
CYBER RANGERS

RED TEAMING

Jan Marek | Cyber Rangers

OSEP | OSCP | eCPPT | Pentest+ | CHFI | CEH | CEI | Microsoft MVP

Co-founder | Ethical Hacker | Forensic Investigator

@n0isegat3 | jan@cyber-rangers.com | www.cyber-rangers.com

CYBER RANGERS
ARMORING YOUR BUSINESS

PURPOSE OF THIS TALK

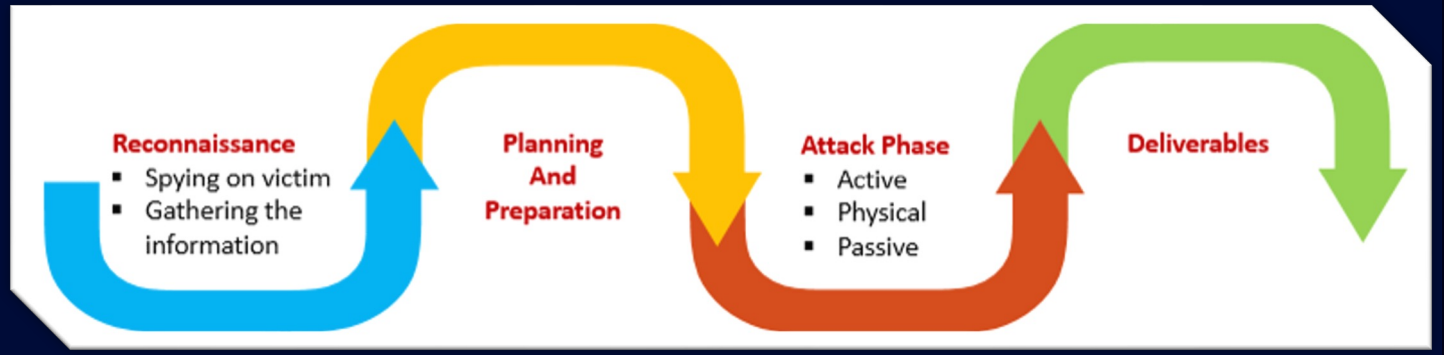
- To share our experience from Red Teaming assessments.
- To demonstrate what Red Teaming is and what its purpose is.
- To motivate you to become BLUE TEAM member!
- To keep you motivated and be ready for the job – psychologically.

