PURPLE PROTOCOL

DEF CON 34

Lab Setup

If you haven't downloaded the VM from the Github, we have Flash Drives with the VMs on them that can be copied over.

You will need VMWare Workstation; this is also on the Flash Drive

These are for you to take home to continue playing in these environments.

Lab Setup Instructions

Unzip

Unzip the file “Purple Protocol.7z”

Launch

Launch VMWare Workstation

Navigate

In VMWare Workstation:

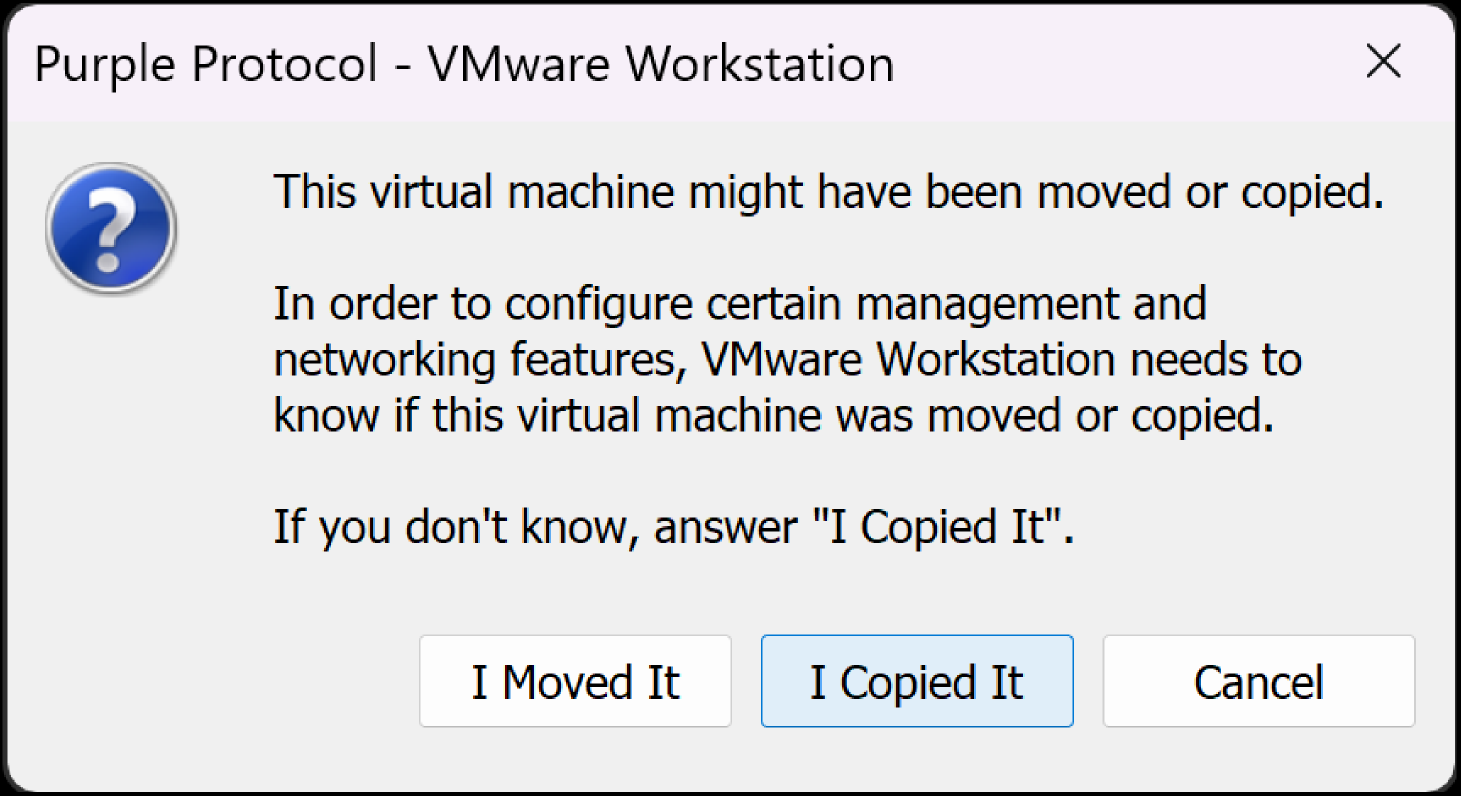
File >
Open >
[FilePath] >
Purple Protocol.vmx

Power on

Power on this Virtual Machine

Lab Setup Instructions Cont.

- Click "I copied it"



Purple Protocol - VMware Workstation

This virtual machine might have been moved or copied.

In order to configure certain management and networking features, VMware Workstation needs to know if this virtual machine was moved or copied.

If you don't know, answer "I Copied It".

“If you know the enemy and know yourself, you need not fear the result of a hundred battles”

-Sun Tzu

Introduction

- Who are we?

