Commando VM: Looking Around

home-lab commando fireeye openvpn burp 7zip winrar cmder greenshot windump payloadsallthethings seclists fuzzdb foxyproxy x64dbg dnspy Ida ghidra gobu

Apr 10, 2019

Having built my CommandoVM in a previous post, now I am going to look at what's installed, and what else I might want to add to the distribution. I'll start with some tweaks I made to get the box into shape, check out what tools are present, and add some that I notice missing. After this, in I'll use the VM to work a HTB target, and report back on in a future post.

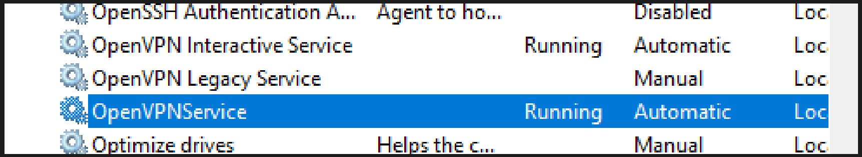
Accounts

I probably should have addressed this in the opening post. Since I'm using this machine exclusively to work on HackTheBox and other CTF challenges, I'm going to take a similar approach as I did with Kali where I run as root, and run a single user in the Administrators group. If I were a PenTester dealing with customer or other sensative data, I would look into running as a non-privileged user and increasing my operational security.

Getting Connected - OpenVPN

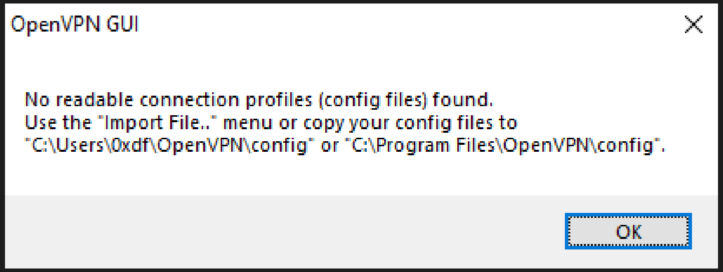
I'll needed to connect to the HackTheBox vpn. In Kali, I'd simple run `openvpn [my config file]` in a terminal window. In Windows, it's different.

First, I enabled the OpenVPN service. I hit windows key and then typed services, and opened it. Then I scrolled down to OpenVPNService, right clicked, and hit run. I did the same with the OpenVPN Interactive Service. I then double clicked on both, and changed their startup type to Automatic:



OpenSSH Authentication A...	Agent to ho...		Disabled	Loc
OpenVPN Interactive Service		Running	Automatic	Loc
OpenVPN Legacy Service			Manual	Loc
OpenVPNService		Running	Automatic	Loc
Optimize drives	Helps the c...		Manual	Loc

Then I opened OpenVPN from the start menu. It's important to run this as an Administer, as only an admin can add the interfaces necessary to complete the connection. The first thing I got was a popup saying that there were no config files found:

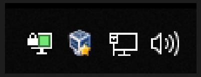


OpenVPN GUI

No readable connection profiles (config files) found.
Use the "Import File.." menu or copy your config files to
"C:\Users\0xdf\OpenVPN\config" or "C:\Program Files\OpenVPN\config".

I also noticed the OpenVPN icon appears in the notification icons:

I right clicked on it, and selected "Import file…". I found `0xdf.ovpn`, and it imported successfully. Now I can right click on the status icon and say "Connect". The status window pops up, and after a minute, goes away. The icon is now green:



And I can `ping` htb hosts:

```
C:\Users\0xdf>\Windows\System32\PING.EXE 10.10.10.113

Pinging 10.10.10.113 with 32 bytes of data:
Reply from 10.10.10.113: bytes=32 time=18ms TTL=63
Reply from 10.10.10.113: bytes=32 time=18ms TTL=63
Reply from 10.10.10.113: bytes=32 time=17ms TTL=63
Reply from 10.10.10.113: bytes=32 time=20ms TTL=63

Ping statistics for 10.10.10.113:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% los." | relative_url }}),
Approximate round trip times in milli-seconds:
    Minimum = 17ms, Maximum = 20ms, Average = 18ms
```

Configurations

Path

When I opened `cmd` and tried to ping something to check my VPN connection, I got a strange result:

```
C:\Users\0xdf>ping 10.10.10.109
Use: C:\Python27\Scripts\ping.py <src ip> <dst ip>
```

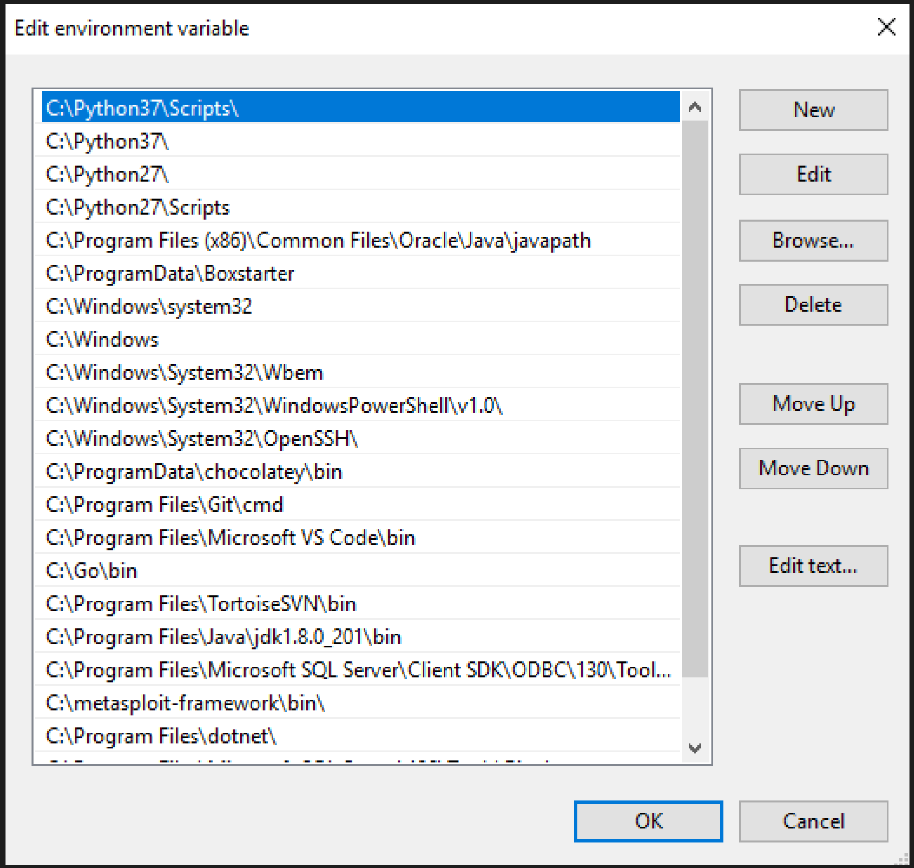
If I try `ping.exe`, it works as expected:

```
C:\Users\0xdf>ping.exe 10.10.10.109

Pinging 10.10.10.109 with 32 bytes of data:
Reply from 10.10.10.109: bytes=32 time=20ms TTL=63
Reply from 10.10.10.109: bytes=32 time=21ms TTL=63
Reply from 10.10.10.109: bytes=32 time=18ms TTL=63
Reply from 10.10.10.109: bytes=32 time=19ms TTL=63

Ping statistics for 10.10.10.109:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% los." | relative_url }}),
Approximate round trip times in milli-seconds:
    Minimum = 18ms, Maximum = 21ms, Average = 19ms
```