WE'RE CONSTANTLY LOOKING FOR MOTIVATED INDIVIDUALS TO JOIN OUR TEAM

RED TEAMING / RED TEAM EXERCISE / RED TEAM OPERATIONS / RED …

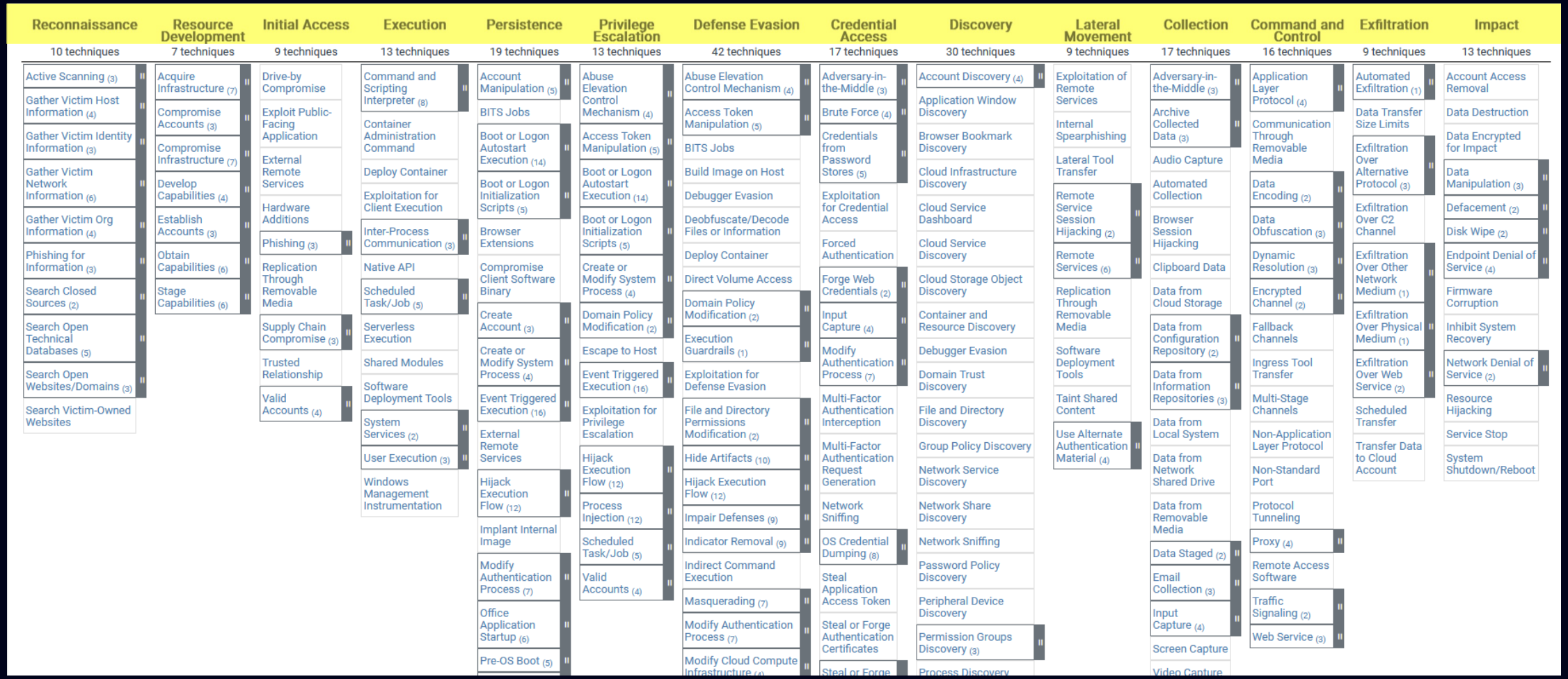
- Red Teaming vs. Adversary Simulation vs. Adversary Emulation
- It’s a team effort.
- Why is it needed? To simulate the real threat and to identify weak spots (technology + people + process).
- All mitigations running – none disabled. Real threat against real defense.

- Cybersec requires day-to-day self-education.
- Be prepared for imposter syndrome and burnouts! – no kidding…



