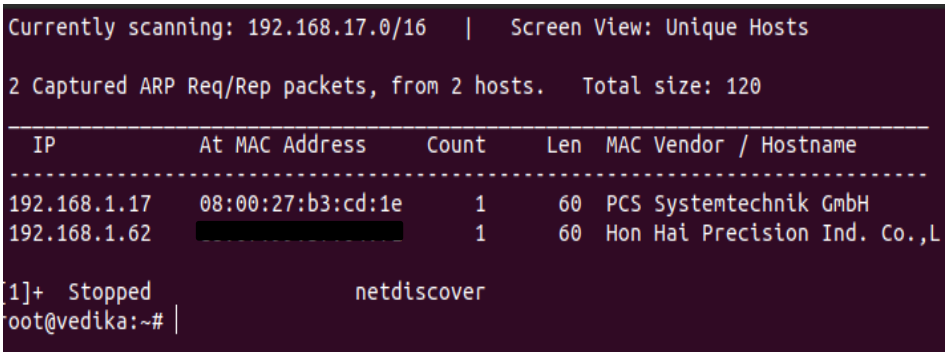
Vulnerability Assessment and Penetration Testing

OS-HAX

Vedika Bang | Learnings: exiftool, awk| Level: Medium-ish.

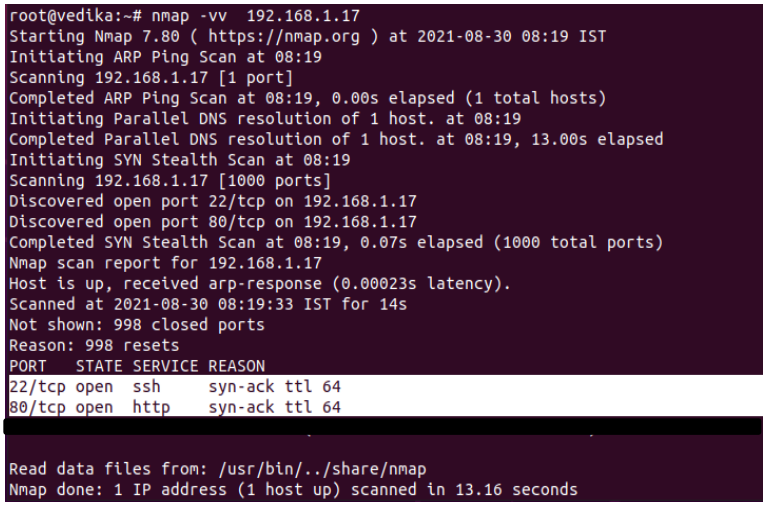
Submitted to: Wattlecorp Cybersecurity Labs.

1. First, we use **NETDISCOVER** tool. Basically, Net discover helps us to gather information about IP addresses, MAC addresses of the devices connected to the network. It works like ARP tool. We need root access to execute the command. We can use flags to reduce the output. (Simply man [command name])



In the above screenshot, we have gotten a few IP addresses. It is ostensible, net discover can be stopped forcefully if we don't want a full scan; or otherwise. Here**, 192.168.1.17** is the required IP address.

2. Since, we have the IP address of the targeted machine, we can use **NMAP (Network Mapper)**, to know if any ports/Services are open/available to exploit.



Here, we can **see port no.22 (SSH service) and port no.80(HTTP service) are open**. So, it's obvious that we should go to that website; since we don't have the username for sting.

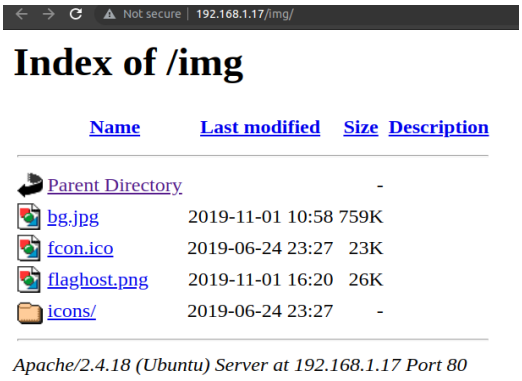
3. After looking it up on the browser, we get an ostentatious website, lol. Well, apart from very “Hacker” kind of vibe it didn’t have much to give. (None in page source code too!)

