Encrypted Protocol Analysis: Decrypting HTTPS

Hypertext Transfer Protocol secure
- uses TLS protocol to encrypt communication

Malicous websites also use HTTPS

Wireshark

HTTPS Parameters

- Request — http.request
- TLS global search — tls
- TLS Client request — tls.handshake.type == 1
- TLS server response — tls.handshake.type == 2
- Local Simple Discovery Protocol (SSDP) — ssdp

SSDP is a network protocol that provides advertisement and discovery of network services.

Filters are helpful to spot which IP addresses are involved in the TLS handshake

Client = (http.request or tls.handshake.type == 1) and !(ssdp)
Server = (http.request or tls.handshake.type == 2) and !(ssdp)

If we want to read HTTPS traffic in Wireshark, we must give Wireshark the temporary TLS session keys that our browser used, Because the packets are encrypted.

The only way to get those keys is to have the browser export them while the connection is happenning

1) Before we load the website, ~~the~~ set SSLKEYLOGFILE so the Browser will export keys
2) Start capturing traffic in Wireshark
3) Browse normally
4) Tell Wireshark where that key log file is
5) Now Wireshark can decrypt those TLS sessions.

```
export SSLKEYLOGFILE = "$HOME/sslkeys.log"
open -a "..."
```

-through this we can get the Keys.

Question

1) What is the frame number of the "Client Hello" message sent to "accounts.google.com"?

```
tls.handshake.type == 1 && tls.handshake.extension.server_name "accounts.google.com"
```

Decrypt the traffic with the "KeysLogFile.txt" file. What is the number of HTTP2 packets?

115

Go to Frame 322. What is the authority heared of the HTTP2 packet?

safebrowsing[.]googleapis[.]com

Investigate the decrypted packet and find the flag! What is the flag

FLAG{THM-PACKETMASTER3}

Bonus: Hunt Cleartext Credentials

Some Wireshark dissector (FTP, HTTP, IMAP, POP and SMTP) extracts cleartext password ~~& entries of field values~~ from the capture file.

Tools → Credentials

what is the number of the credentials using "HTTP Basic-Auth"

237

what is the packet number where "empty password" was submitted?

170

Bonus: Actionable Results

Creating firewall rules in Wireshark:

Tools → Firewall ACL Rules

Access Control list

Select packet number 99. Create a rule for "IPFirewall (ipfw)". What is the rule for "denying source IPv4 address"?

add deny ip from 10.121.70.151 to any in

Select packet number 231. Create "IPFirewall" rules. What is the rule for "allowing destination MAC address"?

add allow MAC 00:d0:5g:aa:af:80 any in