Source: https://www.sisainfosec.com/services/red-team-exercise/

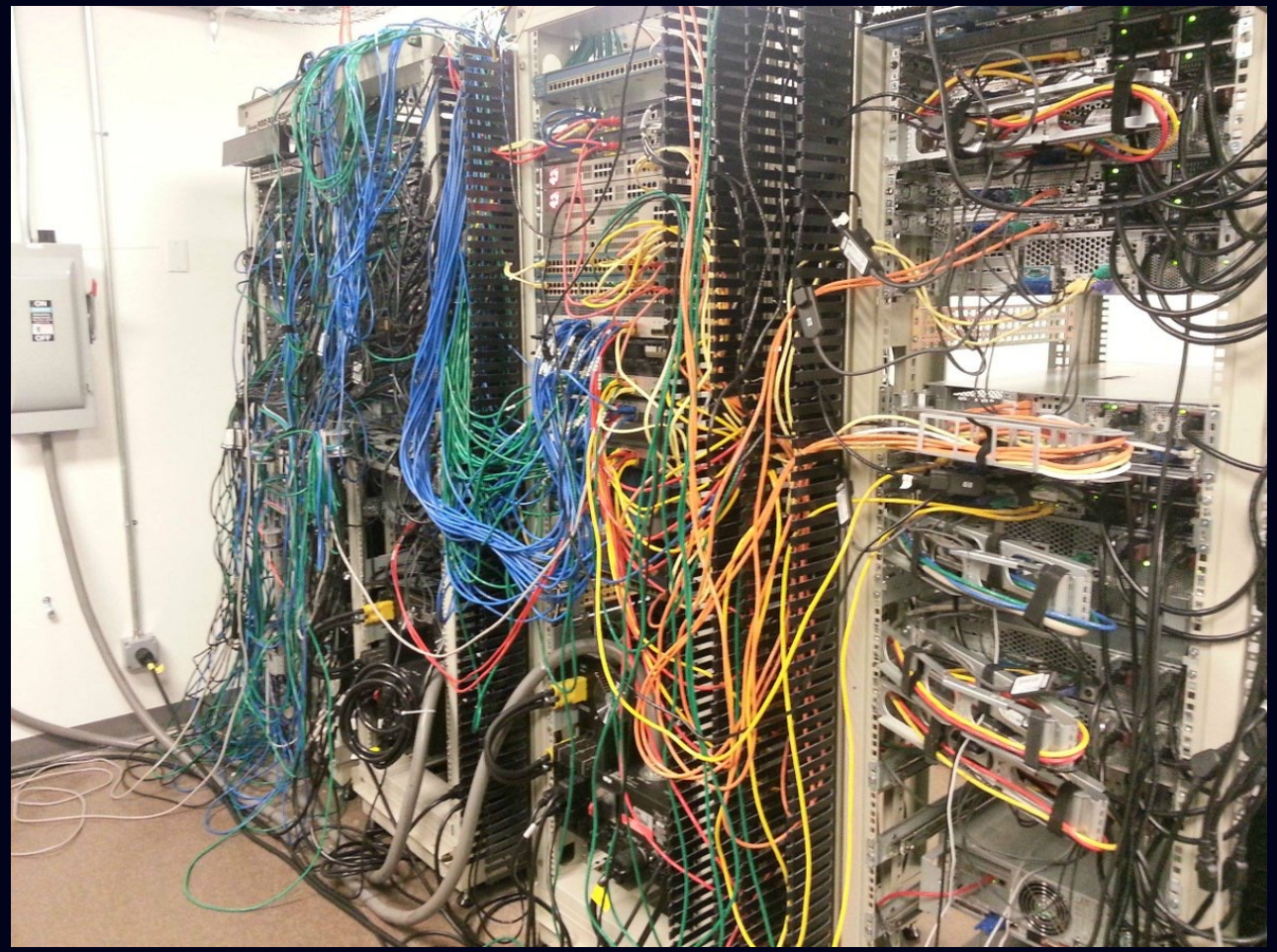
RED TEAMING COVERS THE KILL CHAIN



Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	7 techniques	9 techniques	13 techniques	19 techniques	13 techniques	42 techniques	17 techniques	30 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (3)	Acquire Infrastructure (7)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (5)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (7)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	BITS Jobs	Credentials from Password Stores (5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (3)	Phishing (3)	Inter-Process Communication (3)	Browser Extensions	Create or Modify System Process (4)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (6)	Browser Session Hijacking	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (2)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create Account (3)	Escape to Host	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)		Trusted Relationship	Serverless Execution	Create or Modify System Process (4)	Event Triggered Execution (16)	Direct Volume Access	Modify Authentication Process (7)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (3)		Valid Accounts (4)	Shared Modules	Event Triggered Execution (16)	Exploitation for Privilege Escalation	Domain Policy Modification (2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			Software Deployment Tools	External Remote Services	Hijack Execution Flow (12)	Execution Guardrails (1)	Multi-Factor Authentication Request Generation	Domain Trust Discovery		Data from Local System	Non-Application Layer Protocol		Network Denial of Service (2)
			System Services (2)	Hijack Execution Flow (12)	Process Injection (12)	Exploitation for Defense Evasion	Network Sniffing	File and Directory Discovery		Data from Network Shared Drive	Non-Standard Port		Resource Hijacking
			User Execution (3)	Implant Internal Image	Scheduled Task/Job (5)	File and Directory Permissions Modification (2)	OS Credential Dumping (8)	Group Policy Discovery		Data from Removable Media	Protocol Tunneling		Service Stop
			Windows Management Instrumentation	Modify Authentication Process (7)	Valid Accounts (4)	Hide Artifacts (10)	Steal Application Access Token	Network Service Discovery		Data Staged (2)	Proxy (4)		System Shutdown/Reboot
				Office Application Startup (6)		Hijack Execution Flow (12)	Steal or Forge Authentication Certificates	Network Share Discovery		Email Collection (3)	Remote Access Software		
				Pre-OS Boot (5)		Impair Defenses (9)	Steal or Forge	Network Sniffing		Input Capture (4)	Traffic Signaling (2)		
						Indicator Removal (9)		Password Policy Discovery		Screen Capture	Web Service (3)		
						Indirect Command Execution		Peripheral Device Discovery		Video Capture			
						Masquerading (7)		Permission Groups Discovery (3)					
						Modify Authentication Process (7)		Process Discovery					
						Modify Cloud Compute Infrastructure (4)							