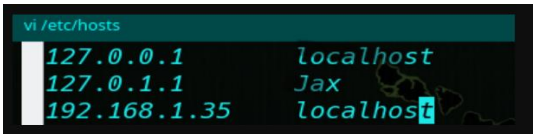
4. Well, we use **dirb** command to enumerate more about the website which isn’t visible to us, clearly. Dirb-it!!

```
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon Aug 30 08:34:10 2021
URL_BASE: http://192.168.1.17/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.17/ ----
==> DIRECTORY: http://192.168.1.17/css/
==> DIRECTORY: http://192.168.1.17/html/
==> DIRECTORY: http://192.168.1.17/img/
+ http://192.168.1.17/index.html (CODE:200|SIZE:3135)
==> DIRECTORY: http://192.168.1.17/js/
+ http://192.168.1.17/server-status (CODE:403|SIZE:277)
==> DIRECTORY: http://192.168.1.17/wordpress/
```

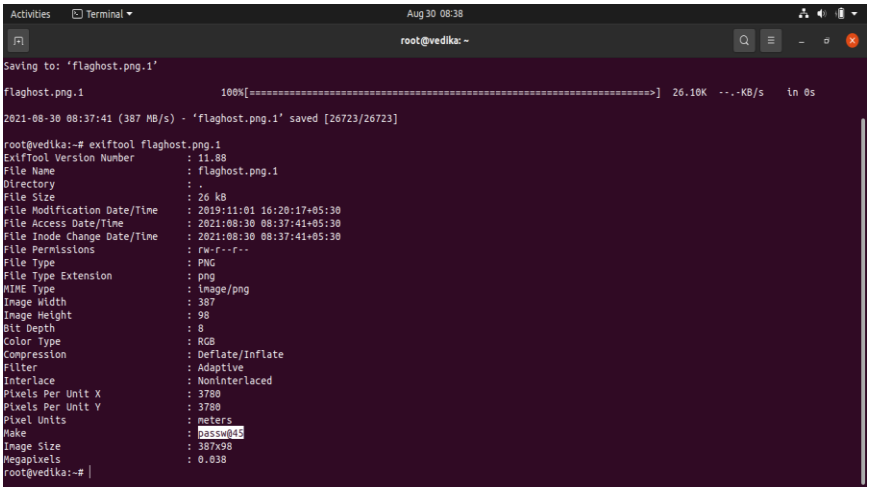
Upon looking closely to the output, we received, other than html, CSS, **img directory** seemed bit intriguing. (Because there was nothing in HTML, CSS anyway)

5. Well, to corroborate my statement in the last step, here we go!
Opening the **flagpost.png** which certainly has an obscure clue (as of now) **JAX**



