

COMP 3355

Lab 2

Network capture and scanning

Wireshark & Nmap

Introduction to Packet Capture

- What is packet capture?
- Packet capture is a process of collecting packets which will be processed and used later for further purposes

Introduction to Wireshark

- ▶ Wireshark is a free and open-source packet capture analyzer.
- ▶ Used for network troubleshooting, analysis, software and communications protocol development, and education.
- ▶ Wireshark is cross-platform, using the Qt widget toolkit in current releases to implement its user interface, and using pcap to capture packets.



Introduction to Wireshark

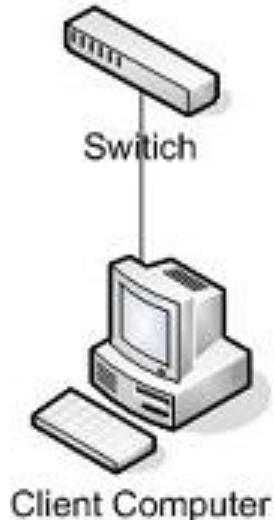
Wireshark can:

1. Capture the **incoming** and **outgoing** traffic of the network interface
2. Capture all communications within a Network

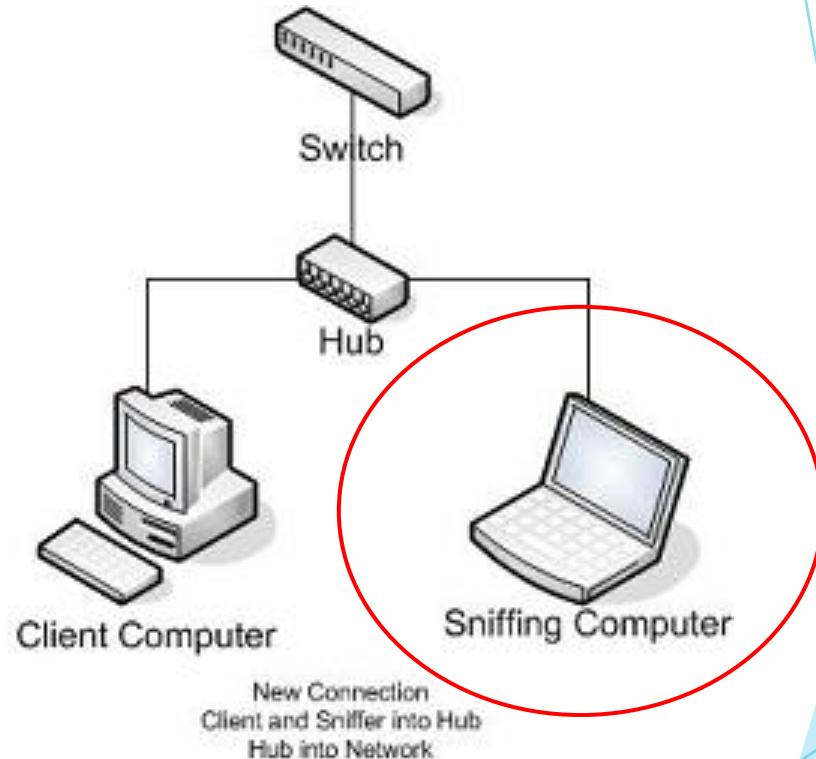
It allows the user to put network interface controllers into promiscuous mode.

See all traffic visible on that interface, not just traffic addressed to one of the interface's configured addresses and broadcast/multicast traffic.

Capture network traffic within a internal network



Initial Connection
Client To Network



New Connection
Client and Sniffer into Hub
Hub into Network

How to install Wireshark

- ▶ Open the browser and go to the website
<https://www.wireshark.org/download.html>

Download Wireshark

The current stable release of Wireshark is 3.0.6. It supersedes all previous releases. You can also download the latest development release (3.1.0) and documentation.

The screenshot shows the 'Stable Release (3.0.6)' section of the Wireshark download page. A red circle highlights the first five download links: 'Windows Installer (64-bit)', 'Windows Installer (32-bit)', 'Windows PortableApps® (32-bit)', 'macOS 10.12 and later Intel 64-bit .dmg', and 'Source Code'. To the right of the 'Windows Installer (64-bit)' link, the text 'Windows version' is overlaid in blue. Below the highlighted links, the text 'MacOS version' is overlaid in blue. The page also includes sections for 'Old Stable Release (2.6.12)', 'Development Release (3.1.0)', and 'Documentation'.