Source: https://attack.mitre.org/

THERE ARE TWO TYPES OF CUSTOMERS ASKING FOR RED TEAMING: UNSECURED AND SECURED




don't WORRY! be Happy!
Good Morning!
Project task 10:00
Go to the bank
meeting at 18.00
Lunch with Jonson 01.07.2015
to check out brocken bills
CALL Jane at 18.00
Pick up dress from cleaner
CALL me
to Fix the car
URGENT! call!
Download photo
CALL MOM!
Go to bank tonorow
Let's talk
mail me
Listen new albums
Check messages!
Just SmiLe
Fix the car!
order the book
Check bill
Meeting with Samanta Sunday
Project task 10: 00
tomorow at 17.00
Listen to your HEART
buy tickets

REQUEST BY UNSECURED CUSTOMER: TRY TO HACK OUR ACTIVE DIRECTORY.

REQUEST BY SECURED CUSTOMER: USE 0-DAY TO BYPASS OUR AV AND EDR AND MOVE STEALTHY


Last week, we get called in by
Cyber Risk
KAPWING

OSINT

- A lot of information and data on public records leads to
  - Know the target environment.
  - Find business critical assets and people.
  - Gain the trust.
- Employees/company sharing juicy information on social networks
  - Visuals of target physical environment.
  - Access and authorization systems used.
  - Weak spots.
  - Head hunting.

PHYSICAL

- No need for lockpicking or cracking locks – open doors and windows.
- Loading doors without camera surveillance.
- WiFi connectivity available outside the physical perimeter.
- ARC system located in the building, but connected to the ARC via SIM card (possibility to jam using GSM jammer).
- No need to attack IT related systems at all.

PROCESSES

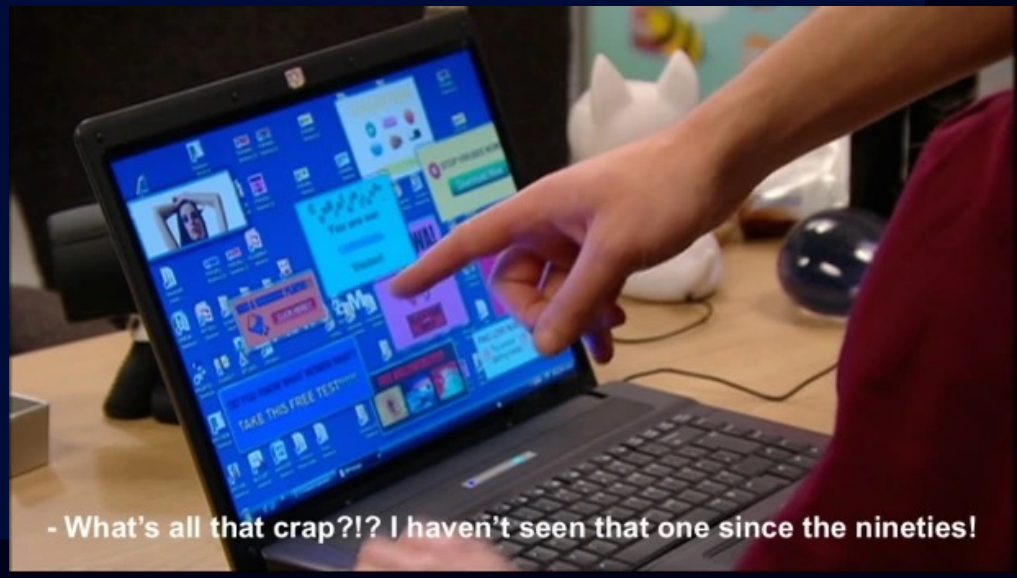
- Wrong process of authorization of a person when entering the building (it is enough to know some basic data and a person is allowed to enter the building without restriction of access).
- No or insufficient control process during the recruitment of new employees - immediately or very quickly the employee gets very large access or high privileges.
- An unattended visitor who goes to the meeting room or to the toilet before or during a meeting (moves alone around the building unattended).
- Staff are happy to assist strangers in accessing the building / happy to help fake police officers enter the building.
- Cybersec/infosec team = IT team. Overloaded employees. Not enough time for IR.
- Cyber defense systems = storing events and logs. No alerting, no intelligence.
- Implemented cyber defence systems with no trained personnel.
- No change management process.