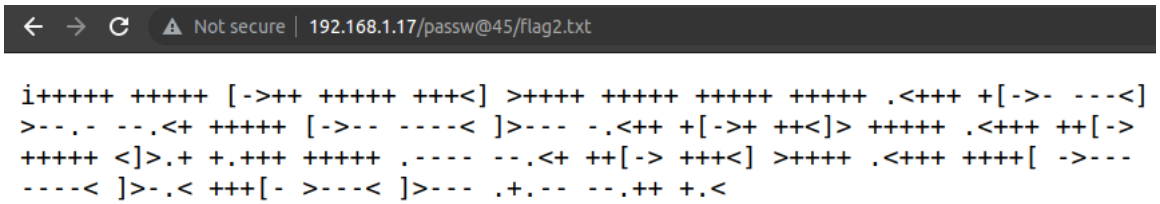


6. Whenever there is an image, steganography is intuitive.
wget the link and **exiftool <filename.png>**

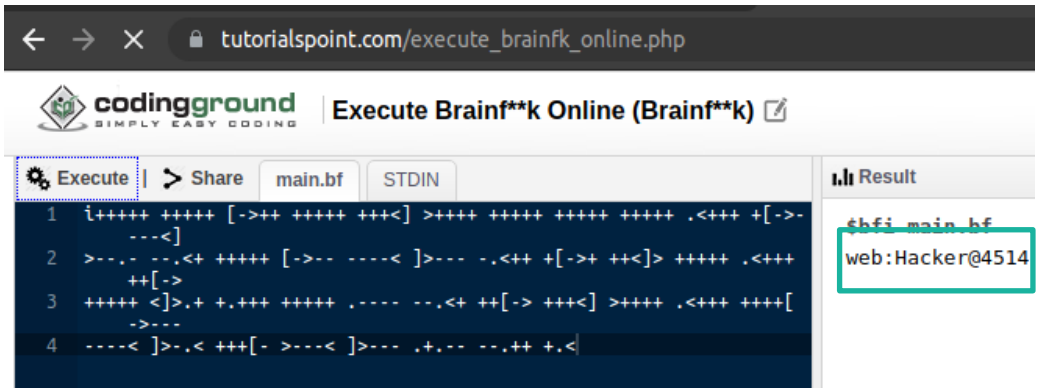


Looking closely to the output, make**: passw@45** makes no sense; hence that is imminent to be our clue. Let's surf it out.
Ta-daa! **Flag2.txt.**

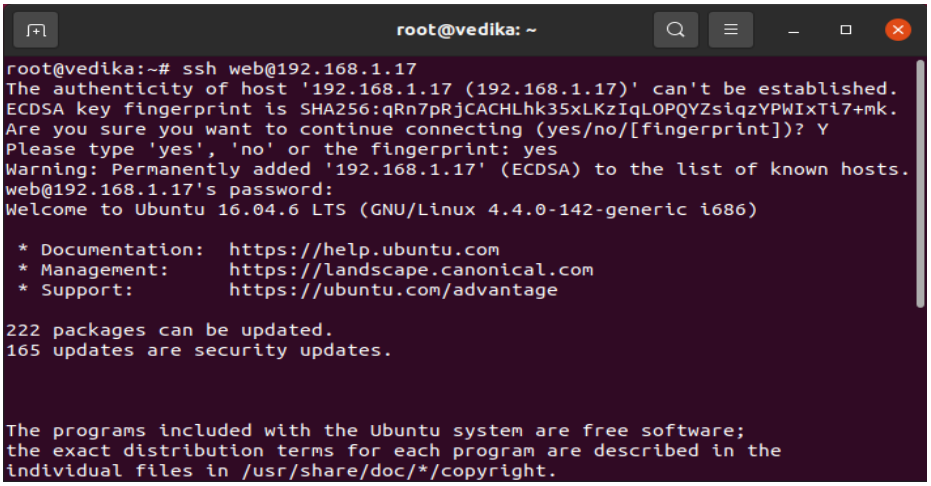
7. And flag2.txt couldn't have been more famaliar! Just when I thought assembly's hello world is not so welcoming, another esoteric language blew my mind. Ingenious enough to not to use again.



Would have loved to write a script to decode, but no ! translated it into english using an online compiler.



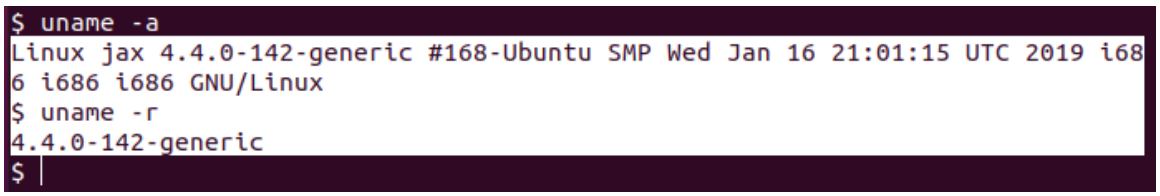
As port 22 is open, SSH service is available. **Command: ssh web@192.168.1.17** After entering the above password, **we are in the targeted machine!**



