Lessons Learned: Explore Key Takeaways of Breaking into City Infrastructure

Oregon Cyber Resilience Summit
October 8, 2025

Josh Schmidt – Managing Partner, Cybersecurity & IT Advisory

Lee Wagoner – Technical Penetration Tester II

Josh Schmidt

Managing Partner, Cybersecurity & IT Advisory

- Multiple roles over the years
  - Ten years offensive security
  - Five years system administration
  - Five years software development
- University of Oregon Education
- Personal interests
  - Mechanical anything
  - Rugby
  - Property remodeling
  - Architecture

jschmidt@bpm.com

Lee Wagoner

Technical Penetration Tester II, Onsite Social Engineering Specialist

- Started at the bottom, now we are here:
  - Three years at BPM
  - Began as an OSINT & Phones specialist
  - Completed 60+ onsite engagements
- Trained through self-education and hands-on experience.
- Personal interests
  - 3D Printing
    - (Vibe) Coding
      - Solo museum exploration
        - Space Games (450+ hrs in Elite Dangerous)

lwagoner@bpm.com

Agenda

- Introduction
- Mapping Assessments - Standards & Frameworks
- Case Study #1 – Medium Sized City with OT, Penetration Test
- Case Study #2 – Large City, Covert Red Team
- Case Study #3 – Small City, Cybersecurity Assessment
- Wrap Up

Questions/comments are encouraged!

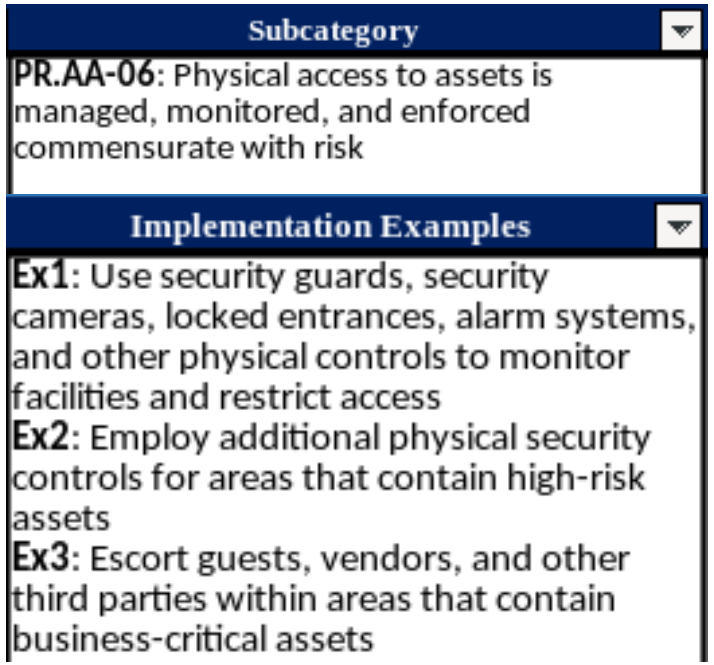
Introduction

Mapping Assessments - Standards & Frameworks

- NIST CSF 2.0
- MITRE ATT&CK
  - https://www.cisa.gov/sites/default/files/2023-01/Best%20Practices%20for%20MITRE%20ATTCK%20Mapping.pdf
  - https://mitre-attack.github.io/attack-navigator/
- OWASP Application Security Verification Standard (ASVS)
- Common Weakness Enumeration: CWE

