ANATOMY OF A PEN TEST

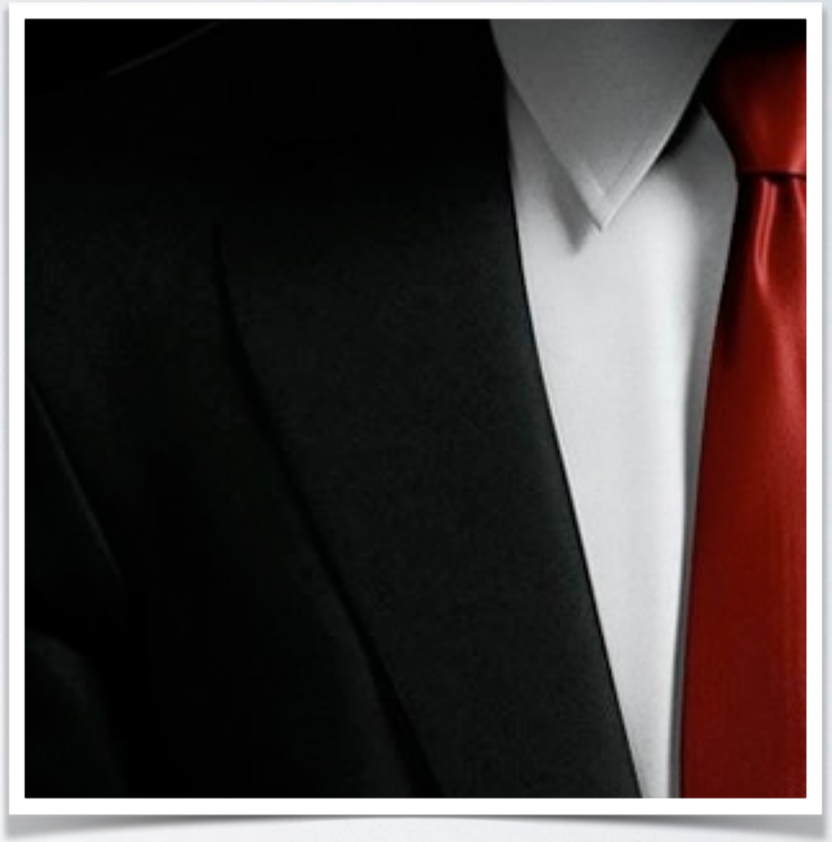
Understanding the [Mindset | Toolset] of Penetration Testers

ANATOMY OF A PEN TEST

Poppin' Boxes Like a Pro

Profile

Alijohn Ghassemlouei



- Handle == [PushPin | Revolver]
- DEF CON Attendee - DC15 - Present[1]
- U.S. Department of Energy Contractor - A few years[3]
- Co authored “The Hacker's Guide to OS X” - Kinda neat
- U.S. Department of State Contractor - For a bit
- Sony PlayStation - Now

Reality Check | Disclaimers

Hacking in movies != Reality

Running scripts != [Hacker | Pentester | Programmer]

Understanding core technologies are crucial

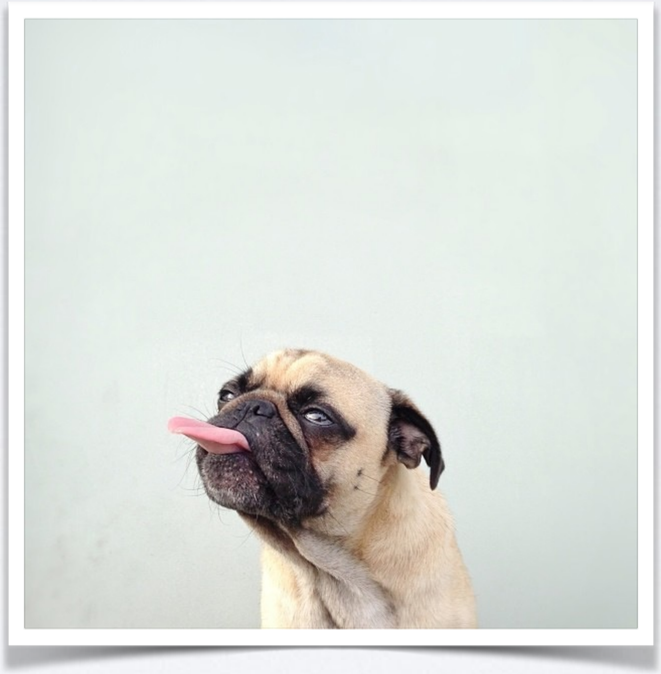
Overnight penetration tester? Hell no.

