ATACURI PRIVIND SECURITATEA REŢELEI - SSL STRIP IN *MAN-IN-THE-MIDDLE* ATTACK

Autor: Eugeniu CUCU, student SI-141

Universitatea Tehnică a Moldovei, catedra Automatică şi Tehnologii Informaţionale

ABSTRACT: *A man-in-the-middle (MITM) attack is a type of cyber attack where a malicious actor inserts him/herself into a conversation between two parties, impersonates both parties and gains access to information that the two parties were trying to send to each other. A man-in-the-middle attack allows a malicious actor to intercept, send and receive data meant for someone else, or not meant to be sent at all, without either outside party knowing until it is too late. A MITM attack exploits the real-time processing of transactions, conversations or transfer of other data. This article presents a case study on interception traffic between client and server.*

CUVINTE CHEIE*: reţea, securitate, atacuri, man-in-the-middle, mitm, sslstrip, ip, gateway.*

INTRODUCERE

Într-o reţea de calculatoare este foarte important ca informaţiile transmise să nu poată fi accesate sau interceptate de către persoane neautorizate. Acest aspect este esenţial în condiţiile în care reţelele de calculatoare au ajuns să fie folosite inclusiv pentru realizarea de operaţiuni bancare.

Unul dintre atacurile prin care se poate intercepta traficul dintre două calculatoare din aceeaşi reţea este MAN-IN-THE-MIDDLE (MITM) ATTACK. Din păcate este greu de detectat şi uşor de folosit în reţelele locale actuale.

1. Ce este SSLStrip?

SSLStrip este un instrument care deturnează transparent traficul HTTP într-o rețea, urmărește link-urile HTTPS şi redirecționările, iar apoi redirecționează aceste link-uri în link-uri HTTP.

În SSLStrip, tot traficul de la aparatul victimei este direcționat printr-un proxy creat de hacker şi poate fi gândit ca MITM atac.

Se presupune că sunteți un atacator şi sunteți capabil să stabiliți o legătură între victimă şi server. Acest lucru înseamnă că tot traficul de la device-ul victimei va curge prin intermediul computerului dvs. care servește ca un server proxy şi va avea ca rezultat, fie o eroare de certificat sau traficul criptat va fi capturat, dar care nu este de nici un folos.

2. O scurtă descriere a atacului

Luăm un scenariu în care există o victimă (A), un atacator (B) şi un server (C) (figura nr.1). SSLStrip rulează pe mașina atacator, care este un server proxy; prin urmare, nu există nici o legătură directă între victimă şi server.

Avantajul lui SSLStrip este că browser-ul dvs. nu va afișa erori de certificate SSL, iar victimele nu au nici un indiciu că un astfel de atac are loc. Acest atac este, de asemenea, cunoscut sub numele de atacuri HTTP-redirecționare, în cazul în care conexiunea stabilită prin browser-ul victimei este redirecționată de la HTTPS la HTTP.

Victima A dorește să transfere bani din contul său folosind un serviciu bancar online şi introduce următoarea adresă URL în bara de adrese a browser-ul: *www.example-bank.com/online_banking*.

Browser-ul victimei conectat la device-ul atacatorului așteaptă un răspuns de la server. Atacatorul B transmite cererea victimei A şi așteaptă răspunsul de la serverul băncii. Conexiunea dintre B şi C este securizată, ceea ce înseamnă că tot traficul care este transferat între ei (B & C), trece prin tunelul SSL.

Ulterior, serverul băncii răspunde cu pagina de autentificare care are următoarea adresă URL: *https://www.examplebank.com/online_banking*. In acest stadiu, atacatorul are acces la pagina de conectare şi poate modifica răspunsul serverului de la HTPPS la HTTP. Odată ce acest lucru se face, atacatorul trimite adresa HTTP către victimă (A), astfel în browser va apărea adresa *www.examplebank.com/online_banking*.

La acest moment, victima are acces la pagina de conectare Internet banking, cu o conexiune nesecurizată. Din acest moment, toate cererile victimei circulă în format simplu, iar atacatorul poate avea acces la datele personale şi poate să colecteze acreditările. Astfel, serverul crede că a stabilit cu succes conexiunea, care, în acest scenariu este între atacator şi server (adică între B & C), iar victima (A) consideră că acesta este un server legitim (C).

