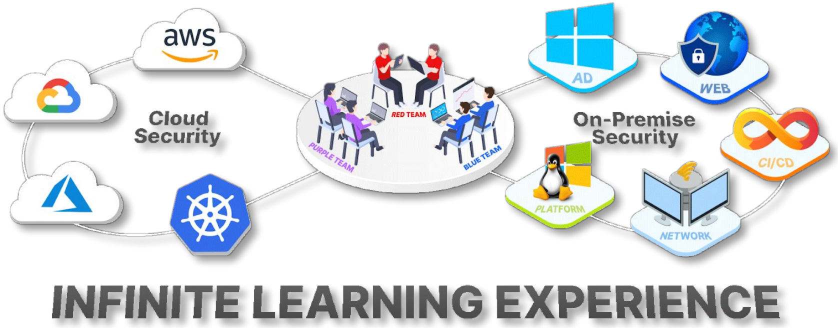
CWL
CyberWarFare Labs

Red Teaming a Bank: Simulating APT Attacks in a Realistic Cyber Range

ABOUT CYBERWARFARE LABS :

CW Labs is a Global Infosec company specializing in cybersecurity practical learning situated across UK, US & India. The company has 2 primary divisions :

1. Niche Cyber Range Labs
2. Continuous Learning : Infinity Platform



About Speaker :

Yash Bharadwaj

Director and Chief Technology Officer at CyberWarFare Labs

Over 7.5 years of experience in offensive security and cyberwarfare research. He specializes in mimicking **real-world adversary tradecraft, red/blue team lab design, and advanced phishing techniques.**

He has trained defense and academic institutions a**cross India and abroad,** and has presented his work at top cybersecurity conferences including **BlackHat USA, DEFCON, and Microsoft BlueHat.**

Red Team Objectives

- New APT Techniques Simulation
- Testing critical access to the infrastructure
- Security Defenses Testing

FOR

Enhanced detection and monitoring

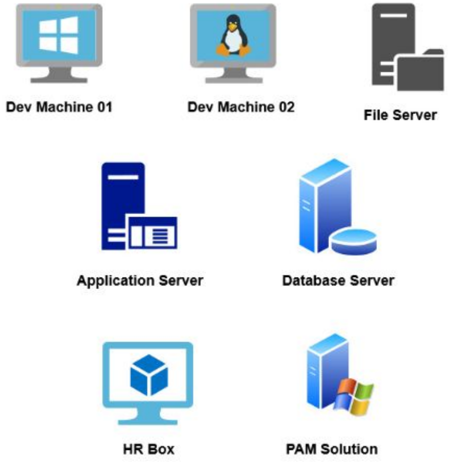
What do they follow?

- Set an Objective and Scope of Red Team Assessment
- Researched & vetted Offensive Security Tooling
- OPSEC safe infrastructure for assessments
- Roadmap and success criteria

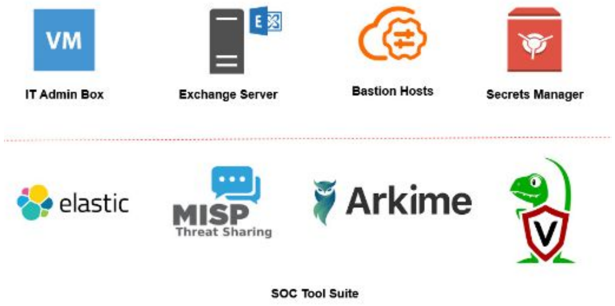
Bank Infrastructure

Identity Providers

Endpoint Security Tools



Bank Resources



Bank Critical Resources

Scope and Techniques

Scope	Technique
External Assessment	Recon, Enumeration and Phishing
Internal Assessment	Authenticated Enumeration, Privilege Escalation and Dominance
Full-Fledged	Recon to Privileged Access