Looking at the path shows me why:

```
C:\Users\0xdf>echo %PATH%
C:\Python37\Scripts\;C:\Python37\;C:\Python27\;C:\Python27\Scripts;C:\Program File
```

I'm sure it makes sense to have all those things in the path, but I'd like to have system32 at the front of that list. I'll hit Windows key, and type "This PC", then right click and select "Properties". –> "Advanced System Settings" –> Environment Variables". I'll find "Path" in System Variables (the bottom window) and click edit:



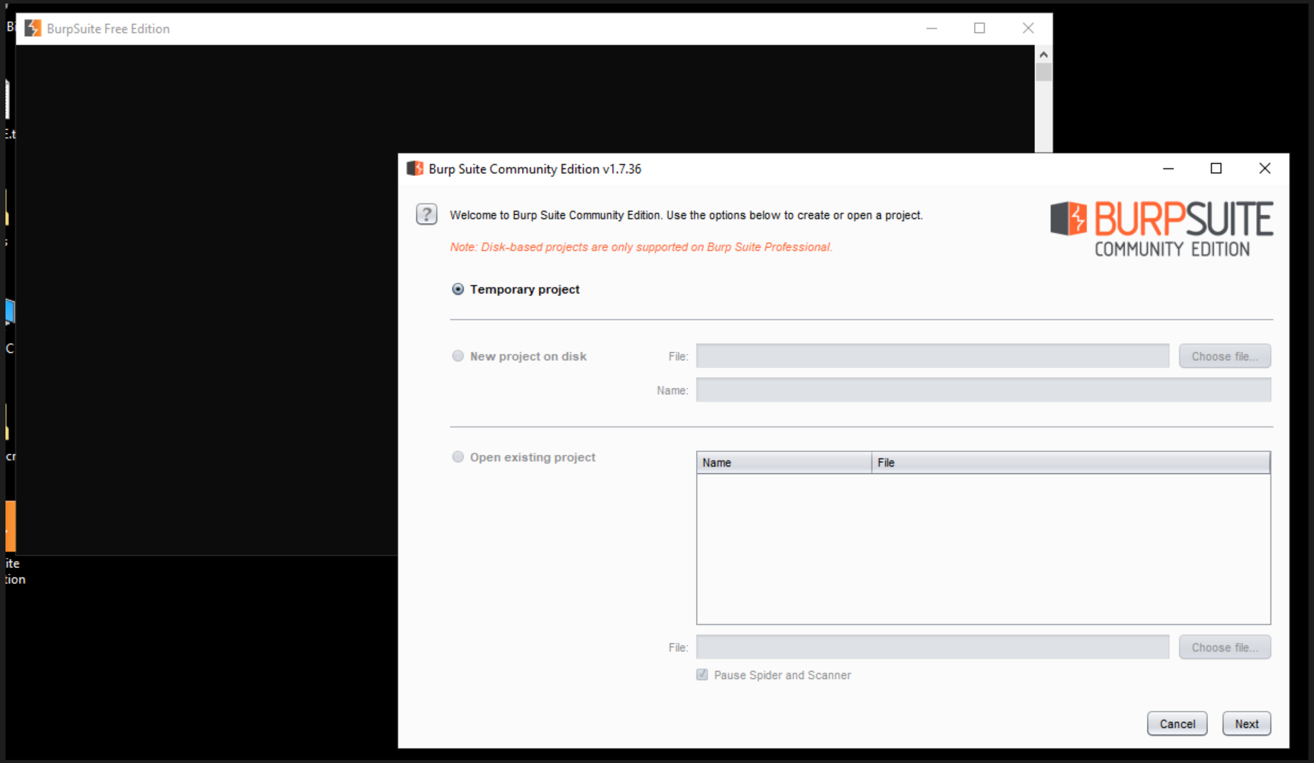
C:\Python37\Scripts\
C:\Python37\
C:\Python27\
C:\Python27\Scripts
C:\Program Files (x86)\Common Files\Oracle\Java\javapath
C:\ProgramData\Boxstarter
C:\Windows\system32
C:\Windows
C:\Windows\System32\Wbem
C:\Windows\System32\WindowsPowerShell\v1.0\
C:\Windows\System32\OpenSSH\
C:\ProgramData\chocolatey\bin
C:\Program Files\Git\cmd
C:\Program Files\Microsoft VS Code\bin
C:\Go\bin
C:\Program Files\TortoiseSVN\bin
C:\Program Files\Java\jdk1.8.0_201\bin
C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\130\Tool...
C:\metasploit-framework\bin\
C:\Program Files\dotnet\

I'll select `C:\Windows\System32` and click "Move Up" until it's at the top. Then hit ok, and `ping` works again.

Burp

I almost always want Burp open when I'm using this VM, but for some reason, Windows doesn't like pinning shortcuts to jar files to the taskbar. I overcame this by creating a copy of the shortcut onto my desktop. Then I edited the “Target” from `C:\ProgramData\chocolatey\lib\burp-suite-free-edition\tools\app\burpsuite.jar` to `%SystemRoot%\System32\cmd.exe /C "C:\ProgramData\chocolatey\lib\burp-suite-free-edition\tools\app\burpsuite.jar"`. I could right click on that shortcut, select “Pin to taskbar”, and now I had it handy. I can also delete the shortcut on the desktop and the pinned shortcut still works.

But that shortcut launches a cmd window that just waits for Burp to close. That’s annoying:



BurpSuite Free Edition

Burp Suite Community Edition v1.7.36

Welcome to Burp Suite Community Edition. Use the options below to create or open a project.

