Nmap In The Windows Bash Shell (WSL)

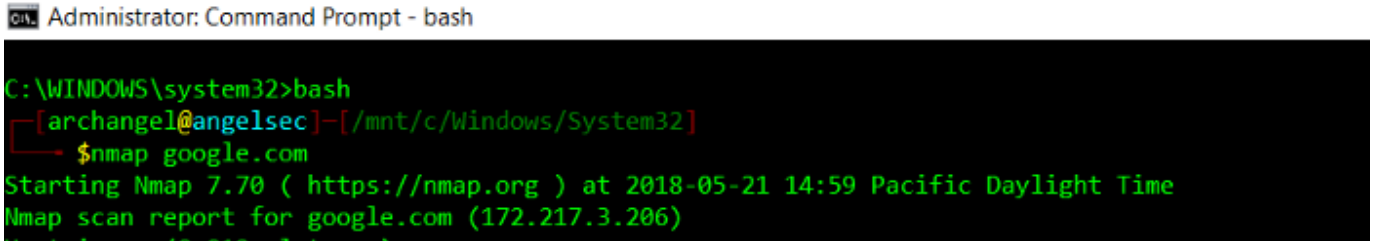
The Archangel Follow
May 21, 2018 · 3 min read

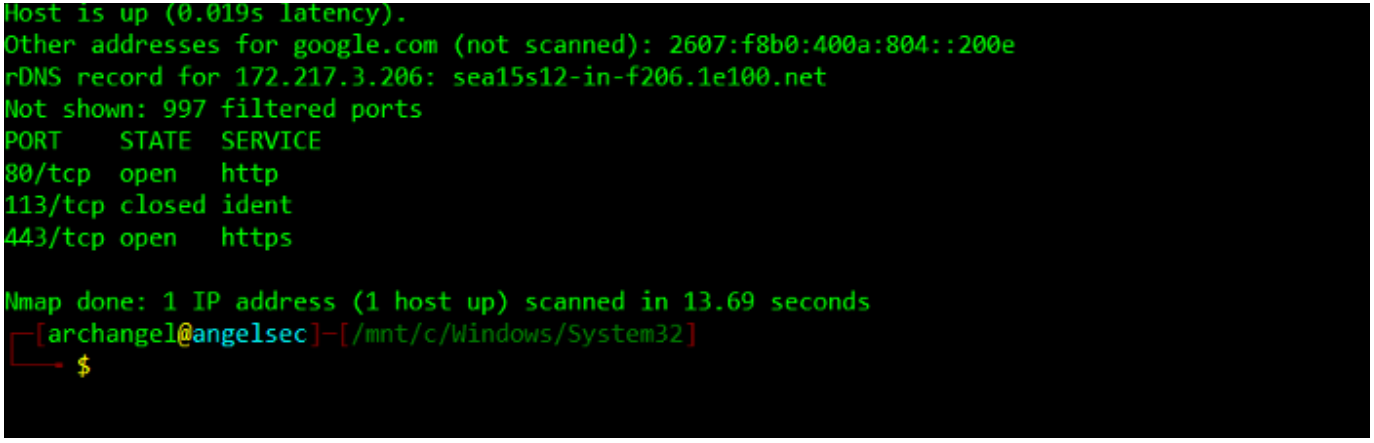
. . .

THIS STORY WAS ORIGINALLY PUBLISHED AT:

https://exploits.run/nmap-wsl/

. . .





Ever since the release of the Windows Subsystem for Linux, a years long unfulfilled hope of using Nmap in this wonderful environment still lingers. If you run:

```
sudo apt-install nmap
```

You can install Nmap in Bash but when you attempt to run it you'll be met with a slew of errors. The way that the shell interacts with the system just simply isn't quite right yet, even after a couple of years of developments on this feature, it still can't run Nmap.

Recently, I began to entertain moving from Linux back to Windows as my main OS and using the versatility of Linux on Windows alongside other great tools like Powershell. One thing is very certain however for me: I cannot work without Nmap. It's a critical part of my toolset. So, after going through all the trouble of installing Parrot OS on my Linux subsystem, I was determined to make it work.

After tons and tons of searching, I still wasn't seeing anyone who had made a breakthrough in getting Nmap to work in this environment. After realizing I wasn't going to find any other tricks out there, I started trying to solve the problem my own way.

