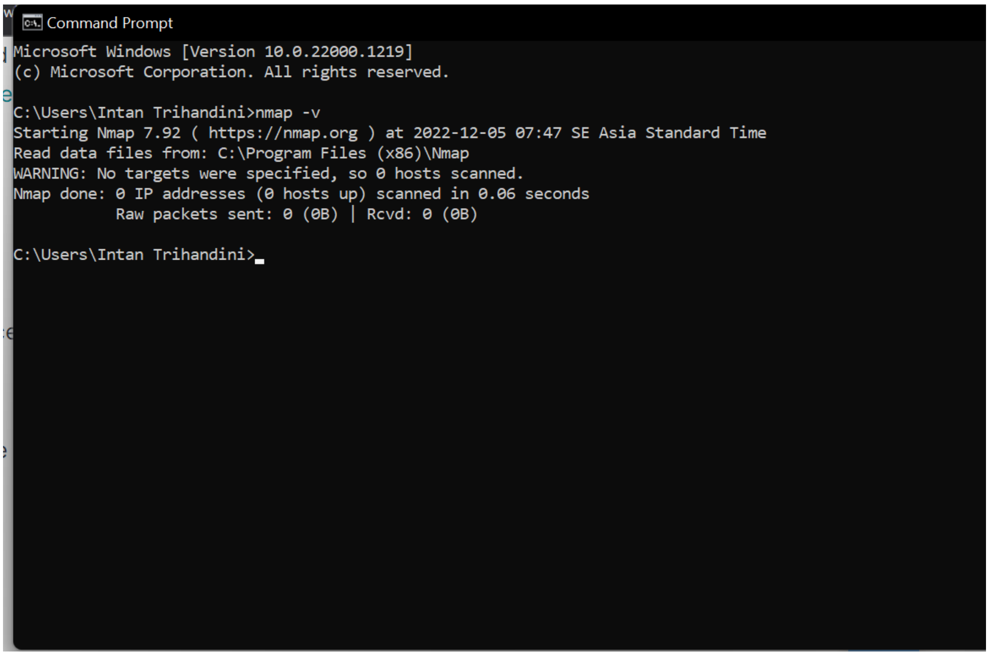
Nama : Intan Trihandini Alawiyah
kelas : 3SI2
NIM : 222011537