Note: Disk-based projects are only supported on Burp Suite Professional.

● Temporary project

○ New project on disk File: Name:

○ Open existing project

Name	File

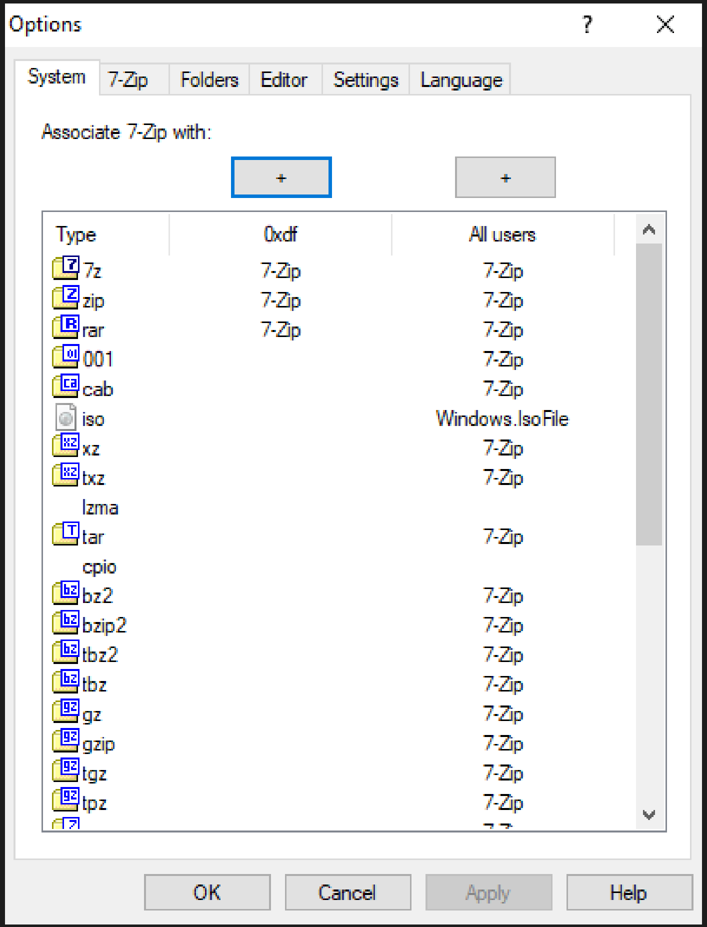
File:

☑ Pause Spider and Scanner

I’ll change the target again to `%SystemRoot%\System32\cmd.exe /C "start ^"^" ^"C:\ProgramData\chocolatey\lib\burp-suite-free-edition\tools\app\burpsuite.jar^"`. Now it starts Burp and then cmd window pops for a flash, but then goes away.

7zip > WinRar

All archive formats are set to open in WinRar by default. I don’t love WinRar, and much prefer 7zip, so I want to change 7zip to be the default. I’ll open 7zip by hitting Windows key and starting to type it out. When I see it, I’ll run it as admin (necessary to change default extension handling). Under “Tools” –> “Options…” the first thing to pop up is the “System” tab, which has a list of types to associate 7zip with. I’ll click on each until it is how I want it:



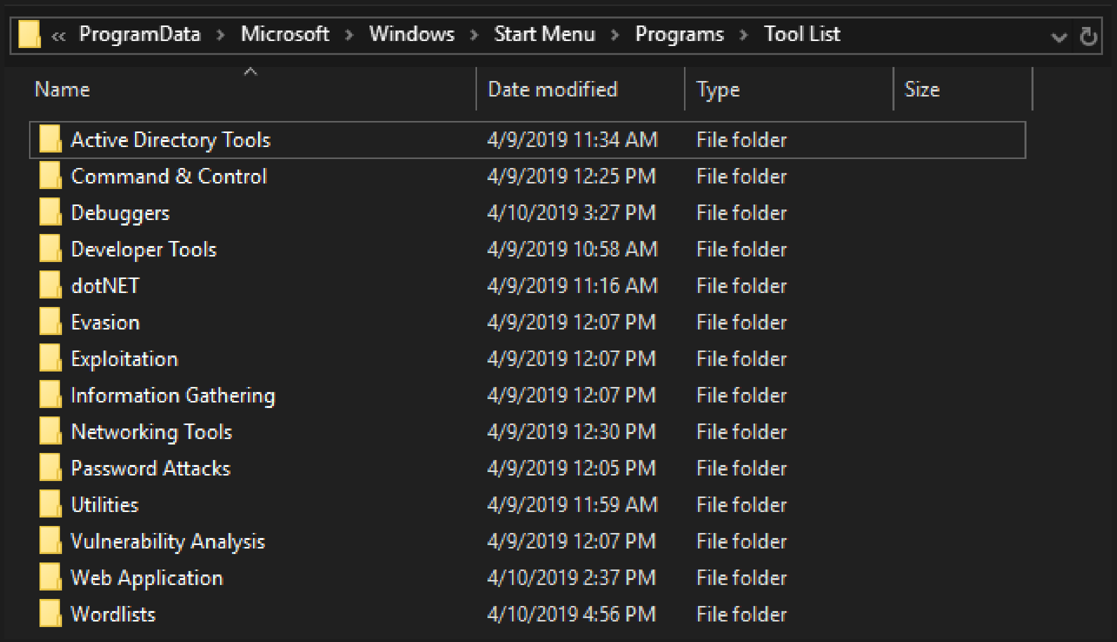
Associate 7-Zip with:

Type	0xdf	All users
7z	7-Zip	7-Zip
zip	7-Zip	7-Zip
rar	7-Zip	7-Zip
001		7-Zip
cab		7-Zip
iso		Windows.IsoFile
xz		7-Zip
txz		7-Zip
lzma		
tar		7-Zip
cpio		
bz2		7-Zip
bzip2		7-Zip
tbz2		7-Zip
tbz		7-Zip
gz		7-Zip
gzip		7-Zip
tgz		7-Zip
tpz		7-Zip

Interesting Tools

General Tools

On the desktop there's a shortcut called "Tools". It points to `C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Tool List`. In it is an organized folder structure of tools:



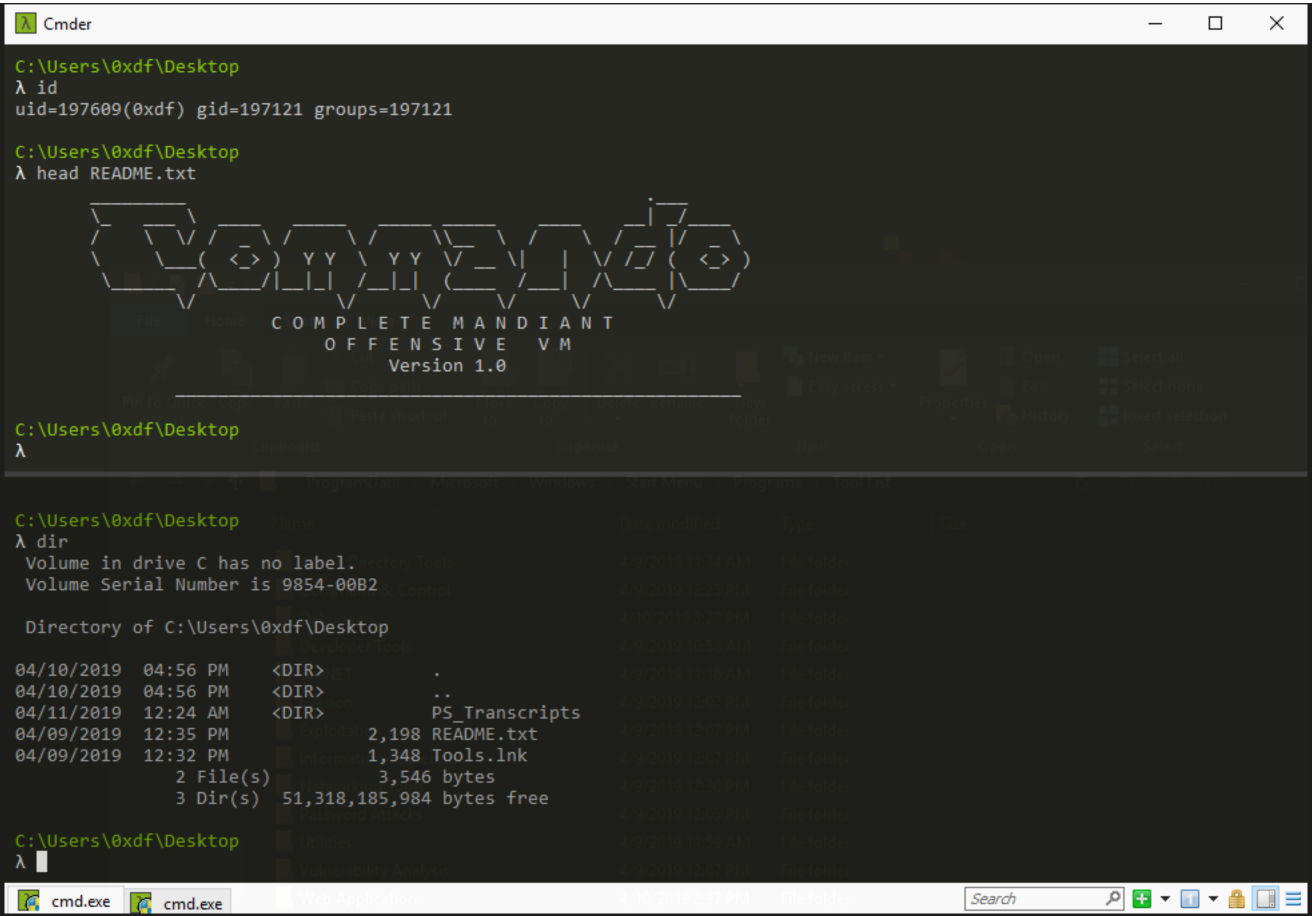
« ProgramData › Microsoft › Windows › Start Menu › Programs › Tool List

Name	Date modified	Type	Size
Active Directory Tools	4/9/2019 11:34 AM	File folder	
Command & Control	4/9/2019 12:25 PM	File folder	
Debuggers	4/10/2019 3:27 PM	File folder	
Developer Tools	4/9/2019 10:58 AM	File folder	
dotNET	4/9/2019 11:16 AM	File folder	
Evasion	4/9/2019 12:07 PM	File folder	
Exploitation	4/9/2019 12:07 PM	File folder	
Information Gathering	4/9/2019 12:07 PM	File folder	
Networking Tools	4/9/2019 12:30 PM	File folder	
Password Attacks	4/9/2019 12:05 PM	File folder	
Utilities	4/9/2019 11:59 AM	File folder	
Vulnerability Analysis	4/9/2019 12:07 PM	File folder	
Web Application	4/10/2019 2:37 PM	File folder	
Wordlists	4/10/2019 4:56 PM	File folder	

This directory is worth exploring to get a feel for what's there.

cmder

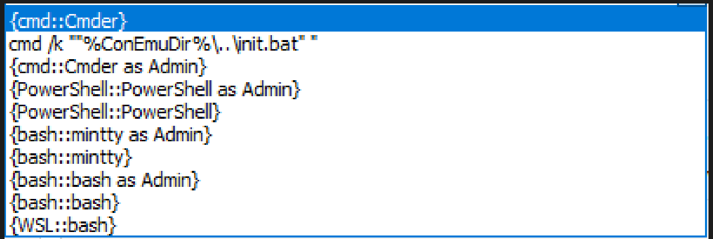
The recommended shell in CommandoVM is cmder. It can run `cmd`, `powershell`, or `bash` in panes and tabs. Here's an example with bash on top and cmd on bottom:



```
C:\Users\0xdf\Desktop
λ id
uid=197609(0xdf) gid=197121 groups=197121

C:\Users\0xdf\Desktop
λ head README.txt
       _________                                           .__
       \_   ___ \  ____   _____   _____ _____    ____    __| _/____
       /    \  \/ /  _ \ /     \ /     \\__  \  /    \  / __ |/  _ \
       \     \___(  <_> )  Y Y  \  Y Y  \/ __ \|   |  \/ /_/ (  <_> )
        \______  /\____/|__|_|  /__|_|  (____  /___|  /\____ |\____/
               \/             \/      \/     \/     \/      \/
                        C O M P L E T E  M A N D I A N T
                             O F F E N S I V E  V M
                                   Version 1.0
               _____________________________________________________

C:\Users\0xdf\Desktop
λ
```