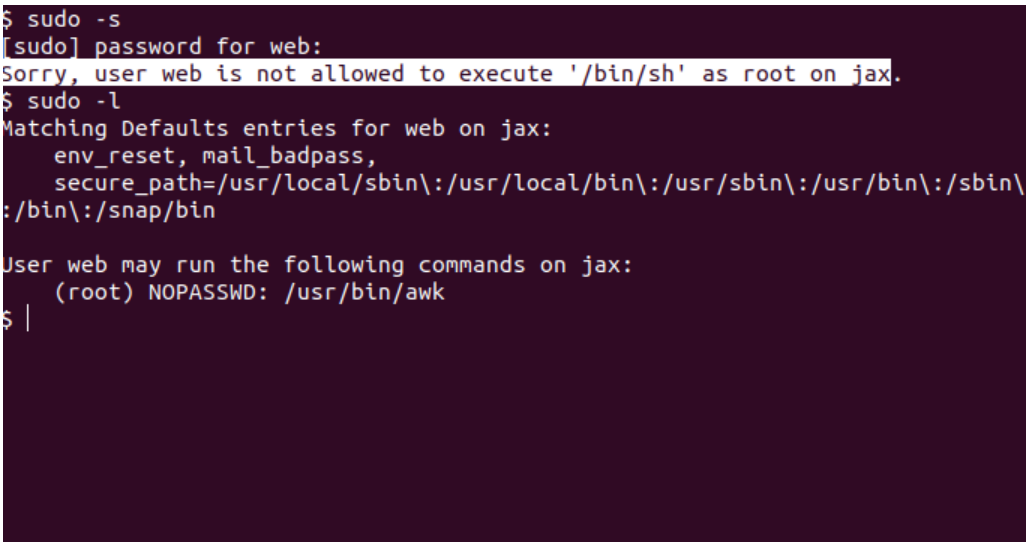
8. After performing some commands like **pwd, cd, ls**

Okay! "let's go to Root"!!

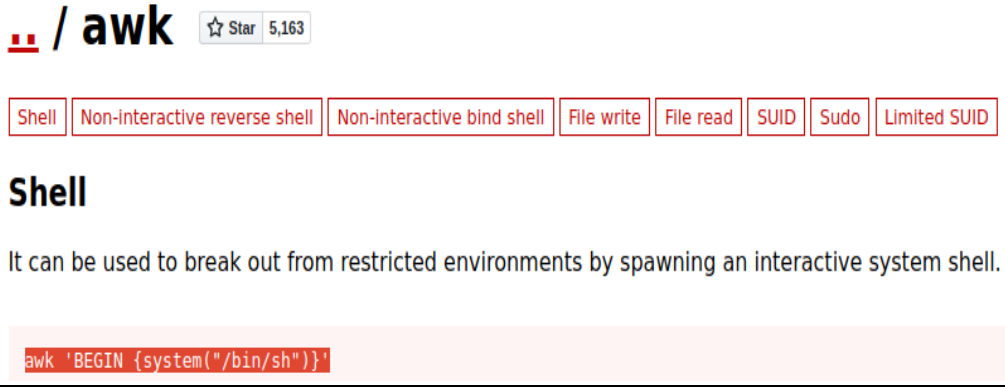
9. Well, very imminent step is to check **About** of the system. Using command **uname-a/uname-r,** we understand the version is older. It's very alike that we might find a vulnerability regarding the same.



10. After enumerating some sudo commands, like sudo -s, sudo -l it shows that awk may run on Jax, which is unlikely but not weird (it's a box after all) I had no idea what awk is, until then.



11. Well, **awk** is a scripting language and work kind of similar to regex in python. It manipulates the data and generate the reports. Having said that and from above, Google-ing was enough to know. :-D GTFObin helps!



12. Running highlighted command got: