# BSides Vancouver: 2018 (Workshop)

Boot2Root challenge.

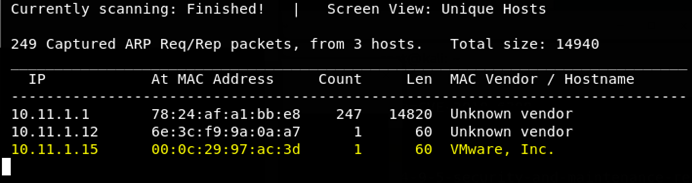
VM image available [here](https://www.vulnhub.com/entry/bsides-vancouver-2018-workshop,231/#download).

Boot the image from VM Player or VirtualBox and keep the network settings in bridge-mode for easier IP assignment and then get the attacker (often, Kali) ready. Would strongly recommend to keep this network out of Internet reach ☺

## *Enumeration:*

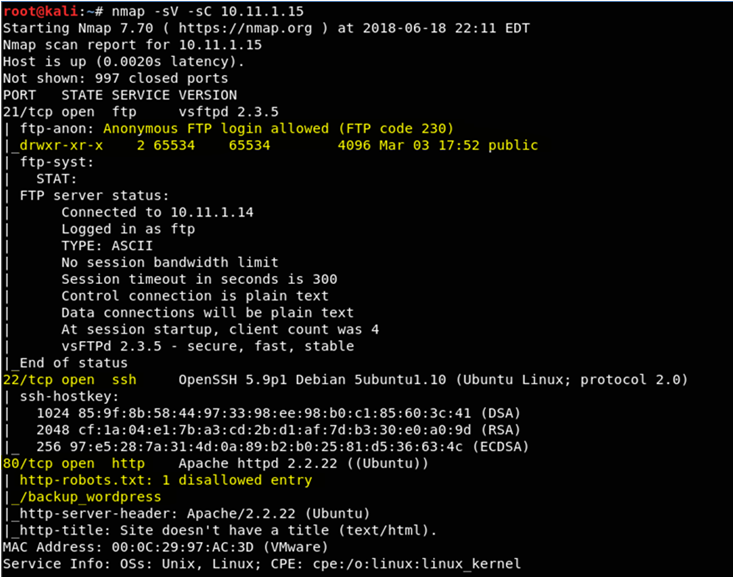
First, find the IP address of the target.

netdiscover –r 10.11.1.0/24



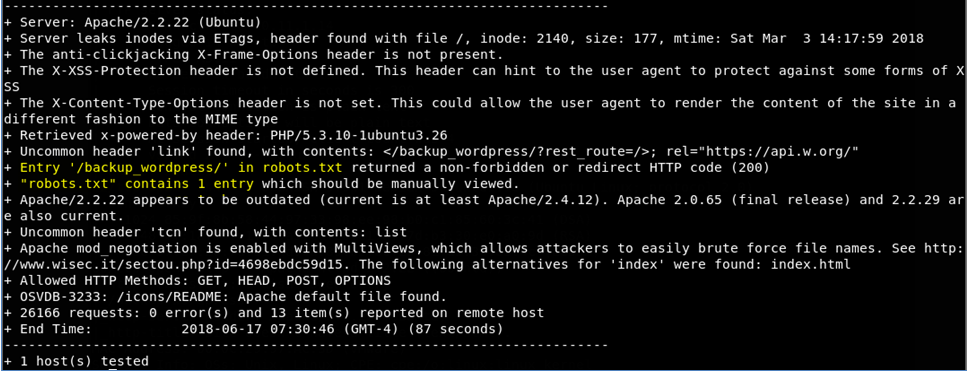
Then fire nmap to find the open ports.

nmap –sV –sC 10.11.1.15



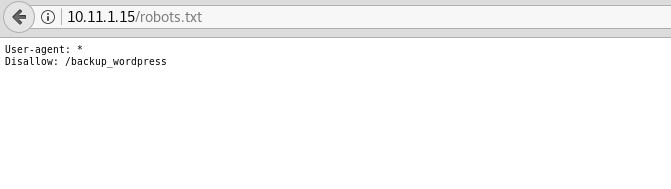
Now we know port 80 - HTTP running, run nikto.

nikto –C all –h 10.11.1.15

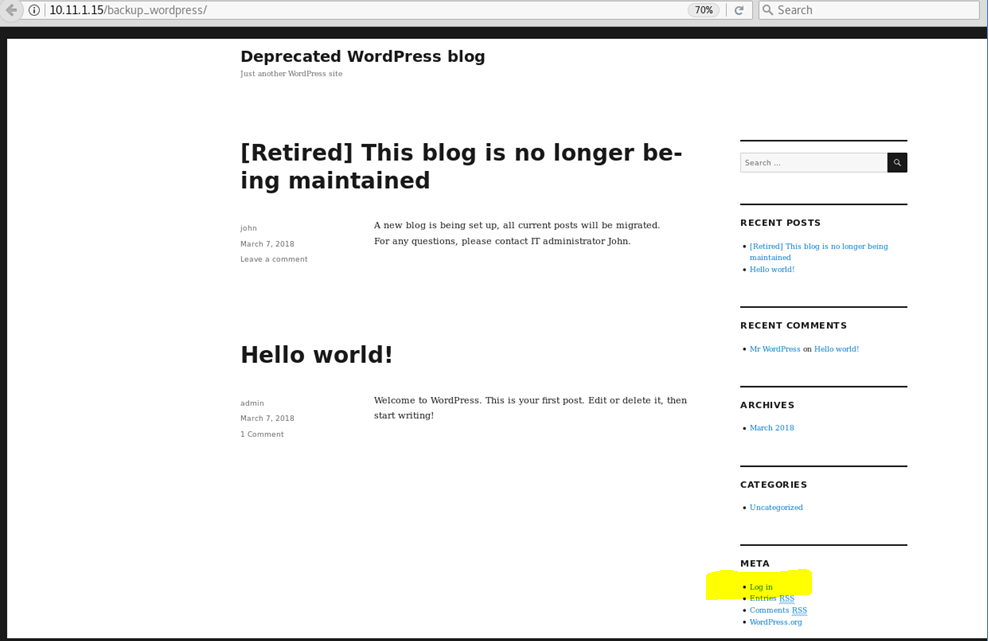


Two catchy things from nikto output: robots.txt and it has entry “/backup\_wordpress/” directory.

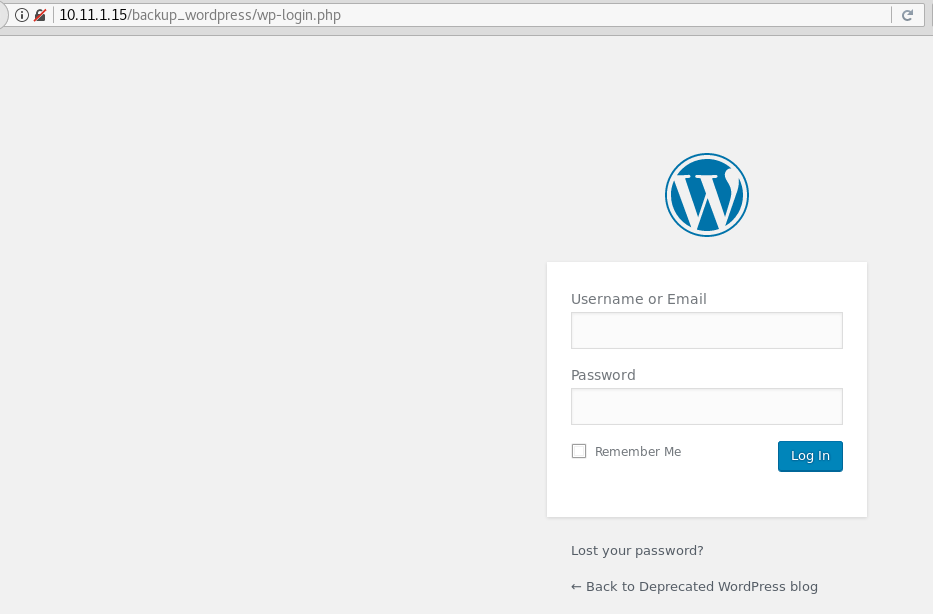
Let’s check robots.txt file.



Let’s also check /backup\_wordpress/ directory too.



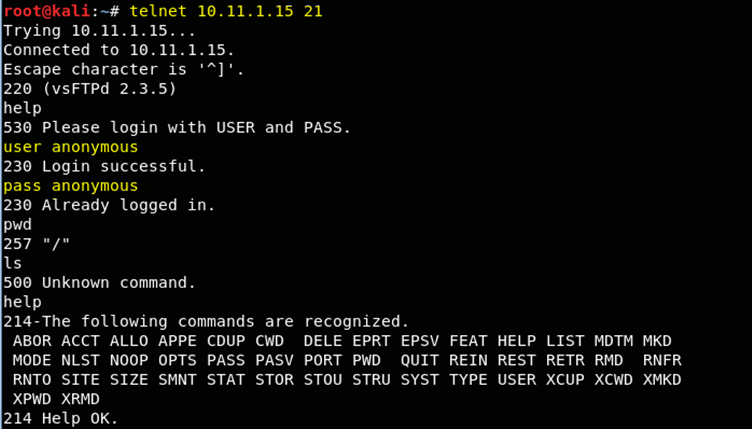
There is link to login page.



