

Forum:[Hack Forums](#)

Thread: [NTP scanning.](#)

SSYN-UDP - May 6, 2017, 3:12 am

Hello community. I was wondering if someone would help me with a basic NTP scanner. It's in perl. You can find below.

Usage: ./scanner.pl [START-IP] [END-IP] [PORT] [THREADS] [TIMEOUT] [OUTPUT]

```
foreach my $pid (@Pids) { waitpid($pid, 0) }  
}[/code]
```

When Scanning the usage is. Quote:Usage: ./scanner.pl [START-IP] [END-IP] [PORT] [THREADS] [TIMEOUT] [OUTPUT]

However when it's scanning it's only showing me the IP address of any NTP's that may be found. Is that because I am specifying what port to search on already?

ProtectNull™ - May 6, 2017, 3:16 am

I wouldn't even recommended using a perl scanner, use a compiled c source one.

SSYN-UDP - May 6, 2017, 3:23 am

Thank you for your advice. Do you have one that you would advise on using? I am using Kali linux if that makes any difference.

ProtectNull™ - May 6, 2017, 3:54 am

(May 6, 2017 03:23 AM)SSYN-UDP Wrote: [\[CITE\]](#) Thank you for your advice. Do you have one that you would advise on using? I am using Kali linux if that makes any difference.

Buy a scanning server, don't bother using your home network as one.

There are heaps of sources here in HF or in pastebin, just look for a NTP c scanner source.

SSYN-UDP - May 6, 2017, 3:58 am

Thanks for the advice. I will be sure to do so. I know it would be very unwise and stupid to do so. But in a test environment in a controlled system. Would I be able to use the List of NTP's from my own connection if I have scappy etc installed or does this require IP spoofing?