Auditarea Securitatii Retelelor

Laborator

- Atacuri la nivel retea

Adrian Furtunã
MSc, CEH
adif2k8@gmail.com

Obiective

- Vom experimenta atacuri de tip MITM (man-in-the-middle) in reteaua locala

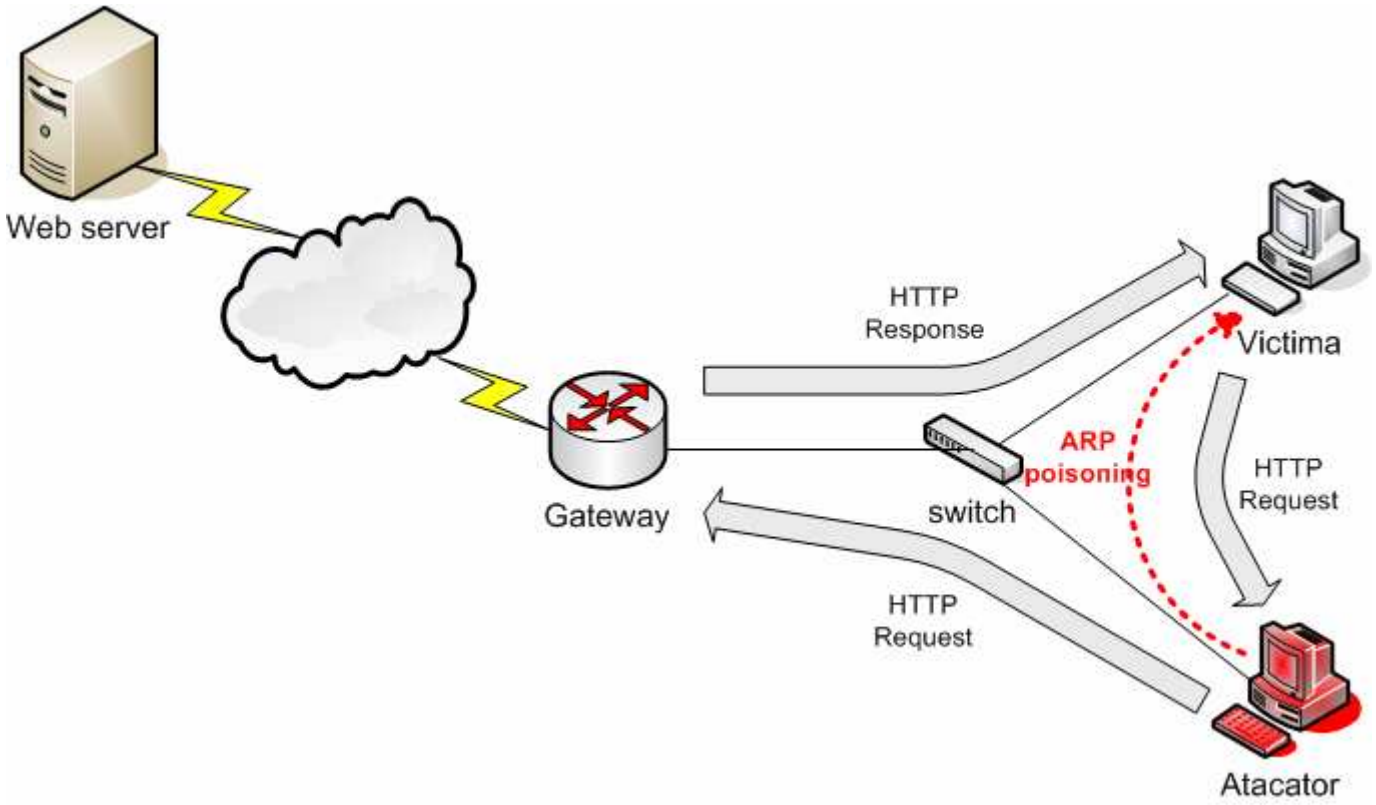
1. Interceptarea traficului facut de o victima ce foloseste un protocol in text clar (HTTP)
   => obtinere session cookies
   => intrarea in sesiunea web a victimei

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:

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. Extrageti informatiile utile din fisierul *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

?