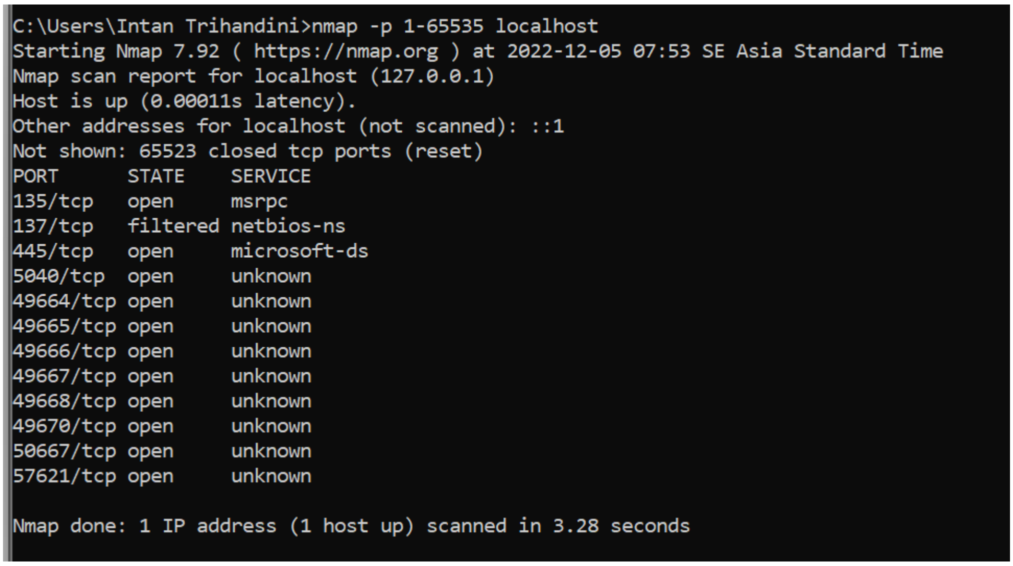
PRAKTIKUM PERTEMUAN 13

berhasil menginstall NMAP



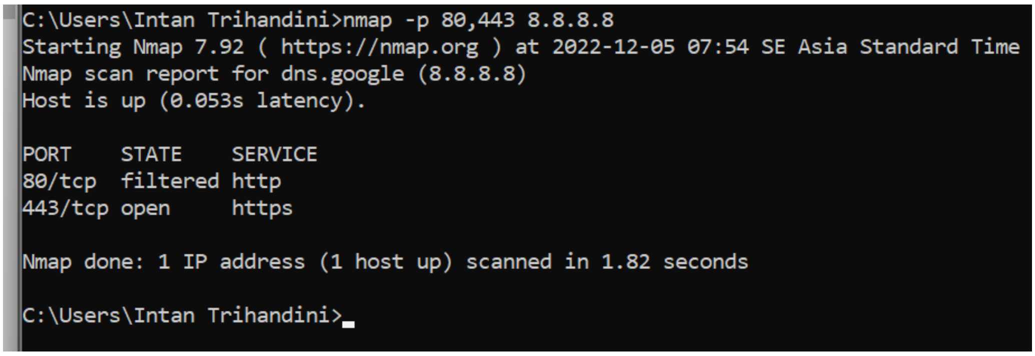
```
Microsoft Windows [Version 10.0.22000.1219]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Intan Trihandini>nmap -v
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-05 07:47 SE Asia Standard Time
Read data files from: C:\Program Files (x86)\Nmap
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.06 seconds
           Raw packets sent: 0 (0B) | Rcvd: 0 (0B)

C:\Users\Intan Trihandini>
```

mengecek seluruh possible port



```
C:\Users\Intan Trihandini>nmap -p 1-65535 localhost
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-05 07:53 SE Asia Standard Time
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00011s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 65523 closed tcp ports (reset)
PORT      STATE    SERVICE
135/tcp   open     msrpc
137/tcp   filtered netbios-ns
445/tcp   open     microsoft-ds
5040/tcp  open     unknown
49664/tcp open     unknown
49665/tcp open     unknown
49666/tcp open     unknown
49667/tcp open     unknown
49668/tcp open     unknown
49670/tcp open     unknown
50667/tcp open     unknown
57621/tcp open     unknown

Nmap done: 1 IP address (1 host up) scanned in 3.28 seconds
```

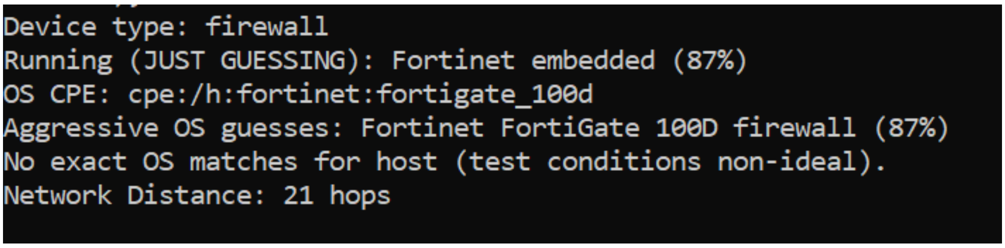
mengecek port secara spesifik, yakin port 80 dan 443



```
C:\Users\Intan Trihandini>nmap -p 80,443 8.8.8.8
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-05 07:54 SE Asia Standard Time
Nmap scan report for dns.google (8.8.8.8)
Host is up (0.053s latency).

PORT    STATE    SERVICE
80/tcp  filtered http
443/tcp open     https

Nmap done: 1 IP address (1 host up) scanned in 1.82 seconds

C:\Users\Intan Trihandini>
```

