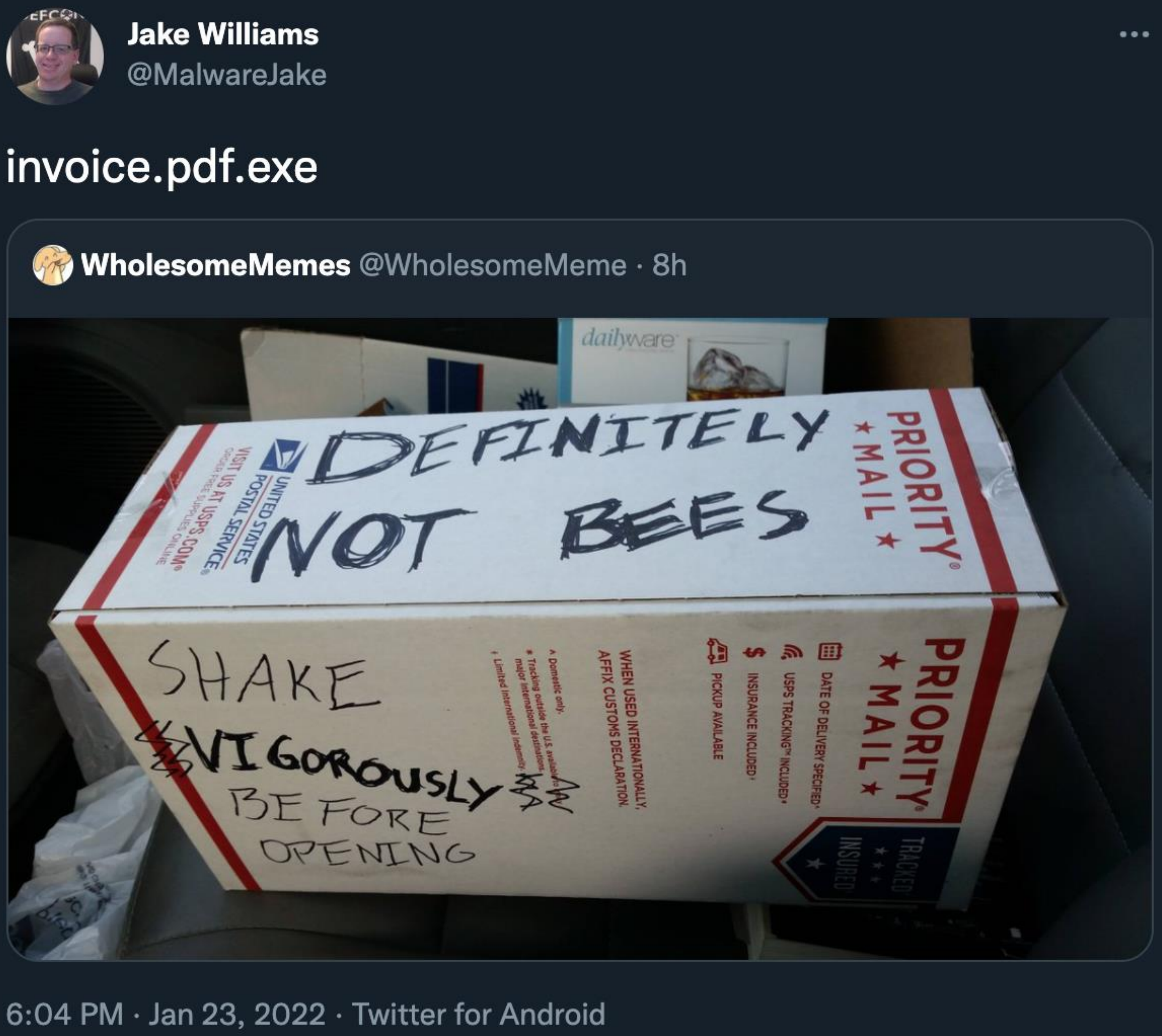


Jake Williams
@MalwareJake

invoice.pdf.exe

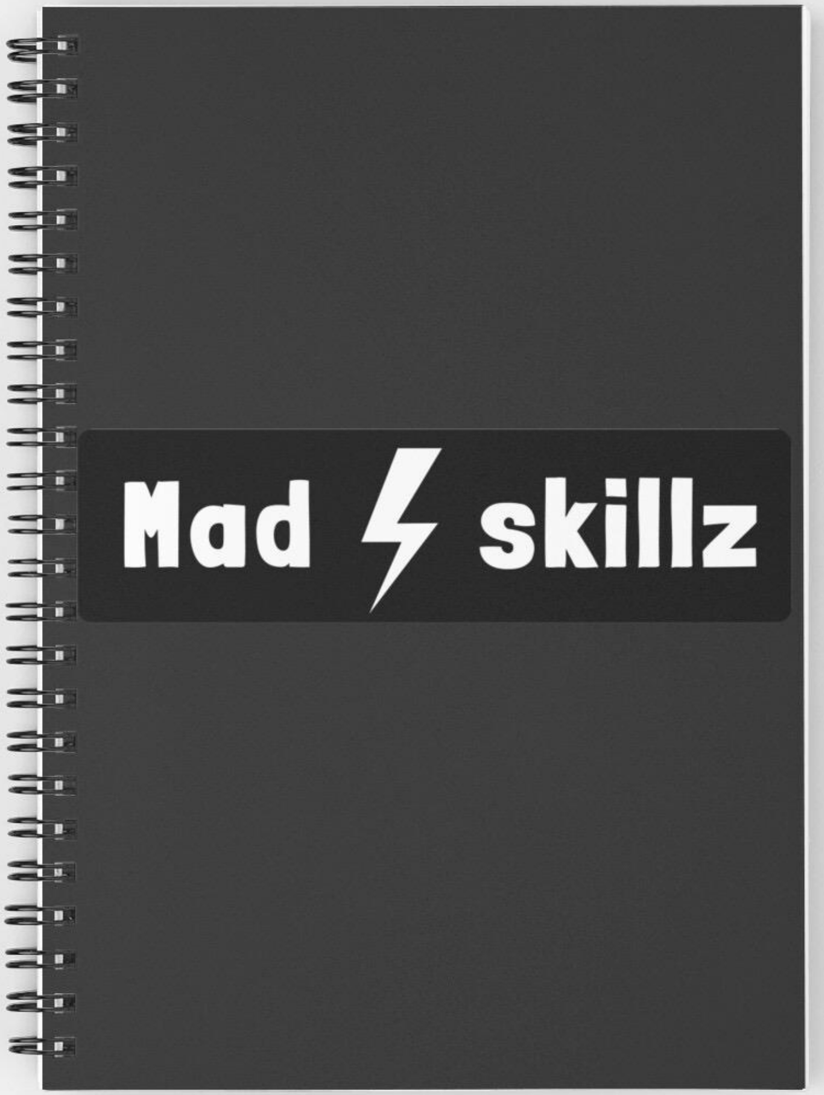
WholesomeMemes @WholesomeMeme · 8h

DEFINITELY NOT BEES
SHAKE VIGOROUSLY BEFORE OPENING
PRIORITY MAIL
UNITED STATES POSTAL SERVICE
VISIT US AT USPS.COM
DATE OF DELIVERY SPECIFIED
USPS TRACKING INCLUDED
INSURANCE INCLUDED
PICKUP AVAILABLE
WHEN USED INTERNATIONALLY, AFFIX CUSTOMS DECLARATION.
TRACKED
INSURED
dailyware

6:04 PM · Jan 23, 2022 · Twitter for Android

Penetration Testing: Overview

- Let’s dive right in and learn some leet skillz!



© BCCL 2020. ALL RIGHTS RESERVED.

All hackers wear a hoodie jacket, ski mask, steampunk goggles, and gloves while at work…

Let’s return to the LIGHT SIDE, shall we?

Ethical Hacking?

Penetration Testing?

Hacking

- Hacking: Manipulating computers into doing something they were not designed to do

(Evil) Hacking – Manipulating computers …. *without* permission

(Ethical) Hacking – Manipulating computers …. *with* permission and/or *intent* of improving security

Are our computers secure?

MegaCorp, Inc.

MegaCorp, Inc.

Leet Security Group, Inc.

Penetration Testing

- *Application of ethical hacking*
- Find security vulnerabilities in a target environment
  - *Think like a criminal – what tools and techniques are available to them?*
- Exploit these security vulnerabilities to gain access and acquire data
  - **Safely** and **professionally**
  - *Otherwise, you're as bad as the criminals!*
- Document vulnerabilities found and level of risk

Penetration Testing

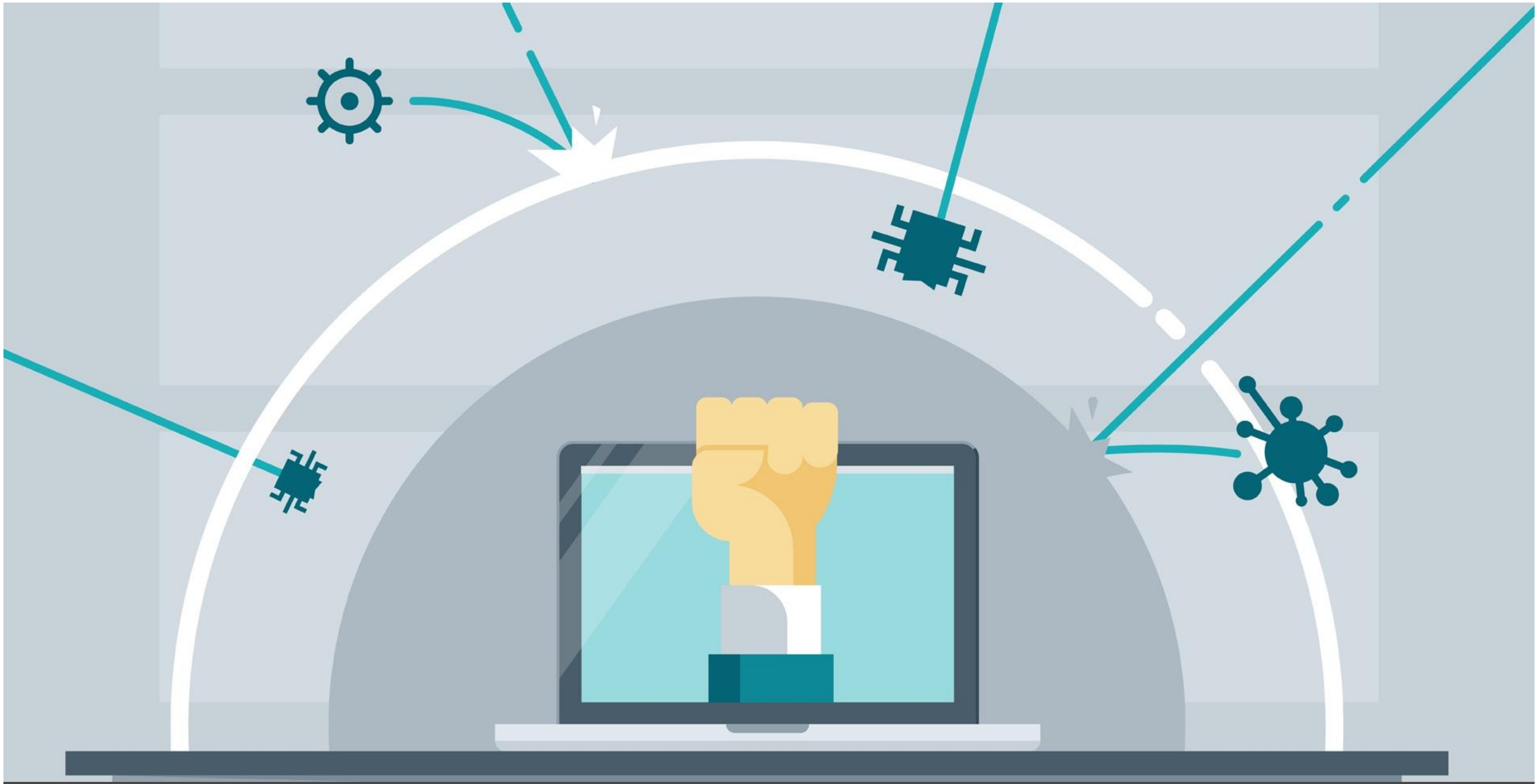
Penetration testers restrict their activities to only systems, machines, facilities, etc. which they have **explicit written permission** to test!

Why Penetration Testing?

- Find vulnerabilities before the criminals do
- Help *MegaCorp* to…
  - Understand and manage its risks
  - Prioritize resources to mitigate highest risks
  - Communicate to decision makers
- Penetration testing (with its emphasis on *exploiting* vulnerabilities) often produces more dramatic results than passive security audits

What Are We Testing?

- Any and all of the following, depending on *MegaCorp* requirements
  - Network servers & applications
  - Local clients & systems
  - Humans (e.g. social engineering)
  - Physical security (e.g. doors, locks, …)
  - Cryptography (a specialty in itself)



Business of Pen Testing

Business of Pen Testing

- Challenge: You are *intentionally* planning to break into *MegaCorp's* systems [virtually or physically]
  - What if you break into the wrong systems? (Either ones they didn't want to be tested, or even worse, not *MegaCorp's* systems at all!)
  - What if you cause damage as a result of your testing?
    - Downtime? Loss of data? PII data breach?
  - What if you embarrass someone powerful who wasn't part of arranging the pen test?