- Windows Installer (64-bit)
- Windows Installer (32-bit)
- Windows PortableApps® (32-bit)
- macOS 10.12 and later Intel 64-bit .dmg
- Source Code

Windows version

MacOS version

Old Stable Release (2.6.12)

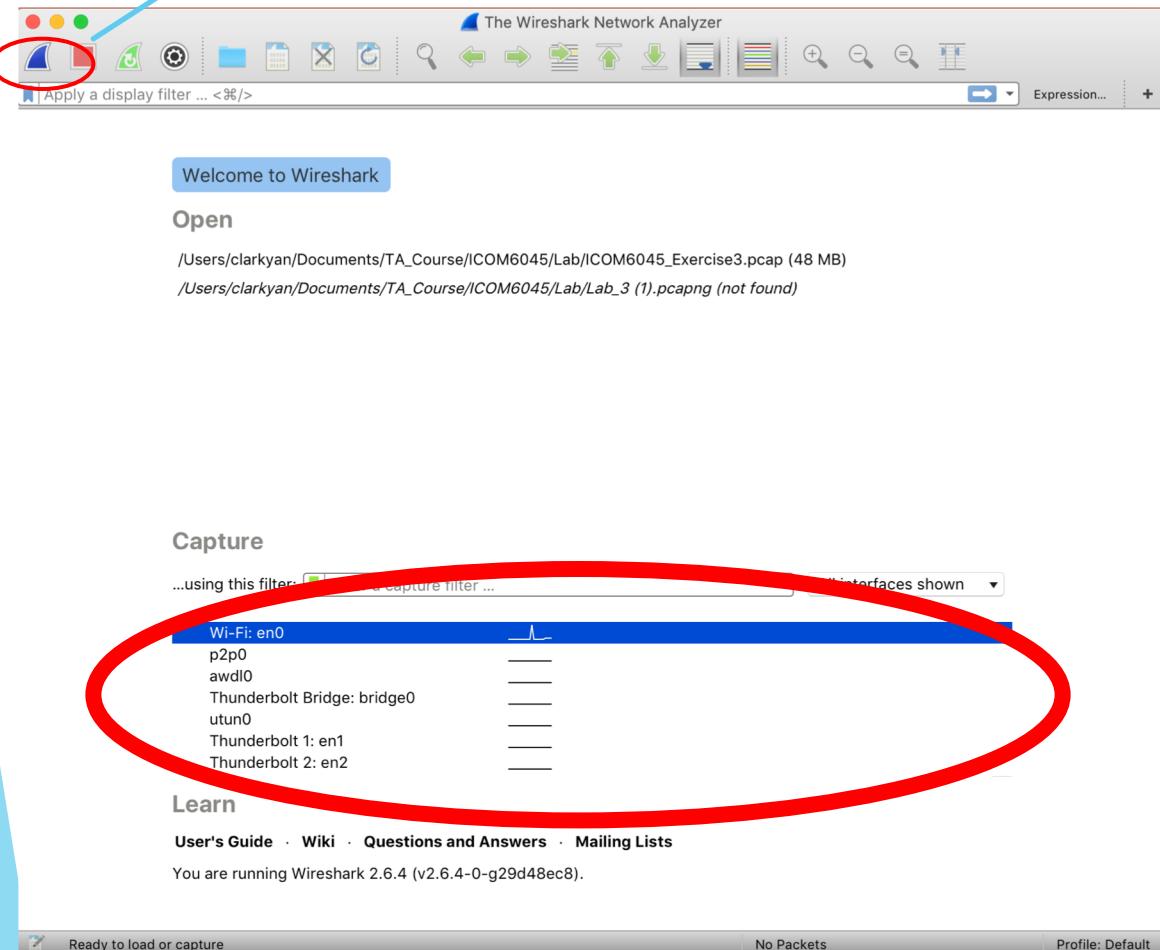
Development Release (3.1.0)

Documentation

Select a version and click to download the software

Capture Packet using Wireshark

Press “Start”



Try it!