PENUGASAN

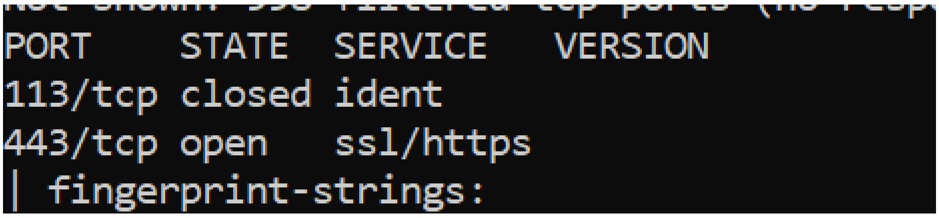
1. Asuransi pemerintahan → jiwasraya (jiwasraya.co.id)
   a. OS yang digunakan



```
Device type: firewall
Running (JUST GUESSING): Fortinet embedded (87%)
OS CPE: cpe:/h:fortinet:fortigate_100d
Aggressive OS guesses: Fortinet FortiGate 100D firewall (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 21 hops
```

   OS yang digunakan adalah fortinet, yakni cpe: /h:fortinet:fortigate_100d

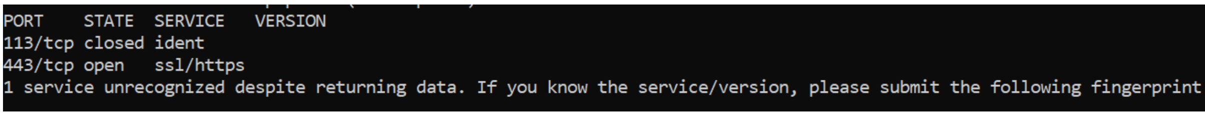
   b. port yang terbuka



```
PORT    STATE  SERVICE   VERSION
113/tcp closed ident
443/tcp open   ssl/https
| fingerprint-strings:
```

   port yang terdeteksi terbuka hanya 443 untuk ssl/https

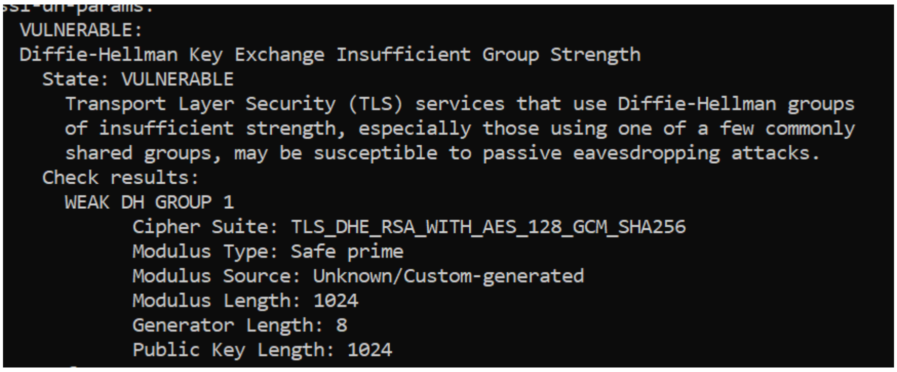
   c. layanan yang disediakan



```
PORT    STATE  SERVICE   VERSION
113/tcp closed ident
443/tcp open   ssl/https
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint
```

   terlihat bahwa hasilnya adalah service unrecognized despite returning data. Tidak ada service yang terdeteksi

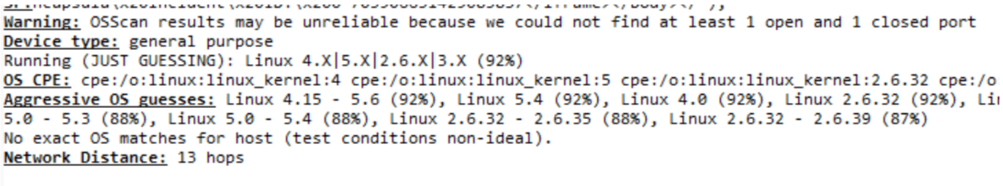
   d. Celah keamanan



```
ssl-dh-params:
  VULNERABLE:
  Diffie-Hellman Key Exchange Insufficient Group Strength
    State: VULNERABLE
      Transport Layer Security (TLS) services that use Diffie-Hellman groups
      of insufficient strength, especially those using one of a few commonly
      shared groups, may be susceptible to passive eavesdropping attacks.
    Check results:
      WEAK DH GROUP 1
            Cipher Suite: TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
            Modulus Type: Safe prime
            Modulus Source: Unknown/Custom-generated
            Modulus Length: 1024
            Generator Length: 8
            Public Key Length: 1024
```

