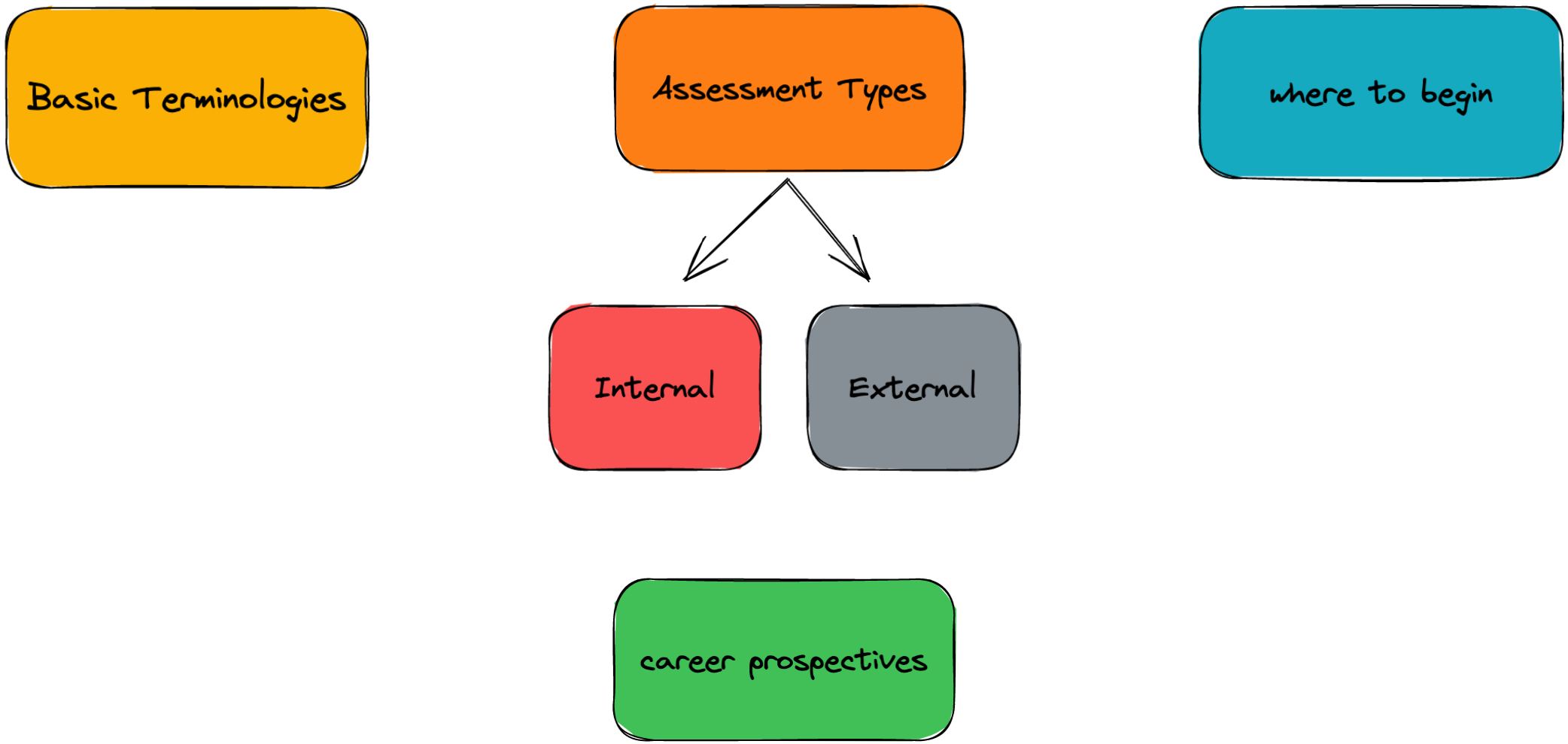
Offensive Security 1o1

Kartik Sharma

Northeastern University

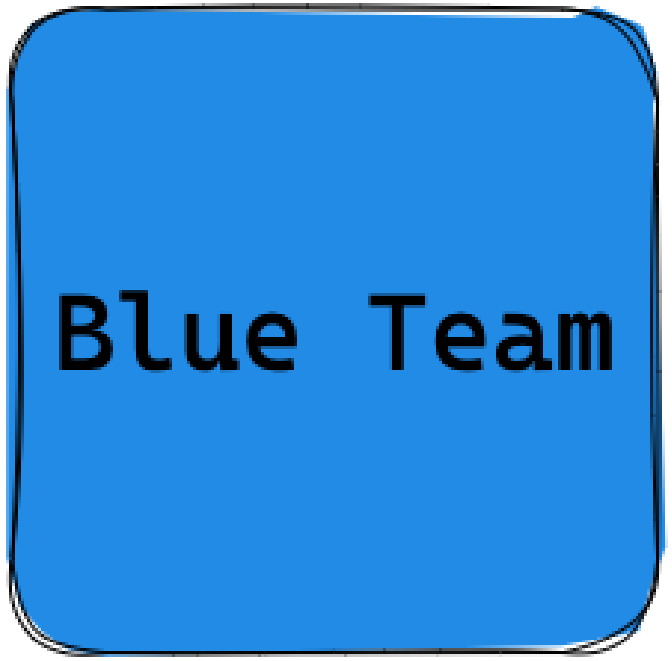
Offensive Security

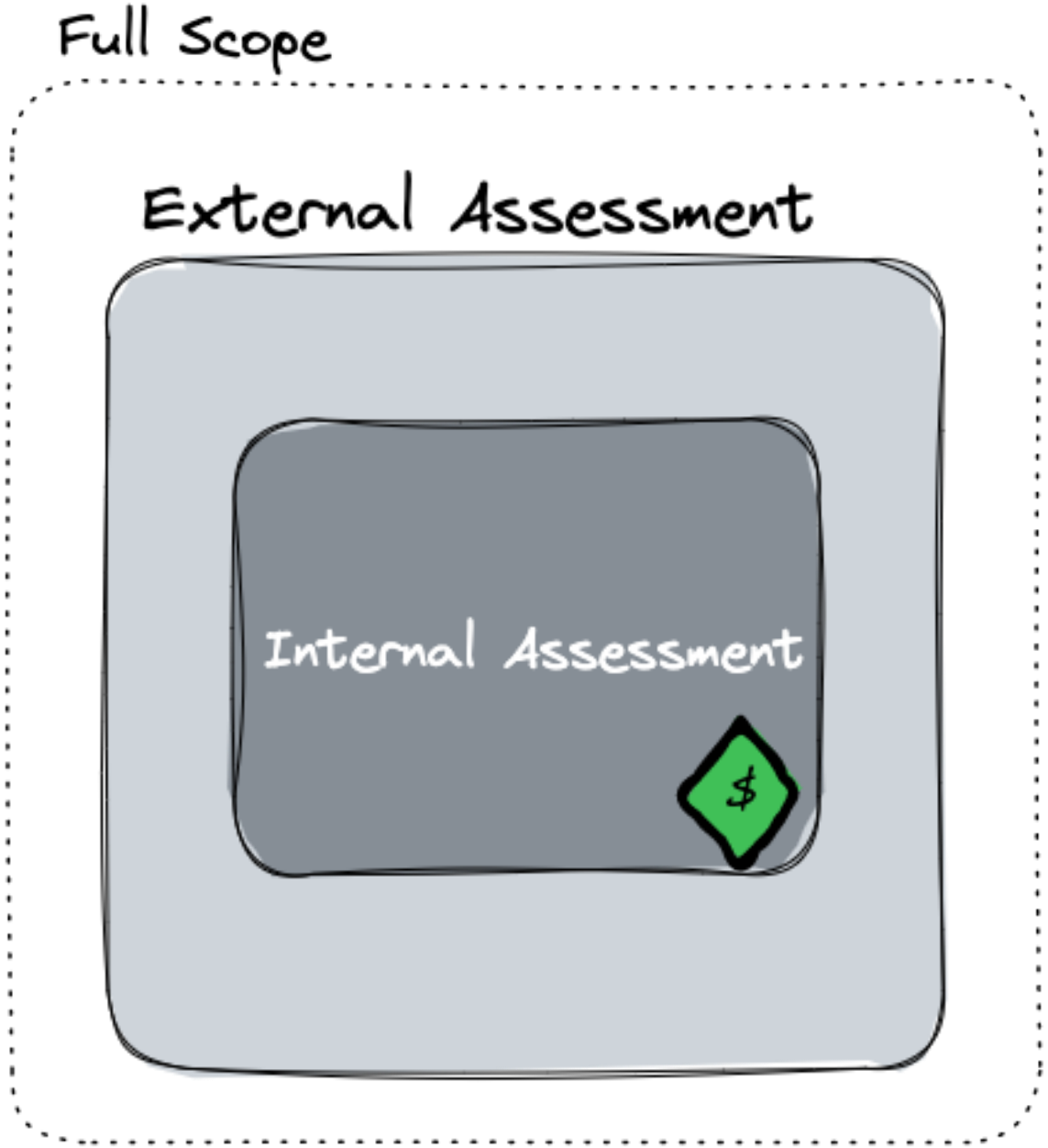
Definition: refers to the proactive approach of identifying and exploiting vulnerabilities in computer systems, networks, and applications with the aim of improving their security posture.