Marba$

- Manager of an Offensive Security Team
- Background in AppSec/Operations 14+ years
- Founder of DC207 (Maine's DEF CON Group)
- Author of The Vulnerability Researcher's Handbook
- 30+ CVEs in various states of publishing

- When not poking holes and exploring tech, I'm picking bluegrass licks on banjos or wrangling my two chaotic cats, Dionysius & Louis Thanksgiving.

‹packt›

1ST EDITION

The Vulnerability Researcher's Handbook

A comprehensive guide to discovering, reporting, and publishing security vulnerabilities

BENJAMIN STROUT

D43m0n

- Senior Penetration Tester with 4+ years of cybersecurity experience
- Advanced Certifications:
  - OSEP, OSWE, OSCP, CRTO, CARTP, EWPTX
- CVE Holder: CVE-2025-26332
- Author of article "Debugging CVE-2023-37679: A Step-by-Step Guide to Fixing the Windows Exploit"

- Passionate researcher with a deep love for the outdoors.

PilotPat

- AKA Patrick
- Holds OSCP and CTRO certifications
- Worked in Cybersecurity for 10 years
  - Incident Response
  - Network Security Engineering
  - Security Architecture
  - Vulnerability Management
  - Penetration Testing/Red Team Ops
- Led the effort to build a new Purple Team program at current organization
- Passionate gamer with a deep love for the indoors

Agenda

- Lab Setup – 10 Min
- Red Team Ops – 10 Min
- Blue Team Ops – 10 Min
- Threat Intelligence – 10 Min
- MITRE ATT&CK – 5 Min
- Lab 1 – 20 Min
- Break – 15 Min
- Lab 1 Review – 20 Min
- Purple Teaming – 10 Min
- Atomic Red Team – 5 Min
- Lab 2 – 20 Min
- Lab 2 Review – 20 Min
- Break – 15 Min
- Vectr – 5 Min
- Lab 3 – 30 Min
- Lab 3 Review – 30 Min
- Finding Artifacts – 5 Min
- Q&A – As time permits

What is
Red Team Ops?

- Threat Intelligence Led Adversary Emulation
- Form of Offensive Security
- Execution of attacks on an organization using Tactics, Techniques, and Procedures (TTPs) of a known Adversary
- Done *without* Blue Team Knowledge
- Tests People, Processes, and Technology

People Processes and Technology

- Testing Technology
  - Do we have logs set up?
  - Do we Alert as needed?
  - Do our tools block Malicious execution?
- Testing Processes
  - Do we have playbooks set up for given response scenarios?
  - Do we have playbooks for Threat Hunters to follow or are they indiscriminately searching through logs?
- Testing People
  - Are our people following those Processes?
  - Are they trained on the Processes and Technology?

Tactics Techniques and Procedures (TTPs)

Tactics	Phase of the attack
Techniques	“How” an adversary achieves its tactical goal
Procedures	The specific implementation an adversary uses for techniques

Tactics

- The adversary’s tactical goal
- What the adversary is attempting to accomplish during that phase of the attack
- Recon, Initial Access, Defense Evasion, Credential Access, etc.

Techniques

- To complete the **Tactic** of "Credential Access," an adversary may use **Techniques** like dumping LSASS, employing credential dumping tools, or exploiting weak password policies.
- Represents the “how” an adversary achieves its tactical goal.
- Example: To achieve “Credential Access” the adversary may dump LSASS

Procedures

- The specific implementation an adversary uses for techniques
- EXAMPLE: The Threat Actor used Mimikatz with the specific command: !SEKURLSA::LOGONPASSWORDS

What is Blue Team Ops?

- Incident Response
- Threat Hunting
- Threat Detection Engineering

Incident Response

- Reactive
- Responds to alerts provided to them via AV/EDR, SIEM, etc.
- Typically responsible for containing, remediating, and eradicating the threat

Threat Hunting

- Proactive
- Searches through logs in SIEM, EDR, etc. to find artifacts of a potential attack
- Uses IOCs from Threat Intelligence to try to determine if threat actors who have breached other networks have done the same to theirs
- Looks for anomalies in datasets that may indicate a Threat Actor’s presence
- Escalates findings to Incident Response if needed

Threat Detection Engineering

- Creates rules in SIEM, UBA, EDR, etc. to generate high-fidelity alerts for Incident Response
- Works with Red Team to generate alerts against relevant TTPs
- Responsible for closing cyber security visibility gaps

