HTTPS Exfil   
(Blue)  
IT420

Graphical user interface, text, application

Description automatically generated

Explains: Using HTTPS to exfiltrate which encryption is involved and that can hide the information and as well as if the blue team detect smb traffic and add on user behavior that can create alerts, then the persistence attack can be defended.

We need to establish HTTP server and enable the server so we can implement HTTPS

The screenshots below show the commands to download and run HTTP/HTTPS services into the kali Linux

Text

Description automatically generated

As we can see by entering localhost in the browser url, we can access the the HTTP/HTTPS server I establish. It indicates the server established successfully

Graphical user interface, text, email

Description automatically generated

Text

Description automatically generatedAdd the SSL certificate in the apache2 php so It enable the HTTPS, as well as can be exfiltrated.

As we see the upload directory, so we can upload malicious files and execute to the windows server by using https.

Graphical user interface, text, application

Description automatically generatedGraphical user interface, text, application

Description automatically generated

These are the directories that we create the apache web server directory to ensure the uploads can be successful.

A picture containing graphical user interface

Description automatically generated

This uploadPS.txt is the malicious file to establish backdoor in the server.

Text

Description automatically generated

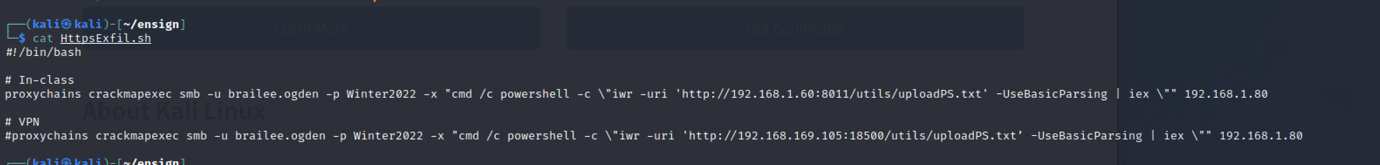
Below two screenshots are to establish tunnels and proxichain for us to hide our identity.

Text

Description automatically generated

Creating this ssh script to run automatically both using internal network and VPN.

Using proxichain to hide our path to attack, and the windows command line to upload and execute directly into the memory so we can hide from antivirus.



As we execute the ssh script, we can see the script uploaded successfully and using HTTPS server to upload and exfiltrate by executing the malicious script at the same time.

Text

Description automatically generated