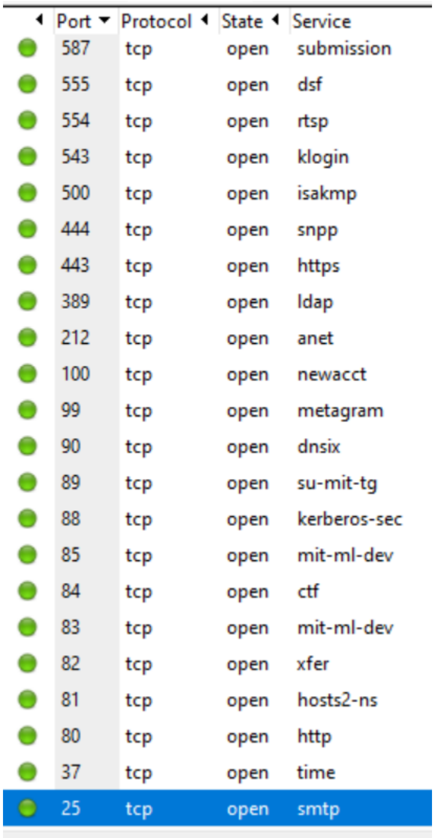
2. asuransi swasta→ Allianz (prudential.co.id)

   a. OS yang digunakan

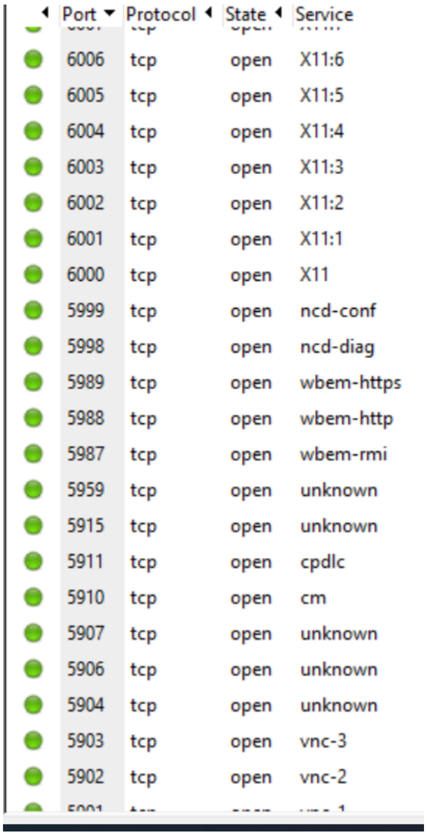


```
[illegible]
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Linux 4.X|5.X|2.6.X|3.X (92%)
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel:2.6.32 cpe:/o
Aggressive OS guesses: Linux 4.15 - 5.6 (92%), Linux 5.4 (92%), Linux 4.0 (92%), Linux 2.6.32 (92%), Li
5.0 - 5.3 (88%), Linux 5.0 - 5.4 (88%), Linux 2.6.32 - 2.6.35 (88%), Linux 2.6.32 - 2.6.39 (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 13 hops
```