What if MegaCorp sics their expensive team of corporate lawyers on you?

Or calls the FBI?

Real-Life Example

COALFIRE®

- Coalfire is a company in the penetration testing business
  - Customers include major corporations, government agencies, etc.
  - Very legitimate & professional
- **Sept 2019**: “Men Arrested at Courthouse Say They Were Sent to Test Its Security”
  - https://www.nytimes.com/2019/09/16/us/iowa-courthouse-burglary.html
  - Two contractors face charges of third-degree burglary [felony!] and possession of burglary tools

Real-Life Example

COALFIRE

- **Jan 30, 2020: "Charges dropped against pentesters paid to break into Iowa courthouse"**
- 12 hours in jail on felony third-degree burglary charges → misdemeanor trespass → dropped
- Disagreement between Iowa *State Court Administration* and Dallas County sheriff's department over who had authority to authorize physical pentest
- **Signed documents on permitted activities were unclear *(big problem when conflict arises!)***
  - Physical attacks, or social engineering?
  - Physical security tests after hours?
  - Lock-picking?

https://arstechnica.com/information-technology/2020/01/criminal-charges-dropped-against-2-pentesters-who-broke-into-iowa-courthouse/

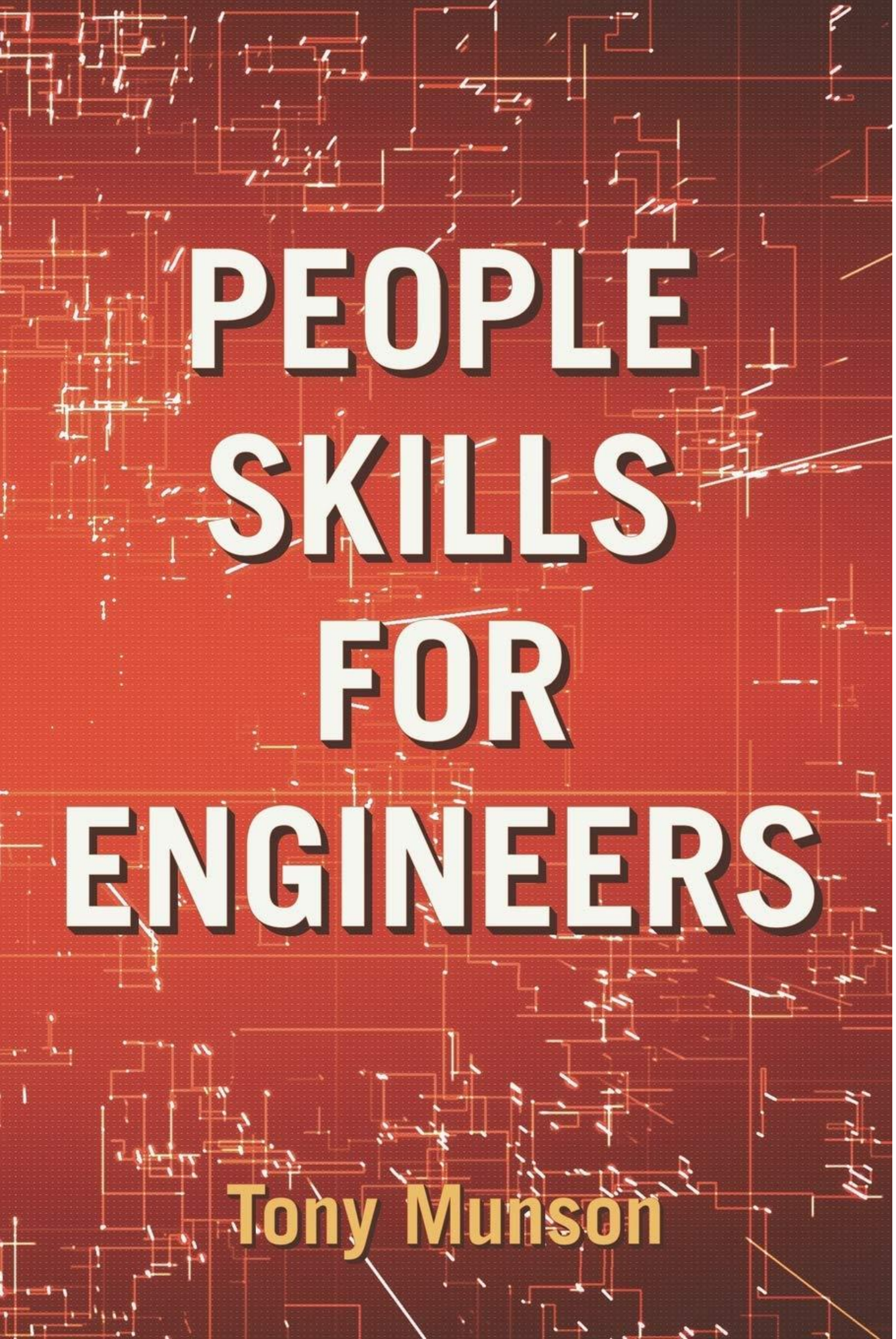
Real-Life Example

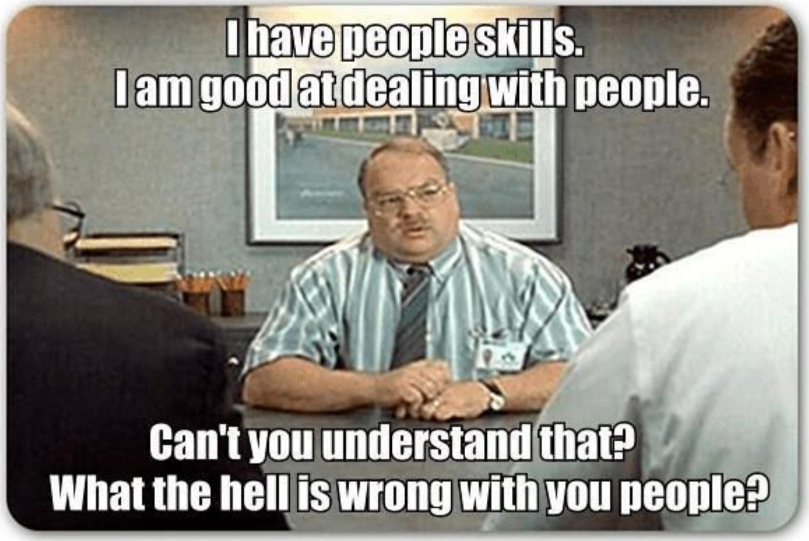
- *Sadly not the only example of real-life perils to pen testers…*
- What can be done to both protect yourself and increase chances of a successful / productive pen test?

Planning…

Communication…

Legal Documentation (Contacts, Disclosures, ….)


PEOPLE
SKILLS
FOR
ENGINEERS
Tony Munson


I have people skills.
I am good at dealing with people.
Can't you understand that?
What the hell is wrong with you people?

Prior to Work

- Clear communication with *MegaCorp* is essential prior to any pen testing work
- Deliverables
  - Rules of Engagement
  - Scoping Document
  - Non-Disclosure Agreement
  - Limitation of Liability and Insurance
  - “Get out of Jail Free Card”

Rules of Engagement