NIST CSF 2.0

- 6 core functions
- 23 controls categories
- 108 subcategories



Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

Image source: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

MITRE ATT@CK - Enterprise

- 14 progressive attack technique categories
- 227 techniques

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration
Accessibility Features	Accessibility Features	Binary Padding	Brute Force	Account Discovery	Application Deployment Software	Command-Line	Automated Collection	Automated Exfiltration
AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Application Window Discovery	Exploitation of Vulnerability	Execution through API	Clipboard Data	Data Compressed
Basic Input/Output System	Bypass User Account Control	Code Signing	Credential Manipulation	File and Directory Discovery	Logon Scripts	Graphical User Interface	Data Staged	Data Encrypted
Bootkit	DLL Injection	Component Firmware	Credentials in Files	Local Network Configuration Discovery	Pass the Hash	PowerShell	Data from Local System	Data Transfer Size Limits
Change Default File Handlers	DLL Search Order Hijacking	DLL Injection	Exploitation of Vulnerability	Local Network Connections Discovery	Pass the Ticket	Process Hollowing	Data from Network Shared Drive	Exfiltration Over Alternative Protocol
Component Firmware	Exploitation of Vulnerability	DLL Search Order Hijacking	Input Capture	Network Service Scanning	Remote Desktop Protocol	Rundll32	Data from Removable Media	Exfiltration Over Command and Control Channel
DLL Search Order Hijacking	Legitimate Credentials	DLL Side-Loading	Network Sniffing	Peripheral Device Discovery	Remote File Copy	Scheduled Task	Email Collection	Exfiltration Over Other Network Medium
Hypervisor	Local Port Monitor	Disabling Security Tools	Two-Factor Authentication Interception	Permission Groups Discovery	Remote Services	Service Execution	Input Capture	Exfiltration Over Physical Medium
Legitimate Credentials	New Service	Exploitation of Vulnerability		Process Discovery	Replication Through Removable Media	Third-party Software	Screen Capture	Scheduled Transfer
						Windows Management		

Image source: https://attack.mitre.org/docs/MITRE_ATTACK_Enterprise_11x17.pdf

MITRE ATT@CK - Enterprise

T1557	Adversary-in-the-Middle	Network segmentation can be used to isolate infrastructure components that do not require broad network access. This may mitigate, or at least alleviate, the scope of AiTM activity.

Mitigations

ID	Mitigation	Description
M1042	Disable or Remove Feature or Program	Disable LLMNR and NetBIOS in local computer security settings or by group policy if they are not needed within an environment. [15]
M1037	Filter Network Traffic	Use host-based security software to block LLMNR/NetBIOS traffic. Enabling SMB Signing can stop NTLMv2 relay attacks.[3][4][16]
M1031	Network Intrusion Prevention	Network intrusion detection and prevention systems that can identify traffic patterns indicative of AiTM activity can be used to mitigate activity at the network level.
M1030	Network Segmentation	Network segmentation can be used to isolate infrastructure components that do not require broad network access. This may mitigate, or at least alleviate, the scope of AiTM activity.

OWASP Application Security Verification Standard (ASVS)

- Level 1 – Low level assurance needs
- Level 2 – Applications that contain sensitive data
- Level 3 – Most critical applications that need high-level of trust

