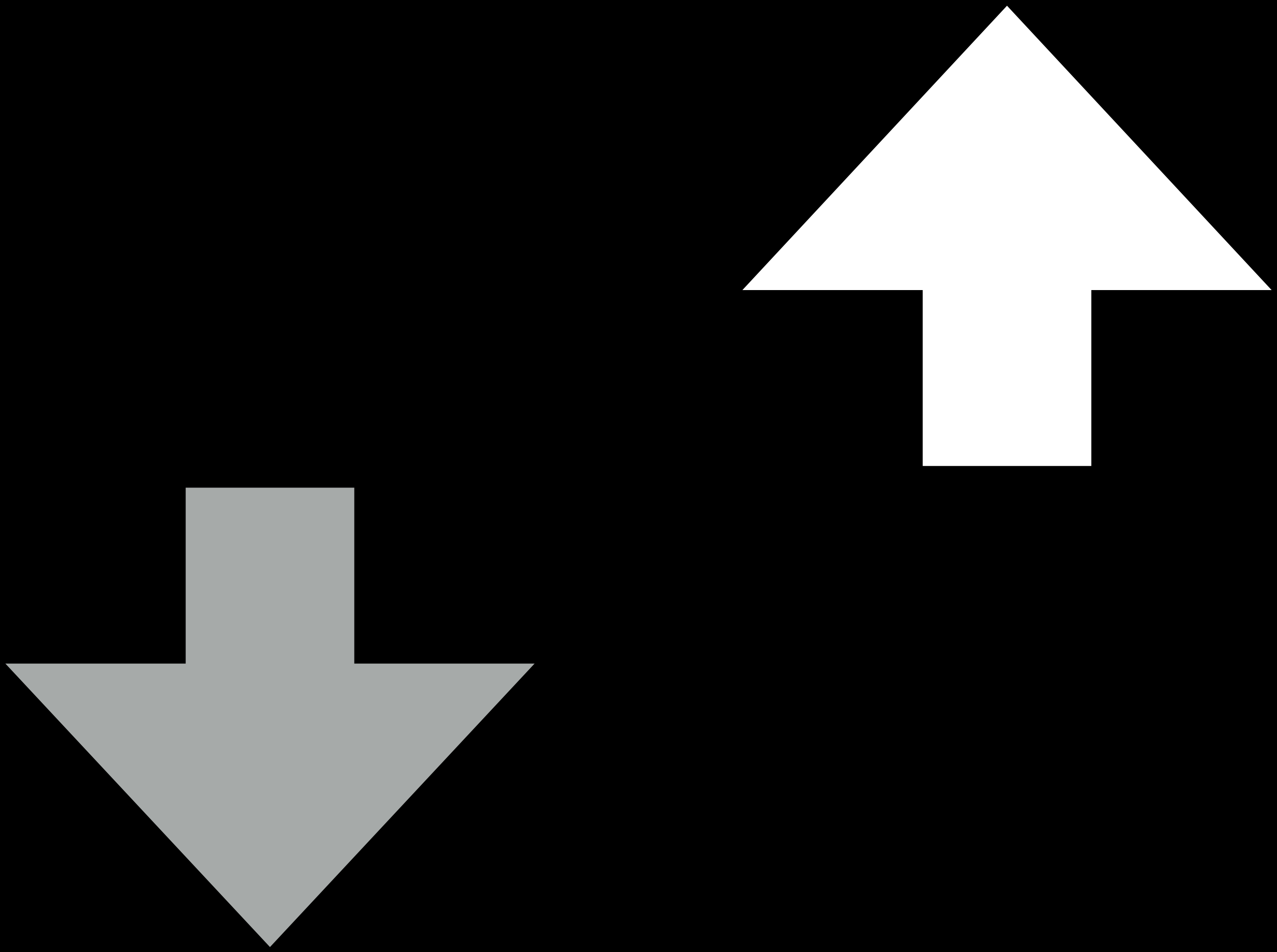
McGrew Security
wesley@mcgrewsecurity.com

Previously ...