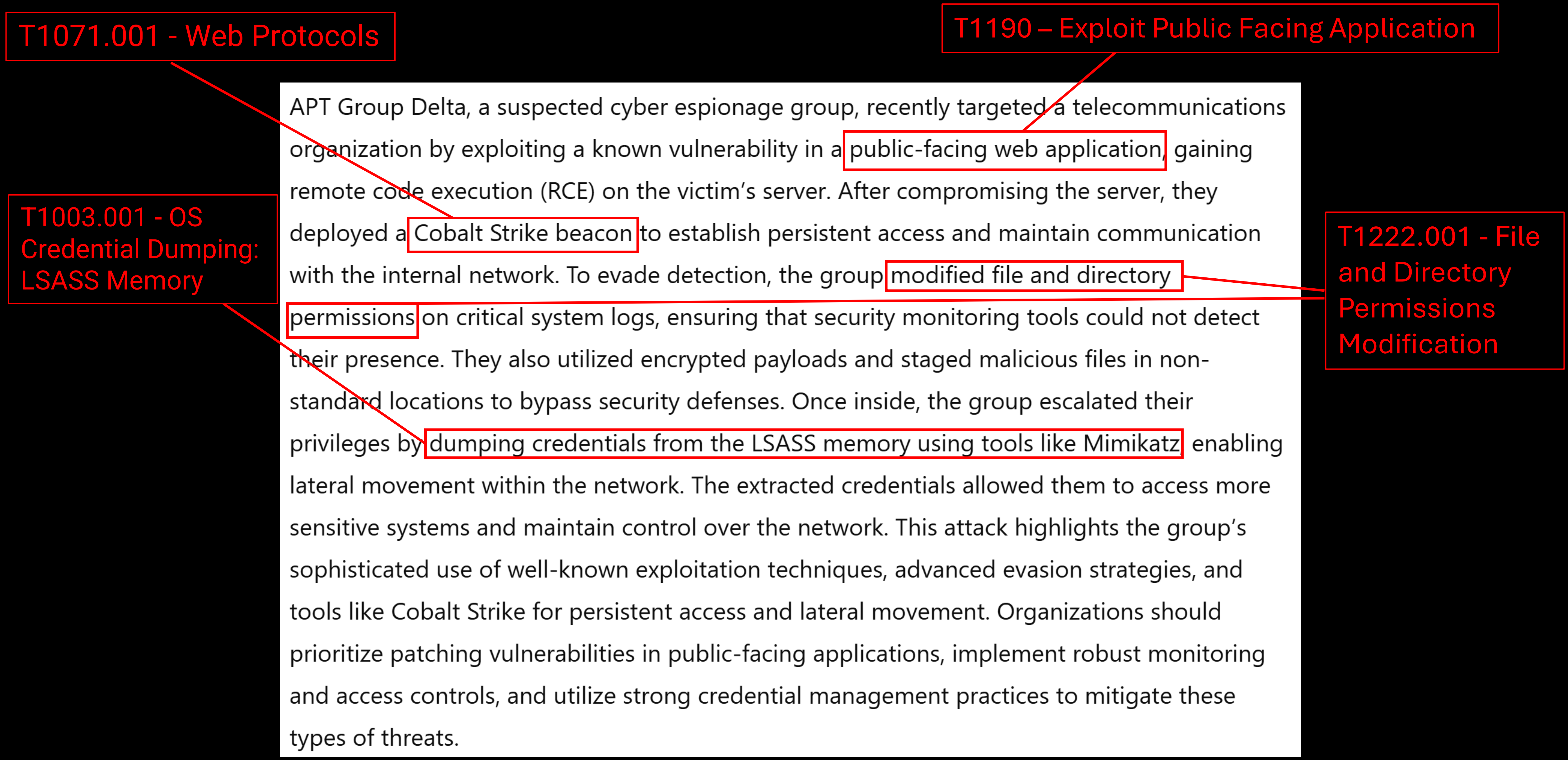
Finding Artifacts

- Local logs
  - Windows Event Viewer
- Centralized Logs
  - Security Information and Event Manager (SIEM)
  - Cloud Managed Endpoint Detection and Response (EDR)
  - Cloud Managed User Behavior Analytics (UBA)
- Alerts
  - Antivirus (AV)/EDR
  - Intrusion Prevention System (IPS)/Intrusion Detection System (IDS)
- Blocks
  - AV/EDR
  - IPS/IDS
  - Web Application Firewall (WAF)

- There are so many vendor solutions for all these items this is something that will have to be learned with experience in each product, but each vendor's solution are relatively similar in nature

What is Threat Intelligence?

- Cyber Research relating to threat actor behaviors
  - Tactics Techniques and Procedures (TTPs)
  - Trends among threat actor groups
    - Who they may be targeting
    - New Tools or Vulnerabilities leveraged
- Provides reports on emerging threats
- Red Team sometimes has to infer TTPs from these reports



