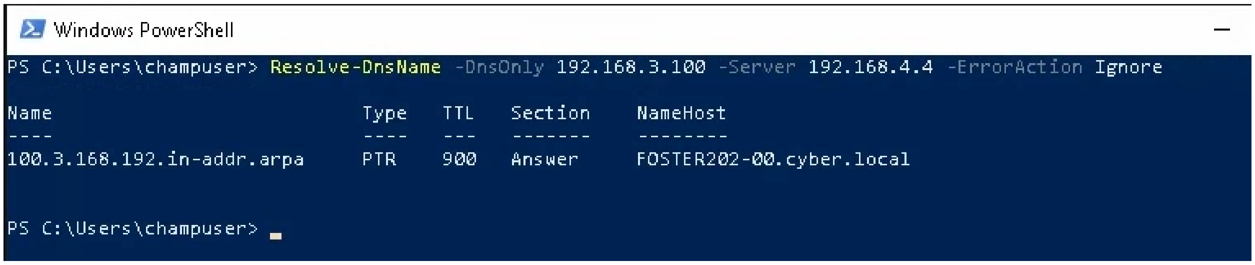
Updated Feb 2, 2022

Assignment 3.1 - Powershell and DNS

💡We don't always have a Kali box handy when we are trying to get information on a target, we can also scan laterally using a system we have targeted and exploited. Consider the following powershell one liner.

We are asking the DNS Server on 192.168.4.4 to resolve the IP Address 192.168.3.100. It turns out this is the instructor's PC in FOSTER 202.

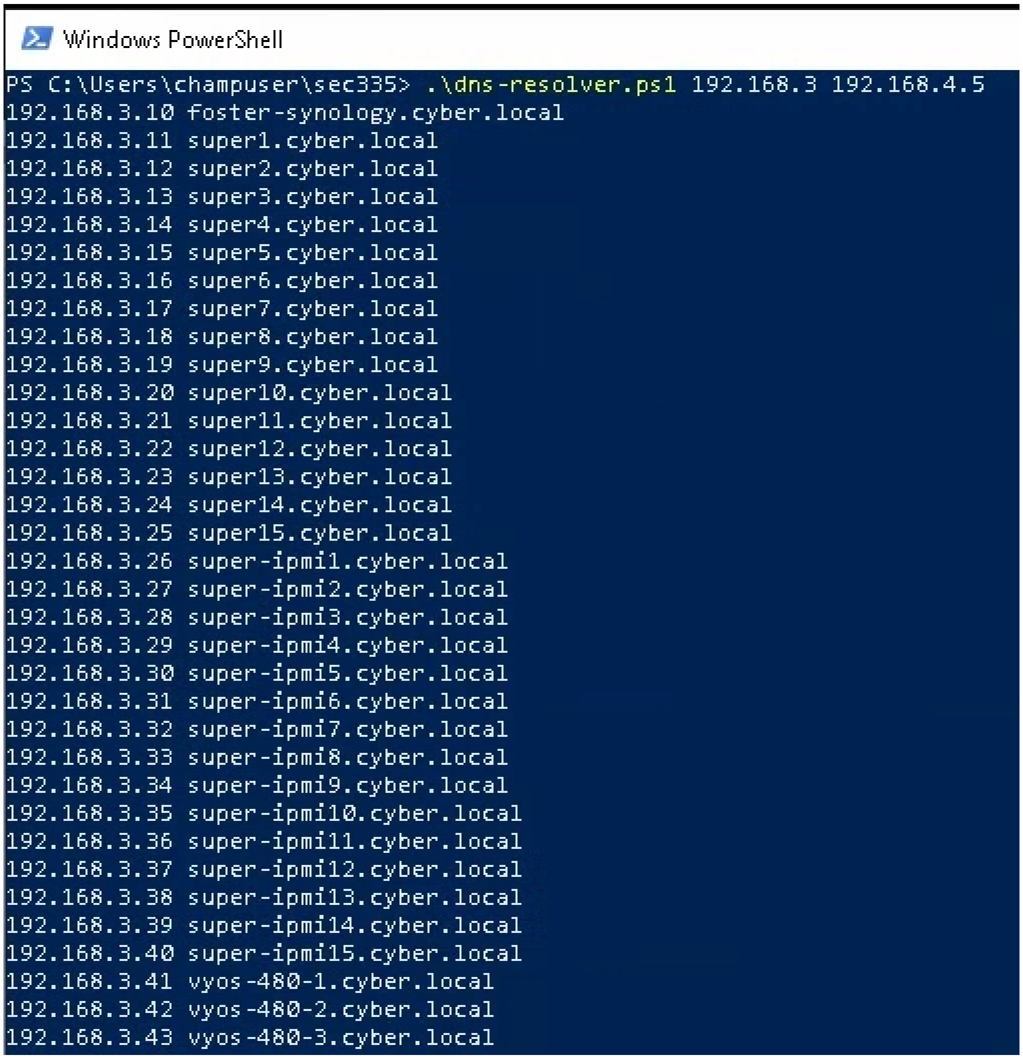


```
PS C:\Users\champuser> Resolve-DnsName -DnsOnly 192.168.3.100 -Server 192.168.4.4 -ErrorAction Ignore

Name                          Type   TTL   Section    NameHost
----                          ----   ---   -------    --------
100.3.168.192.in-addr.arpa    PTR    900   Answer     FOSTER202-00.cyber.local


PS C:\Users\champuser>
```

Extend the one liner by creating a powershell script that takes a network prefix, the dns server to use (one of the cyber.local dns servers).

Updated Feb 2, 2022

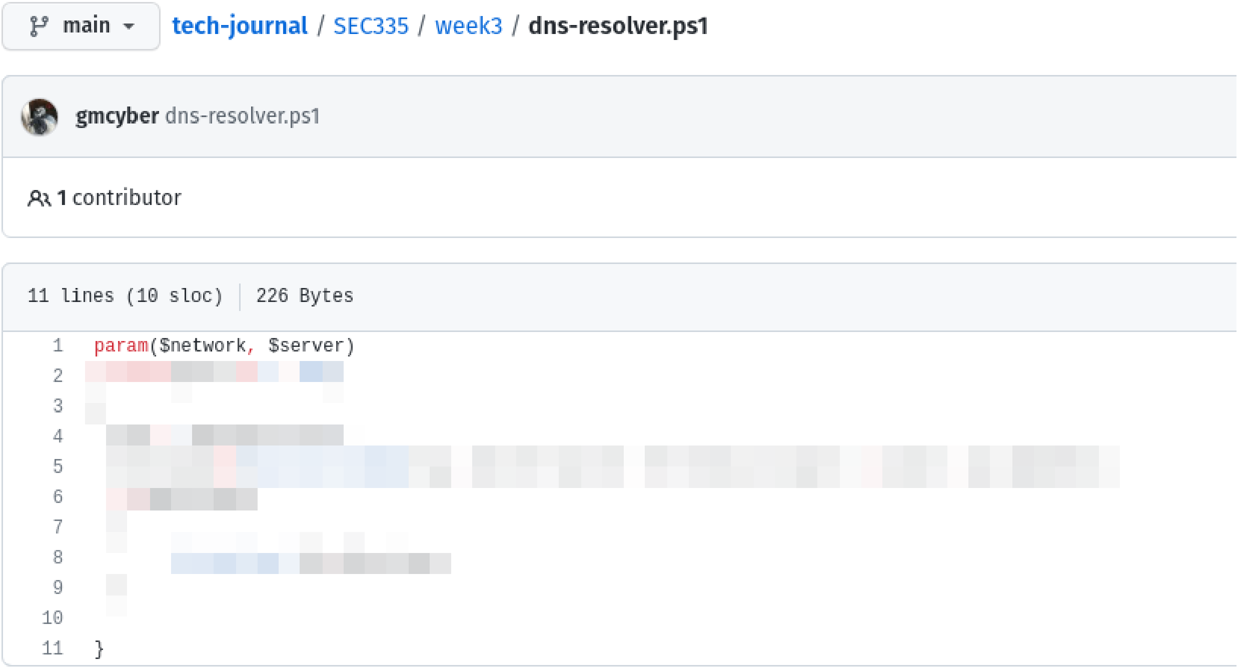
Deliverable 1. Provide a screenshot similar to the one below showing the program run against the foster subnet. The simplistic run shown here, just increments the octet in the 192.168.3.0/24 from 1 to 254.



```
PS C:\Users\champuser\sec335> .\dns-resolver.ps1 192.168.3 192.168.4.5
192.168.3.10 foster-synology.cyber.local
192.168.3.11 super1.cyber.local
192.168.3.12 super2.cyber.local
192.168.3.13 super3.cyber.local
192.168.3.14 super4.cyber.local
192.168.3.15 super5.cyber.local
192.168.3.16 super6.cyber.local
192.168.3.17 super7.cyber.local
192.168.3.18 super8.cyber.local
192.168.3.19 super9.cyber.local
192.168.3.20 super10.cyber.local
192.168.3.21 super11.cyber.local
192.168.3.22 super12.cyber.local
192.168.3.23 super13.cyber.local
192.168.3.24 super14.cyber.local
192.168.3.25 super15.cyber.local
192.168.3.26 super-ipmi1.cyber.local
192.168.3.27 super-ipmi2.cyber.local
192.168.3.28 super-ipmi3.cyber.local
192.168.3.29 super-ipmi4.cyber.local
192.168.3.30 super-ipmi5.cyber.local
192.168.3.31 super-ipmi6.cyber.local
192.168.3.32 super-ipmi7.cyber.local
192.168.3.33 super-ipmi8.cyber.local
192.168.3.34 super-ipmi9.cyber.local
192.168.3.35 super-ipmi10.cyber.local
192.168.3.36 super-ipmi11.cyber.local
192.168.3.37 super-ipmi12.cyber.local
192.168.3.38 super-ipmi13.cyber.local
192.168.3.39 super-ipmi14.cyber.local
192.168.3.40 super-ipmi15.cyber.local
192.168.3.41 vyos-480-1.cyber.local
192.168.3.42 vyos-480-2.cyber.local
192.168.3.43 vyos-480-3.cyber.local
```

Updated Feb 2, 2022

Deliverable 2. Provide a screenshot similar to the one below that shows your directory structure and the source code of your powershell dns resolver. Alternatively, you can provide a link to your one liner in your github documentation.



tech-journal / SEC335 / week3 / dns-resolver.ps1

gmcyber dns-resolver.ps1

11 lines (10 sloc) | 226 Bytes

```
param($network, $server)
[redacted]
}
```