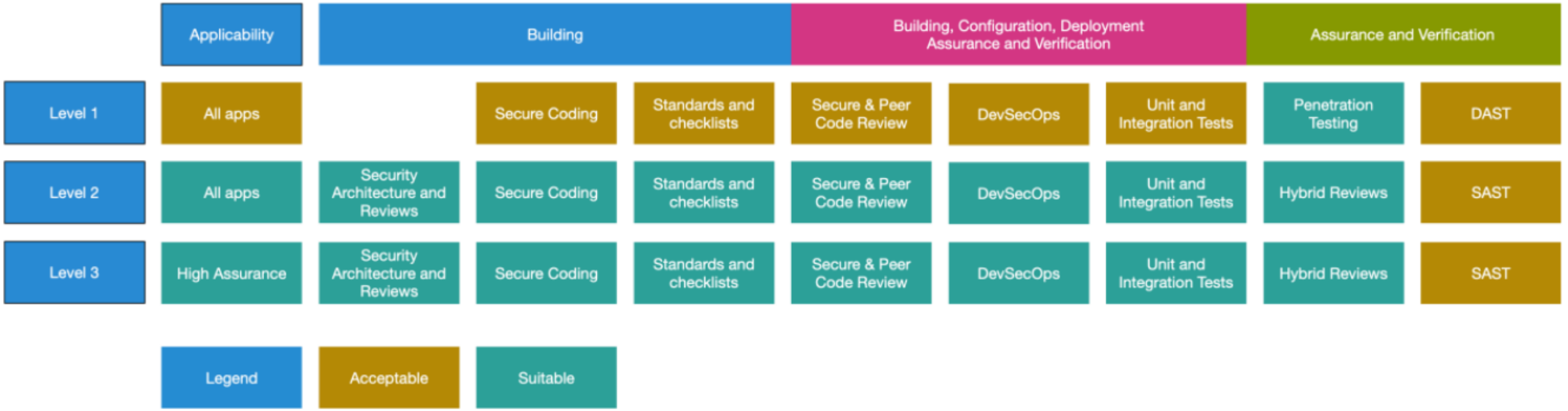


Image source: https://raw.githubusercontent.com/OWASP/ASVS/v4.0.3/4.0/OWASP%20Application%20Security%20Verification%20Standard%204.0.3-en.pdf

OWASP Application Security Verification Standard (ASVS)

V6.3 Random Values

True Pseudo-random Number Generation (PRNG) is incredibly difficult to get right. Generally, good sources of entropy within a system will be quickly depleted if over-used, but sources with less randomness can lead to predictable keys and secrets.

#	Description	L1	L2	L3	CWE
6.3.1	Verify that all random numbers, random file names, random GUIDs, and random strings are generated using the cryptographic module's approved cryptographically secure random number generator when these random values are intended to be not guessable by an attacker.		✓	✓	338
6.3.2	Verify that random GUIDs are created using the GUID v4 algorithm, and a Cryptographically-secure Pseudo-random Number Generator (CSPRNG). GUIDs created using other pseudo-random number generators may be predictable.		✓	✓	338
6.3.3	Verify that random numbers are created with proper entropy even when the application is under heavy load, or that the application degrades gracefully in such circumstances.			✓	338

Image source: https://raw.githubusercontent.com/OWASP/ASVS/v4.0.3/4.0/OWASP%20Application%20Security%20Verification%20Standard%204.0.3-en.pdf

Case Study #1 – Medium Sized City With OT

Organization Profile

- Population served around 100,000
- Annual IT budget between $5M+
- <30 IT staff members
- <2 dedicated security staff
- Critical services include police, fire, and water supply

Image source: https://www.wfla.com/wp-content/uploads/sites/71/2024/01/GettyImages-1176976078.jpg