Basic Terminologies
Assessment Types
where to begin
Internal
External
career prospectives

Basic Terminologies

Types of Teams




Full Scope
External Assessment
Internal Assessment
$

External Assessment (1/3)

Application Layer

- Web Applications
- Mobile Applications
- Thick-client applications
- Network/Cloud

External Assessment (2/3)

Human Layer/Social Engineering

- Phishing/Smishing
- Vishing

External Assessment (3/3)

Physical Layer

- Wireless Security
- Tailgating
- Lockpicking
- Dumpster diving

Internal assessment

Low-privilege user assessment

- hardened machine
- low privileged Active Directory user

High-privilege user assessment

- Service accounts
- Domain admins
- Local admins

Other Important Terminologies (1/2)

Crown Jewels $

- AV server
- Domain controller
- Customer Transaction database

Other Important Terminologies (2/2)

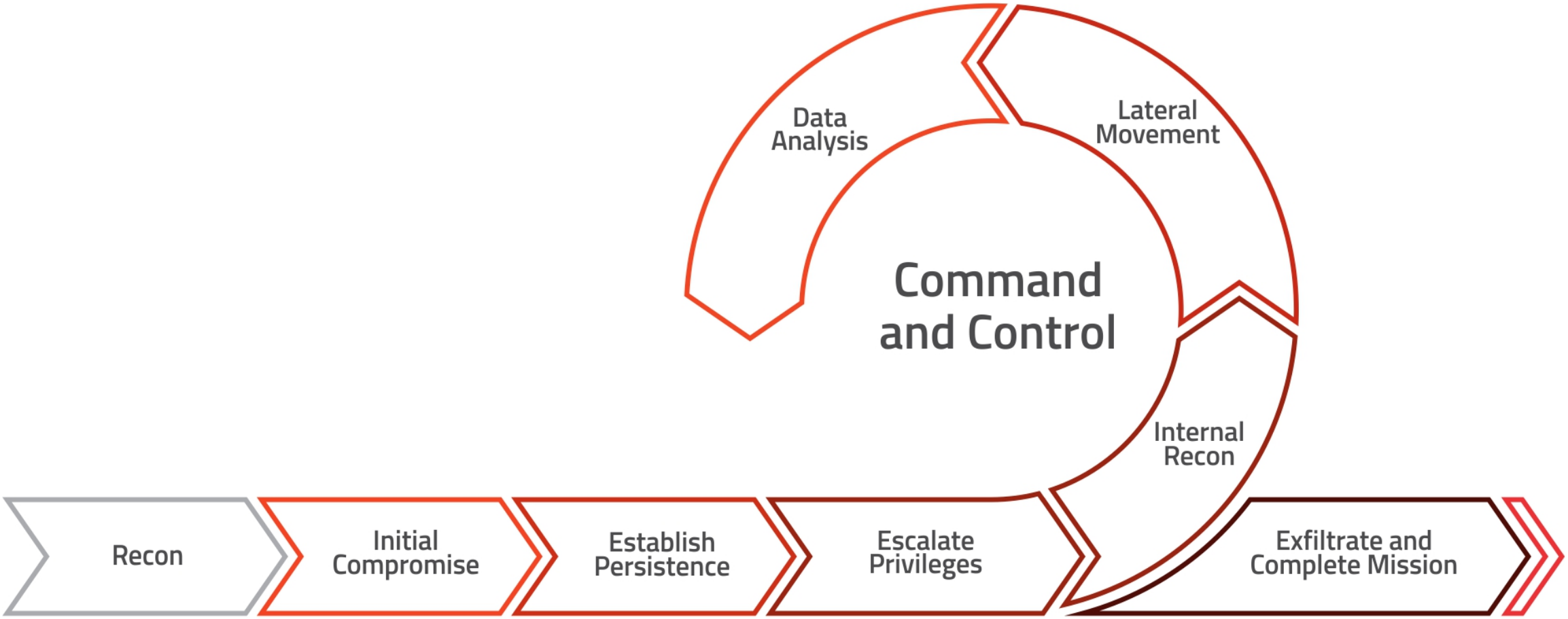
Full Scope Assessment

- Depends on the maturity of the organization
- Generally, involve both internal and external assets in-scope with listed crown jewels

Out of Scope assets and attacks

- Non prod assets
- DDoS/Phishing
- Live Hacking Event (Casinos were out of scope)

Red Team Assessment Lifecycle



External Assessment

Reconnaissance (1/3)

Asset Discovery

- Identifying the assets present in the scope of the assessment
- Active enumeration
- Passive enumeration
- Tool: amass (setup) [walkthrough]

Reconnaissance (2/4)

Content Discovery

- Identifying files, folders, etc
- Tool: ffuf

Wordlists

- Assetnote [link]
- Seclists [link]
- can be used for exploitation as well**

Reconnaissance (3/4)

Network Monitoring

- Masscan for identifying active hosts and open ports (Quickscan)
- NMAP for identifying the most common ports and service enumeration
- Shodan for monitoring (free credits)
- Write your own script for Network Monitoring**
  - CIDR -> resolve -> massscan -> nmap -> save results >> iterate

Reconnaissance (4/4)