NETWORK

- Non-segmented networks, no 802.1x.
- Firewall disabled for the domain profile.
- Writable domain controllers located in DMZ/internet facing.
- VPN authenticated using the Active Directory with account lockout turned on (it is possible to lock the entire AD via VPN) and the possibility of creating a smoke screen attack.
- Backups of firewall configurations are available on the PC -> they often contain passwords in plain-text.
- Passwords everywhere – scripts containing passwords stored on user accessible shared folders.

DEVICES

- Unsecure kiosk devices, televisions, mini-computers connected to internal network.
- VOIP connected to the internal network without NAC and/or network level encryption.
- Insufficient protection for computers - permanently logged-in user on 24/7 systems.
- Missing updates. Vulnerabilities ”for free” – Zerologon, HiveNightmare.
- Package readers connected to the internal information systems, authenticated and free to use.
- Flash drives with data lying around on desks.
- Unattended devices, unlocked screens, USB ports enabled.
- FVE without preboot authentication or no FVE at all.



IDENTITY

- Forgotten user accounts still members of privileged groups.
- Users use the same passwords to the company as to private services/social networks (often leaked passwords).
- Users with local admin rights.
- Service accounts with high privileges.
- Supplier accounts, which are used only occasionally, have super strong permissions and weak passwords, as well as test accounts, which remain unremoved after implementation.
- MFA as the ultimate security feature.

SAMPLE ENGAGEMENT

- OSINT
  - to get IT personnel and HR personnel contact names
  - to find active job opportunity
- Social Engineering
  - to trick IT personnel to create user account and VPN access
- Access
  - the organization environment and enumerate AD
  - to identify the user has privileges to join his/her computer to AD domain
- Move laterally
  - evade AV/AppWhitelisting and by waiting for the device management to manage the newly joined computer and get the plain text passwords (MECM)
  - connect to IT admin workstation and implant the keylogger to get AD domain admin credentials

SAMPLE ENGAGEMENT

SoW

Get-out-of-jail-letter

- OSINT
  - to get IT personnel and HR personnel contact names
  - to find active job opportunity
- Social Engineering
  - to trick IT personnel to create user account and VPN access
- Access
  - the organization environment and enumerate AD
  - to identify the user has privileges to join his/her computer to AD domain
- Move laterally
  - evade AV/AppWhitelisting and by waiting for the device management to manage the newly joined computer and get the plain text passwords (MECM)
  - connect to IT admin workstation and implant the keylogger to get AD domain admin credentials

SAMPLE ENGAGEMENT

SoW

Get-out-of-jail-letter

- OSINT
  - to get IT personnel and HR personnel contact names
  - to find active job opportunity
- Social Engineering
  - to trick IT personnel to create user account and VPN access
- Access
  - the organization environment and enumerate AD
  - to identify the user has privileges to join his/her computer to AD domain
- Move laterally
  - evade AV/AppWhitelisting and by waiting for the device management to manage the newly joined computer and get the plain text passwords (MECM)
  - connect to IT admin workstation and implant the keylogger to get AD domain admin credentials