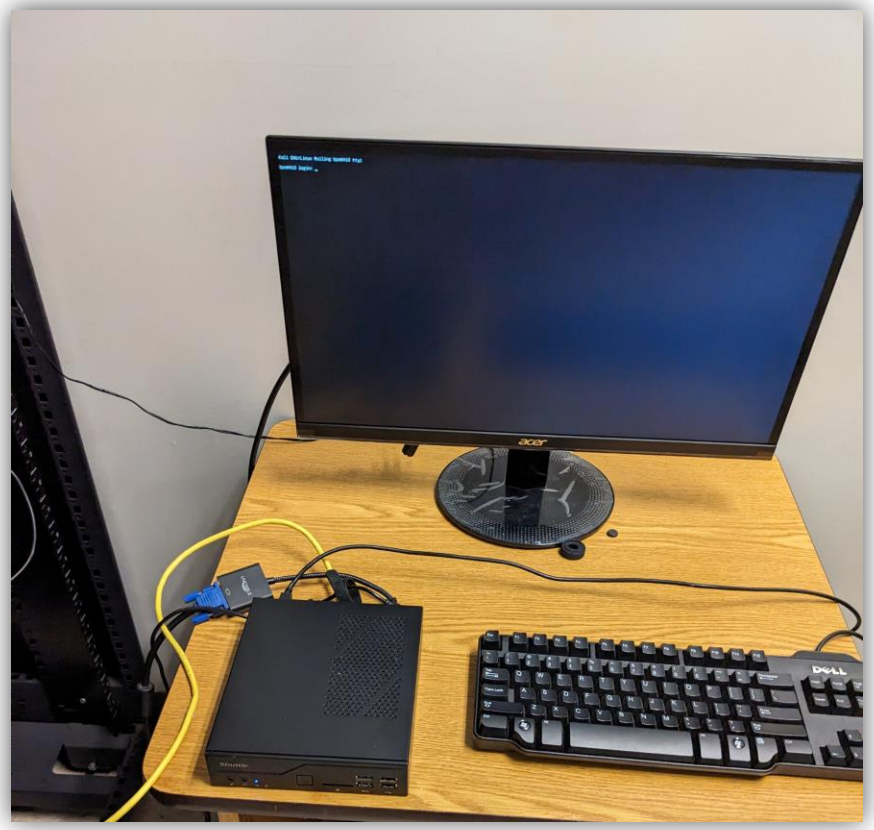
Engagement Scope

- Comprehensive network, building, OT, and employee security assessment
- Gain network credentials
- Compromise VPN access
- Access sensitive emails
- Corporate IT, CJIS, & OT/SCADA
- Demonstrate compromise of Active Directory
- Collaborative public works physical security assessment
- Three-person assessment team
- 14 day assessment window

Image source: https://tenor.com/view/my-voice-in-my-passport-verify-me-gif-15855016659239818687

Outcomes

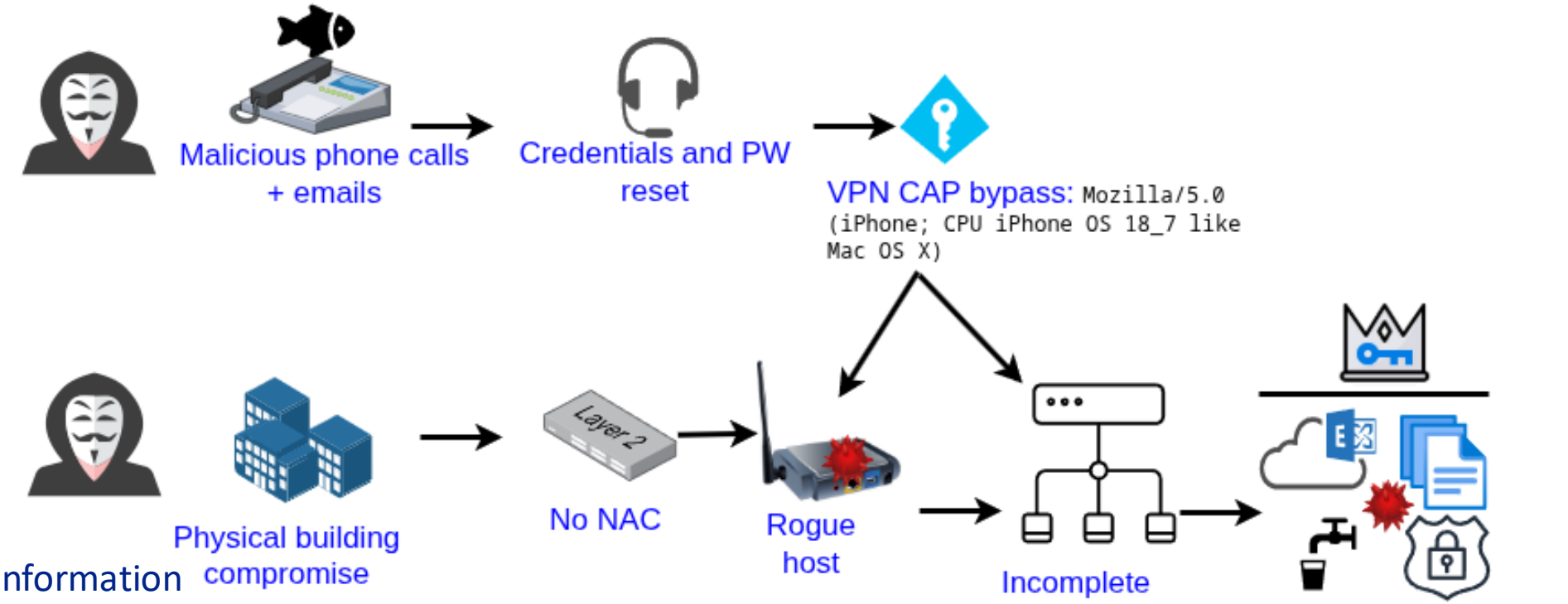
- Phone social engineering produced sensitive disclosures and one password
- Phishing yielded data submissions that enabled external footholds
- Visitor verification gaps enabled entry and movement without badges
- Door hardware misalignment enabled secure-area bypass
- Unlocked or weakly controlled server rooms allowed direct access
- A live internal port allowed a rogue host into the environment
- Internal AD & segmentation gaps enabled lateral movement + data exposure
- Perimeter was comparatively strong, but onsite paths bridged it to core systems