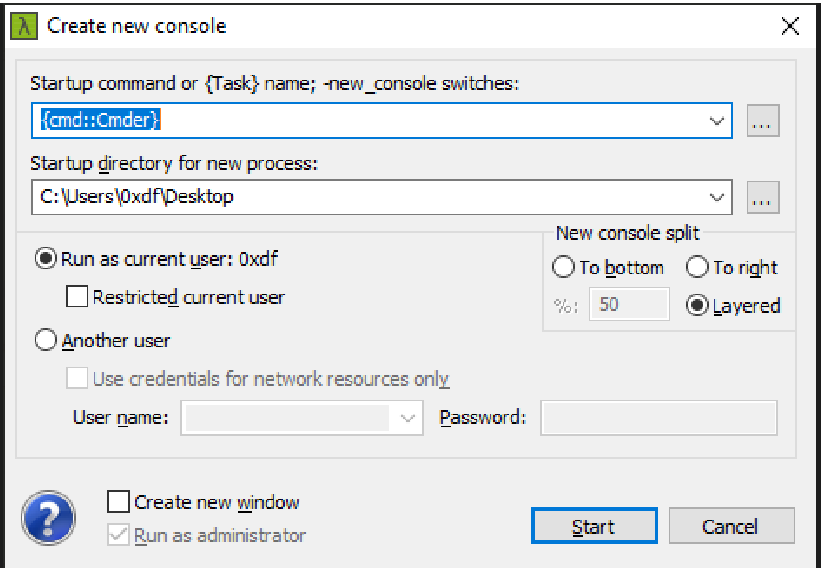
```
C:\Users\0xdf\Desktop
λ dir
 Volume in drive C has no label.
 Volume Serial Number is 9854-00B2

 Directory of C:\Users\0xdf\Desktop

04/10/2019  04:56 PM    <DIR>          .
04/10/2019  04:56 PM    <DIR>          ..
04/11/2019  12:24 AM    <DIR>          PS_Transcripts
04/09/2019  12:35 PM             2,198 README.txt
04/09/2019  12:32 PM             1,348 Tools.lnk
               2 File(s)          3,546 bytes
               3 Dir(s)  51,318,185,984 bytes free

C:\Users\0xdf\Desktop
λ █
```

I’ve played around with it a bit. I can Ctrl+t to create a new tab, and Ctrl+Tab to switch between tabs. When I create a tab, a pop up asks me what it should be, and I can choose various shell types:



```
{cmd::Cmder}
cmd /k ""%ConEmuDir%\..\init.bat" "
{cmd::Cmder as Admin}
{PowerShell::PowerShell as Admin}
{PowerShell::PowerShell}
{bash::mintty as Admin}
{bash::mintty}
{bash::bash as Admin}
{bash::bash}
{WSL::bash}
```

I can also give a directory to start in, the user to run as, if it should be a new tab or split window:



Create new console

Startup command or {Task} name; -new_console switches:

{cmd::Cmder}

Startup directory for new process:

C:\Users\0xdf\Desktop

● Run as current user: 0xdf

□ Restricted current user

○ Another user

□ Use credentials for network resources only

User name: Password:

New console split

○ To bottom ○ To right

%: 50 ● Layered

□ Create new window

☑ Run as administrator

I can also tell it to create a new window, and then I can Alt+Tab between them.

There's not enough keyboard shortcut support built in for my liking off the bat, but I might be able to get used it it, and it looks like there's a powerful macro language that might allow me to define tmux-like shortcuts.

GreenShot

GreenShot is pinned in the taskbar by Commando-VM, and is a pretty slick screen capture tool that I was previously unfamiliar with.

When I click it, no windows open, but rather a Greenshot icon shows up in the System Tray:

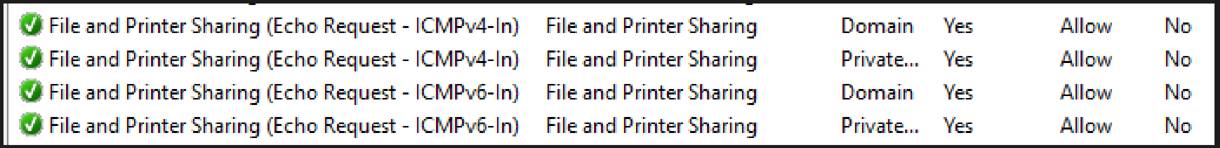
Once it's running, I can use the PrintScreen button to get a crosshairs. I can then click and drag out the area to capture. When I let go, it prompts me as to what to do to.

WinDump

I use `tcpdump` all the time on Kali, and it seems that `WinDump.exe` will do basically the same thing. There's also Wireshark on the box, but I like to work command line. `WinDump` takes basically the same arguments as `tcpdump`, so if I want to watch for pings, I can do something like this and see the pings:

```
λ windump.exe -i3 -n icmp
C:\ProgramData\chocolatey\lib\windump.fireeye\tools\windump.exe: listening on \Dev
01:36:02.716853 IP 10.10.14.14 > 10.10.10.109: ICMP echo reply, id 9443, seq 1, le
01:36:03.719388 IP 10.10.14.14 > 10.10.10.109: ICMP echo reply, id 9443, seq 2, le
```

I did have to adjust my windows Firewall to allow the pings in bound by enabling these rules:



✓ File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing	Domain	Yes	Allow	No
✓ File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing	Private...	Yes	Allow	No
✓ File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	Domain	Yes	Allow	No
✓ File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	Private...	Yes	Allow	No

That's a state I'll want anyway, so that if I'm trying to test for RCE by pinging myself, I can see the pings.

Wordlists

PayloadsAllTheThings, SecLists, and FuzzDB all install by default. SecLists was actually failing to install when I originally built this VM, but that has been fixed. You can find shortcuts starting from the `Tools` shortcut on the desktop, in `Tools\Wordlists`.