T1071.001 - Web Protocols

T1190 – Exploit Public Facing Application

T1003.001 - OS Credential Dumping: LSASS Memory

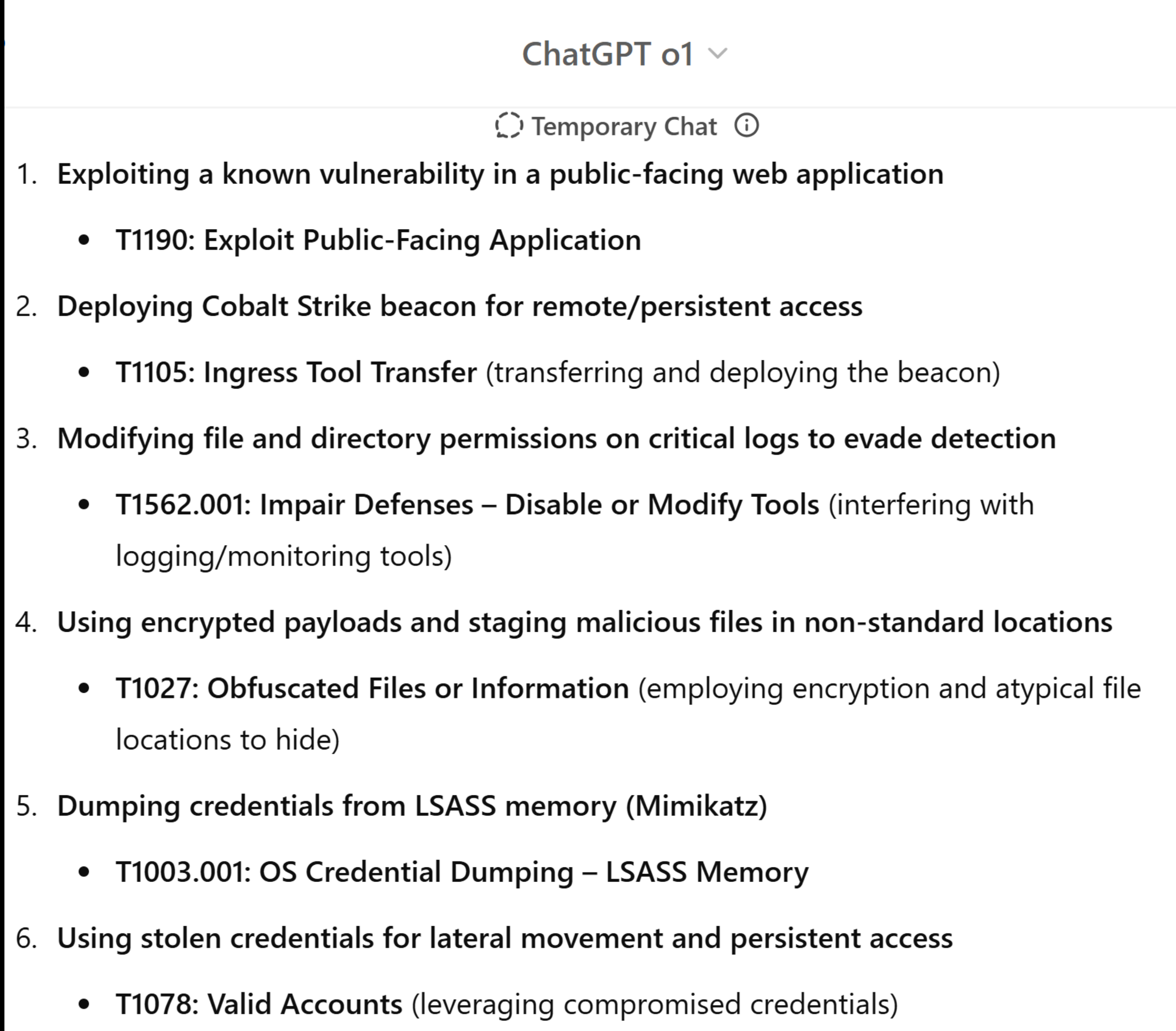
T1222.001 - File and Directory Permissions Modification

APT Group Delta, a suspected cyber espionage group, recently targeted a telecommunications organization by exploiting a known vulnerability in a public-facing web application, gaining remote code execution (RCE) on the victim's server. After compromising the server, they deployed a Cobalt Strike beacon to establish persistent access and maintain communication with the internal network. To evade detection, the group modified file and directory permissions on critical system logs, ensuring that security monitoring tools could not detect their presence. They also utilized encrypted payloads and staged malicious files in non-standard locations to bypass security defenses. Once inside, the group escalated their privileges by dumping credentials from the LSASS memory using tools like Mimikatz, enabling lateral movement within the network. The extracted credentials allowed them to access more sensitive systems and maintain control over the network. This attack highlights the group's sophisticated use of well-known exploitation techniques, advanced evasion strategies, and tools like Cobalt Strike for persistent access and lateral movement. Organizations should prioritize patching vulnerabilities in public-facing applications, implement robust monitoring and access controls, and utilize strong credential management practices to mitigate these types of threats.