Putting It All Together

NIST CSF 2.0

- Risk Assessment
- Awareness and Training
- Data Security
- Continuous Monitoring
- Incident Analysis



MITRE ATT@CK

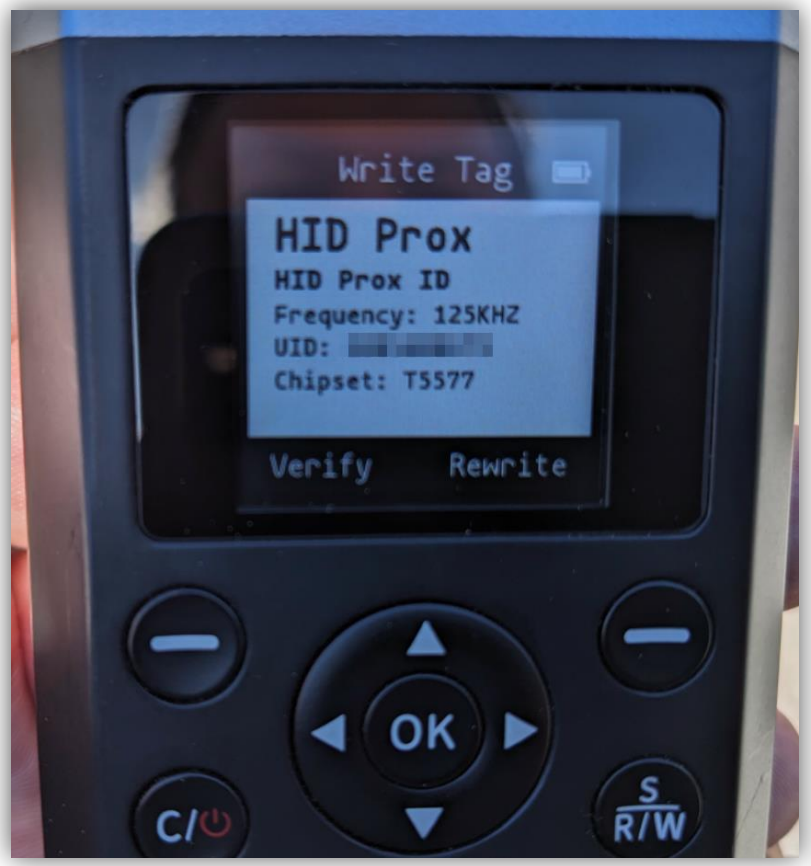
- T1589 – Gather Victim ID Information
- T1566 – Phishing
- T1078 – Valid Accounts
- T1556 – Modify Authentication Process
- T1200 – Hardware Additions
- T1039 – Data From Networked Drive
- T1550.003 – Steal or Forge Kerberos Tickets
- T1021 – Remote Services

Image source: https://xkcd.com/936/

- Shim tool made to disengage door latches

- Shrum tool made from plastic water jug

- Hook tool made from thick gauge piano wire



- iCopy-XS revealing HID Prox unencrypted RFID

- REX Sensor with temperature delta disabled

- “Secure” Shred Bin

Case Study #2 – Large City

Organization Profile

- Within the top 50 largest cities in the country
- Annual IT budget over $15M
- Over 100 IT staff members
- Five dedicated security staff