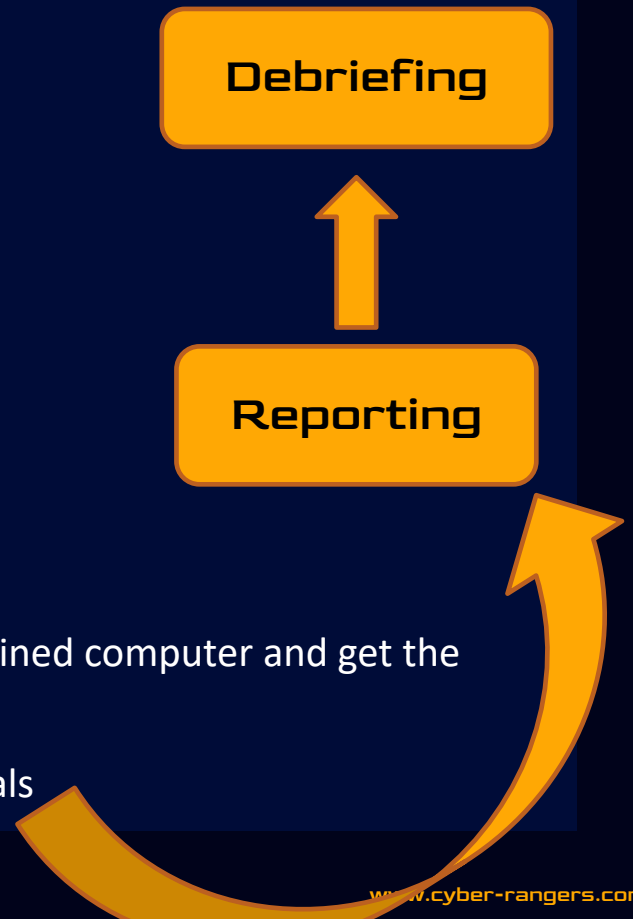
Reporting

SAMPLE ENGAGEMENT

SoW

Get-out-of-jail-letter

- OSINT
  - to get IT personnel and HR personnel contact names
  - to find active job opportunity
- Social Engineering
  - to trick IT personnel to create user account and VPN access
- Access
  - the organization environment and enumerate AD
  - to identify the user has privileges to join his/her computer to AD domain
- Move laterally
  - evade AV/AppWhitelisting and by waiting for the device management to manage the newly joined computer and get the plain text passwords (MECM)
  - connect to IT admin workstation and implant the keylogger to get AD domain admin credentials



SAMPLE ENGAGEMENT

SoW

get-out-of-jail letter

- OSINT
  - to get IT personnel and HR personnel contact names
  - to find active job opportunity
- Social Engineering
  - to trick IT personnel to create user account and VPN access
- Access
  - the organization environment and enumerate AD
  - to identify the user has privileges to join his/her computer to AD domain
- Move laterally
  - evade AV/app-whitelisting and by waiting for the device management to manage the newly joined computer and get the plain text passwords (MECM)
  - connect to IT admin workstation and implant the keylogger to get AD domain admin credentials

Debriefing

Reporting

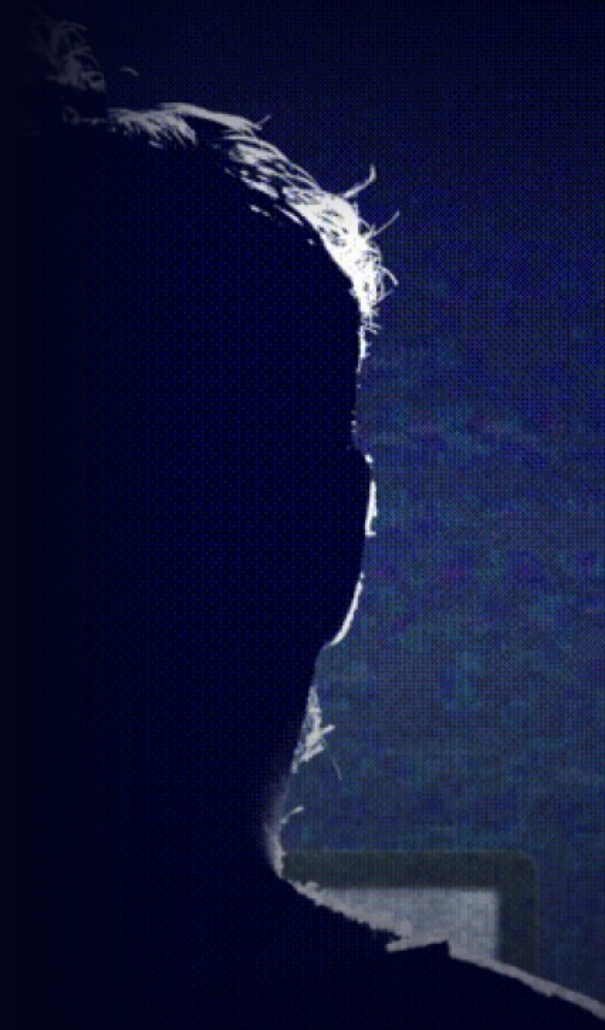
KEY TAKEAWAYS

- We need to think different – to find flaws!
- We need to be afraid, assume breach – it's needed!
- It's not possible to test everything internally – we need to get help!
- We need to demand answers, explanations – to understand it!

vulnerability assessment != penetration test != red teaming

Q & A

RED TEAMING



Jan Marek | Cyber Rangers

OSEP | OSCP | eCPPT | Pentest+ | CHFI | CEH | CEI | Microsoft MVP

Co-founder | Ethical Hacker | Forensic Investigator

@n0isegat3 | jan@cyber-rangers.com | www.cyber-rangers.com

CYBER RANGERS
ARMORING YOUR BUSINESS

www.cyber-rangers.com