Parsing TTPs from a Threat Intel Report

ChatGPT

Because aint nobody got time for that



1. **Exploiting a known vulnerability in a public-facing web application**
   - **T1190: Exploit Public-Facing Application**
2. **Deploying Cobalt Strike beacon for remote/persistent access**
   - **T1105: Ingress Tool Transfer** (transferring and deploying the beacon)
3. **Modifying file and directory permissions on critical logs to evade detection**
   - **T1562.001: Impair Defenses – Disable or Modify Tools** (interfering with logging/monitoring tools)
4. **Using encrypted payloads and staging malicious files in non-standard locations**
   - **T1027: Obfuscated Files or Information** (employing encryption and atypical file locations to hide)
5. **Dumping credentials from LSASS memory (Mimikatz)**
   - **T1003.001: OS Credential Dumping – LSASS Memory**
6. **Using stolen credentials for lateral movement and persistent access**
   - **T1078: Valid Accounts** (leveraging compromised credentials)

Advanced Persistent Threats (APTs)

- Threat Actors are organized into APTs based on the following:
  - Countries they target
  - Industries they target
  - Their motivations
    - Financial
    - Hacktivist
    - Espionage
- The APTs you want to emulate are the ones who attack organizations similar to yours.

APT Spotlight: Scattered Spider

- Wrecked MGM and Caesars Casinos soon after DC31
- This cost these organizations over $100M in damages

Image Source: CrowdStrike, Jan. 2023

MGM/Caesars Breach Comparison

MGM Breach

- Initial Access:
  - Spearphishing via Voice – T1566.004
- Persistence:
  - Valid Accounts – T1078
  - Create Account – T1136
  - Domain Trust Modification: Add Trusted Domain – T1484.002
- Privilege Escalation:
  - Valid Accounts: Cloud Accounts – T1087.004

Caesars Breach

- Initial Access:
  - Spearphishing via Voice – T1566.004
- Persistence:
  - Valid Accounts – T1078
  - Create Account – T1136
  - Domain Trust Modification: Add Trusted Domain – T1484.002
- Privilege Escalation:
  - Valid Accounts: Cloud Accounts – T1087.004