Select the Network interface

Try the following scenario

- Start capture packet in Wireshark
- Open your web browser, access
<http://moodle.hku.hk/>
- Stop the packet capture

- Use "http" filter to find all http requests
- After selecting the GET information

Wi-Fi: en0

No.	Time	Source	Destination	Protocol	Length	Info
+ 1508	12.440328	10.68.165.188	147.8.2.150	HTTP	151	GET / HTTP/1.1
- 1543	12.889384	147.8.2.150	10.68.165.188	HTTP	1410	HTTP/1.1 200 OK (text/html)

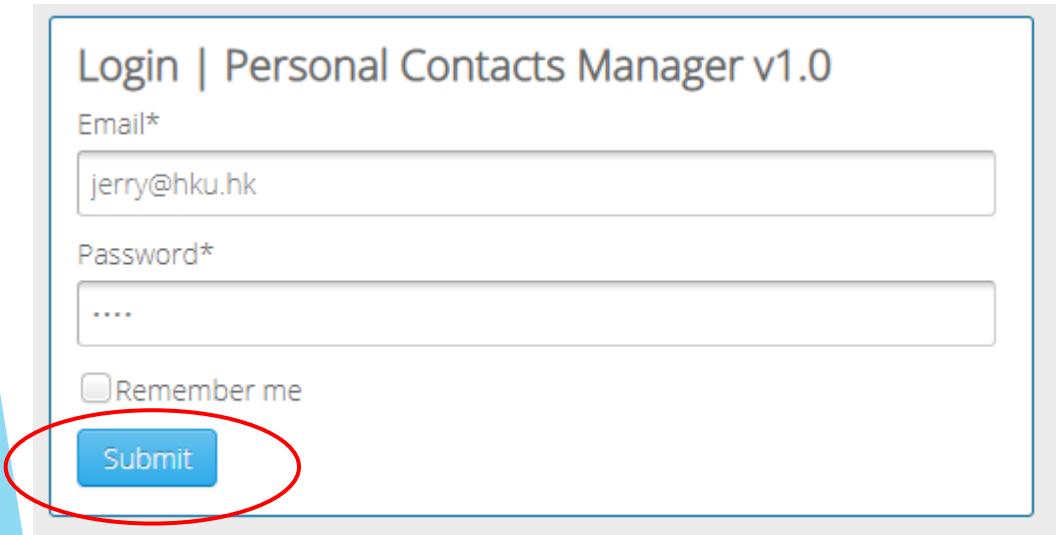
```

Frame 1508: 151 bytes on wire (1208 bits), 151 bytes captured (1208 bits) on interface 0
Ethernet II, Src: Apple_04:54:69 (a0:99:9b:04:54:69), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
Internet Protocol Version 4, Src: 10.68.165.188, Dst: 147.8.2.150
Transmission Control Protocol, Src Port: 50327, Dst Port: 80, Seq: 1369, Ack: 1, Len: 85
[2 Reassembled TCP Segments (1453 bytes): #1508(1368), #1508(85)]
Hypertext Transfer Protocol
  GET / HTTP/1.1\r\n
  Host: moodle.hku.hk\r\n
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: zh-CN,zh;q=0.9\r\n
  [Truncated]Cookie: __utma=162991397.301046638.1472485157.1491987602.1503653698.7; __ga=GA1.2.301046638.1472485157; sis_msg=1; hcms_msg=1; esd_from_sys=CAS; dlptmp="https://moodle
\r\n
Full request URI: http://moodle.hku.hk/
[HTTP request 1/1]
[Response in frame: 1543]
```

0000 00 00 5e 00 01 01 a0 99 9b 04 54 69 08 00 45 00 ..^..... Ti..E..
0010 00 89 00 00 40 00 40 06 f4 d0 0a 44 a5 bc 93 08@. @. D...
0020 02 96 c4 97 00 50 d9 f1 7d 84 75 80 b6 bd 80 18P. } u....
0030 ff ff 90 52 00 00 01 01 08 0a 2f 79 ce 41 ed 5f ..R.y A...
0040 c8 e1 36 61 38 63 33 36 31 61 65 39 63 32 34 ..6a8c36 1ae9cc24
0050 36 63 36 36 32 39 65 33 38 37 63 34 61 34 33 63 6c6629e3 87c4a43c
0060 33 66 66 61 36 61 66 39 61 64 62 30 38 31 38 32 3ffa6af9 adb08182

Try the following scenario

- Start capture packet in Wireshark
- Open your web browser, access
<http://www.techpanda.org/>



Login | Personal Contacts Manager v1.0

Email*

Password*

Remember me

Submit

Click
“Submit”
Here!

- Stop the packet capture
- Use “http” filter to find all http requests
- After selecting the POST information

Screenshot of NetworkMiner tool showing captured HTTP traffic. A red circle highlights the selected POST request (Frame 751) and its details.

Selected Frame:

No.	Time	Source	Destination	Protocol	Length	Info
354	9.990208	192.168.1.100	72.52.251.71	HTTP	473	GET / HTTP/1.1
365	10.195604	72.52.251.71	192.168.1.100	HTTP	1219	HTTP/1.1 200 OK (text/html)
414	10.431884	192.168.1.100	192.168.1.1	HTTP	245	GET /igd.xml HTTP/1.1
422	10.486123	192.168.1.1	192.168.1.100	HTTP/X...	241	HTTP/1.1 200 OK
751	20.352183	192.168.1.100	72.52.251.71	HTTP	734	POST /index.php HTTP/1.1 (application/x-www-form-urlencoded)
755	20.568557	72.52.251.71	192.168.1.100	HTTP	377	HTTP/1.1 500 Internal Server Error

Selected Request Details:

```

> Frame 751: 734 bytes on wire (5872 bits), 734 bytes captured (5872 bits) on interface 0
> Ethernet II, Src: Micro-St_24:97:25 (30:9c:23:24:97:25), Dst: Tp-LinkT_a0:4a:c0 (7c:8b:ca:a0:4a:c0)
> Internet Protocol Version 4, Src: 192.168.1.100, Dst: 72.52.251.71
> Transmission Control Protocol, Src Port: 57343, Dst Port: 80, Seq: 1, Ack: 1, Len: 680
> Hypertext Transfer Protocol
  < HTML Form URL Encoded: application/x-www-form-urlencoded
    > Form item: "email" = "jerry@hku.hk"
    > Form item: "password" = "1234"
  
```

Selected Hex Dump:

0280	3d 30 2e 39 0d 0a 43 6f 6f 6b 69 65 3a 20 50 48	=0.9 Co okie: PH
0290	50 53 45 53 53 49 44 3d 66 35 38 33 66 39 65 64	PSESSID= f583f9ed
02a0	31 36 37 62 36 62 66 36 39 32 63 38 35 63 64 34	167b6bf6 92c85cd4
02b0	39 35 38 39 61 62 39 30 0d 0a 0d 0a 65 6d 61 69	9589ab90 ... emai
02c0	6c 3d 6a 65 72 72 79 25 34 30 68 6b 75 2e 68 6b	l=jerry% 40hku.hk
02d0	26 70 61 73 73 77 6f 72 64 3d 31 32 33 34	&passwor d=1234

Try the following scenario

- Start capture packet in Wireshark
- Open your web browser, access
<https://hkuportal.hku.hk>

The screenshot shows the login interface of the HKU Portal. At the top, there's a banner with several students waving. The header includes the HKU logo, the text 'THE UNIVERSITY OF HONG KONG | HKU PORTAL', and links for 'FAQ', 'Create User ID (for staff)', 'Security Tips', and 'Feedback'. Below the banner is a large 'LOG IN' section. It has input fields for 'UID' and 'PIN', both of which are currently empty. A red circle highlights the green 'LOG IN' button. Below the input fields is a link 'Forgot your PIN/Passwords?'. To the right of the log-in form, there are three links: 'FAQ', 'Create User ID (for staff)', and 'Security Tips'. A small illustration of two people is at the bottom left.

Click
“Login
In” Here!

- Stop the packet capture
- Use "ssl" filter to find all https requests
- Can you find the record? Why and Why not?

