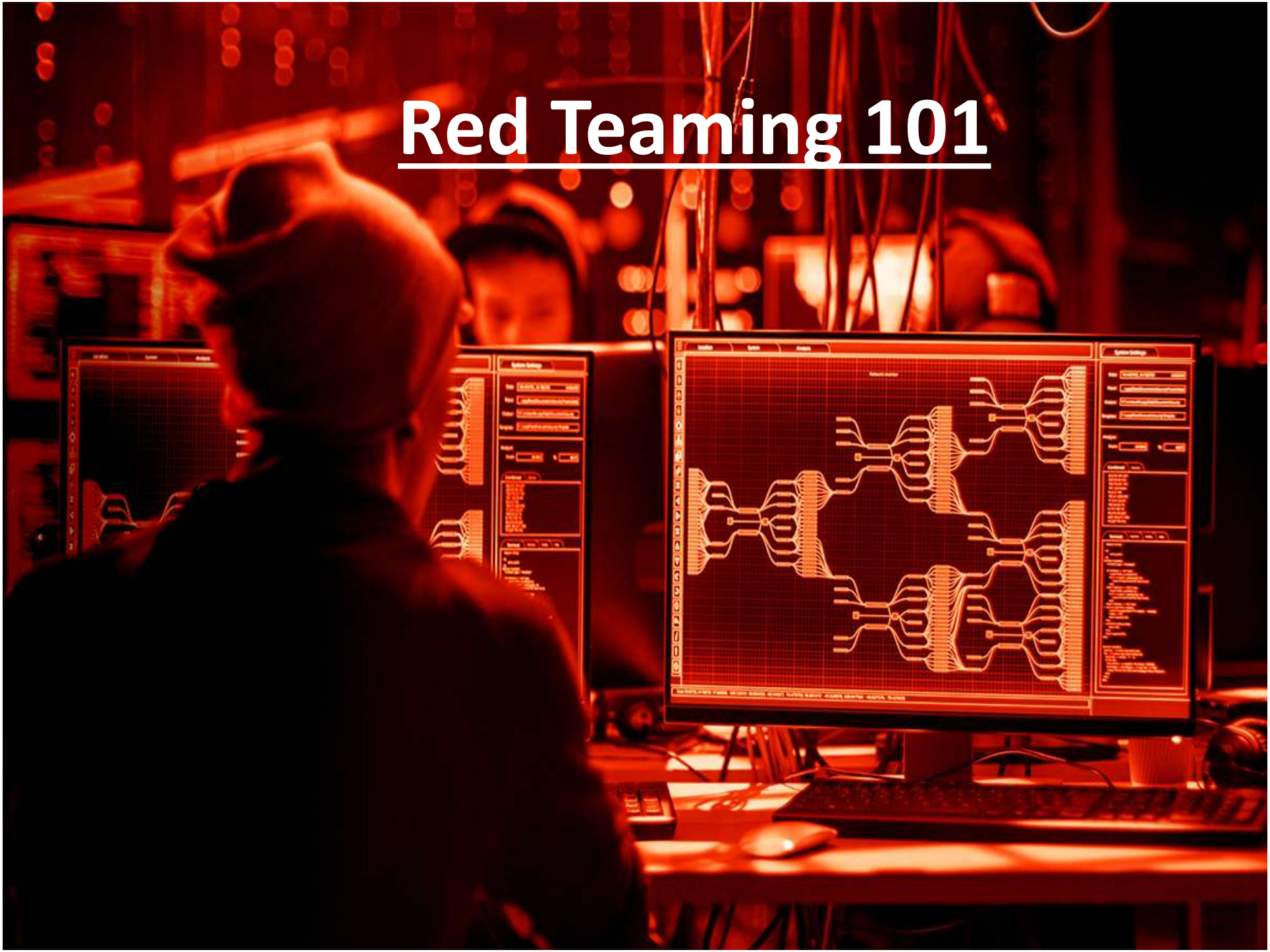
Red Teaming 101




#$WHO AM I
HARSH TANDEL
SECURITY RESEARCHER
CYBER WARRIOR

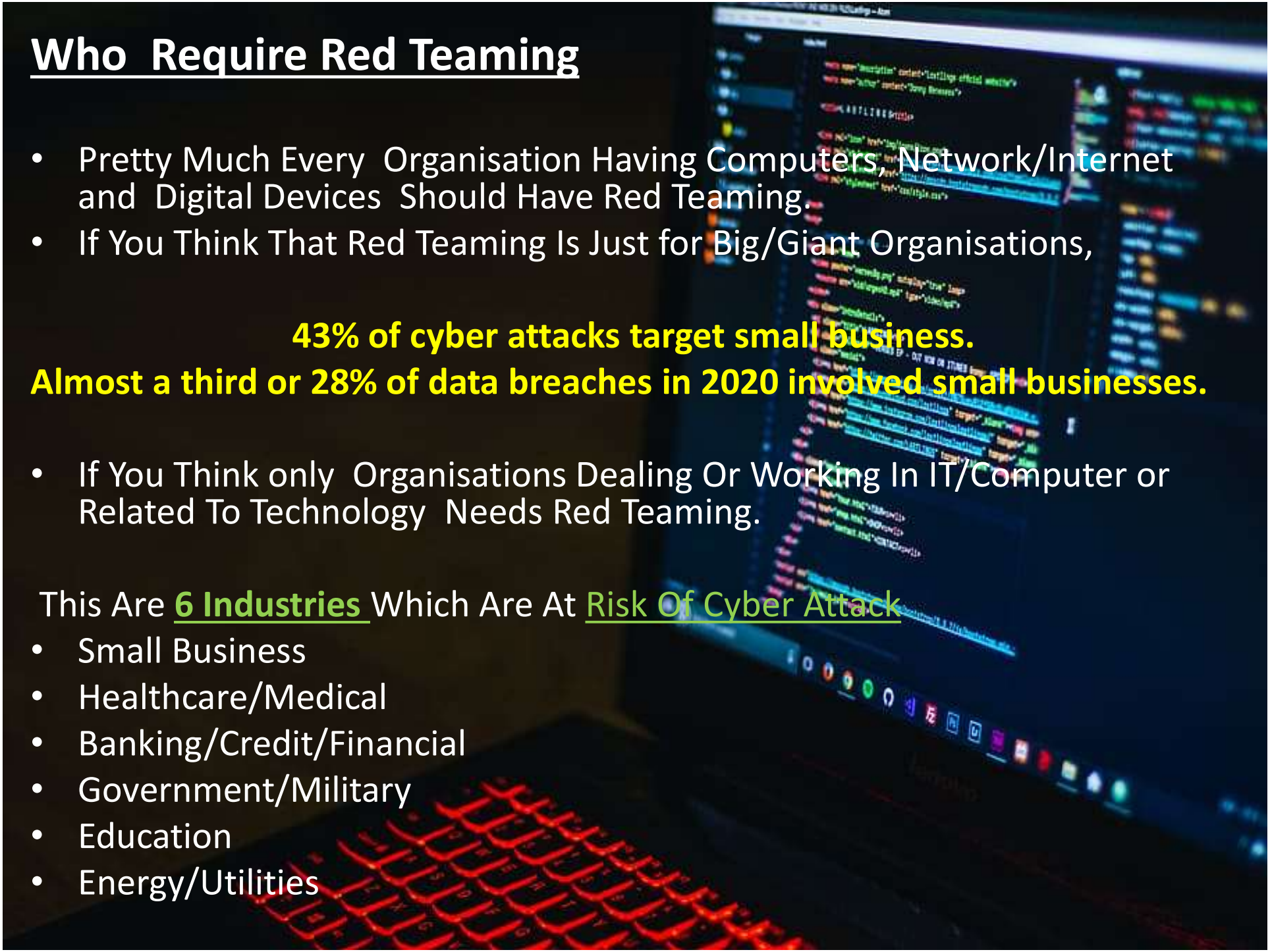
Introduction

- The origins of Red Teams are military. It was realized that to better defend there was a need to attack your own defenses to find weak points that could then be defended better.

- This morphed into "War Games" where defenders or friendly forces were denoted as **BLUE** and the opposing forces were RED. Now Days We Have Purple Team Also In Industry Who Can Do Both.

- Red Teaming is a multi-leveled attack simulation designed to measure how well your defenses will hold up to a real-world attack.