Fine, now let’s try other 2 open ports, start with FTP.

telnet 10.11.1.15 21

It’s already been noticed from the nmap output that the FTP allows anonymous login.



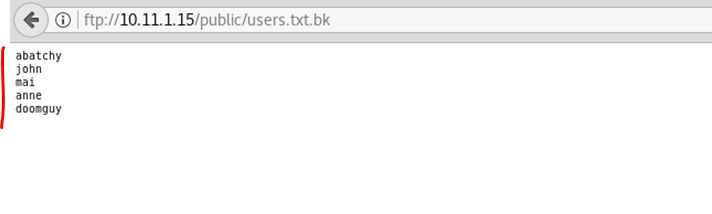
Nothing interesting... let’s try accessing FTP from browser as nmap showed the presence of public directory.



Under that folder, there is user.txt file, seems interesting.



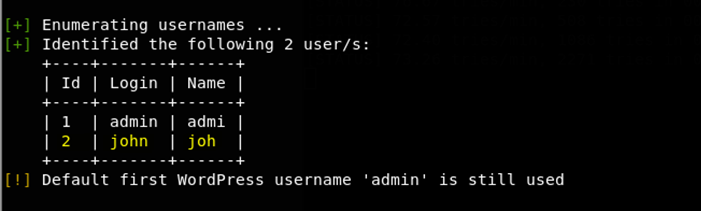
And there were list of users in it.



Since website uses wordpress, tried wpscan for users enumeration.

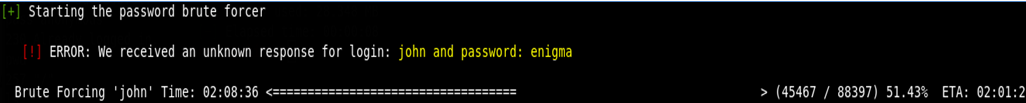
wpscan –url <http://10.11.1.15/backup_wordpress/> --enumerate u

The output listed 2 login names, note that john user also present in the list of users taken from FTP.

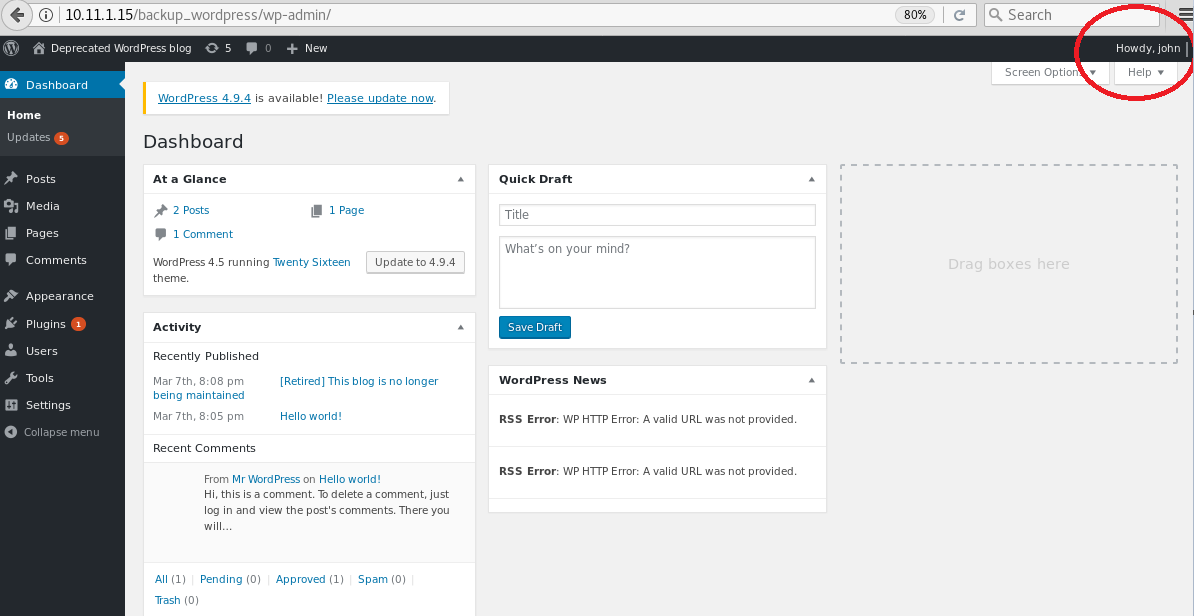


Run wpscan to bruteforce for john’s password. Since it takes time, give a try to brute forcing SSH with other user names.

wpscan --url [http://10.11.1.15/backup\_wordpress /](http://10.11.1.15/backup_wordpress%20/) --username john --wordlist /usr/share/wordlists/metasploit/password.lst

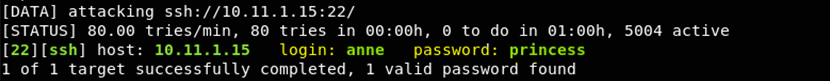


After a while, we have got the password for user john, this allows login to wordpress.