Previously ...

@IHuntPineapples

Value of Pen Testing Data

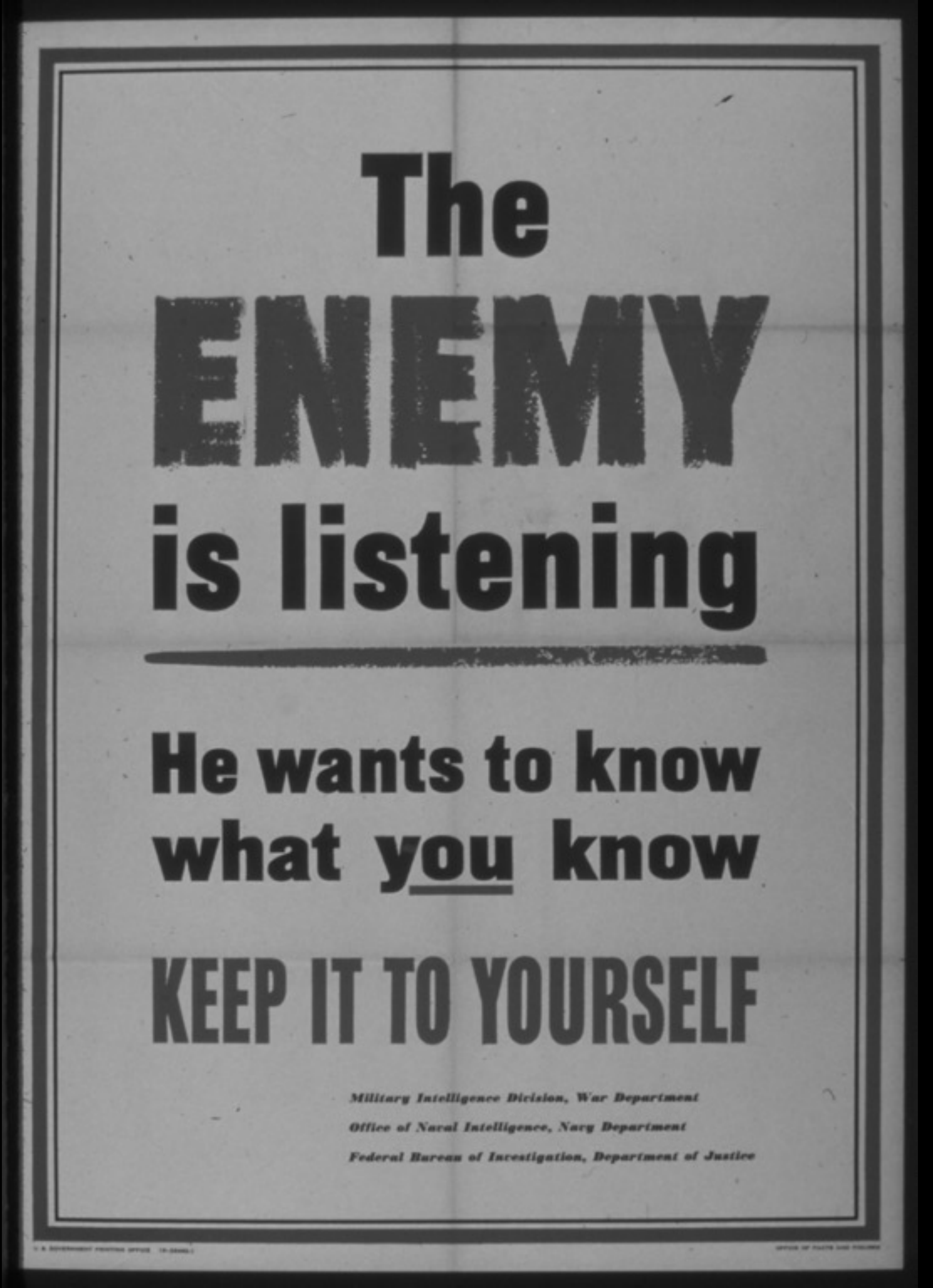


Awareness/Understanding
of Risk/Vulnerabilities

Counter-Intuitive

- Penetration testers, presumed experts of offense, largely aren't mindful of their own security.
- Reasons
    - Training - Classes, books, certifications
    - Toolchain maturity
    - Lack of documented incidents

When we lack the
capability to
understand our tools,
we operate at the
mercy of those
that do.