Developing and refining your skill set takes time

Documentation & boring stuff? Unfortunately, yes

Set expectations and common terminology early

Audience | Query



Audience | Query

What is your definition of a penetration test?

Considerations | Penetration Testing

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

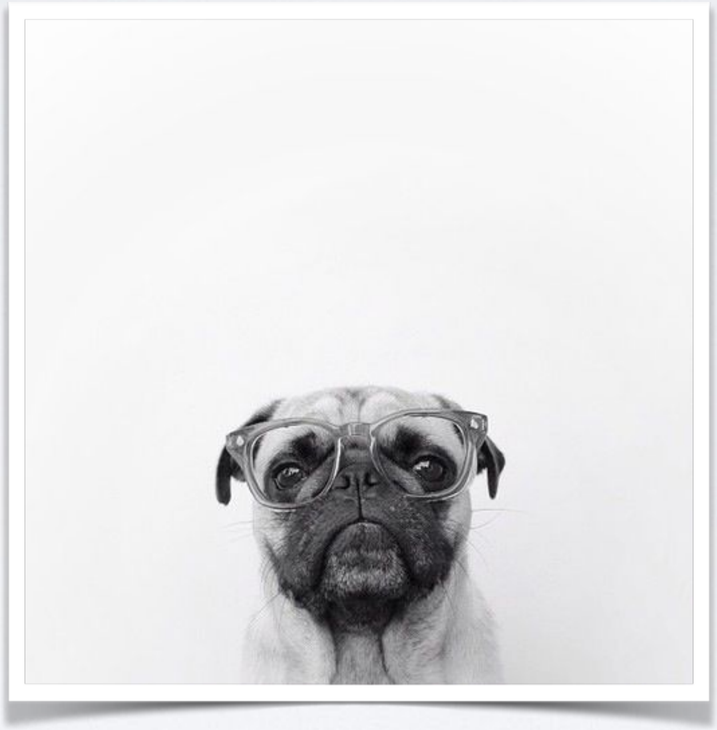
Considerations | Penetration Testing

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

Audience | Vote

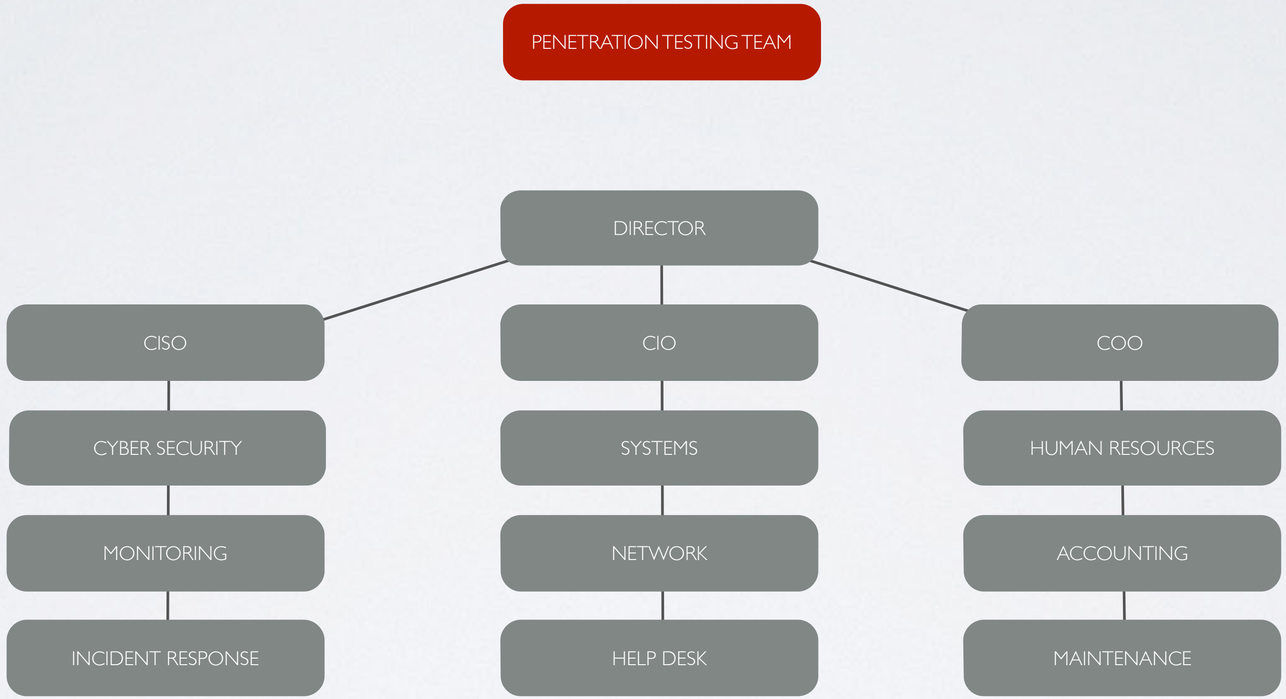


Audience | Vote

IN HOUSE or EXTERNAL

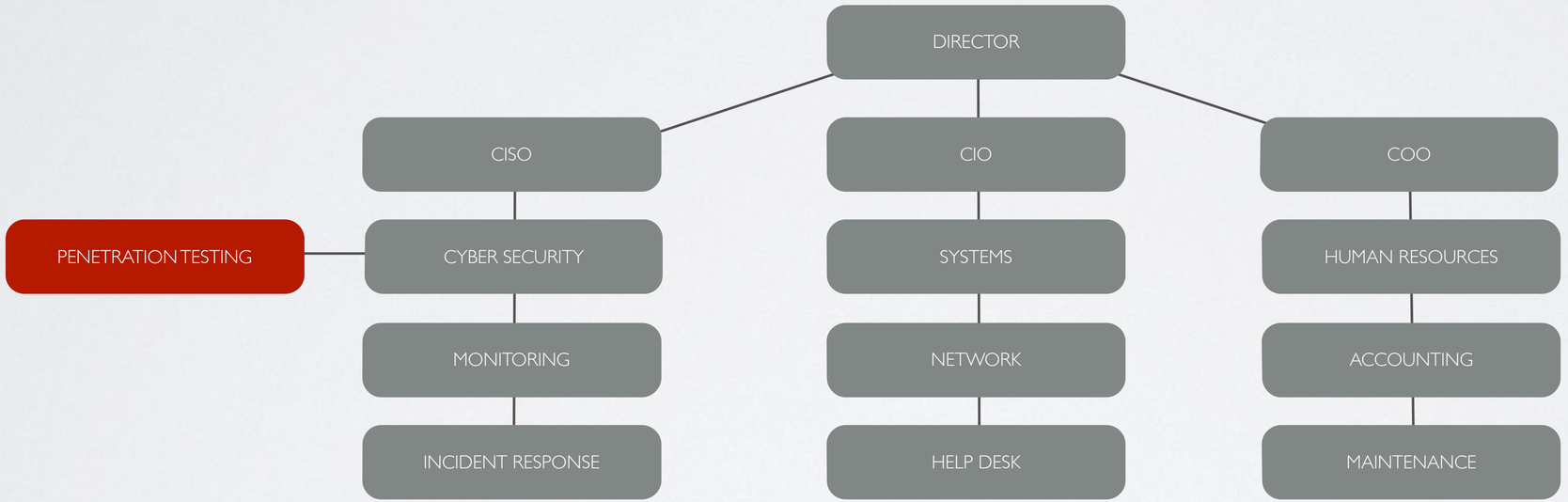
Placement | Penetration Testing

INDEPENDENT OVERSIGHT / THIRD PARTY / EXTERNAL ENT-TITTY



Placement | Penetration Testing

IN-HOUSE



Audience | Query

intelligent assholes

or

somewhat slightly less skilled but personable

Technical Team Members | General Information

Knowledge	Mindset	Personality	Presentation
Past Experience	Identification of true vulnerabilities	Detail Oriented	Communication
Tool Usage	Prioritization of identified vulnerabilities	Driven	Attire
Methodologies	Creativity	Lazy	Writing Ability
General Technical Knowledge	Observant	Cheeky	
Credentials	Meticulous	Always willing to learn	
	Knowing when to quit		

Objective

To enhance and improve the state of security throughout the organization through high profile and impactful assessments.

Yes, seriously.