Wi-Fi: en0

ssl

No.	Time	Source	Destination	Protocol	Length	Info
1578	58.733409	17.252.201.246	10.68.165.188	TLSv1.2	117	Change Cipher Spec, Encrypted Handshake Message
1579	58.733414	17.252.201.246	10.68.165.188	TLSv1.2	117	Change Cipher Spec, Encrypted Handshake Message
1582	58.737457	10.68.165.188	17.252.201.246	TLSv1.2	486	Application Data
1583	58.737534	10.68.165.188	17.252.201.246	TLSv1.2	484	Application Data
1584	58.742937	17.252.201.246	10.68.165.188	TLSv1.2	161	Application Data
1585	58.742948	17.252.201.246	10.68.165.188	TLSv1.2	161	Application Data
1590	60.692583	10.68.165.188	17.252.201.246	TLSv1.2	97	Encrypted Alert
1591	60.694012	10.68.165.188	17.252.201.246	TLSv1.2	97	Encrypted Alert
1594	60.697762	17.252.201.246	10.68.165.188	TLSv1.2	97	Encrypted Alert
1596	60.697768	17.252.201.246	10.68.165.188	TLSv1.2	97	Encrypted Alert
1609	62.974471	138.91.254.234	10.68.165.188	TLSv1.2	112	[TCP ACKed unseen segment] , Application Data
1610	62.974478	138.91.254.234	10.68.165.188	TLSv1.2	97	[TCP ACKed unseen segment] , Encrypted Alert
1616	63.093214	10.68.165.188	52.109.88.39	TLSv1.2	151	Encrypted Alert
1632	64.612123	23.7.219.212	10.68.165.188	TLSv1.2	97	Encrypted Alert
1638	64.612612	10.68.165.188	23.7.219.212	TLSv1.2	97	Encrypted Alert

[Calculated window size: 262]
[Window size scaling factor: -1 (unknown)]
Checksum: 0x6e44 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
▶ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
▶ [SEQ/ACK analysis]
▶ [Timestamps]
TCP payload (46 bytes)
▼ Secure Sockets Layer
▼ TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
Content Type: Application Data (23)
Version: TLS 1.2 (0x0303)
Length: 41
Encrypted Application Data: ca47c0751289163912e3a97c5fcf8b11150603ca2fa8c506...

0000	a0	99	9b	04	54	69	48	d5	39	4c	32	1e	08	00	45	00	...	TiH	9L2	..E
0010	00	62	83	4d	40	00	2c	06	92	02	8a	5b	fe	ea	0a	44	..	b·M@[...]
0020	a5	bc	01	bb	c5	02	63	32	a1	99	59	bb	c3	7f	80	18	...	c2	..Y	..
0030	01	06	6e	44	00	01	01	08	0a	53	44	c6	28	2f	82nDSD	(/..
0040	c6	62	17	03	03	00	29	ca	47	c0	75	12	89	16	39	12	..	b·(..G	u..9
0050	e3	a9	7c	5f	cb	8b	11	15	06	03	ca	2f	a8	c5	06	deJ(/..
0060	68	fa	28	fd	93	97	fe	f1	4b	18	86	b5	a9	95	b6	b1	h·(..	..K

NMAP - the Network MAPper

- ▶ In order to crack into a computer system, an attacker has to find a target machine, and then find out what ports the machine is listening on before a system can be compromised.
- ▶ By using scanners such as Nmap, the attacker are able to sweep networks and look for vulnerable targets.
- ▶ Once these targets are identified, an intruder is able to scan for listening ports.
- ▶ <https://nmap.org/>



Ping Sweep: Which hosts are up?

- ▶ Intruders are able to sweep entire networks by looking for targets with Nmap. This is usually done with a ping scan by using the "-sP" flag.
- ▶ Nmap will allow you to specify networks with wild cards, such as 10.6.1.*, meaning from 10.6.1.0 to 10.6.1.255.
- ▶ E.g.: nmap -sP 147.8.178.*

```
Tianyiis-MacBook-Pro:~ wang$ nmap -sP 147.8.178.*  
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-05 11:16 HKT  
Nmap scan report for www2.cs.hku.hk (147.8.178.79)  
Host is up (0.0097s latency).  
Nmap scan report for waterman-nat1.cs.hku.hk (147.8.178.109)  
Host is up (0.0056s latency).  
Nmap scan report for host-178-116.cs.hku.hk (147.8.178.116)  
Host is up (0.0044s latency).  
Nmap scan report for host-178-172.cs.hku.hk (147.8.178.172)  
Host is up (0.0052s latency).  
Nmap done: 256 IP addresses (4 hosts up) scanned in 24.81 seconds
```

Port Scanning: Any vulnerable services available?