The

ENEMY

is listening

He wants to know
what you know

KEEP IT TO YOURSELF

Military Intelligence Division, War Department
Office of Naval Intelligence, Navy Department
Federal Bureau of Investigation, Department of Justice

U. S. GOVERNMENT PRINTING OFFICE [illegible]

OFFICE OF FACTS AND FIGURES

Assumptions Regarding Realistic Attacks

- An attacker may operate with sophistication, skill, and resources that exceed that of the targeted pentester

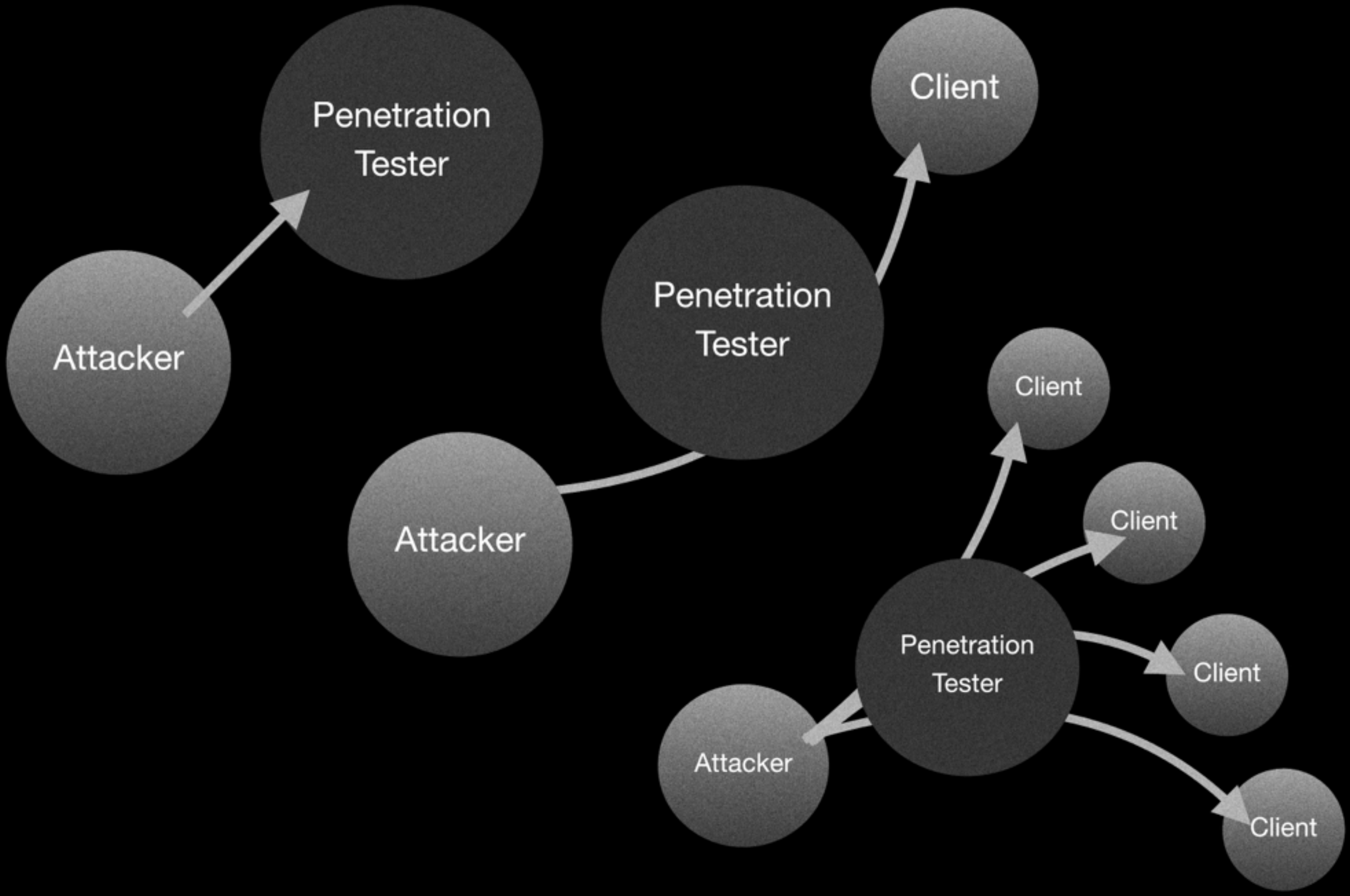
    - (Maybe this work can repair the imbalance)