Resources

- Jason Haddix Tesla recon [link]
- TraceLabs CTF (OSINT)

Exploitation (1/3)

Web Application Security

- OWASP Top 10
- Proxy Tools: BurpSuite [Walkthrough]

Resources:

- Jason Haddix Application Analysis
- Web Application Hacker's Handbook Chapter 21

1. A1-Injection
2. A2-Broken Authentication and Session Management
3. A3-Cross-Site Scripting (XSS)
4. A4-Insecure Direct Object References
5. A5-Security Misconfiguration
6. A6-Sensitive Data Exposure
7. A7-Missing Function Level Access Control
8. A8-Cross-Site Request Forgery (CSRF)
9. A9-Using Components with Known Vulnerabilities
10. A10-Unvalidated Redirects and Forwards

Exploitation (2/3)

API Security

- OWASP Top 10 for APIs
  - IDORS, Injections, Misconfigurations
- Resources
  - Hacking APIs (Corey J Ball)

API1:2019 — Broken object level authorization

API2:2019 — Broken authentication

API3:2019 — Excessive data exposure

API4:2019 — Lack of resources and rate limiting

API5:2019 — Broken function level authorization

API6:2019 — Mass assignment

API7:2019 — Security misconfiguration

API8:2019 — Injection

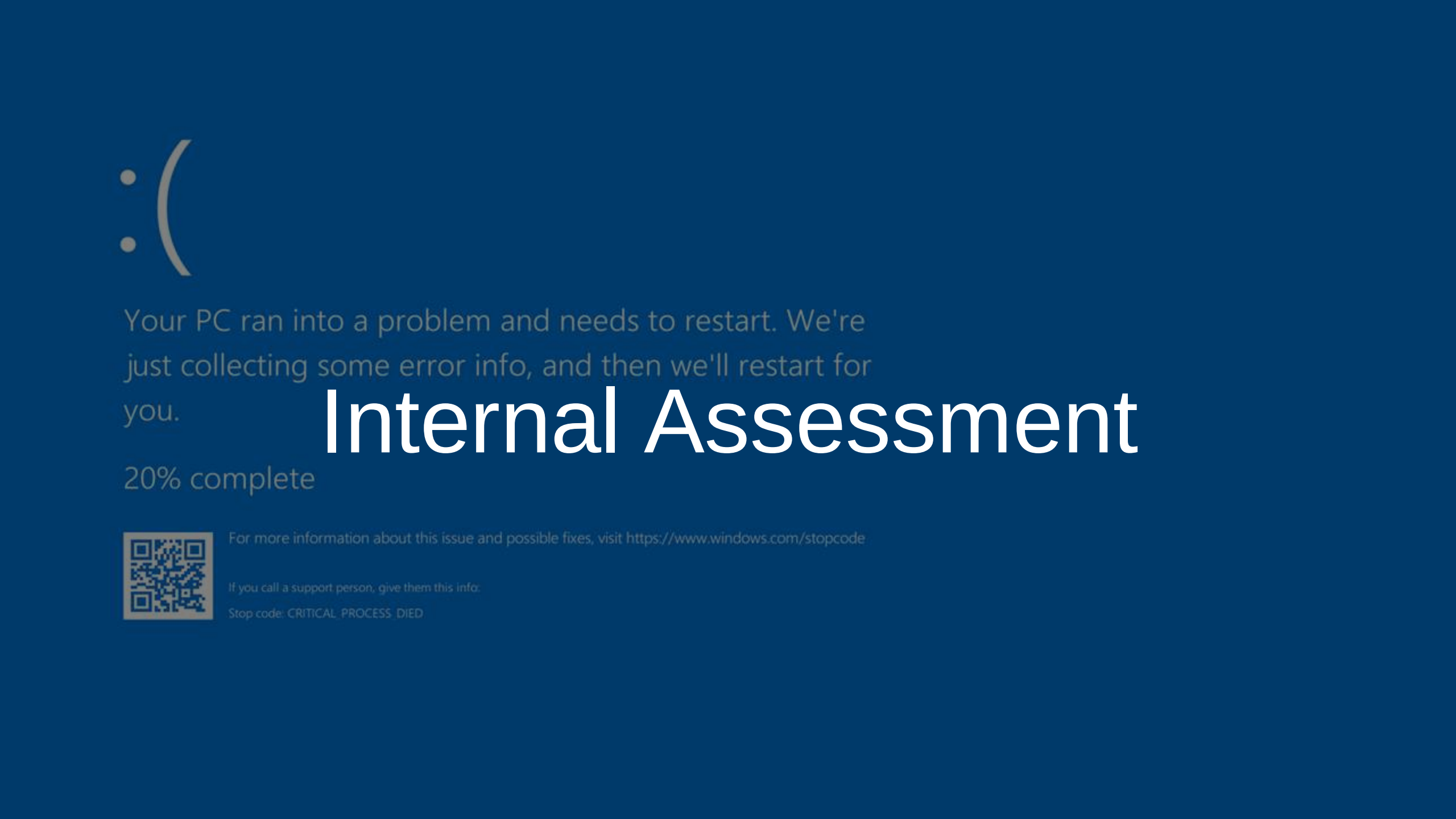
API9:2019 — Improper assets management

API10:2019 — Insufficient logging and monitoring

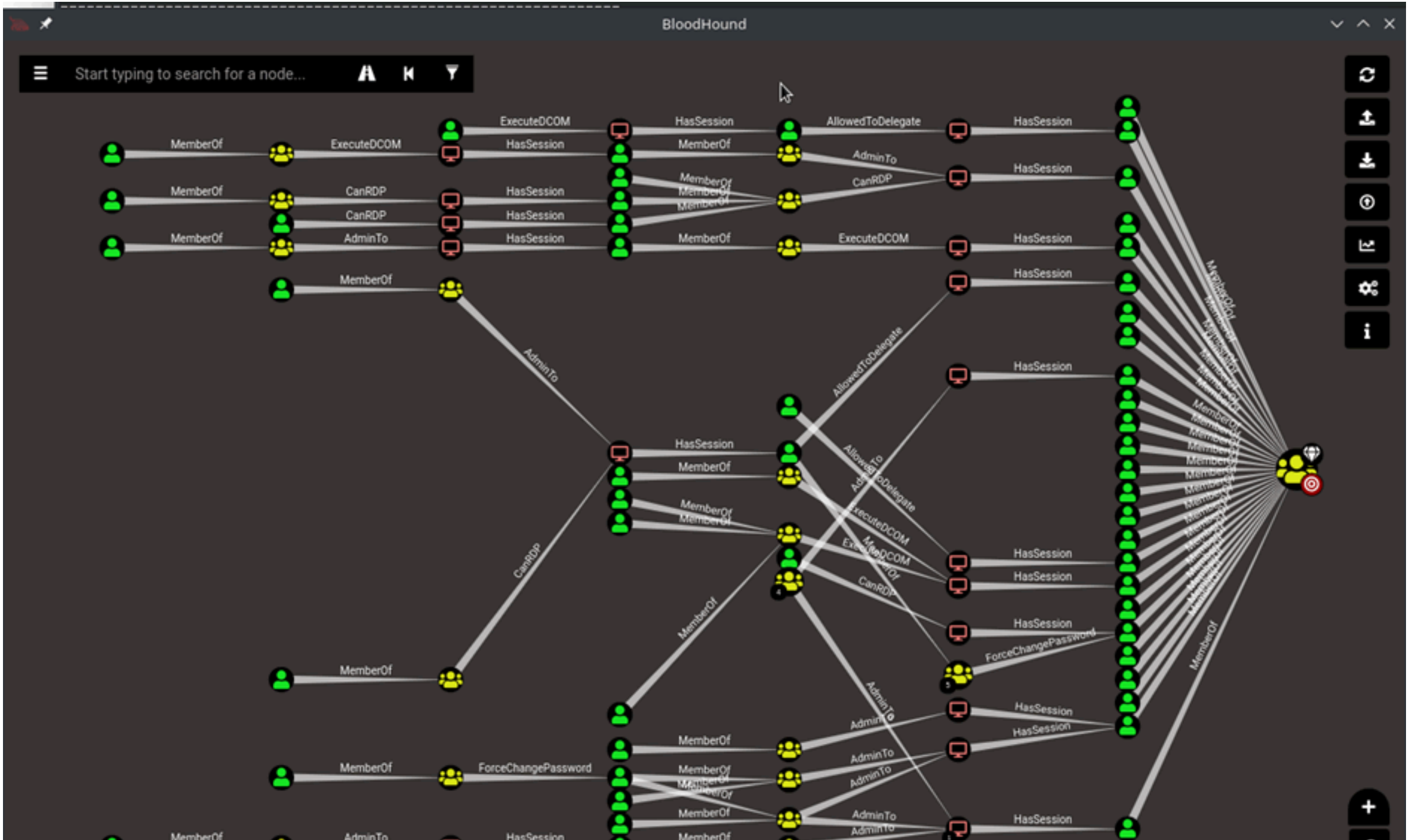
Exploitation (3/4)

Social Engineering

- Phishing tools (GoPhish)
- SECTF [link]
- What Every BODY is Saying- Joe Navarro



Internal Assessment


BloodHound
Start typing to search for a node...
MemberOf
ExecuteDCOM
HasSession
CanRDP
AdminTo
AllowedToDelegate
ForceChangePassword

Lateral Movement and Persistence

Kerberos Authentication** [link]

- Pre-Auth disabled Attacks
- Kerberoasting
- Golden Ticket (persistence)
- Silver Ticket

- DSRM (Directory Services Restore Mode)
- DC-Sync Attack

Problem with learning

Lack of infrastructure

- VPS for automation
- Setup an active directory?