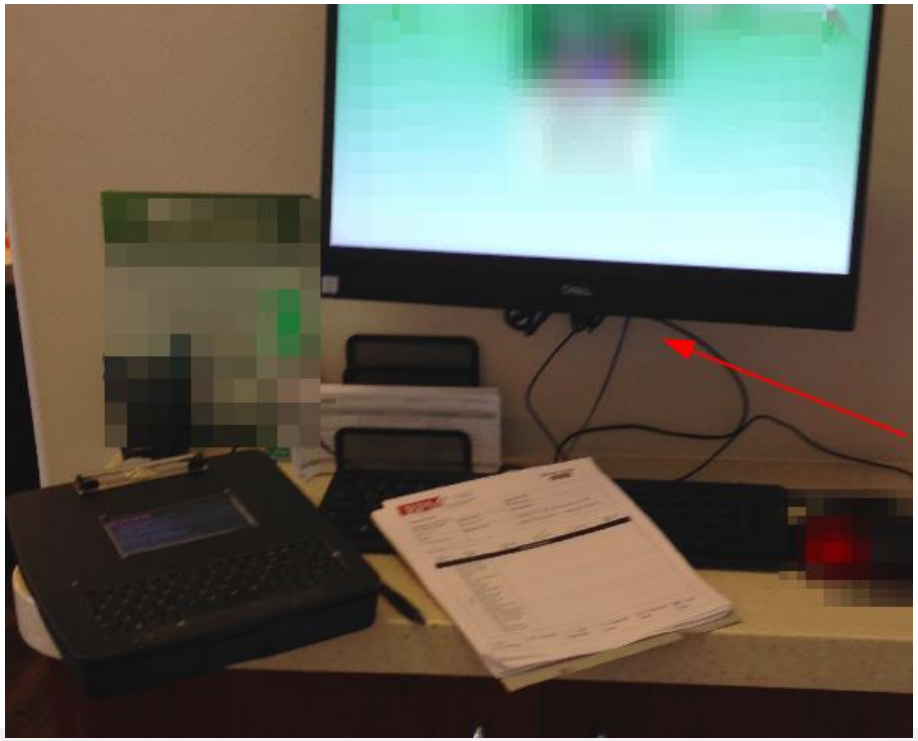
Image source: https://www.cisa.gov/sites/default/files/styles/hero_large/public/2022-12/banner_aboutcisa.png

Engagement Scope

- Targeted Red Team
- In-person physical assessment of 4 locations
- Attempt to gain internal network foothold
- Gain network credentials
- Compromise vulnerable SAP environment
- Demonstrate compromise of Active Directory
- One assessor went onsite
- Two remote operators on inbound shells
- 14 days of preparations
- 5 day assessment window

Outcomes

- In-person social engineering and physical security gaps led to full building access
- RFID badge credentials were found unattended and were cloned for later use
- Multi-function printers were trusted devices, network access controls did not recognize the spoofing of a MAC address
- A malicious rogue host was deployed to the internal network for persistence, an LTE modem provided external connectivity
- Unattended & unlocked workstations presented the opportunity to deploy C2 payloads
- High-end EDR was installed but did not prevent the deployment of C2 payloads
- EDR prevented common exploits, such as LSASS process extraction, but alerts were not monitored
- Internal Active Directory weaknesses enabled privilege escalation and environment compromise