Others

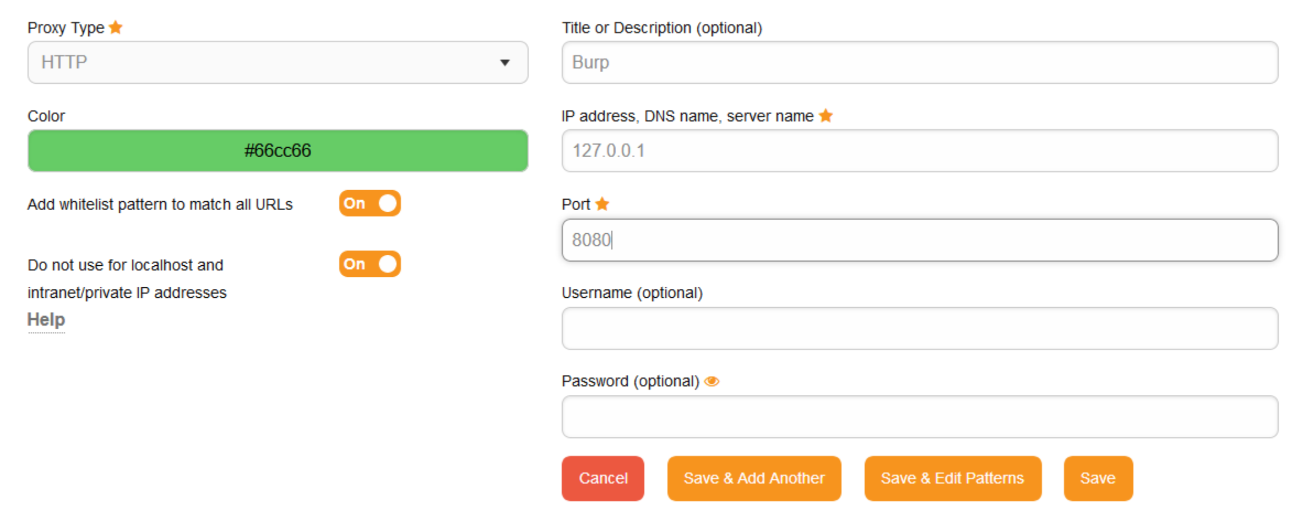
The full list of tools is on the Commando-VM GitHub Page. So others that I found worth mentioning were Subline Text as an editor, both Visual Studio Code and Visual Studio development environments and Wireshark. SysInternals, a handful of C2 frameworks and obfuscation frameworks, and other interesting PowerShell scripts can be found just surfing through the Tools List directory. There's a stand-alone copy of CyberChef, HxD, and KeepPass. Like I said earlier, once you install, it's worth taking a minute to look through the tool-set.

Additional Tools

FoxyProxy

FoxyProxy is indispensable for me as I send most of my web traffic to target through Burp, but don't want my Google searches to go there. I'll head to the FoxyProxy website and click "+ Add to Firefox" and after a few clicks it's installed. I see it in the top right of Firefox:

Now I'll set up Burp. I'll click on the FoxyProxy icon shown above, and select "Options". In the page that comes up, I'll select "Add". I'll set the Type to HTTP, call it Burp, and point it to localhost:8080:



Proxy Type ★: HTTP

Title or Description (optional): Burp

Color: #66cc66

IP address, DNS name, server name ★: 127.0.0.1

Add whitelist pattern to match all URLs: On

Port ★: 8080

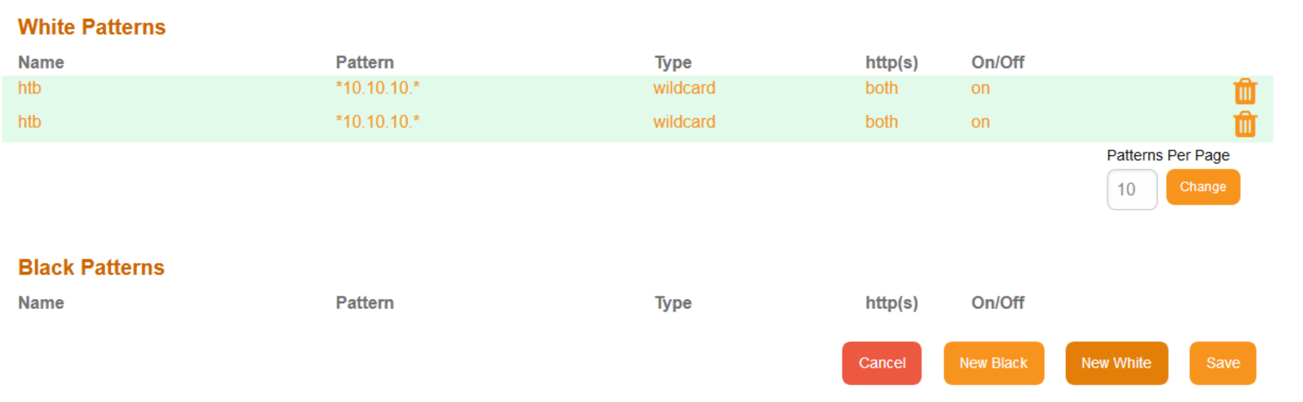
Do not use for localhost and intranet/private IP addresses: On

Help

Username (optional):

Password (optional):

Now I'll hit "Save & Edit Patterns". I'm going to set it up so that traffic to hackthebox targets goes through Burp, and the rest does not. I'll start by using the 🗑 to delete all the rules that are already there. Then I'll hit "New White" and create my first rule. I'll name it htb, and the pattern will be `*10.10.10.*`. This should direct all traffic going to a 10.10.10.0/24 address to Burp. I'll hit new-rule again and add one with pattern `*.htb*` to get domain traffic as well.



White Patterns

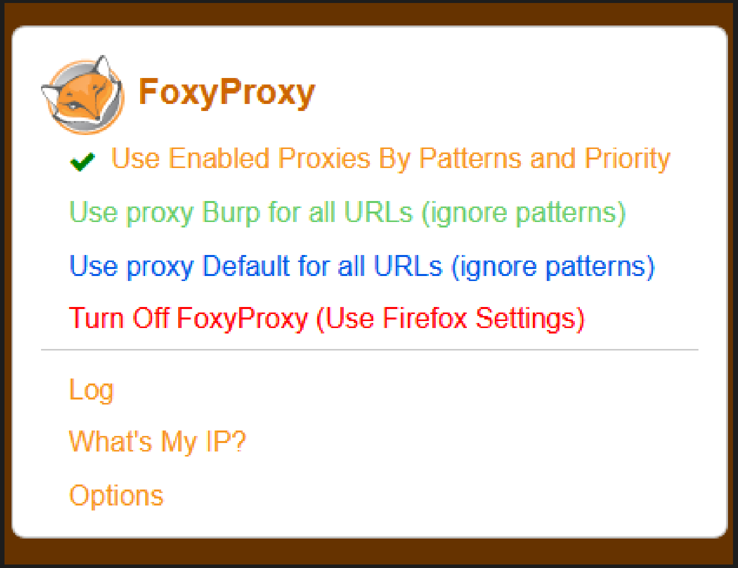
Name	Pattern	Type	http(s)	On/Off	
htb	*10.10.10.*	wildcard	both	on	🗑
htb	*10.10.10.*	wildcard	both	on	🗑