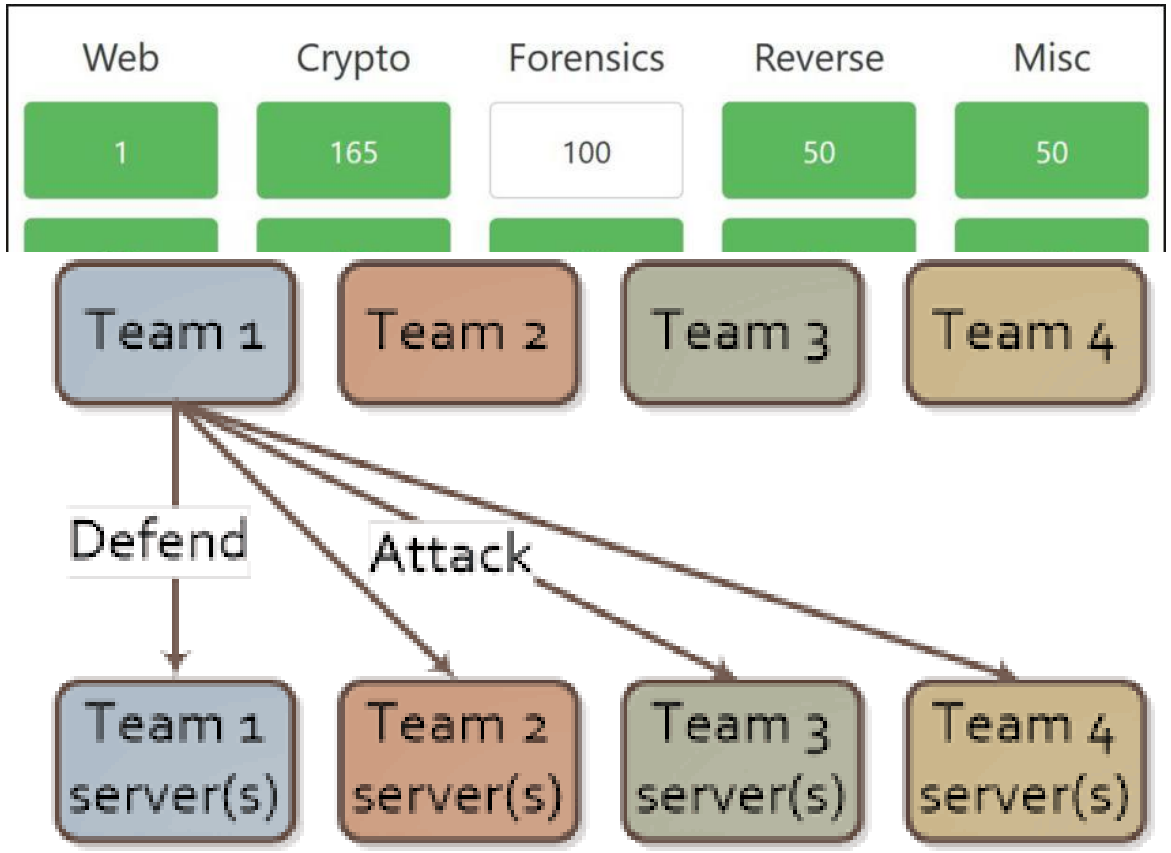
Overwhelmed with resources

Lack of Debugging skills

Where to begin? (1/3)

Capture the Flags (CTFs)

- Jeopardy style
- Attack and Defense
- CTF archives [link] (walkthrough)



Where to begin? (2/3)

Web Security Hands-on labs

Where to begin? (3/3)

Machines/Boxes

- IPPSEC [link]

Scripting/Coding (1/2)

Automation

- Network Port Monitoring
- Subdomain Monitoring
- Chaining Tools
  - Network scan -> Amass -> ffuf -> slack/discord notification
  - /?id=xss check -> Basic XSS regex -> check reflection -> notification

