**HTTP Proxy Tunnelling**

**In order to find the proxies that a firewall is using (if it’s auto-connect/transparent), you will need to find the PAC file**

* Should have the proxy servers ips and ports in the file

Many HTTP proxies only proxy HTTP and not TLS/SSL as it makes the job a lot more burdensome with encryption certificates etc.

So, it will usually just forward HTTPS traffic to its destination using the HTTP-CONNECT command

* Will open a private tunnel for the proxy to use
* Proxies that do this are usually easier to bypass as there’s no content inspection of the HTTPS traffic and can create a good tunnel

**HTTPS proxy**

Full proxying of HTTPS protocol – no e2e encryption

Encryption broken at the firewall, allowing inspection of traffic

Done by attaching certificate to the browser being used, will then create an SSL/TLS connection to the proxy and that’s where it ends and is broken

* Proxy then examines proxy
* If okay, will then form a second SSL/TLS connection to the destination

If there is no certificate installed on the browser then the proxy wont work

**CorkScrew**

A tool for tunnelling SSH through HTTP proxies

Open up a dynamic socks proxy on local machine that’ll send traffic through the HTTP proxy and on to the SSH server

Ssh -p **22** -o ‘ProxyCommand corkscrew 192.168.1.1 8118 %h %p ‘ -D 8080 [root@demo.stationx.net](mailto:root@demo.stationx.net)

* Creates an SSH on port 22
  + Port 22 needs to be changed to whatever port the proxy/firewall allows
  + Ssh on port 80 or 443
* ProxyCommand adds additional commands
* Corkscrew is to run the program
* IP and port of proxy to be known
* -D 8080 will then open up a dynamic SOCKS proxy on local port 8080 that connects to the StationX server

After, you can put in 127.0.0.1:8080 (local ip) into the browser and the browser will tunnel through local port 8080 (HTTP proxy) and then SSH onto the server

**ProxyTunnel**

ssh -p 22 -o ‘ProxyCommand proxytunnel -p 192.168.1.1:8118 -d %h:%p’ -D 8080 [root@demo.stationx.net](mailto:root@demo.stationx.net)

When entering all this information for a command, it can get a bit much just for a command

So, you can edit the .ssh/config file to have all the parameters in it already so you can just run the file

* Host demo
* User root
* HostName demo.stationx.net (url or ip)
* Port 22 (that you are connecting to)
* DynamicForward 8080 (local dynamic port)
* ProxyCommand proxytunnel -p 192.168.1.1:8118 -d %h:%p -H “ Mozilla/5.0 $ etc.

‘ssh demo’, demo is the host so using this command will ssh to the demo server but using the parameters in the .ssh/config file

**Other Software:**

HTTP Tunnel (instead of ssh)

BarbaTunnel (Windows)

Cntlm Authentication Proxy (Windows)