- ▶ TCP Scanning
 - ▶ When an attacker is using TCP connect scans, Nmap will open connections to interesting ports on the target host
 - ▶ E.g.: nmap -sT localhost

```
[Tianyi-MacBook-Pro:~ wang$ nmap -sT localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-05 11:25 HKT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00025s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 973 closed ports, 26 filtered ports
PORT      STATE SERVICE
631/tcp    open  ipp
```

Port Scanning: Any vulnerable services available?

- ▶ UDP Scanning
 - ▶ Using the UDP scan “-sU” an attacker can determine what ports are open to UDP on a host. Nmap will send a 0-byte UDP packet to each port. If the host returns a "port unreachable" message, that port is considered closed.
 - ▶ E.g.: nmap -sU localhost

```
[Tianyi-MacBook-Pro:~ wang$ sudo nmap -sU localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-05 11:30 HKT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000098s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 997 closed ports
PORT      STATE          SERVICE
137/udp    open|filtered netbios-ns
138/udp    open|filtered netbios-dgm
5353/udp   open|filtered zeroconf
```

May Need Root Privileges

OS Fingerprinting: Which OS is Running on the host?

- ▶ Often an intruder may be more familiar with exploits for a particular operating system, and may be looking for machines he's able to compromise easily. A common option is TCP/IP fingerprinting with the "-O" option to determine the remote operating system.
- ▶ Nmap accomplishes this by sending different types of probes to the host, which will narrow the target operating system.
- ▶ E.g.: nmap -O localhost
- ▶ May Need Root Privileges

CVE detection using Nmap

- ▶ CVE: Common Vulnerabilities and Exposures
- ▶ One of Nmap's greatest features that not all the network and systems administrators know about is something called “Nmap Scripting Engine” (known as NSE).
- ▶ Using NSE is crucial in order to automate system and vulnerability scans.
- ▶ E.g.: nmap -Pn --script vuln localhost

```
PORT      STATE SERVICE
631/tcp    open  ipp
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_http-aspnetsvc-debug: ERROR: Script execution failed (use -d to debug)
| http-phpmyadmin-dir-traversal:
|   VULNERABLE:
|     phpMyAdmin grab_globals.lib.php subform Parameter Traversal Local File Inclusion
|       State: UNKNOWN (unable to test)
|       IDs:  CVE:CVE-2005-3299
|         PHP file inclusion vulnerability in grab_globals.lib.php in phpMyAdmin 2.6.4 and
|         2.6.4-pl1 allows remote attackers to include local files via the $___redirect parameter, p
|         ossibly involving the subform array.
|
```

CVE (And)

```
[root@securitytrails:~]nmap -Pn --script vuln 192.168.1.105
Starting Nmap 7.60 ( https://nmap.org ) at 2018-10-01 09:46 -03
Pre-scan script results:
| broadcast-avahi-dos:
| Discovered hosts:
| 224.0.0.251
| After NULL UDP avahi packet DoS (CVE-2011-1002).
|_ Hosts are all up (not vulnerable).

Nmap scan report for 192.168.1.105
Host is up (0.00032s latency).

Not shown: 995 closed ports
PORT STATE SERVICE
80/tcp open http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| 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:
| http://ha.ckers.org/slowloris/
|_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)

1900/tcp open upnp
20005/tcp open btx
49152/tcp open unknown
49153/tcp open unknown
```

Reference

- Security arrangement with mobile app development

https://www.pcpd.org.hk/mobileapps/files/Sharing_of_Security_Arrangement_with_Mobile_App_De.pdf

- NIST - Vetting the Security of Mobile Applications

<https://www.nist.gov/publications/vetting-security-mobile-applications>

- Testing Website <http://aavtrain.com>

Thanks!