- The objective of Red Teaming is to optimize the security posture of your organization. This is achieved by detecting vulnerabilities in your controls that Blue Teams may then remediate to prevent the risk of a future breach.



Who Require Red Teaming

- Pretty Much Every Organisation Having Computers, Network/Internet and Digital Devices Should Have Red Teaming.
- If You Think That Red Teaming Is Just for Big/Giant Organisations,

43% of cyber attacks target small business.

Almost a third or 28% of data breaches in 2020 involved small businesses.

- If You Think only Organisations Dealing Or Working In IT/Computer or Related To Technology Needs Red Teaming.

This Are **6 Industries** Which Are At Risk Of Cyber Attack

- Small Business
- Healthcare/Medical
- Banking/Credit/Financial
- Government/Military
- Education
- Energy/Utilities

Why Red Teaming Is Required

Attack is the secret of defense, Defense is the planning of an attack .

-The Art of War, Sun Tzu

- Let's Get Into Real Example to answer To this Questions

1]How Many Data Breaches Happened in last year and this year in corporate Sector ?

2]Government OR Public Infrastructure Got Attacked In Last Year And This Year ?

3]Zero-Days & APTs

4]Red Teaming Costs is So Much Cheaper Than Cost Of Breach/Cyber Attack and Penalties.

- Red Teaming helps protect your company and all of its assets from compromise. Red Teams offer great insight into data exploitation and the prevention of future breaches.
- Red Teaming focuses on your company's technology, people and physical areas to make sure you are ready for anything.

When And How Often To Do IT

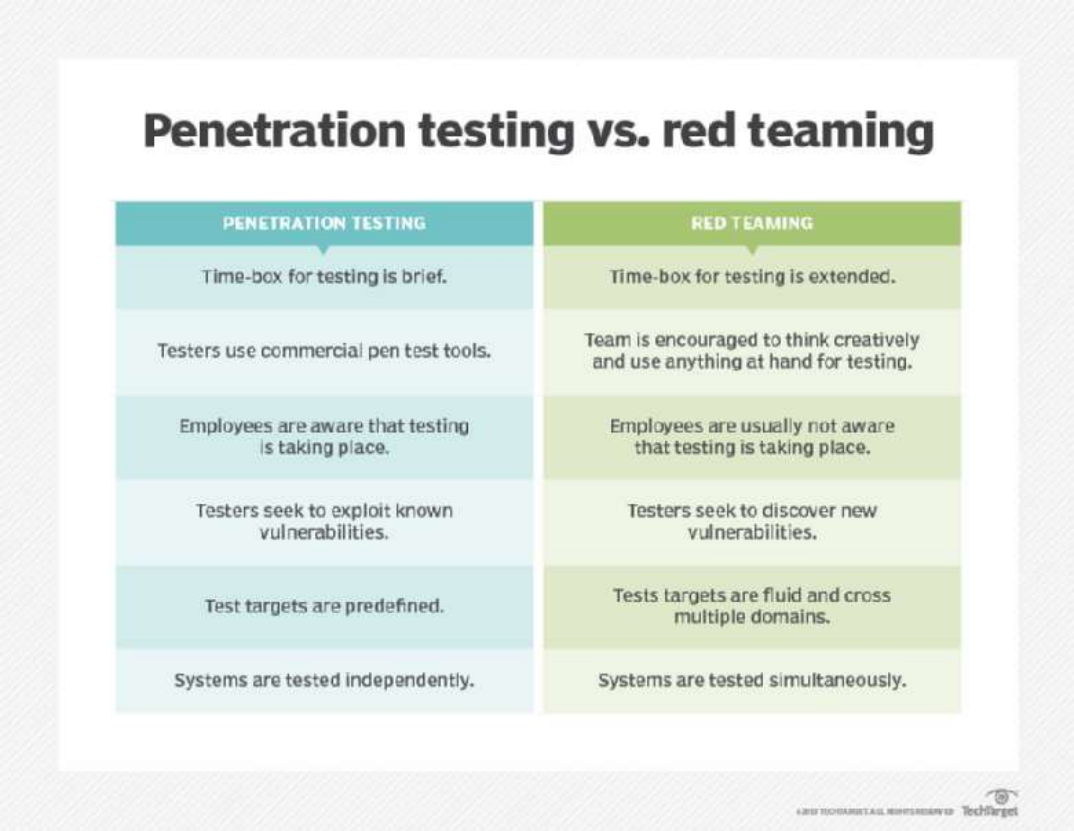
- Every organisation Should Perform Red Teaming Regularly on their Environments.
- How Often Depends On Organisations but at least Once Or Twice A Year Expected.
- If any GRC, Regulation is related with it Then as per it's Requirements.