   b. port yang terbuka



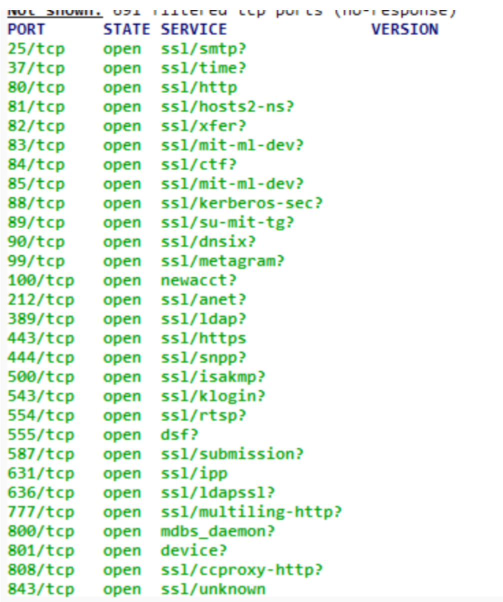
	Port	Protocol	State	Service
●	587	tcp	open	submission
●	555	tcp	open	dsf
●	554	tcp	open	rtsp
●	543	tcp	open	klogin
●	500	tcp	open	isakmp
●	444	tcp	open	snpp
●	443	tcp	open	https
●	389	tcp	open	ldap
●	212	tcp	open	anet
●	100	tcp	open	newacct
●	99	tcp	open	metagram
●	90	tcp	open	dnsix
●	89	tcp	open	su-mit-tg
●	88	tcp	open	kerberos-sec
●	85	tcp	open	mit-ml-dev
●	84	tcp	open	ctf
●	83	tcp	open	mit-ml-dev
●	82	tcp	open	xfer
●	81	tcp	open	hosts2-ns
●	80	tcp	open	http
●	37	tcp	open	time
●	25	tcp	open	smtp



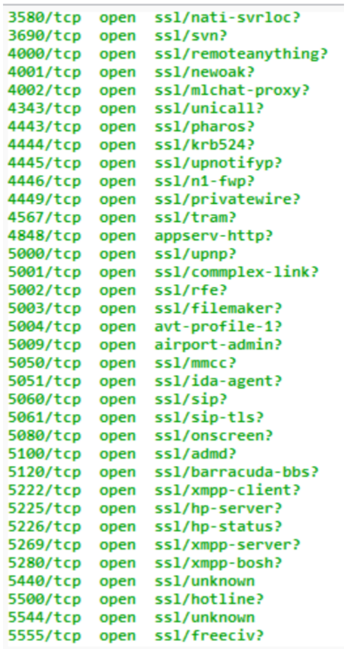
	Port	Protocol	State	Service
●	6006	tcp	open	X11:6
●	6005	tcp	open	X11:5
●	6004	tcp	open	X11:4
●	6003	tcp	open	X11:3
●	6002	tcp	open	X11:2
●	6001	tcp	open	X11:1
●	6000	tcp	open	X11
●	5999	tcp	open	ncd-conf
●	5998	tcp	open	ncd-diag
●	5989	tcp	open	wbem-https
●	5988	tcp	open	wbem-http
●	5987	tcp	open	wbem-rmi
●	5959	tcp	open	unknown
●	5915	tcp	open	unknown
●	5911	tcp	open	cpdlc
●	5910	tcp	open	cm
●	5907	tcp	open	unknown
●	5906	tcp	open	unknown
●	5904	tcp	open	unknown
●	5903	tcp	open	vnc-3
●	5902	tcp	open	vnc-2

Terdapat beberapa port yang terdeteksi terbuka, diantaranya adalah port 443 untuk https dan port 80 untuk http dengan versi awselb/2.0