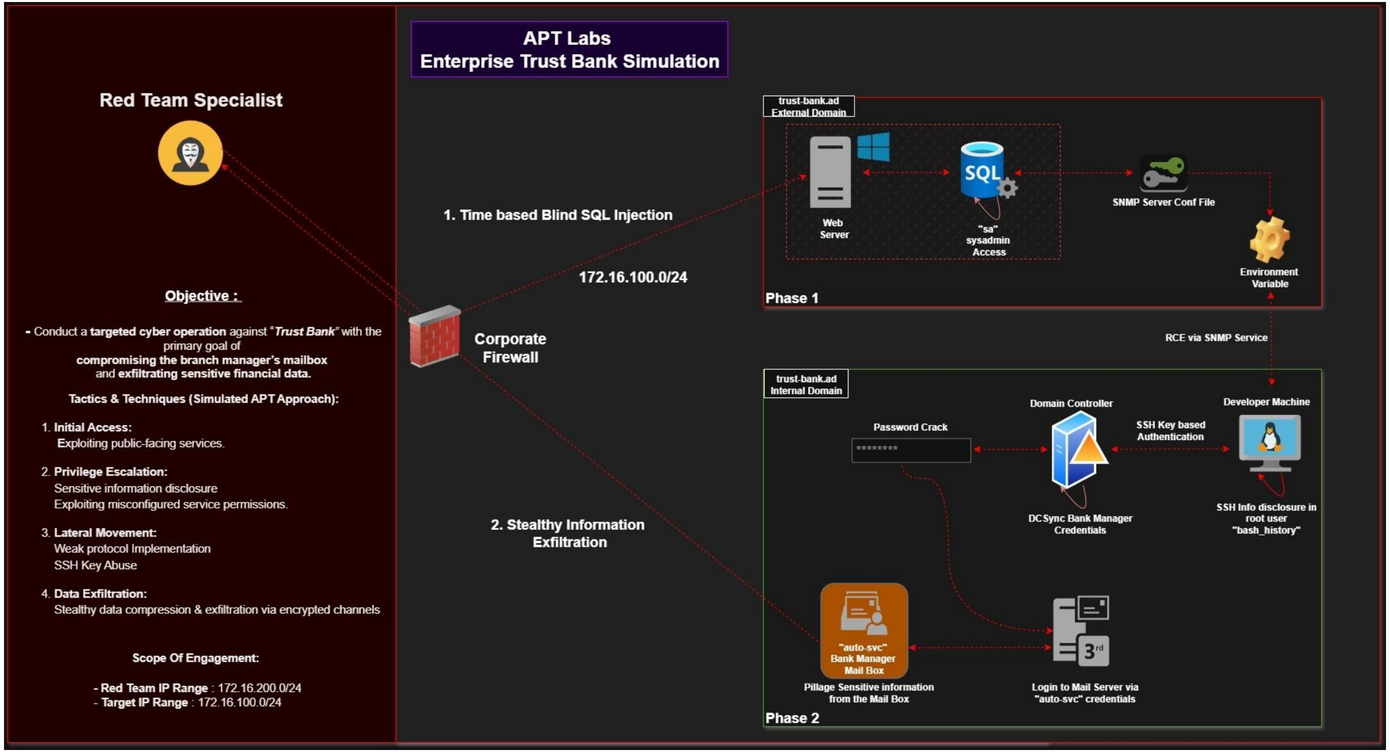
Objectives

Objectives	Value
High Value Target Credentials Access	Privileged Access to the internal environment
Infrastructure Access	Pivoting and further expansion
Security Controls Evasion	Execute payloads & bypass proxies in boxes
C-Level Executive Box Access	Access to sensitive information

Introducing Scenario Based APT Labs

- Realistic Scenarios and top tech stack coverage
- Execute Red Team Simulation from Recon to Data Exfil
- Learn by hacking into scenario based APT Labs
- From Identity Providers, Containerized apps, AD, Cloud etc in a realistic scenario.

Challenge : Hack into Trust Bank



Red Team Specialist

Objective :

- Conduct a **targeted cyber operation** against "***Trust Bank***" with the primary goal of **compromising the branch manager's mailbox** and **exfiltrating sensitive financial data.**

Tactics & Techniques (Simulated APT Approach):

1. **Initial Access:**
   Exploiting public-facing services.
2. **Privilege Escalation:**
   Sensitive information disclosure
   Exploiting misconfigured service permissions.
3. **Lateral Movement:**
   Weak protocol Implementation
   SSH Key Abuse
4. **Data Exfiltration:**
   Stealthy data compression & exfiltration via encrypted channels

Scope Of Engagement:

- **Red Team IP Range** : 172.16.200.0/24
- **Target IP Range** : 172.16.100.0/24

APT Labs
Enterprise Trust Bank Simulation
1. Time based Blind SQL Injection
172.16.100.0/24
Corporate Firewall
2. Stealthy Information Exfiltration
trust-bank.ad External Domain
Web Server
SQL
"sa" sysadmin Access
SNMP Server Conf File
Environment Variable
Phase 1
RCE via SNMP Service
trust-bank.ad Internal Domain
Password Crack
****
Domain Controller
SSH Key based Authentication
Developer Machine
DC Sync Bank Manager Credentials
SSH Info disclosure in root user "bash_history"
"auto-svc" Bank Manager Mail Box
Pillage Sensitive information from the Mail Box
3rd
Login to Mail Server via "auto-svc" credentials
Phase 2

Available at Infinity Platform

CWL
CyberWarFare Labs

Thank You

For Professional Red Team / Blue Team / Purple Team / Cloud Cyber Range labs / Trainings

Please Contact :
support@cyberwarfare.live

To know more about our offerings, please visit: **https://cyberwarfare.live**