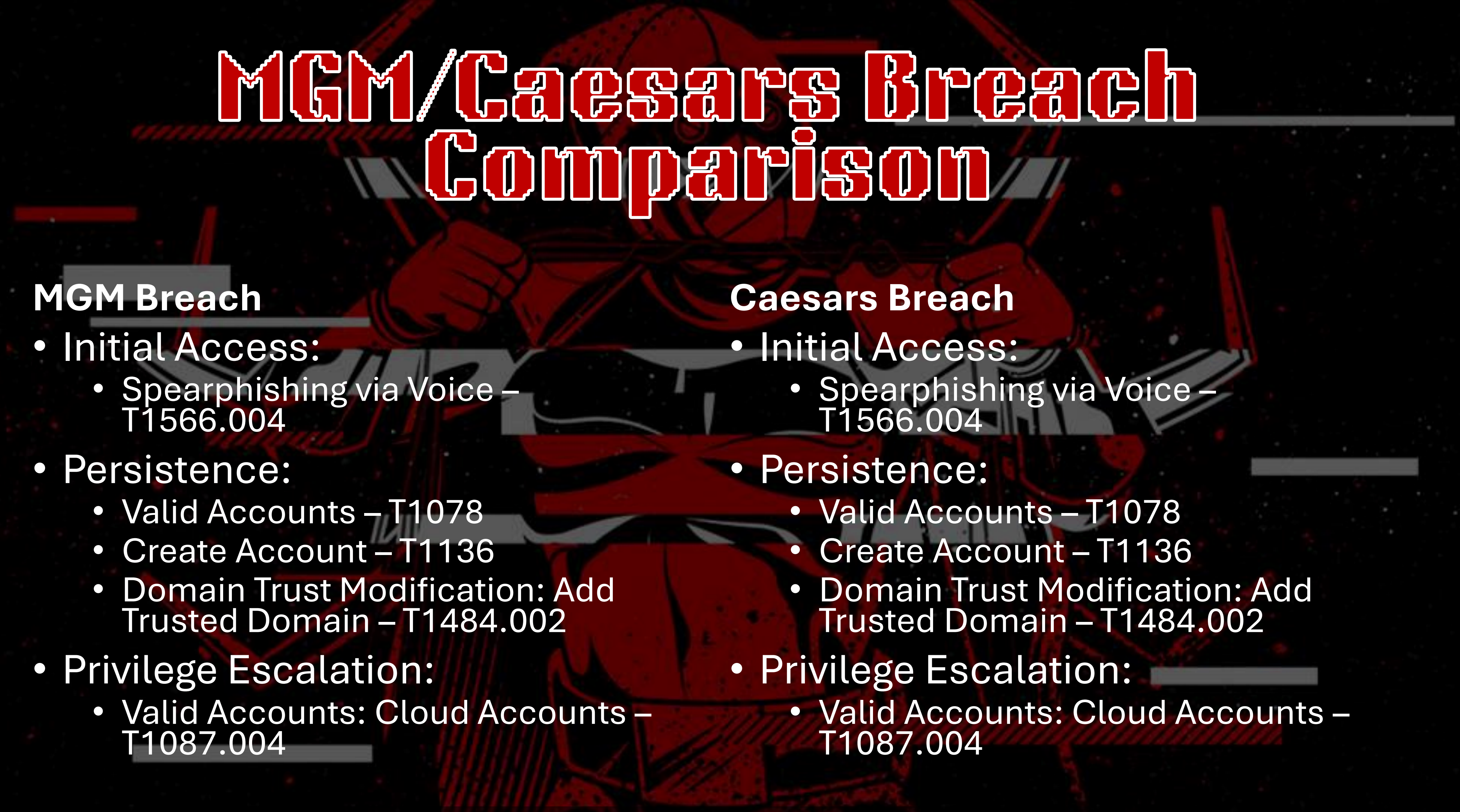
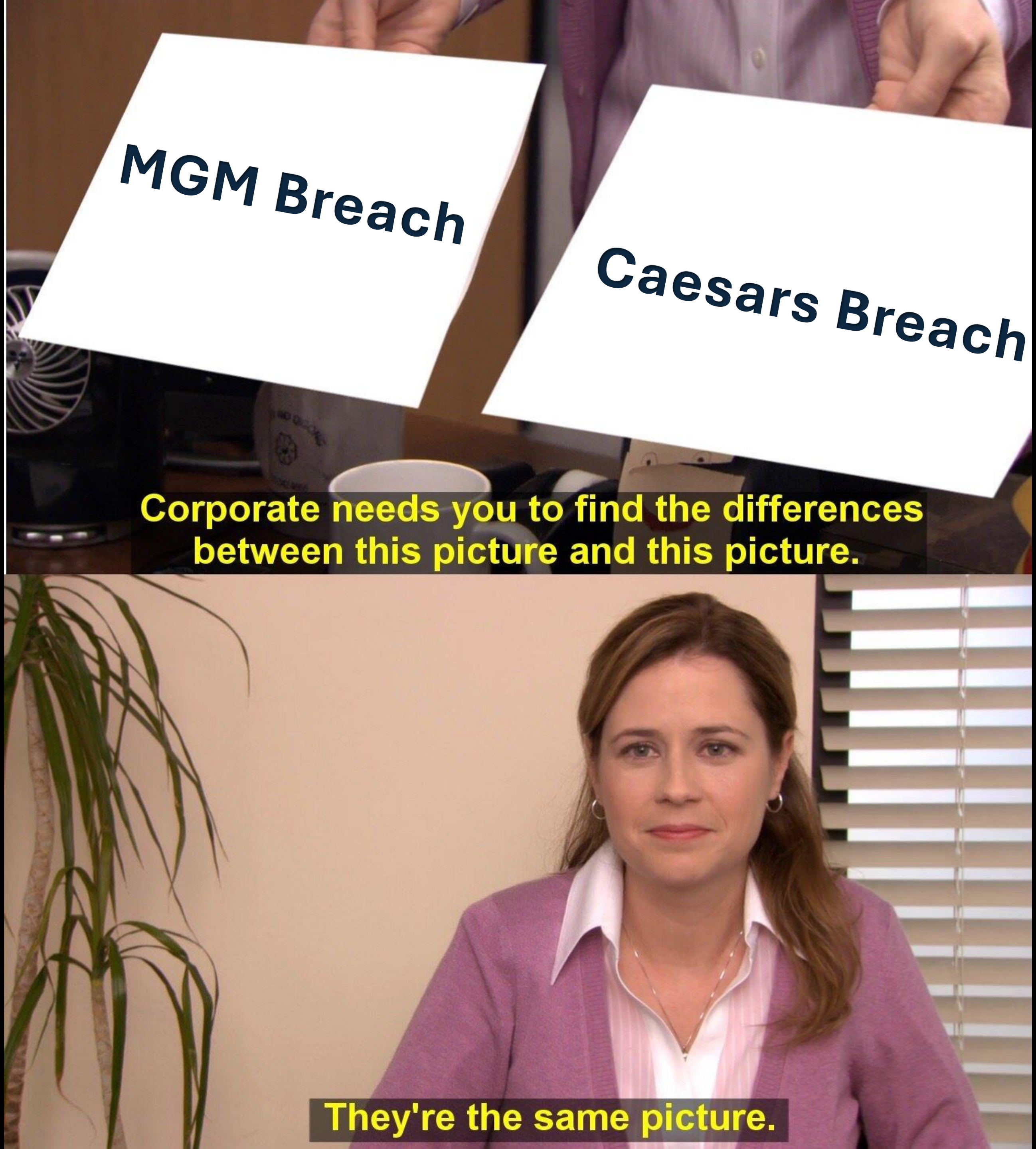


Image Source: CrowdStrike, Jan. 2023


MGM Breach
Caesars Breach
Corporate needs you to find the differences between this picture and this picture.
They're the same picture.