Scripting/Coding

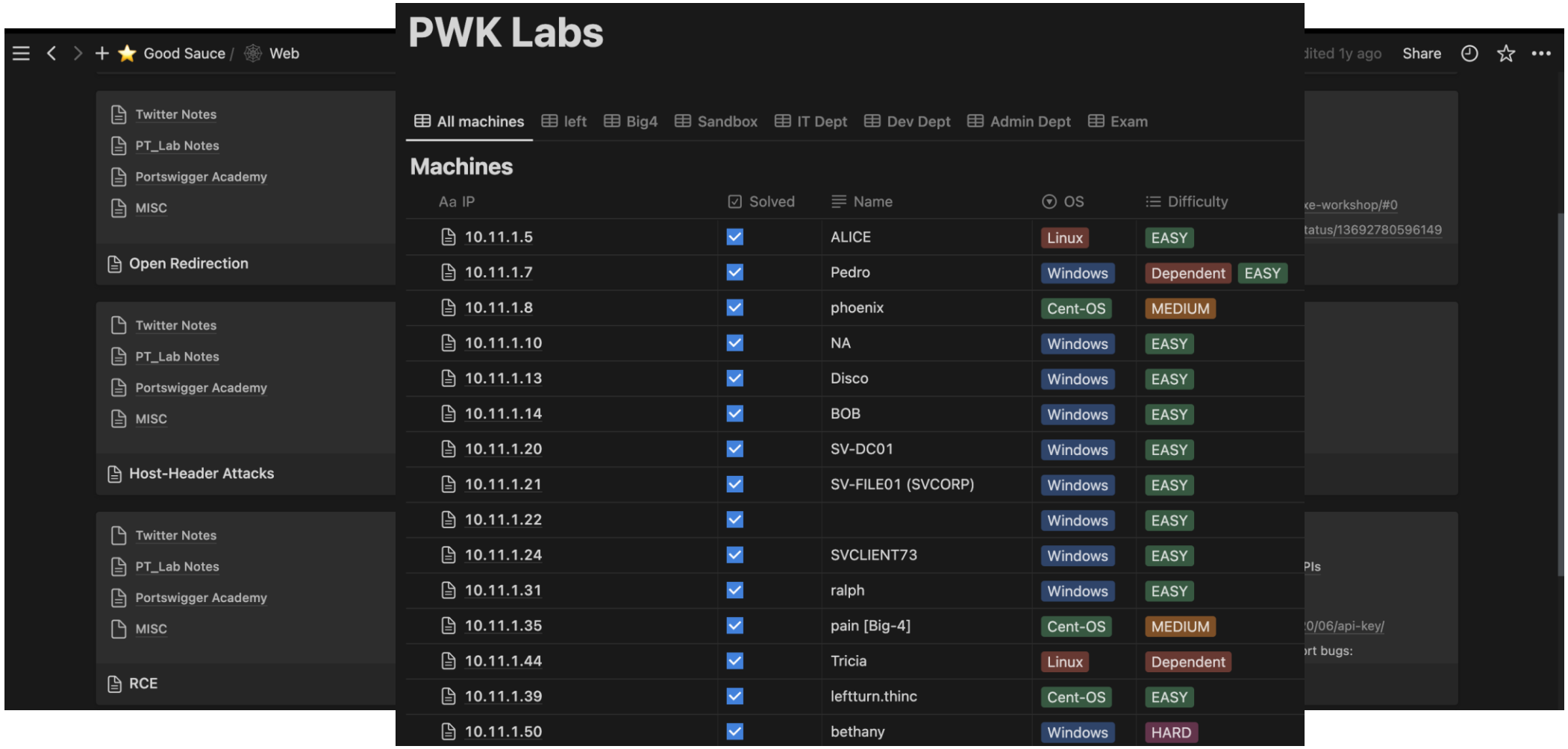
Python/Golang

- Learn 3 things:
  - File manipulation (R/W a file)
  - Web Requests (JSON manipulation, GET/POST requests)
  - Web scraping (Beautiful Soup)
- Tools (ffuf/httpx/nuclei/gobuster/subfinder)

Bash Scripting

- Data manipulation on the fly
- cut, grep, awk, jq

Note Taking


Good Sauce / Web
Share
Twitter Notes
PT_Lab Notes
Portswigger Academy
MISC
Open Redirection
Twitter Notes
PT_Lab Notes
Portswigger Academy
MISC
Host-Header Attacks
Twitter Notes
PT_Lab Notes
Portswigger Academy
MISC
RCE
PWK Labs
All machines
left
Big4
Sandbox
IT Dept
Dev Dept
Admin Dept
Exam
Machines
Aa IP
Solved
Name
OS
Difficulty
10.11.1.5 ALICE Linux EASY
10.11.1.7 Pedro Windows Dependent EASY
10.11.1.8 phoenix Cent-OS MEDIUM
10.11.1.10 NA Windows EASY
10.11.1.13 Disco Windows EASY
10.11.1.14 BOB Windows EASY
10.11.1.20 SV-DC01 Windows EASY
10.11.1.21 SV-FILE01 (SVCORP) Windows EASY
10.11.1.22 Windows EASY
10.11.1.24 SVCLIENT73 Windows EASY
10.11.1.31 ralph Windows EASY
10.11.1.35 pain [Big-4] Cent-OS MEDIUM
10.11.1.44 Tricia Linux Dependent
10.11.1.39 leftturn.thinc Cent-OS EASY
10.11.1.50 bethany Windows HARD