On the other side, hydra tries brute forcing the users and hydra finds password for the user anne (seems other users have no SSH keys to login).

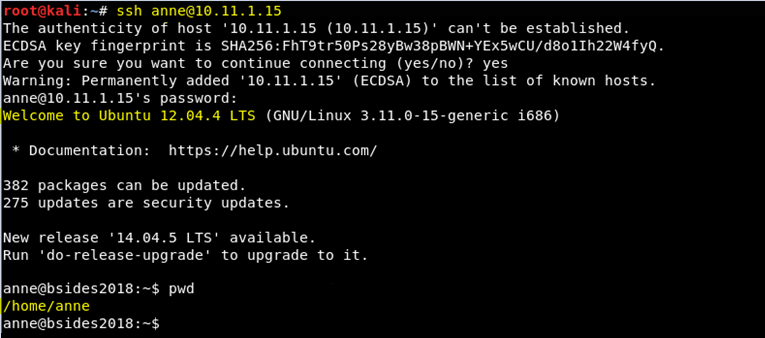
hydra –l anne –P /usr/share/wordlists/nmap.lst –t 5 ssh://10.11.1.15



## Low Privilege Shell:

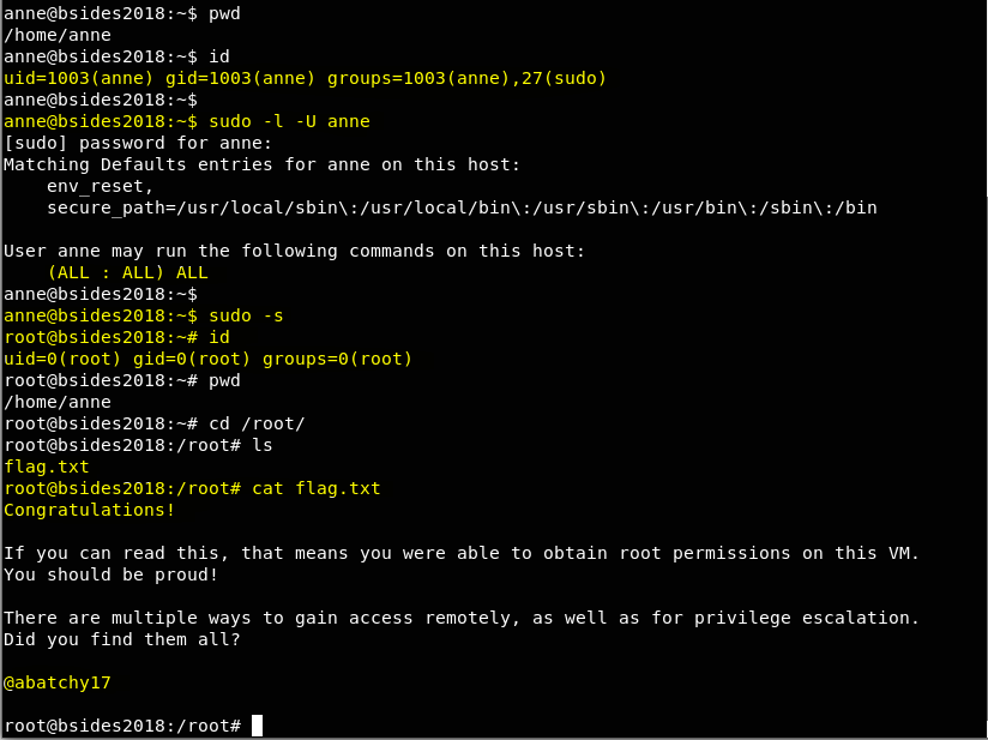
Login through SSH with user anne and it works as expected.

ssh anne@10.11.1.15



## Privilege Escalation – Getting Root:

Just tried if this user has sudo access and unfortunately, anne has sudo access - sudo –s.



Bingo! Got the flag!!

But the flag says that there are many ways to get the root. So there should be a way to get the root through wordpress logging (remember user John?).