•From Methods, Factors and Characteristics You Are Thinking Red Teaming Is Just A Hyped Pen testing You Are Not True.

•Actually Both Are Different Although In Industry Most People Think it as same or use as synonyms.

•Red Team Consists Of Red Teaming But It's Not A Penetration Testing.

•Let's Check What's Difference



Methods

- Internal in-house team
- External independent testing

Characteristics

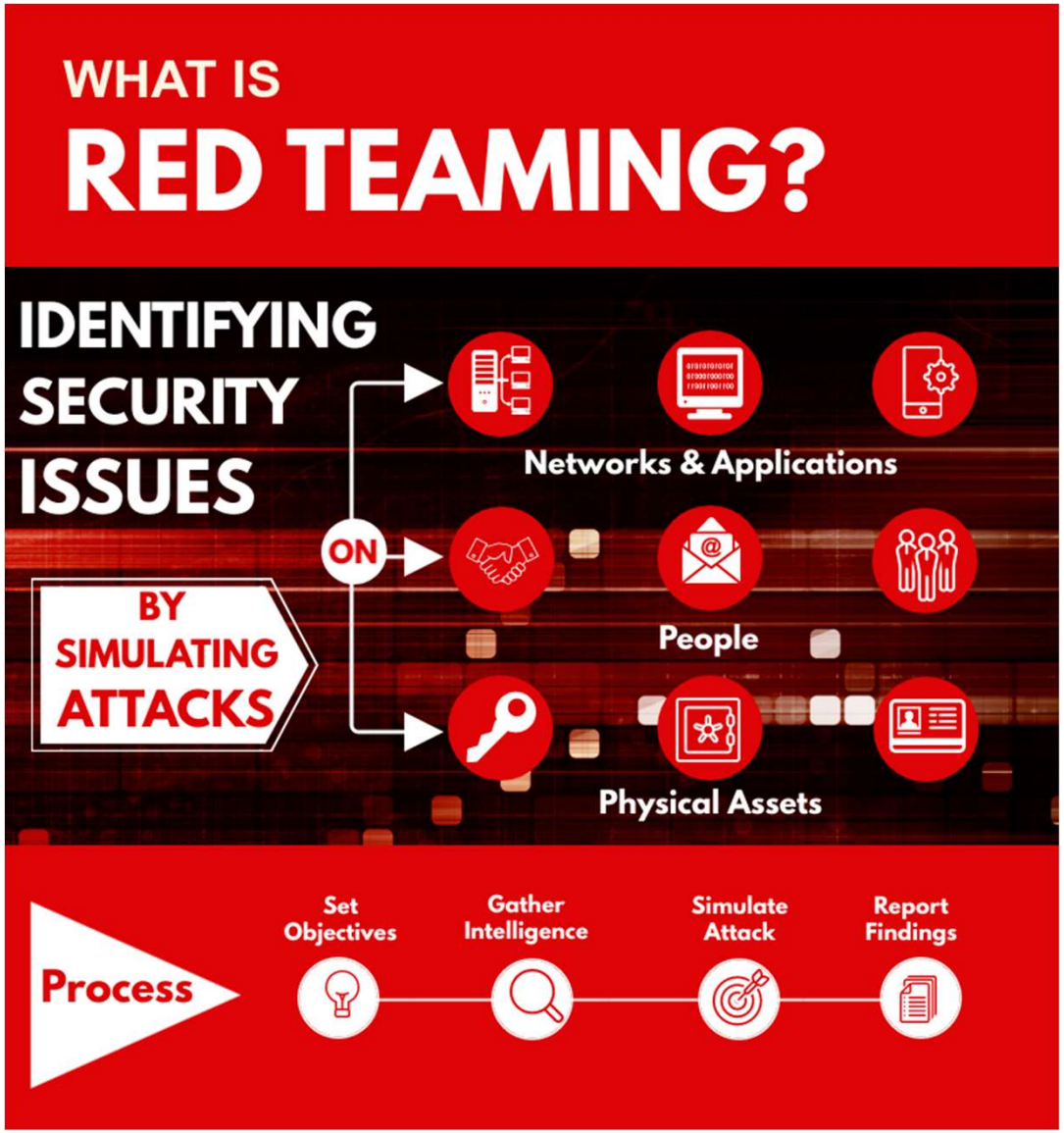
1. Wide Scope To Exploit
2. Few Dates/Times That an attack may be lunched
3. Longer Durations
4. Parallel Execution and Fluid re-prioritization.