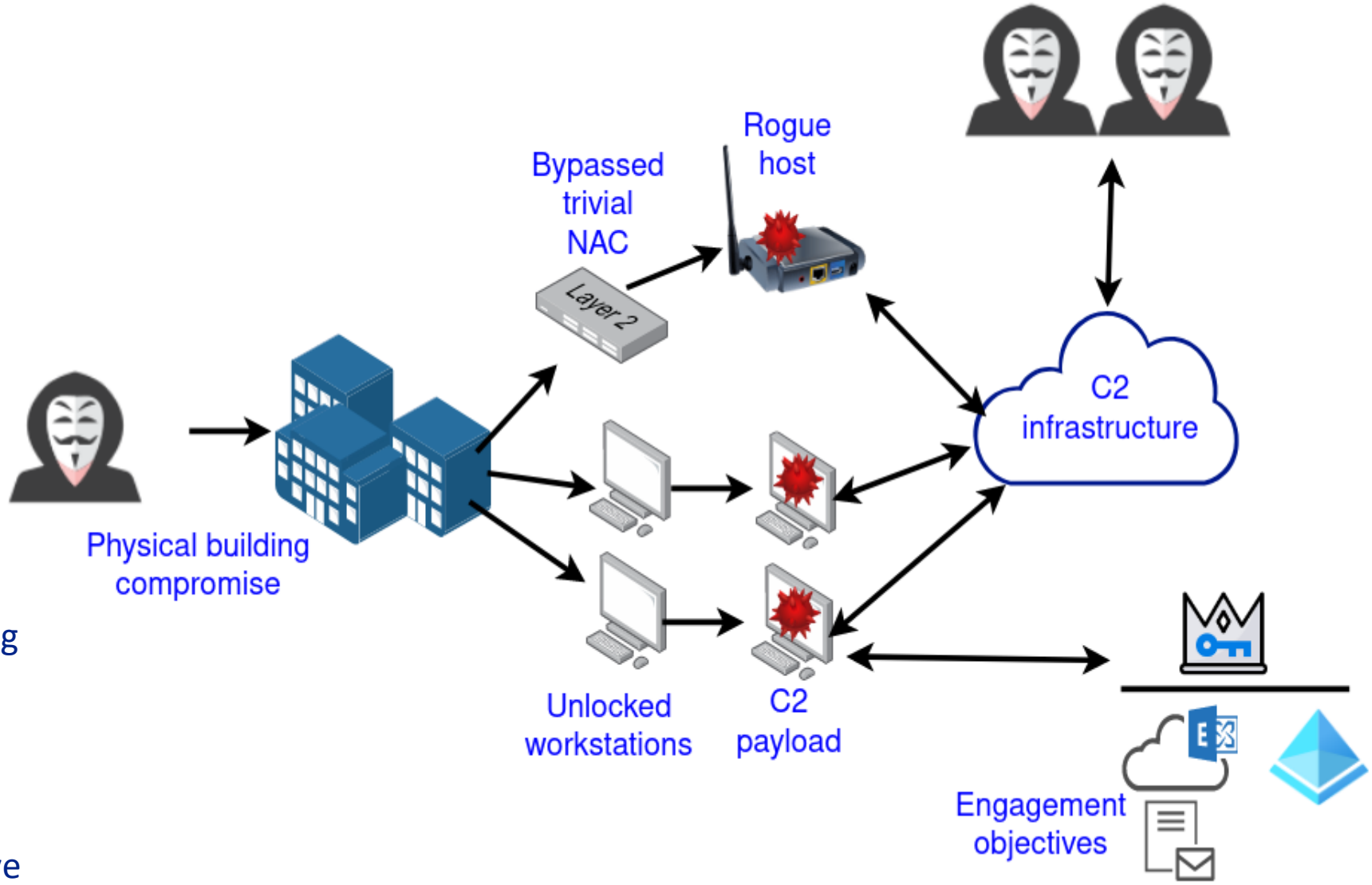
Putting It All Together

NIST CSF 2.0

- Risk Assessment
- Awareness and Training
- Data Security
- Continuous Monitoring
- Incident Analysis

MITRE ATT@CK

- T1078 – Valid Accounts
- T1098 – Account Manipulation
- T1543 – Create or Modify Process
- T1053 – Scheduled Task
- T1599 – Network Boundary Bridging
- T1562 – Impair Defenses
- T1539 – Steal Web Session Cookie
- T1083 – File & Directory Discovery
- T1135 – Network Share Discovery
- T1039 – Data From Networked Drive
- T1113 – Screen Capture



Case Study #3 – Small City

Organization Profile

- Not in the top 500 largest cities in the country
- Annual IT budget under $2M
- 2 IT staff members
- 0 dedicated security staff
- Public works of water treatment and distribution

Image source: https://www.wfla.com/wp-content/uploads/sites/71/2024/01/GettyImages-1176976078.jpg

Engagement Scope

- Expansive Network, Building, OT, and Employee Security Assessment
- Gain network credentials
- Compromise VPN access
- Access sensitive emails
- Facilitate a collaborative public works security assessment
- Three-person assessment team
- 14 day assessment window

Outcomes

- External network credentials were successfully guessed
- External email access located cleartext CJIS data
- A guessed employee account did not have MFA configured
- Multiple physical controls were ineffective
- Internal network access was accomplished VPN
- Internal file share access highlighted Police Department CJIS data being available to low-privilege users
- Well-known C2 binaries were not detected by EDR software