- Summarizes how the test should be conducted
- Signed and agreed upon by both pen testers and customers
- Protects you! *(if things go awry)*
- Improves likelihood of success *(by forcing conversation with MegaCorp prior to start of test)*

Rules of Engagement – Topics to Discuss

- **Test Scheduling**
  - When does the test start?
  - When does the test end? (~1-3 weeks…)
  - Can testing occur 24/7, or only outside normal business hours?
- **Regular briefings**
  - Schedule for these (daily, weekly?)
  - What have we done so far? Next steps?
  - Any significant discoveries?
  - Have we been discovered yet?

Rules of Engagement – Topics to Discuss

- **Contact information** for both parties
  - **Accessible 24/7** for duration of test
  - What if you break something?
  - What if you discover evidence of an ongoing attack?
  - What if they notice systems "acting funny"?
- Is the test **announced** or **unannounced** to the IT team?
  - Are we testing the IT team's response to intrusion?
  - May learn a lot, but an IT team that is actively fighting the pen testers (e.g. blocking their scans / IPs) can also make it challenging to do a comprehensive test

Rules of Engagement – Topics to Discuss

Black Box

- **No knowledge** of *MegaCorp's* network & systems?
- **Just like the attackers**
- Unless it's an inside job! (uh oh)

White Box (Clear Box)

- **Prior knowledge** of *MegaCorp's* network, systems, software?
- Faster / cheaper start to productive pen testing
- Safer? (Have an idea of what are mission critical systems)

Rules of Engagement – Topics to Discuss

- What happens if pen testers access / stumble upon **sensitive** or **confidential data** as a result of the test?
  - Default posture is typically that pen testers should *avoid* accessing personally identifiable information (PII) – Many pitfalls with laws (HIPPA, etc.)
  - Businesses *may* want a small sample of PII in order to understand exactly what data has been compromised
- Will *MegaCorp* employees observe the pen test team?