Audience | Query

Audience | Query

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

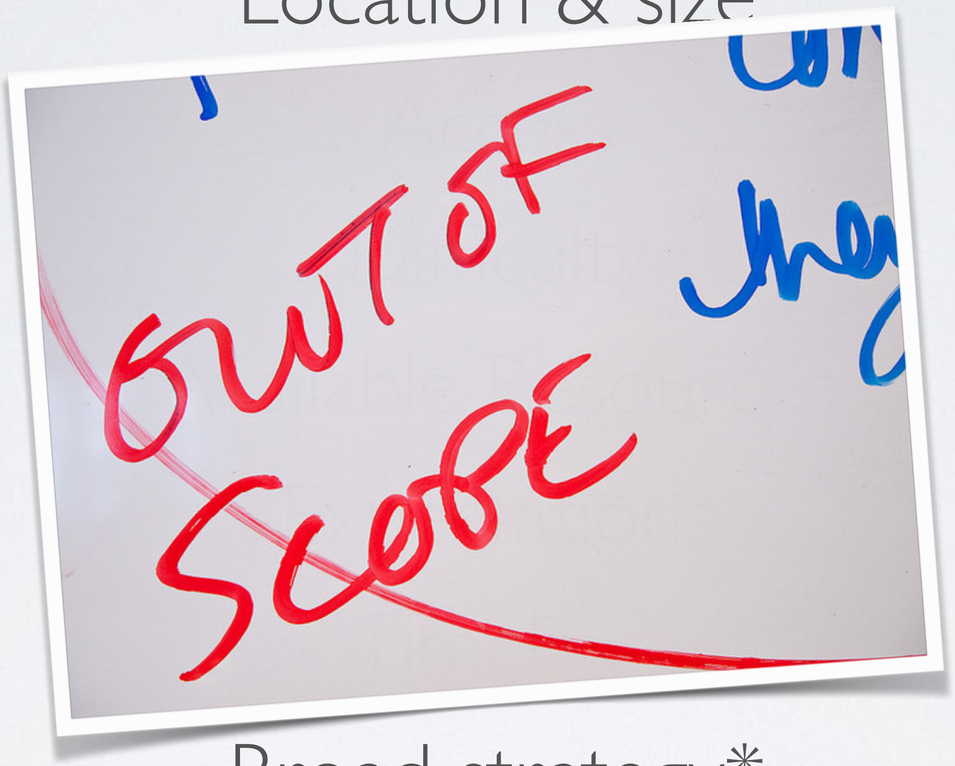
Expectations

Timeline

Broad strategy*

Scoping | Super Important General Information

Location & size



Broad strategy*

Timeline | Hybrid Assessment

	Reconnaissance	Attack		Reporting
S1	Scanning, site profile generation, and service detection with manual verification of potential vulnerabilities via exploitation.	Manual exploitation, establish foothold, migrate laterally, and complete objective.	Vulnerability scanning begins, web application scans begin.	Collect team notes and begin writing report.
S2	Review network layout, firewall configs, and gpo's.	see above	see above	Collect team notes and continue writing report.
S3	Interview administrators and responsible parties.	Continue exercise if objective has not been completed, otherwise begin testing site response capability.		Begin writing up findings and opportunities for improvement.
S4				Allow team lead to review notes, generate report, and send to management.

Rhetorical Question [STFU] | Query

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 cohesion[1]
  - Take notes as assessment occurs with daily synopsis[11]
  - Team member rotation to improve shared skillset / methodologies
  - Rules of Engagement

Software Tools | General Information

- General Unix/Linux/Windows Binaries[1]
  - nc, sed, awk, wc, vi,
  - tcpdump, grep, cut
  - net, dig, cat
- Nmap
- Nessus Professional Feed[2]
- 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[1]
  - 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

Hardware Tools | General Information

Understanding how to use a tool does not make you a skilled penetration tester

Hardware Tools | General Information

a hacker mindset is required

Poppin' the Truth | Boxes be Dropping

10,000 ft, oral, technical walkthrough of an attack

Poppin' the Truth | Boxes be Dropping

clear, condensed, overarching strategy/methodology

Potential Attack Avenues

Social Engineering[1]

Web Drive By

Misconfiguration[2]

Remote Exploitation

Lateral Migration

Zero Day

Custom Malware

Outline | Walkthrough

Goals

Locate & exfiltrate sensitive organization information

Stages

0 - Reconnaissance
1 - Phishing
2 - Exploitation
3 - Privilege Escalation
4 - Lateral Migration
5 - Data Exfiltration
6 -Tasteful Communication of Findings

Audience | Query

Audience | Query

How do you exfiltrate all your hard work?

Exfiltration* | Possibilities

SCP / FTP / HTTPS

DNS

CUSTOM

Exfiltration* | Possibilities

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[I]

Lack of Network Restriction & Segmentation[II]

Lack of Antivirus or HIDS

Reporting

- 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

Noteworthy Individuals | Thank You

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

Contact Information

EMAIL

pushpin@logicode-networking.com

WEBSITE

logicode-networking.com

BLOG

blog.logicode-networking.com

LINKEDIN

linkedin.com/in/alijohnghassemlouei