Patterns Per Page: 10

Black Patterns

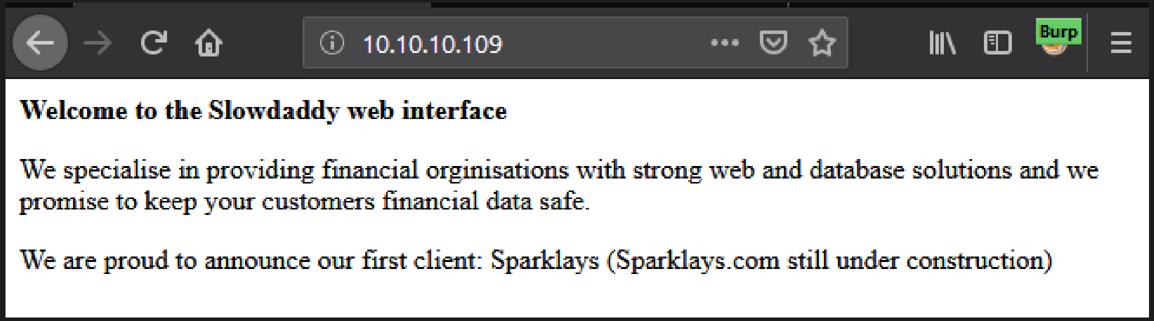
Name	Pattern	Type	http(s)	On/Off

Now I can hit save and close that page. I’ll click on the Foxy icon again, and select “Use Enabled Proxies by Patterns and Priority”:



FoxyProxy
✓ Use Enabled Proxies By Patterns and Priority
Use proxy Burp for all URLs (ignore patterns)
Use proxy Default for all URLs (ignore patterns)
Turn Off FoxyProxy (Use Firefox Settings)
Log
What's My IP?
Options

Now, I can visit `http:10.10.10.109` and get the Vault page through Burp (and see the green Burp on the FP icon):

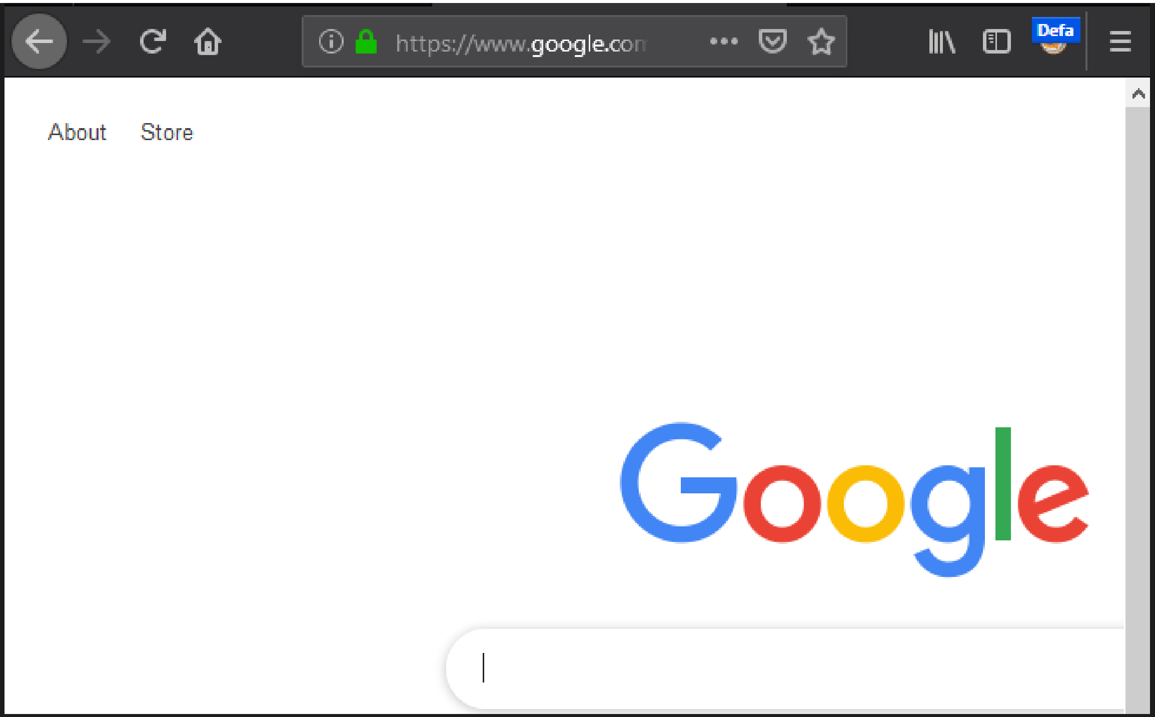


Welcome to the Slowdaddy web interface

We specialise in providing financial orginisations with strong web and database solutions and we promise to keep your customers financial data safe.

We are proud to announce our first client: Sparklays (Sparklays.com still under construction)

And without changing the settings, open another tab and go to `google.com` and it doesn’t go through burp:



RE

The distribution already has `x64dbg` (and `x32dbg`) for Windows debugging and `dnSpy` for dotNET reversing and debugging. Those are both tools I would add if they weren't there.

I want to add IDA and Ghidra. I'll grab each from their sites. IDA installs by running the installer.

For Ghidra, I'll open the archive and drop the `ghidra_9.0.2` folder into `C:\Program Files`, and drop a shortcut to `ghidrarun.bat` somewhere useful, like in the tools directory with all the shortcuts. I'll also need to get the latest JDK installer and run it.

Dirbuster Lists

I regularly use the dirbuster wordlists for web enumeration. I created a directory in `\tools\` and used `wget` to get them:

```
C:\Tools\dirbuster-lists>wget https://raw.githubusercontent.com/daviddias/node-dir
--16:51:22--  https://raw.githubusercontent.com/daviddias/node-dirbuster/master/li
           => `directory-list-2.3-medium.txt'
Resolving raw.githubusercontent.com... 151.101.248.133
Connecting to raw.githubusercontent.com[151.101.248.133]:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2,200,599 [text/plain]

100%[====================================>] 2,200,599     --.--K/s

16:51:22 (27.26 MB/s) - `directory-list-2.3-medium.txt' saved [2200599/2200599]


C:\Tools\dirbuster-lists>wget https://raw.githubusercontent.com/daviddias/node-dir
--16:51:30--  https://raw.githubusercontent.com/daviddias/node-dirbuster/master/li
           => `directory-list-2.3-small.txt'
Resolving raw.githubusercontent.com... 151.101.248.133
Connecting to raw.githubusercontent.com[151.101.248.133]:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 813,102 [text/plain]

100%[====================================>] 813,102       --.--K/s

16:51:30 (25.85 MB/s) - `directory-list-2.3-small.txt' saved [813102/813102]


C:\Tools\dirbuster-lists>wget https://raw.githubusercontent.com/daviddias/node-dir
--16:51:47--  https://raw.githubusercontent.com/daviddias/node-dirbuster/master/li
           => `directory-list-lowercase-2.3-small.txt'
Resolving raw.githubusercontent.com... 151.101.248.133
Connecting to raw.githubusercontent.com[151.101.248.133]:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 758,408 [text/plain]

100%[====================================>] 758,408       --.--K/s
```

```
16:51:47 (15.72 MB/s) - `directory-list-lowercase-2.3-small.txt' saved [758408/758


C:\Tools\dirbuster-lists>wget https://raw.githubusercontent.com/daviddias/node-dir
--16:51:54--  https://raw.githubusercontent.com/daviddias/node-dirbuster/master/li
           => `directory-list-lowercase-2.3-medium.txt'
Resolving raw.githubusercontent.com... 151.101.248.133
Connecting to raw.githubusercontent.com[151.101.248.133]:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2,057,312 [text/plain]

100%[====================================>] 2,057,312     --.--K/s

16:51:54 (31.65 MB/s) - `directory-list-lowercase-2.3-medium.txt' saved [2057312/2
```