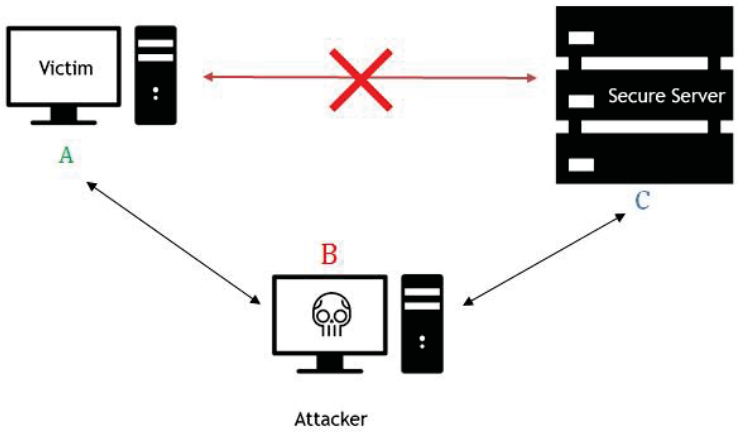

Figura nr.1 Man-in-the-middle attack

3. SSLSTRIP ÎN PRACTICĂ

Vom folosi SSLStrip pentru sniffing sau pentru sustragerea parolelor de la o victimă prin WLAN. Pentru acest lucru avem nevoie de careva instrumente, şi anume, Kali OS şi codul sintaxă SSLStrip. SSLStrip este deja instalat în sistemul de operare Kali. Se vor parcurge următorii paşi:

Pasul 1: Deschideţi terminalul;

Pasul 2: Pentru a rula SSLStrip în MITM, trebuie să cunoaştem IP-ul victimei şi IP-ul Gateway-ului routerului. Pentru a găsi IP Gateway scriem următorul cod:

route –n or ***netstat –nr***

Pasul 3: Schimbăm acceptarea IP-ului - dezactivat = 0; activat = 1.

echo "1" > /proc/sys/net/ipv4/ip_forward **(figura nr.2).**

Vedeţi imaginea mai jos:

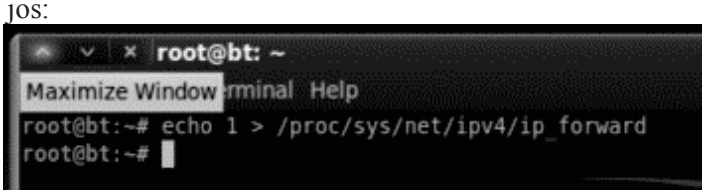

Figura nr.2

Pasul 4: Vom folosi ARPSPOOF. De la pasul 2 ştim IP-ul gateway-ul 192.168.1.1. Pentru a afla IP-ul victimei vom folosi *Nmap*. De fapt, vom descoperi toate dispozitivele care sunt în reţeaua scanată.

nmap –sP gatewayIP.1-254

Pentru ARPSPOOF avem:

arpspoof -i eth0 -t victimip routerip (figura nr.3,4)

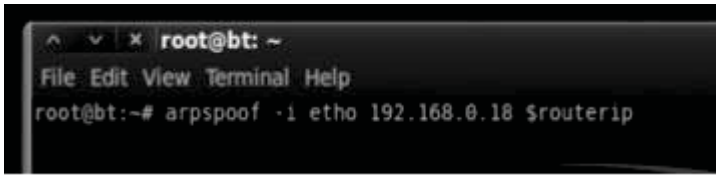

Figura nr.3

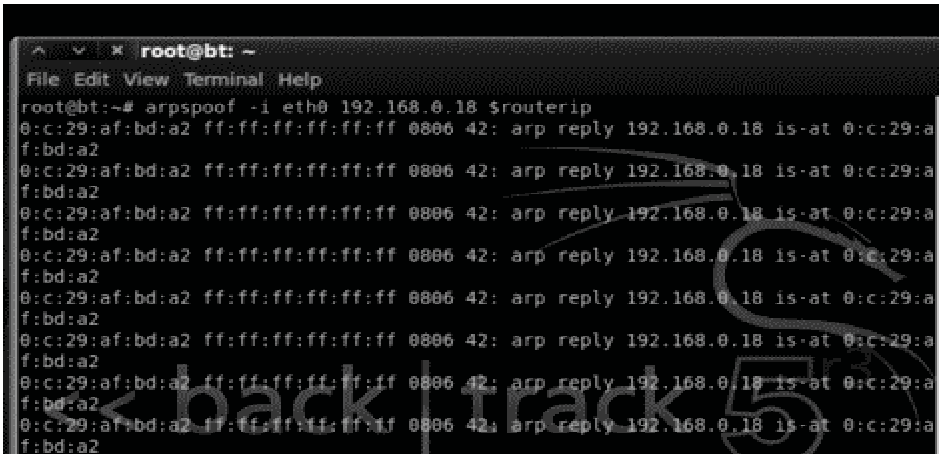

Figura nr.4

Pasul 5: Modificăm tabela IP. Iptables preia traficul de intrare pe mașina noastră Kali Linux, cu destinația portul 80 și redirecționează traficul catre portul 1000, care va fi interceptat de SSLStrip.

iptables -t nat -A PREROUTING -p tcp –destination-port 80 -j REDIRECT –to-port 10000 **(Figura nr.5).**

Figura nr.5

Pasul 6: Utilizăm SSLStrip pe portul 1000.

sslstrip -l 100

Pasul 7: Se interceptează momentul când victima se loghează pe hotmail, un serviciu securizat de protocolul HTTPS (figura nr.6).