MITRE ATT&CK Framework

MITRE ATT&CK Framework

- Framework used to help organize TTPs used by Threat Actors
- 14 Tactics
- 202 Techniques
- 435 Sub-Techniques

MITRE ATT&CK Navigator

Open-Source tool by MITRE to help visualize an APT's attack chain

Helps organize APTs into executable test cases in an automated way, vs cross referencing threat intel and mapping to MITRE ATT&CK manually

Lab 1: Threat Intel

20 Minutes

Lab 1 Review

20 minutes

What is Purple Teaming?

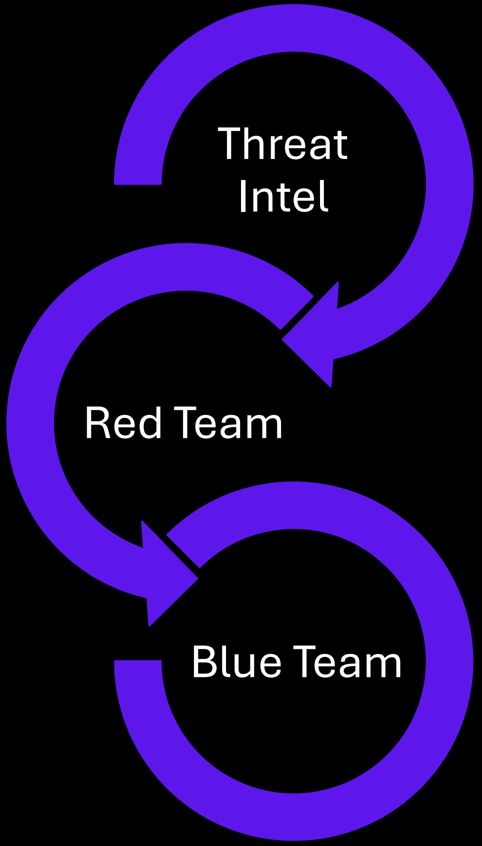
(Finally)

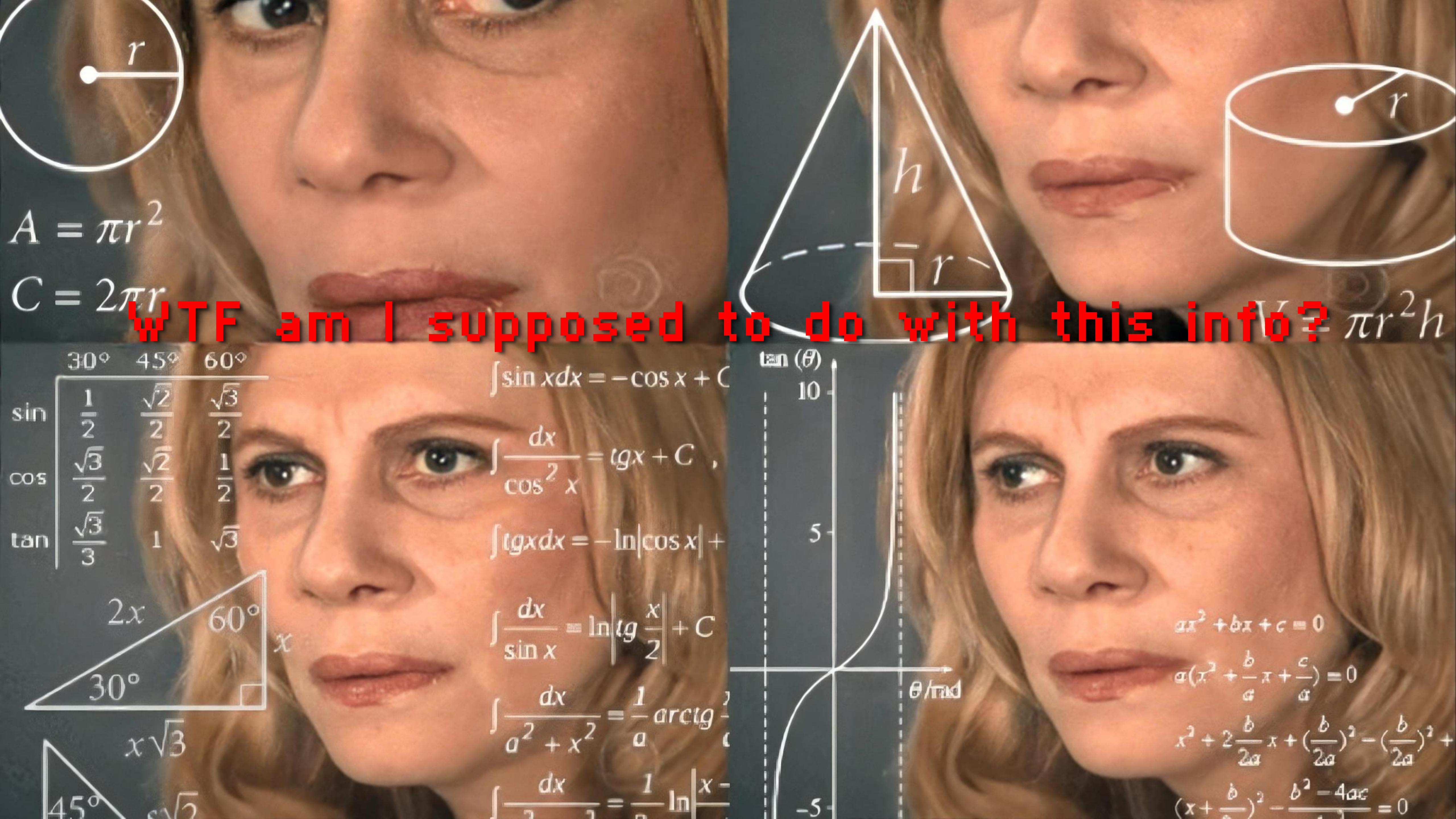
What is Purple Teaming?