Factors

1. **Know What You Are Looking For** : Understand Your Own System And Patch Any Oblivious vulnerability Before You Start And Engagement.
2. **Know your Network** :The Better able You Are To quantify Your Testing Environment, More accurate and Specific Your Red Team can be.
3. **Know Your Budget** : Understand How Much You Can Spend On Red Team Engagement and Set Scope Accordingly.
4. **Know Your Risk Level** :Focus On The Risks That Actually Present consequences for your business.

Steps For Red Teaming

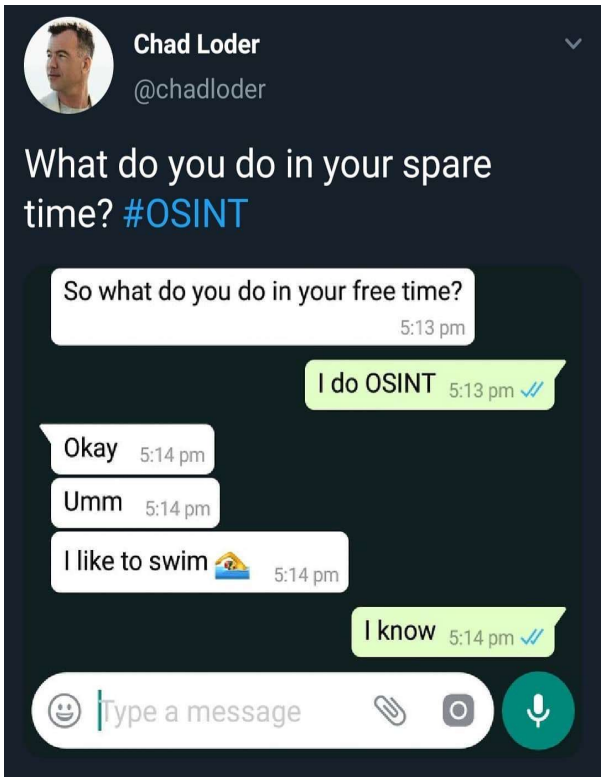
1. Set An Objective
2. Gather Information
3. Simulate Attack
4. Report Findings



1)Set An Objective : Get in Meeting With Client's Most Upper Personals like CEO,CTO,CISO & Legal Consultant (cause Red Teaming Will be done secretly and apart from these Most Of People Will Not Aware about it.)

- Know Their Requirements and Expectations Discuss About Budget, Timing and Reporting Methods(if any specific they want).This will prevent any Financial and legal problems during or after Engagement.
- Set an Goal/Objective According to factors.

2)Gather Intelligence : Here We Will Be Collecting Every Bit Of Information We Could from Everywhere.



- **Passive Recon** : LinkedIn, Github, Shodan, Pastebin, Job Portals, Emails & SM, Dark Net Monitoring, WiGle Look Up Onto Google Dorks and Third Party Services Dockers, Clouds, Acquisitions and Subsidiaries etc

Tools: Metagoofil, The Harvester, FOCA

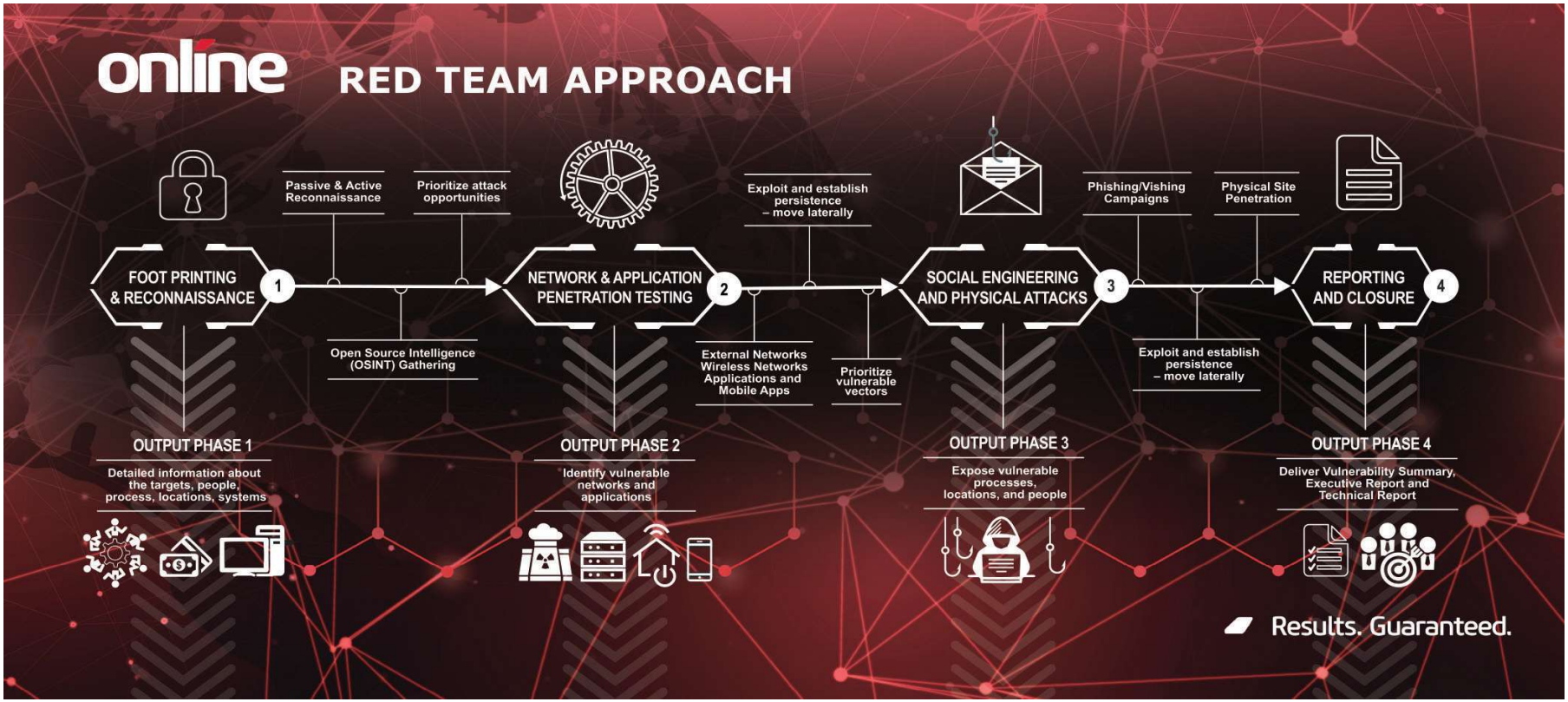
- **Active Recon** : Visiting Websites ,Applications, Software documents and sometimes decompiling or reverse engineering it.
- Visiting Physically Parameter, War Driving, Social Engineering.

Tools : Nmap, Aquatone ,dnsrecon ,Eye Witness ,AWSBucketDump

3)Simulate The Attack : In This Phase We Will Actually Perform The Attack With Our Best Try To be Stealthy. Attack Would be According to Objective and Discussion we have done with client.

It May be Simulating attack which was recently done by APT to some other Facility or organisation or Data breach Case study or any other Cyber Attack or Industrial Espionage.

- This is The Longest and Hardworking Phase It Could be up to some months to year or more and if Blue team is able to found out them Your blue Side Is Very much Good and as per Current Scenario/Situation You Are protected.



- **Battle Ground**

1]Application Pen testing : Here Pen testers Find Vulnerability And Exploit it to required Level Of Depth and Escalate Further according to Objective it may be Data Exfill or getting Access in Accounts of others etc.

- Here Apps include Web, Android, IOS all.

Web App :Burp Suite, Acunetix, Netsparker,Nikto

Mobile : MobSf, Jdax, Drozer, APK tools

2]Network & Infrastructure Pen Testing : Here Pen Testers Test Vulnerability in Networks, Clouds/Dockers , IOT and SCADA and Then Exploit Vulnerability and Escalate it for further more and also do Lateral Movement according to Objectives Monitoring Or Performing actual Attack.

Tools: Nmap,Nessues,Wireshark

3]Physical Security : Here Physical Security Experts Try to Break into Physical Facilities Of Organisation like Server Rooms ,Data Ware house, Office etc. Here They Try To Get Actually into Facilities and Get Everything they can or they want

- They might copy data from servers directly or place key loggers, RAT/Backdoor in systems , Sniffers etc according to objective.

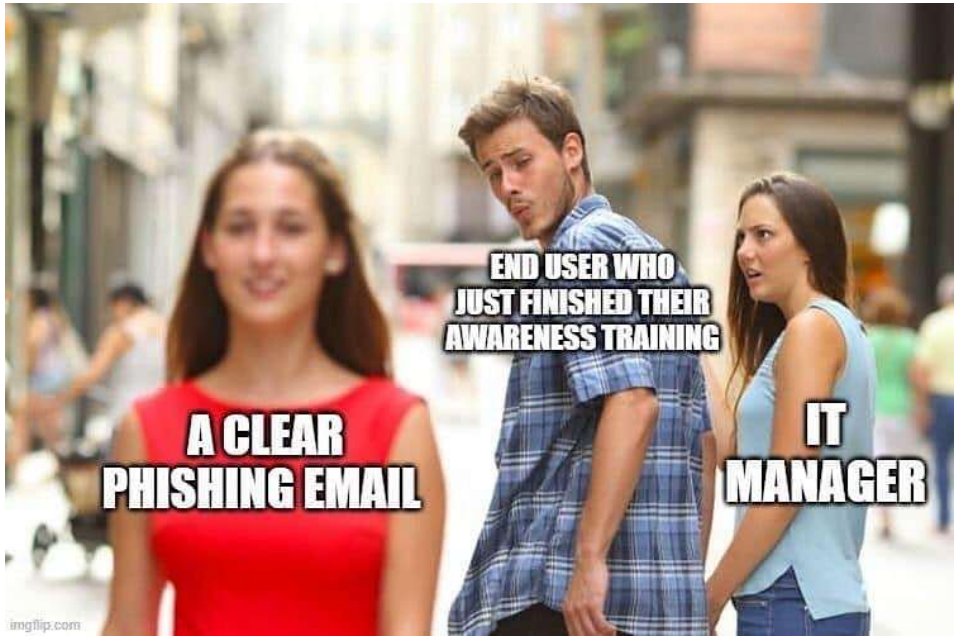
- It Can Be Done Before Application Testing Phase and after Social Engineering Phase.