c. layanan yang disediakan

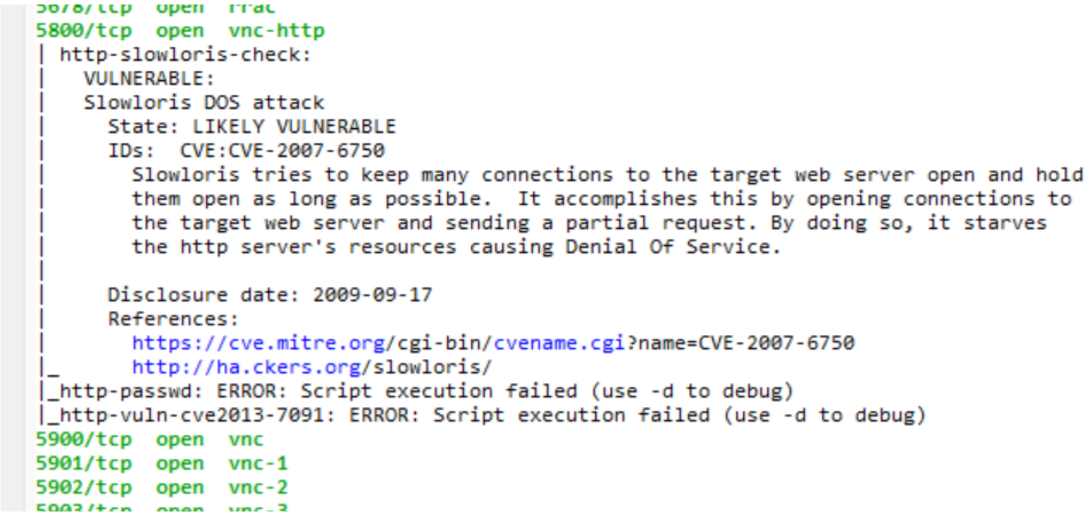


```
Not shown: 891 filtered tcp ports (no-response)
PORT      STATE SERVICE           VERSION
25/tcp    open  ssl/smtp?
37/tcp    open  ssl/time?
80/tcp    open  ssl/http
81/tcp    open  ssl/hosts2-ns?
82/tcp    open  ssl/xfer?
83/tcp    open  ssl/mit-ml-dev?
84/tcp    open  ssl/ctf?
85/tcp    open  ssl/mit-ml-dev?
88/tcp    open  ssl/kerberos-sec?
89/tcp    open  ssl/su-mit-tg?
90/tcp    open  ssl/dnsix?
99/tcp    open  ssl/metagram?
100/tcp   open  newacct?
212/tcp   open  ssl/anet?
389/tcp   open  ssl/ldap?
443/tcp   open  ssl/https
444/tcp   open  ssl/snpp?
500/tcp   open  ssl/isakmp?
543/tcp   open  ssl/klogin?
554/tcp   open  ssl/rtsp?
555/tcp   open  dsf?
587/tcp   open  ssl/submission?
631/tcp   open  ssl/ipp
636/tcp   open  ssl/ldapssl?
777/tcp   open  ssl/multiling-http?
800/tcp   open  mdbs_daemon?
801/tcp   open  device?
808/tcp   open  ssl/ccproxy-http?
843/tcp   open  ssl/unknown
```



```
3580/tcp  open  ssl/nati-svrloc?
3690/tcp  open  ssl/svn?
4000/tcp  open  ssl/remoteanything?
4001/tcp  open  ssl/newoak?
4002/tcp  open  ssl/mlchat-proxy?
4343/tcp  open  ssl/unicall?
4443/tcp  open  ssl/pharos?
4444/tcp  open  ssl/krb524?
4445/tcp  open  ssl/upnotifyp?
4446/tcp  open  ssl/n1-fwp?
4449/tcp  open  ssl/privatewire?
4567/tcp  open  ssl/tram?
4848/tcp  open  appserv-http?
5000/tcp  open  ssl/upnp?
5001/tcp  open  ssl/commplex-link?
5002/tcp  open  ssl/rfe?
5003/tcp  open  ssl/filemaker?
5004/tcp  open  avt-profile-1?
5009/tcp  open  airport-admin?
5050/tcp  open  ssl/mmcc?
5051/tcp  open  ssl/ida-agent?
5060/tcp  open  ssl/sip?
5061/tcp  open  ssl/sip-tls?
5080/tcp  open  ssl/onscreen?
5100/tcp  open  ssl/admd?
5120/tcp  open  ssl/barracuda-bbs?
5222/tcp  open  ssl/xmpp-client?
5225/tcp  open  ssl/hp-server?
5226/tcp  open  ssl/hp-status?
5269/tcp  open  ssl/xmpp-server?
5280/tcp  open  ssl/xmpp-bosh?
5440/tcp  open  ssl/unknown
5500/tcp  open  ssl/hotline?
5544/tcp  open  ssl/unknown
5555/tcp  open  ssl/freeciv?
```

d. Celah keamanan



```
5678/tcp open  rrac
5800/tcp open  vnc-http
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_      http://ha.ckers.org/slowloris/
|_http-passwd: ERROR: Script execution failed (use -d to debug)
|_http-vuln-cve2013-7091: ERROR: Script execution failed (use -d to debug)
5900/tcp open  vnc
5901/tcp open  vnc-1
5902/tcp open  vnc-2
5903/tcp open  vnc-3
```