Nmap-ssl-parser

Kerberos Username Enumeration – Top 500 Common Usernames

JUN
23

Auto-sslscan (Automatic SSL Scanning)

By matt in Tools

Auto-sslscan

As I mentioned in the previous post whilst Nessus and Nmap do a reasonable job of enumerating SSL protocols and ciphers I often find myself utilising other 3rd party SSL scanning tools. One I find myself turning to on a regular basis is sslscan, I like the output it provides and issues become immediately apparent, although if you prefer using SSL scanning tool X or Y, the auto-sslscan code can be easily amended to cater for your tool of choice.

Auto-sslscan is a python script designed to automate the process of conducting ssl scanning via sslcan. The Auto-sslscan script parses an nmap.xml output file, extracts all SSL services and automatically performs an sslscan of them.

Step 1 – Create a valid nmap .xml file:

Note: Some form of Nmap version scanning must be utilised to create the XML ouput i.e. `-sV` or `-A` (In order to determine whether the service is SSL enabled)

```
root@cyclops:/scripts/auto-sslcan# nmap -sS -sV -p 443 -iL targets.txt -oX output.xml

Starting Nmap 7.50 ( https://nmap.org ) at 2017-06-23 22:08 BST
Nmap scan report for 185.176.90.16
Host is up (0.018s latency).

PORT    STATE SERVICE  VERSION
443/tcp open  ssl/http nginx

Nmap scan report for 199.101.100.186
Host is up (0.11s latency).

PORT    STATE SERVICE  VERSION
443/tcp open  ssl/http Apache httpd

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 2 IP addresses (2 hosts up) scanned in 15.10 seconds
```

Step 2 – Process the Nmap XML file with auto-sslscan.py:

```
root@cyclops:/scripts/auto-sslcan# ./auto-sslscan.py output.xml sslscan-output.txt
auto-sslscan - v0.1 ( https://github.com/attackdebris/auto-sslscan )

Performing sslscan of 185.176.90.16:443
Performing sslscan of 199.101.100.186:443

sslscan results saved to: sslscan-output.txt
SSL services list saved to: ssl-services.txt
```

SSL Services:

That's effectively job done, we now have a list of SSL services if we wish to target them again with another tool:

```
root@cyclops:/scripts/auto-sslcan# cat ssl-services.txt
185.176.90.16:443
199.101.100.186:443
```

SSL Scan Ouput:

The actual SSL scanning "sslscan" ouput is saved to a concatenated file (truncated image below):

```
root@cyclops:/scripts/auto-sslcan# cat sslscan-output.txt
================================================================
auto-sslscan - v0.1 ( https://github.com/attackdebris/auto-sslscan )
================================================================

Version: 1.11.10-static
OpenSSL 1.0.2-chacha (1.0.2g-dev)

Testing SSL server 185.176.90.16 on port 443 using SNI name

  TLS Fallback SCSV:
Server supports TLS Fallback SCSV

  TLS renegotiation:
Secure session renegotiation supported

  TLS Compression:
Compression disabled

  Heartbleed:
```

The code and installation instructions can be found here: https://github.com/attackdebris/auto-sslscan

Also check out nmap-ssl-parser, which simply parses the nmap XML file and provides a list of SSL services: https://github.com/attackdebris/nmap-ssl-parser

Credit – The base code I used to create nmap-ssl-parser: https://github.com/DanMcInerney/nmap-parser/blob/master/nmap-parser.py

Tools

Leave a Reply

Your email address will not be published.

Your message

Name

Email

Website (optional)

Notify me of follow-up comments by email.

Notify me of new posts by email.

Submit Comment

Search

Follow @attackdebris

RECENT POSTS

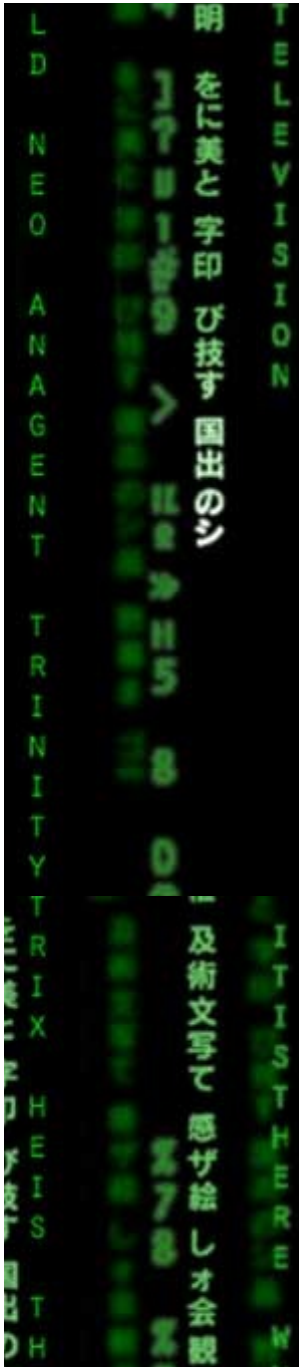
- Troubleshooting Empire and PoshC2_Python HTTPS Connections
- Low Privilege Active Directory Enumeration from a non-Domain Joined Host
- Cracking Cisco ASA SHA-512 Hashes with Hashcat
- Kerberos Username Enumeration – Top 500 Common Usernames
- Auto-sslscan (Automatic SSL Scanning)

USEFUL LINKS

- Hack, Whack and Smack
- Phillips321
- rewt dance
- Scriptmonkey

ARCHIVES

- December 2018
- February 2018



January 2018

June 2017

November 2016

October 2014

February 2014

October 2013

August 2013

May 2013

September 2012

CATEGORIES

Active Directory

Conferences

Host Lockdown Testing

Passwords

PowerShell

Red Team

Tools