Gobuster

I prefer `gobuster` for website path enumerations (and more). I grabbed the latest install from the releases page and dropped it at `C:\Tools\gobuster\gobuster.exe`. Then I added that directory to my path. I tested it on vault:

```
C:\Users\0xdf>gobuster -u http://10.10.10.109/sparklays/ -w \Tools\dirbuster-lists

=====================================================
Gobuster v2.0.1              OJ Reeves (@TheColonial)
=====================================================
[+] Mode         : dir
[+] Url/Domain   : http://10.10.10.109/sparklays/
[+] Threads      : 50
[+] Wordlist     : \Tools\dirbuster-lists\directory-list-2.3-small.txt
[+] Status codes : 200,204,301,302,307,403
[+] Timeout      : 10s
=====================================================
2019/04/10 17:29:45 Starting gobuster
=====================================================
/design (Status: 301) (0.53%)
=====================================================
2019/04/10 17:30:50 Finished
=====================================================
```

This version seems to work fine, though I did submit a feature request to get it installed by default.

WFuzz

Installing `wfuzz` *should* be as simple as `pip install wfuzz`. However, there is a curveball. On Linux, `python` and `python3` are typically different binaries. On windows, both are named `python`, and both are in my path:

```
C:\Users\0xdf>where python
C:\Python37\python.exe
C:\Python27\python.exe
```

And the one that runs is `python3`:

```
C:\Users\0xdf>python --version
Python 3.7.3

C:\Users\0xdf>pip --version
pip 19.0.3 from c:\python37\lib\site-packages\pip (python 3.7)
```

I had a hard time getting pycurl to install using python3's `pip`, but when I switched to python2's `pip`, it worked instantly:

```
C:\Users\0xdf>\Python27\python.exe -m pip install wfuzz
DEPRECATION: Python 2.7 will reach the end of its life on January 1st, 2020. Pleas
Collecting wfuzz
```

```
  Downloading https://files.pythonhosted.org/packages/1a/72/05b7a91322092a2b99edfa
    100% |UUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUU| 81kB ...
Requirement already satisfied: pycurl in c:\python27\lib\site-packages (from wfuzz
Requirement already satisfied: pyparsing in c:\python27\lib\site-packages (from wf
Requirement already satisfied: future in c:\python27\lib\site-packages (from wfuzz
Requirement already satisfied: six in c:\python27\lib\site-packages (from wfuzz) (
Collecting configparser (from wfuzz)
  Using cached https://files.pythonhosted.org/packages/ba/05/6c96328e92e625fc31445
Requirement already satisfied: chardet in c:\python27\lib\site-packages (from wfuz
Collecting colorama (from wfuzz)
  Downloading https://files.pythonhosted.org/packages/4f/a6/728666f39bfff1719fc94c
Installing collected packages: configparser, colorama, wfuzz
  Running setup.py install for wfuzz ... done
Successfully installed colorama-0.4.1 configparser-3.7.4 wfuzz-2.3.4
```

It runs… poorly. It won't run beyond a crawl in cmd or powershell. It prints each line, and then removes it if hidden very slowly. But I got it to run in cmder. The text updating is clearly optimized for Linux. And it seems to run a little slow. That said, it still works:

```
λ wfuzz -w \Tools\dirbuster-lists\directory-list-2.3-small.txt -u http://10.10.10.
********************************************************
* Wfuzz 2.3.4 - The Web Fuzzer                         *
********************************************************

Target: http://10.10.10.109/sparklays/FUZZ
Total requests: 87664

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

000370:   C=301      9 L       28 W          323 Ch        "design"
000680:   C=404
```

```
Finishing pending requests...
^C
```

I put in a feauture request to see if they can get it working better and bring it by default, and they said it has been added to the roadmap.

Conclusion

That’s all for my initial overview. There’s a ton I didn’t cover. Leave a comment with your favorite thing I didn’t talk about that people should know about, or what you changed or would change in your VM.

Up next, I’m going to try to do a box through this VM, and report back on what worked and what I struggled with.

« Installation

Lessons Learned »

What do you think?

14 Responses

👍 Upvote 😝 Funny 😍 Love 😯 Surprised 😤 Angry 😥 Sad

1 Comment **0xdf**

1 **Login**

♡ **Recommend** **Tweet** **Share**

Sort by Best

Join the discussion…

LOG IN WITH

OR SIGN UP WITH DISQUS ?

Name

dmcxblue • 6 months ago

Incredible, looks like something that needs to be added to your personal arsenal of tools to have even on Version 1.0 still looks promising and that it will be something that many would use in the future can't wait for more good things to come from this... Kali you still the coolest!!
:P

^ | ˅ • Reply • Share ›

ALSO ON **0XDF**

Commando VM: Lessons Learned | 0xdf hacks stuff

5 comments • 6 months ago

Avatar **Blake Townsend** — -sT was the problem, thanks

HTB: Luke | 0xdf hacks stuff

2 comments • a month ago

Avatar **0xdf** — Glad you enjoyed it! Thanks for the comment

HTB: BigHead | 0xdf hacks stuff

2 comments • 5 months ago

Avatar **0xdf** — Hard to say. It was spread out over a week or so...little chunks here and there.

HTB: Conceal | 0xdf hacks stuff

4 comments • 5 months ago

Avatar **0xdf** — Glad you enjoy them!

✉ **Subscribe** **Add Disqus to your site** **Disqus' Privacy Policy** **DISQUS**

0xdf hacks stuff

0xdf hacks stuff
0xdf.223@gmail.com

0xdf_
0xdf
oxdf
feed

CTF solutions, malware analysis, home lab development