- May be positioned physically/network-wise convenient for interception and modification of traffic

    - MiTM may not be feasible for general skiddie schemes, but makes sense in this context

Goals

- Victimology: Is the ultimate target…
  - The penetration tester?
    - Firm information used for fraud
    - Sabotage
    - Embarrassing leak (zf0-esque)
  - The client(s)?
    - Sensitive information
    - Vulnerabilities
    - Persistence


Penetration Tester
Attacker
Client
Penetration Tester
Attacker
Client
Client
Client
Penetration Tester
Client
Attacker
Client

Why this is attractive

- Penetration tester exist outside of the client’s culture/structure
    - …yet wind up with extensive access
    - …break technical/policy measures, by definition
    - …already ought to look like good attackers, why not ride along?
- Theft of tools and techniques (if they’re any good)
    - Private exploits, feeds, commercial tools
- Hide bugs from testers, prevent identification/remediation
- Smoke screen

Operational Security Issues

- Standalone Exploits' Payloads
  - Rarely annotated, testers frequently not trained in disassembly/ comprehension
  - Frequently acquired in desperation, wielded without discretion
  - Each encoded string and payload represents a part of the exploit's code that the penetration tester must either fully understand or place trust in by association with its source.
- Trust decision forced by he lack of training and skill in programming, vulnerability analysis, and exploit development among penetration penetration testers.

Operational Security Issues

- From an early draft
  - “Many websites where exploits are distributed, including the popular Exploit Database, operate over plaintext HTTP, which would allow an attacker in the right position to man-in-the-middle rewrite or replace exploit code being downloaded by penetration testers.”
  - This is no longer true for exploit-db.com! Kudos!

Operational Security?

- Exploitation
  - How to compromise a system, without “everyone” knowing how you compromised the system?
  - How to prevent them from modifying your payload?
- Tunnelling to dropped/installed appliances to reduce exposure?

Metasploit,
The Gold Standard

- Most versatile free payload: Meterpreter
- Supports encryption since 2009
  - Primarily for evasion?
  - How to establish keys, secure communication against an attacker who gets involved EARLY in the process?

Extending the Network

- Low-power physical implants
  - Rogue WiFi
  - Cellular Data
  - SMS
- Are out-of-band extensions opening up attack surface/ intercept opportunities?

Data at Rest

- Exfiltrated data, information for reports… what are you storing?
- Where is it located?
- Implanted devices? Physically secure?
- Data encrypted? If volume-based, how much time does it spend unlocked?
- Where are the keys? Who has access?
- Secure deletion? When?