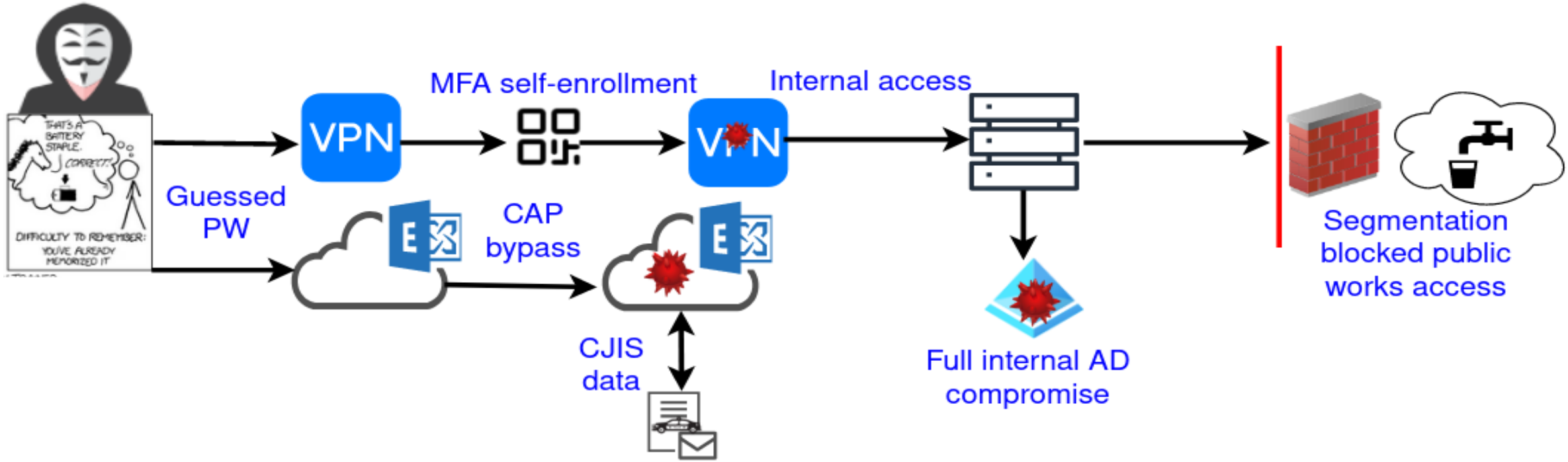


Image source: https://xkcd.com/936/

Outcomes

- External network credentials were successfully guessed
- External email access located cleartext CJIS data
- A guessed employee account did not have MFA configured
- Multiple physical controls were ineffective
- Internal network access was accomplished VPN

- Internal file share access highlighted Police Department CJIS data being available to low-privilege users
- Well-known C2 binaries were not detected by EDR software

- **A systemic lack of employee security training**

ONSITE SOCIAL ENGINEERING MATRIX				
Roaming	Authentication	Verification	Monitoring	
Challenged on Entry	Government photo ID	Verification call	Challenged without Escort	Fully Escorted
▼	▼	▼	▼	▼
▲	▲	▲	▲	▲
▼	▼	▼	▼	▼
▼	▼	▼	▼	▼
▼	▼	▼	▼	▼
▼	▼	▼	▲	▼
▼	▼	▼	▼	▼
▼	▼	▼	▼	▼
▼	▼	▼	▼	▼
▼	▼	▼	▼	▼
▼	▼	▼	▼	▼

Image source: https://xkcd.com/936/

Wrap Up

Key Takeaways

1. Regardless of budget, local government IT departments are at a disadvantage
2. Existing frameworks support internal dialogue and efficient security program structure
3. External social engineering and MFA bypass techniques dominate initial access
4. Role-based access controls often fall short & are not updated for privilege drift
5. Network access controls should be a top priority to protect public facing facilities
6. No EDR platform is infallible
7. Network segmentation is highly effective at reducing breach impact

Questions?

jschmidt@bpm.com - https://linkedin.com/in/jschmidt-bpm

lwagoner@bpm.com

http://bpm.com/cybersecurity