Certification Route

- ~~CEH~~
- Security+
- eJPT
- OSWA
- PNPT
- OSCP
- CRTP
- OSWE

Networking/Conferences

Offensive/Red Teaming

- Defcon

Research

- USENIX

SWAGS

- Black Hat/BSides

Don’t attend talks at Conferences**

Career Prospects in Offensive Security

Red Teaming

Security Engineer (Automation)

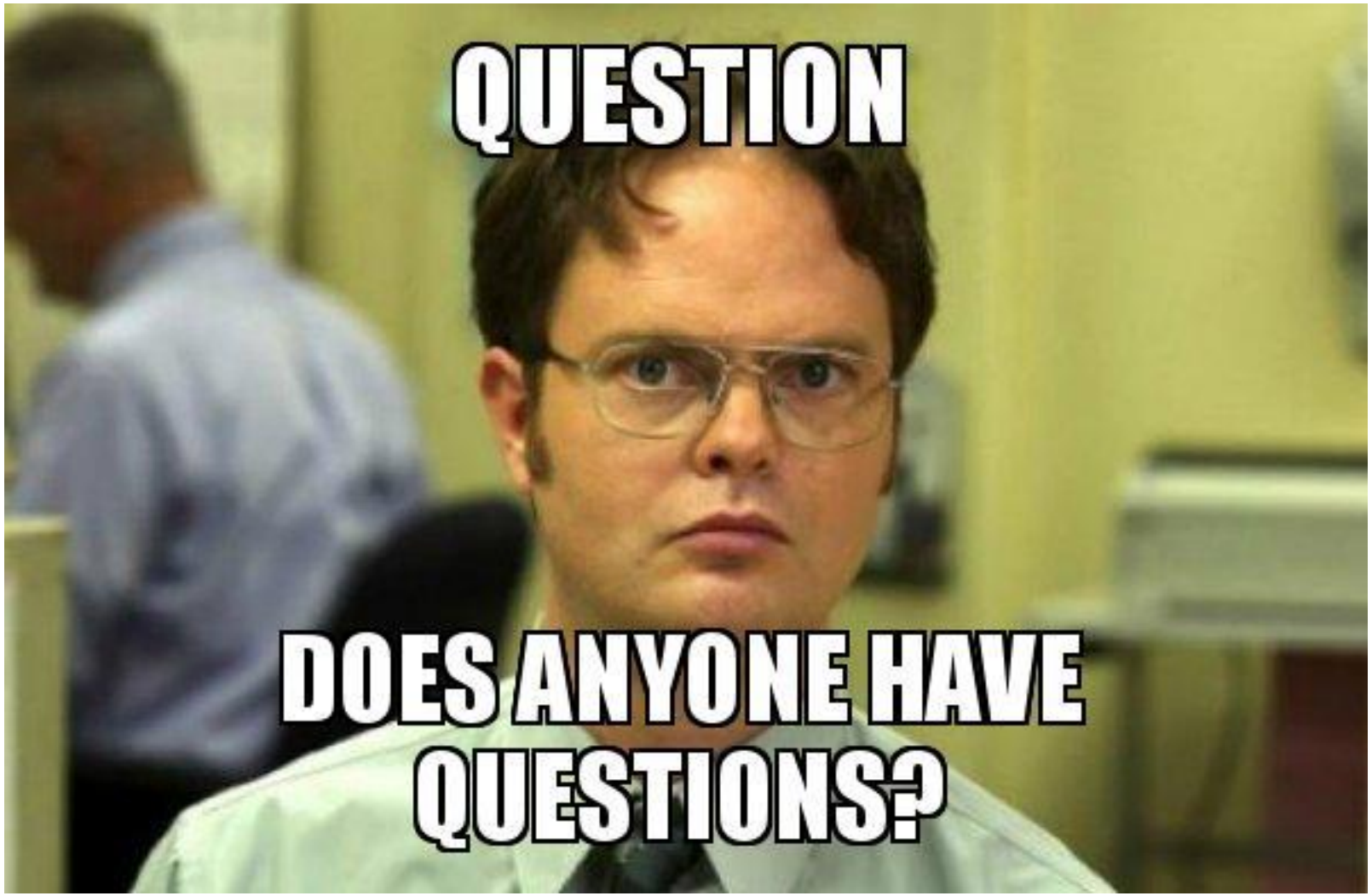
Penetration Testing

- Web Application
- Android/IOS
- Network
- Thick Client
- Source Code analysis

Career Prospects in Offensive Security

Bug bounties $$$

- Vulnerability Disclosure Programs (VDPs)
- Vulnerability Reward Programs (VRPs)
- Google Dorks [link]
- Good VDPs programs to begin with
  - Depart of Defense [link]
  - US Department of State [link]
  - any programs where you have paid/premium access to products**


QUESTION
DOES ANYONE HAVE QUESTIONS?

Get Involved Today!

Joining null NEU is easy and open to all who are passionate about cybersecurity. To get involved, simply visit our website, https://bio.link/null_neu, and fill the form to become a member.