- **Red Team** and **Blue Team** collaboration
- Red Team uses Threat Intelligence research to determine which adversaries to test against, which techniques to test against, then executes the test cases with the Blue Team watching
- Results are documented
- Failed Test Cases are then remediated by Blue Team

Purple Team Lifecycle

- Threat Intel Provides TTPs for a relevant threat actor to Red Team
- Red Team tests TTPs against environment
- Blue Team takes results of tests, documents them, and works on remediating failed test cases




WTF am I supposed to do with this info?
r
A = πr²
C = 2πr
h
r
V = πr²h
30° 45° 60°
sin 1/2 √2/2 √3/2
cos √3/2 √2/2 1/2
tan √3/3 1 √3
2x
60°
x
30°
x√3
45°
∫sin xdx = −cos x + C
∫dx/cos²x = tgx + C
∫tgxdx = −ln|cos x| + C
∫dx/sin x = ln|tg x/2| + C
∫dx/(a² + x²) = 1/a arctg
tan (θ)
10
5
−5
θ/rad
ax² + bx + c = 0
a(x² + b/a x + c/a) = 0
x² + 2 b/2a x + (b/2a)² − (b/2a)² +
(x + b/2a)² − (b² − 4ac)/4a² = 0

Red Canary
Atomic Red Team

- Developed by Red Canary, a Managed Detection and Response organization.
- An open-source library of adversary emulation tests that are pre-packaged and organized by MITRE Technique and Sub-technique Number
- Easy way to execute test cases in an organized and methodical way

Lab 2: Atomic Red Framework

20 Minutes

Lab 2 Review

10 Minutes

Purple Team Organization with Vectr™

Security Risk Advisor's Open-Source Purple Teaming Platform

vectr

- Platform for organizing Purple Team activities
- Threat Simulation Index
  - Threat Intel Led benchmark of common threat actor TTPs
- Build out Assessments
  - Build Campaigns inside of assessments
- Manages Attack Timeline, Operators Guidance, Defense Activity, Detection Time, Outcome Notes, Detection/Prevention Guidance, Test Case Outcome, and Evidence Files

Lab 3:
Purple Team Planning and Execution

30 Minutes

Lab 3 Review

30 Minutes

Recap

Setting up a Purple Team

- **Identify your adversary**
  - MITRE CTI/MITRE ATT&CK Navigator
- **Create an assessment/campaign**
  - Add Test Cases to Vectr
- **Execute Test Cases**
  - Utilize Atomic Red Team's Atomics to help with Test Case execution
- **Generate Reporting**
  - Utilize Vectr Reports for Stakeholders
- **Remediate**
  - Send Failed Test Cases to Blue Team for remediation
- **Repeat for new Adversaries**

Q&A

CTF

Sources/References:

- https://www.atomicredteam.io/
- https://vectr.io/
- https://attack.mitre.org/matrices/enterprise/
- https://mitre-attack.github.io/attack-navigator/
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-263a
- https://cloud.google.com/blog/products/identity-security/okta-social-engineering-campaign-unc3944
- https://www.microsoft.com/en-us/security/blog/2023/10/04/scattered-spider-ransomware-gang-uses-identity-attacks-in-recent-campaigns/
- https://www.wired.com/story/mgm-caesars-hack-scattered-spider-ransom/
- https://www.bloomberg.com/news/articles/2023-09-14/caesars-paid-millions-to-hackers-while-mgm-battled-ransomware
- https://www.bleepingcomputer.com/news/security/alphv-ransomware-gang-took-6tb-of-data-in-mgm-cyberattack/
- https://www.reuters.com/technology/caesars-paid-tens-millions-ransom-after-recent-cyberattack-wsj-2023-09-13/
- https://www.securityweek.com/scattered-spider-hackers-use-social-engineering-against-okta/