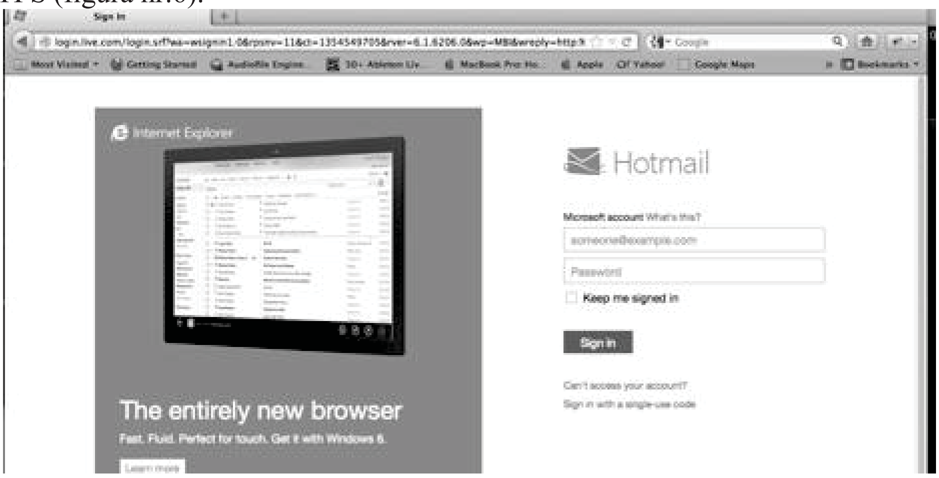

Figura nr.6

Pasul 8: Deschidem sslstrip.log

cat sslstrip.log (**Figura nr.7**)

Figura nr.7

4. Protecție

SSLStrip este un atac greu de prevenit într-o aplicație web, de aceea, recomandăm mai multe etape de care trebuie de ținut cont pentru a diminua acest risc.

Cum pot utilizatorii să se protejeze?

1. Instalați fie HTTPS sau ForceTLS. Acest lucru indică browser-ului dvs. să utilizeze versiunile SSL a site-urilor web, unde este posibil.
2. De obicei, SSLStrip nu afișează o eroare de certificat, dar dacă totuși a apărut un astfel de mesaj, nu trebuie de ocolit avertizarea și de oprit navigarea pe acel site web.
3. Pentru site-uri critice, cum ar fi servicii bancare on-line, accesați doar de la device-uri conectate la o rețea securizată și doar prin HTTPS (SSL) a site-ului, unde marcați acestă pagină. Întotdeauna accesați site-ul prin marcajul salvat.
4. Verificați întotdeauna adresa URL pentru site-urile critice, să fie cu https în bara de adrese sau în hyperlink-uri.

Cum pot organizațiile să se protejeze?

1. Activați site-ul SSL.
2. Utilizați HSTS.
3. Activați Cert Pinning.
4. Utilizați cookie-urilor sigure, adică, toate cookie-urile să fie cu atributul securizat.
5. Dezactivați accesurile non-SSL, sau redirecționați toți utilizatorii la versiunea SSL a site-ului.

Concluzie

Putem observa cât de uşor se realizează acest tip de atac, doar cu câteva utilitare gratuite sslstrip, arpspoof, iptables care sunt prezente in sistemul de operare Kali Linux. Unica problemă ar fi accesarea reţelei locale. Într-o rețea Wi-Fi necunoscută, avem nevoie, cel puțin, de parola de acces, pe când într-o rețea deschisa, este foarte simplu de utlizat aceste unelte știind doar gateway-ul serverului.

Avantajul principal al instrumentului SSLStrip este că browser-ul dvs. nu va afișa orice eroare de certificat SSL, iar victimele nu au nici un indiciu că un astfel de atac are loc, dar poate fi prevenit.

SSLStrip nu funcționează doar în cazul în care site-urile folosesc conexiune SSL. Atacatorul, printr-o cerere HTTP poate primi automat o conexiune HTTPS.

Atunci când se dorește să se utilizeze doar o conexiune HTTPS, deținînd un server puteți migra parțial utilizând HTTP Strict Transport Security(HSTS) pentur a atenționa utlizatorii că folosesc doar HTTPS. De asemenea, puteți folosi un firewall.

Bibliografie

1. https://github.com/moxie0/sslstrip
2. http://www.paladion.net/ssl-stripping-revisiting-http-downgrading-attacks/
3. http://www.veracode.com/security/man-middle-attack