Point of Contact Communications

- Communications
  - Scoping
  - Emergency contacts during tests
  - Report delivery

Classifying Tool Safety

- Dangerous - May cause vulnerability. Known vulnerabilities, or communications clearly subject to interception/modification
- Use With Care - Defaults that lead to Dangerous situation, but can be configured in a way that mitigates risk
- Naturally safe - Defaults to secure communications, safe for normal use cases
- Assistive - Non-penetration-testing attack tools, but can be utilized to help with concerns above
- Imperfect: Ex. so few pentesting tools protect saved results, it isn't even considered here

Example: Tools in Kali

Tool	Classification	Rationale
BeEF	Dangerous	Default pen tester interface is HTTP listening for connections from anywhere, with a default username and password. Recommend at least configuring/firewalling it to only listen on the localhost (or specific remote ones), changing passwords in the config file. Hooked clients communicate with the server via unencrypted HTTP, which may be unavoidable. This is incredibly useful software, though, just be *very* careful with where it's deployed and where the hooked clients are.
sqlninja	Use With Care	Interacts with the target database over a vulnerable web application, so communications-wise you're at the mercy of the target application being accessible over HTTPS. Be mindful of where you launch this from when targeting HTTP-only apps.
dirbuster	Use With Care	This classification could be valid for nearly any scanning software. If pointed at unencrypted services (in this case, HTTP), then your findings are essentially shared with anyone listening in.
searchploit	Assistive	By providing a mechanism for searching a local copy of the Offensive Security Exploit Database acquired as a secure package that would otherwise be accessed through the non-HTTPS exploit-db.com, this tool provides a set of standalone exploits that have gone through at least some vetting.
Metasploit exploitation with Meterpreter payload	Use With Care	Metasploit has a lot of functionality, but specifically for launching an exploit and deploying a meterpreter payload, the communication channel is fairly safe. An attacker may be able to observe and conduct the same attack, though.
SET with Meterpreter payload	Use With Care	Similar rationale as Metasploit. The resulting channel is safe, unless you are hijacked on the way there.
cymotha	Dangerous	None of the provided injectable backdoors offer encryption. Could potentially modify this to include some more robust backdoors, or use the "script execution" backdoor to configure an encrypted channel.
nc	Dangerous	Good old vanilla netcat, like your favorite book/trainer taught you, gives you nothing for communications security.
ncat	Naturally Safe	Netcat, but with SSL support that one can use. You'll need to set up certificates for it.

Security of Implantable Devices

- Pwnie Express Pwn Plug 1.1.2
  - Pwn the Pwn Plug - DEF CON 23
  - Crafted packet > XSS > CSRF > Command Injection
- Hak5 WiFi Pineapple Mark V <2.0.0
  - Authentication bypass
  - Recent improvements
- Clone devices: WORSE
- Inherent problems with low-powered penetration testing devices

New Pineapple Stuff

Come to the talk.

Recommendations

- Check six.
- Test tools and exploits before operational use
- Be aware of exposed information
- Know the network environment between you and the target. Minimize it.

VALUE SIZE
COMPARE TO the active ingredient of TUMS® ULTRA STRENGTH
*See back panel
NDC 30142-103-27
Kroger®
FAST RELIEF OF UPSET STOMACH, HEARTBURN, AND ACID INDIGESTION
ULTRA STRENGTH
Antacid
Tablets
Calcium Carbonate USP 1,000 mg
Assorted Berry Flavor
Our Pharmacists Recommend
PAREVE
160
CHEWABLE

Recommendations

- Take care when extending networks
- Keep client data, at rest & in transit, encrypted
- Secure archiving, deletion between engagements
- Secure communication with client

Recommendations

- Stay Alert!
- Training, Education, Instruction
  - Paint a more realistic picture (or any picture at all) of the network environment between the attacker and the target
  - Post-exploitation focus on establishing secure command and control, exfiltration

Contributions? Hopes and Dreams?

- Reduced client exposure
- Improved tools and training
- Maturity and advancement of penetration testing as a profession
    - (I’m not holding my breath but maybe you could give it a shot)

Questions?

I'll be around.

(or, contact Wesley)
wesley@mcgrewsecurity.com   @mcgrewsecurity