THE SOLUTION

Part of the beauty of using Bash on Windows is you get the power of both operating environments. This includes, launching Windows side applications from Bash. Now Nmap for Bash on Windows may be very broken, but Nmap for Windows certainly is not. SO, I decided to install Nmap on the Windows side. Now typing out that path is going to get very annoying every time I want to launch Nmap from Bash so I decided to

create the alias below in my .bashrc file to just run Nmap, in Bash, from the Windows side.

```
alias nmap='"/mnt/c/Program Files (x86)/Nmap/nmap.exe"'
```

Viola! Even if the backend is running somewhere else, we can still easily invoke and run the full Nmap program from Bash as if it were installed right on the Linux side.

. . .

Since I wasn't able to find many solutions like this on my initial hunt, I hope this post can help some weary Nmappers find some hope that they TOO can run Nmap right here on a Windows/Linux hybrid environment. Thank you all for reading :)

. . .

UPDATE 5/22/18:

Apparently one of the Nmap devs agrees. Thanks Daniel!

Linux Windows Bash Nmap Subsystem

256 claps

WRITTEN BY

The Archangel

Cyber Warfare Research Team (ADi) | OSINT Researcher (Trace Labs) | Army Vet

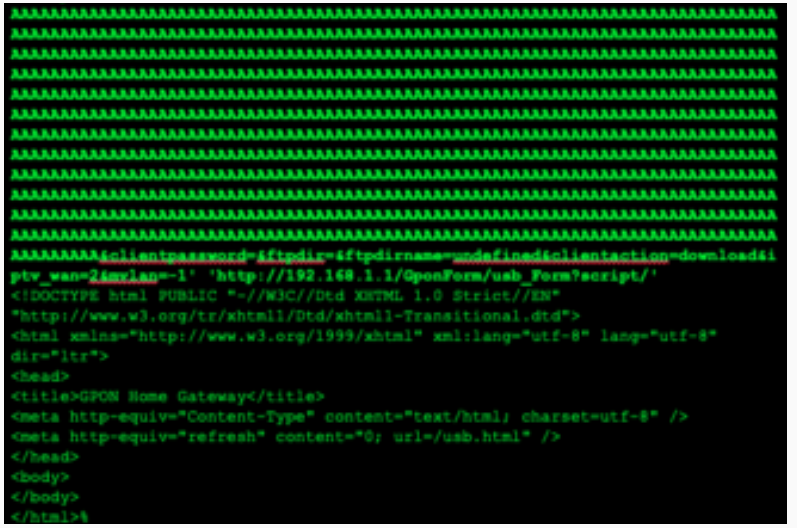
Follow

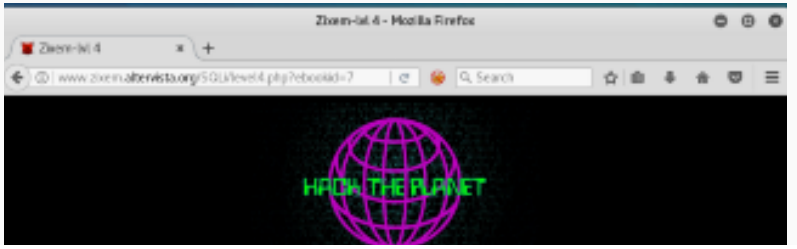
See responses (8)

More From Medium

Related reads

GPON Home Gateway RCE threatens tens of thousands users




Artem Metla in Tenable TechBlog
Feb 27 · 6 min read

695

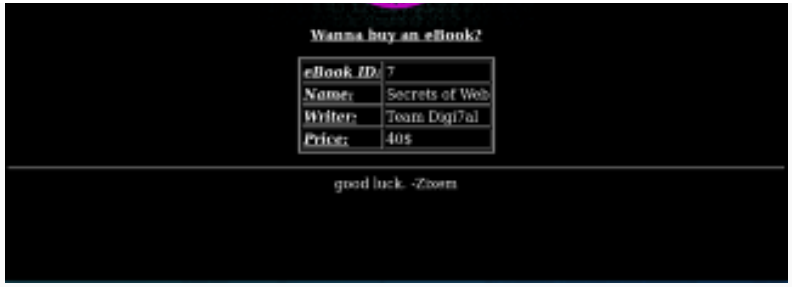
Related reads

Union SQLi Challenges (Zixem

Write-up)

George O in CTF Writeups
Oct 21, 2018 · 9 min read

719



Related reads

Nullcon-HackIM CTF 2019-MLAuth-Misc(500)Writeup

Aagam shah in InfoSec Write-ups
Feb 3 · 4 min read

405