Documented,
Signed,
Sealed,
Dated

Scope of Work

- **What security concerns keep customer awake at night?**
  - Data leaks?
  - System downtime?
  - Persistent threats?
- **Perspective?**
  - External (internet) attacker with no prior knowledge
  - Internal attacker with credentials or internal network access

Scope of Work

- Specific systems to be tested?
  - Hostname, IP address, applications, …
- Specific systems to **not** be tested?
  - Hostname, IP address, applications, …
  - Maybe the system is too mission critical to risk
  - Maybe the system is known to be vulnerable and fragile (no need to waste $$ confirming that!)
- What about third party equipment? (networks, servers, etc…)
  - Explicit written permission needed for those too!

Scope of Work

- What about cloud providers specifically?
  - Example: Amazon Web Services (AWS)

AWS Customer Support Policy for Penetration Testing
AWS customers are welcome to carry out security assessments or penetration tests against their AWS infrastructure without prior approval for 8 services…

Permitted Services

- Amazon EC2 instances, NAT Gateways, and Elastic Load Balancers
- …

Only a **small** subset of AWS services!

Prohibited Activities

- Denial of Service (DoS), Distributed Denial of Service (DDoS), Simulated DoS, Simulated DDoS
- Port flooding
- Protocol flooding
- Request flooding (login request flooding, API request flooding)
- …

https://aws.amazon.com/security/penetration-testing/

Scope of Work

- What about cloud providers specifically?
  - Example: Amazon Web Services (AWS)

AWS Customer Support Policy for Penetration Testing

Note: Customers are not permitted to conduct any security assessments of AWS infrastructure, or the AWS services themselves.

What does this mean?
Why might a customer ask for this?

Other Simulated Events (<u>formal approval required in advance</u>)

- *Red/Blue/Purple Team Testing*
- *Network Stress Testing*
- *DDOS Simulation Testing*
- *Simulated Phishing*
- *Malware Testing*

https://aws.amazon.com/security/penetration-testing/

Scope of Work

Test Environment?

- No confidential data to protect
- No concerns about crashing critical systems

Production Environment?

- Test environment may not exist or may not fully/realistically model the deployed environment
- **Most common scenario** (despite risks)

Scope of Work

- **Methods permitted?**
  - Port scans
  - Ping sweeps
  - Vulnerability scans
  - Penetration / exploitation
  - Application-level testing & manipulation
  - Pivoting (using one system to attack another, e.g. external->internal access)
  - Client systems (i.e. office admin desktop)
  - Physical penetration (lock picking, etc…)
  - Social engineering

Scope of Work

- **Methods permitted?**
  - **Denial of service?**
    - Check to see if a a DOS is possible (perhaps by checking application version) but don't launch?
    - Or … actually attempt it to confirm vulnerability?
    - Customer may have "concerns" if this is done during normal business hours!
  - **Other dangerous tests?**
    - Some probes (particularly to known-vulnerable applications and services) **may cause a system crash**
    - Useful information to know! But also impacts the real-world business environment…
    - No pen tester can promise "100% zero risk" testing

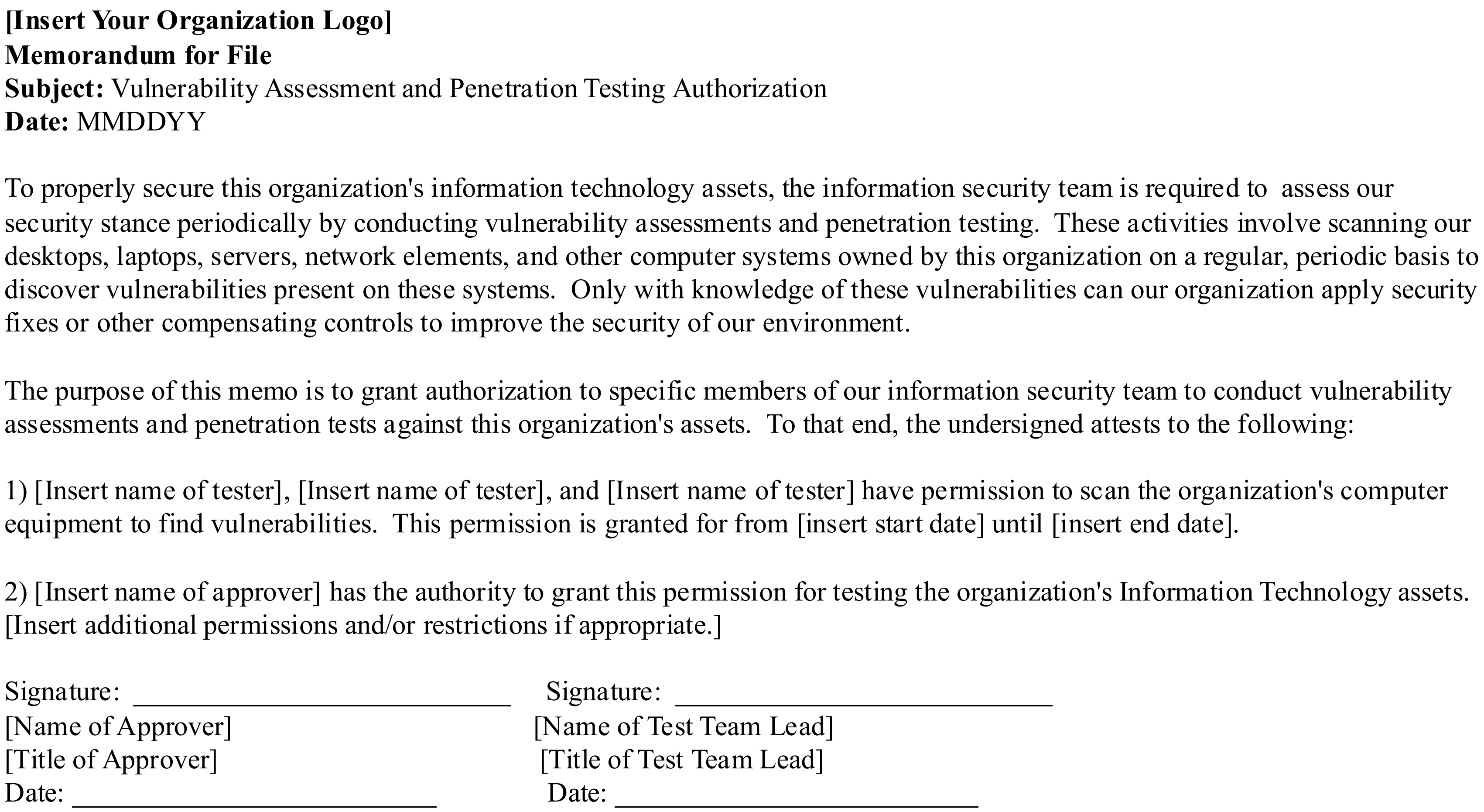
Documented,

Signed,

Sealed,

Dated

“Get Out of Jail Free” Card



[Insert Your Organization Logo]
Memorandum for File
Subject: Vulnerability Assessment and Penetration Testing Authorization
Date: MMDDYY

To properly secure this organization's information technology assets, the information security team is required to assess our security stance periodically by conducting vulnerability assessments and penetration testing. These activities involve scanning our desktops, laptops, servers, network elements, and other computer systems owned by this organization on a regular, periodic basis to discover vulnerabilities present on these systems. Only with knowledge of these vulnerabilities can our organization apply security fixes or other compensating controls to improve the security of our environment.

The purpose of this memo is to grant authorization to specific members of our information security team to conduct vulnerability assessments and penetration tests against this organization's assets. To that end, the undersigned attests to the following:

1) [Insert name of tester], [Insert name of tester], and [Insert name of tester] have permission to scan the organization's computer equipment to find vulnerabilities. This permission is granted for from [insert start date] until [insert end date].

2) [Insert name of approver] has the authority to grant this permission for testing the organization's Information Technology assets. [Insert additional permissions and/or restrictions if appropriate.]

Signature: ______________________________
[Name of Approver]
[Title of Approver]
Date: _____________________________

Signature: ______________________________
[Name of Test Team Lead]
[Title of Test Team Lead]
Date: _____________________________

Example at http://www.counterhack.net/permission_memo.html

Limitation of Liability

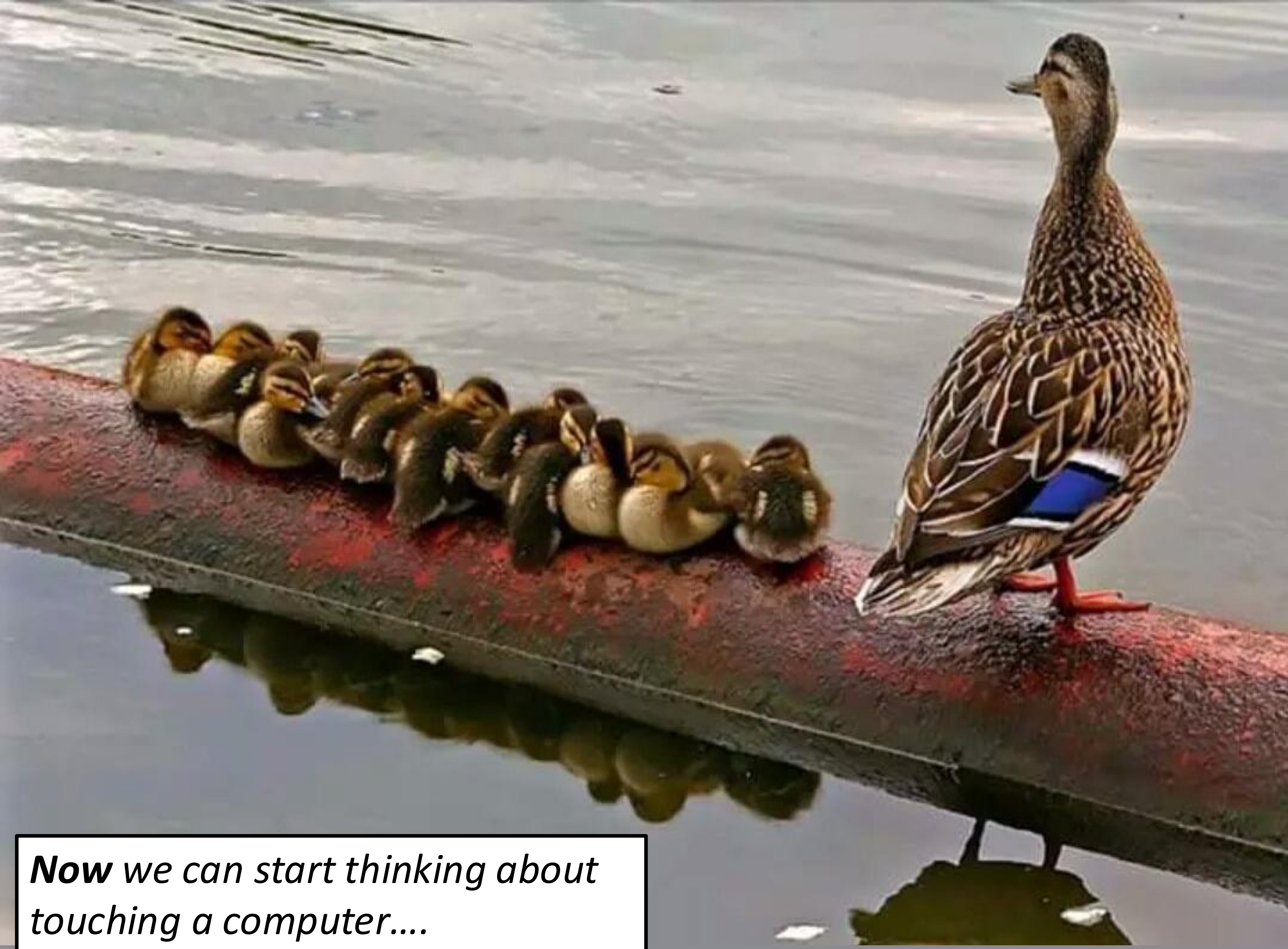
- You need your own lawyer and professional advice!
- Limitation of Liability agreement
  - Cap damages (liability) associated with penetration testing activity
  - Ideally limited to to the cost of the test itself
- Intellectual property agreement
  - Are test documents (covering both *methods* and *results*) the property of the testers or of the customer?
- Knowledge of applicable laws in both your country and the country where target systems are located

Documented,

Signed,

Sealed,

Dated



Now *we can start thinking about touching a computer….*

Q
A
Answer

Schedule

Due

- Lab 1: VM Setup
  - **Due Today**
- *Note: You should have CTC 214 card swipe access enabled this week…*

Upcoming

- Lab 2: Reconnaissance
  - **Start Thursday**
  - Due in 1 week