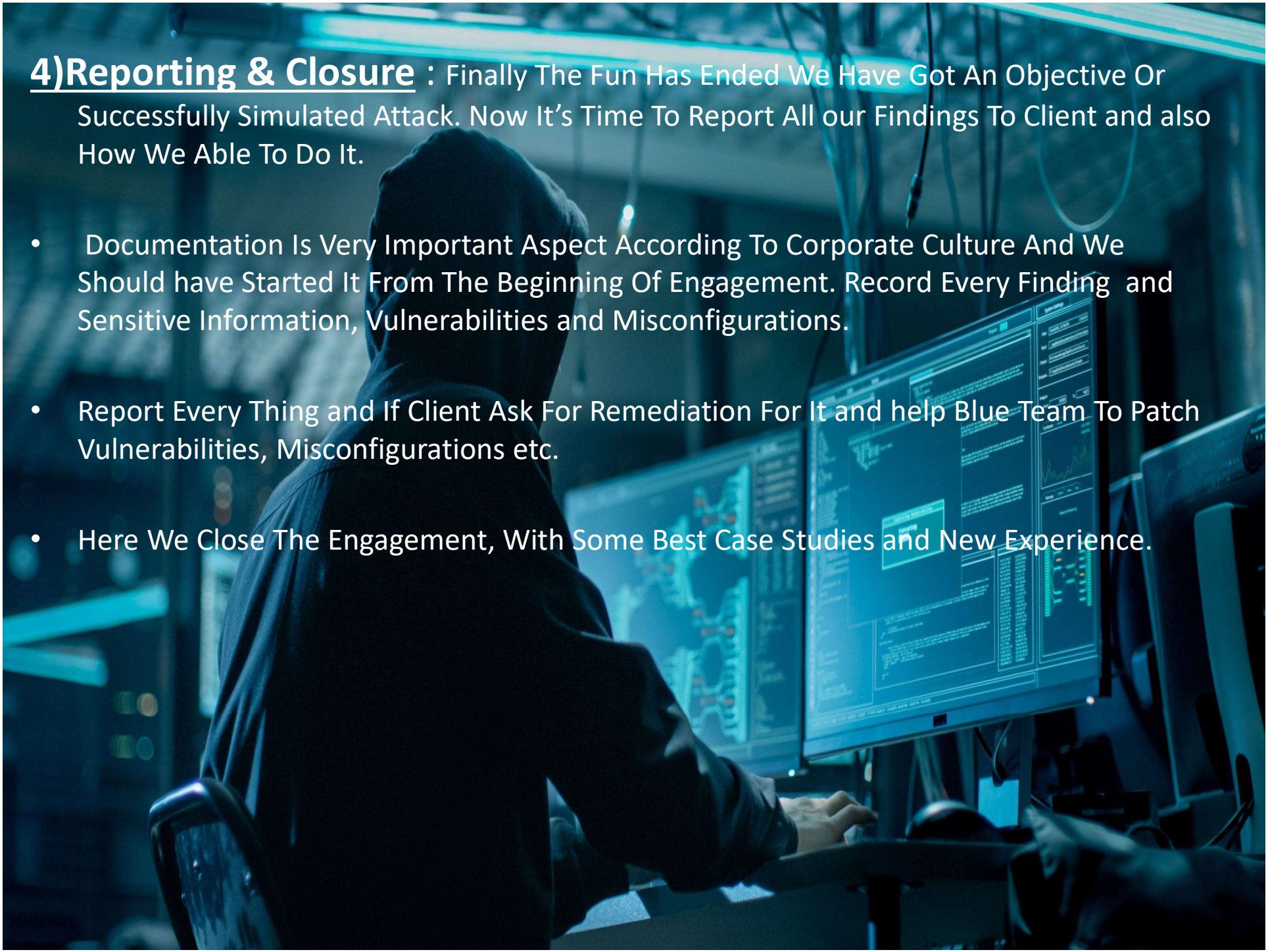
4]Social Engineering : Here Con Artists Or Human Mind Exploitation Experts Will Get Engaged With Their Employees and Get Information With them also use Spear - Phishing ,Pharming, Vishing ,Tail getting, Pretexting and others.

- These Can be Done at First Stage Of Simulating Attack Or Even During Intelligence Gathering For Enhancement Of Other Attacks.

“Wickets And Strongest Chain of Defence Is Humans Mind ”

- 95% Of Data Breaches Are Happened Due To Human Errors.





4)Reporting & Closure : Finally The Fun Has Ended We Have Got An Objective Or Successfully Simulated Attack. Now It's Time To Report All our Findings To Client and also How We Able To Do It.

- Documentation Is Very Important Aspect According To Corporate Culture And We Should have Started It From The Beginning Of Engagement. Record Every Finding and Sensitive Information, Vulnerabilities and Misconfigurations.

- Report Every Thing and If Client Ask For Remediation For It and help Blue Team To Patch Vulnerabilities, Misconfigurations etc.

- Here We Close The Engagement, With Some Best Case Studies and New Experience.

Resources

- The Red Teaming Guide
- The Red Team journal
- Red Team Village
- Infosec Institute
- Red Team Security
- Black Hat
- https://danielmiessler.com/
- https://github.com/yeyintminthuhtut/Awesome-Red-Teaming#-training--free-
- https://github.com/infosecn1nja/Red-Teaming-Toolkit

Ambush Questions !

Thank You All