TIW4 : SÉCURITÉ DES SYSTÈMES D'INFORMATION

VULNÉRABILITÉS LOGICIELLES

romuald.thion@univ-lyon1.fr

http://liris.cnrs.fr/~rthion/dokuwiki/enseignement:tiw4

Master « Technologies de l'Information »

Vulnérabilité dans EBIOS

Source de menace *(threat source)* Chose ou personne à l'origine de menaces.

Menace *(threat)* Moyen type utilisé par une source de menace.

Vulnérabilité *(vulnerability)* Caractéristique d'un bien support qui peut constituer une faiblesse ou une faille au regard de la sécurité des systèmes d'information.

Scenario de menace *(vector)* Scénario, avec un niveau donné, décrivant des modes opératoires.

Conduite d'attaque

Principales étapes

Reconnaissance en connaître le plus possible sur la cible

Exploitation cibler une vulnérabilité d'un support

Escalation de privilèges devenir `root`.

Couverture des traces logs, patches

Conduire les objectifs voir événements redoutés

Scenario de menace

Mode opératoire : plusieurs vulnérabilités

Reconnaissance

Sun Tzu, “The Art Of War”, ch. XIII, “The Use Of Spies”

. . . what enables the wise sovereign and the good general to strike and conquer, and achieve things beyond the reach of ordinary men, is foreknowledge. Now this foreknowledge cannot be elicited from spirits ; it cannot be obtained inductively from experience, nor by any deductive calculation. Knowledge of the enemy’s dispositions can only be obtained from other men.

L’Art de la Guerre

Informations précises, fiables pour une attaque réussie. . .

. . . hypothèse sous-jacente : être en train de faire la (cyber)guerre

Reconnaissance

Sun Tzu, “The Art Of War”, ch. XIII, “The Use Of Spies”

. . . what enables the wise sovereign and the good general to strike and conquer, and achieve things beyond the reach of ordinary men, is foreknowledge. Now this foreknowledge cannot be elicited from spirits ; it cannot be obtained inductively from experience, nor by any deductive calculation. Knowledge of the enemy’s dispositions can only be obtained from other men.

L’Art de la Guerre

Informations précises, fiables pour une attaque réussie. . .

. . . hypothèse sous-jacente : être en train de faire la (cyber)guerre

Reconnaissance

Information sur l'organisation

- localisation géographique
- identité & fonctions d'employés, de clients
- boîte aux lettre, téléphones
- processus d'entreprise

Information sur le système informatique

- matériel utilisés
- systèmes d'exploitation (version)
- services utilisés (version)
- topologie du réseau

Collecte semi-passive

Sources publiques

- Registrar (`whois`)
- DNS (liste des hôtes)
- En-tête (HTML, mail)
- Pages web (commentaires)
- Google (`http://www.hackersforcharity.org/ghdb/`)

Collecte de l'information publique

Passer pour un utilisateur *légitime*

Collecte active

Pros

- informations précises & détaillées
- outils puissants
- adaptable sur-mesure

Cons

- génération de traffic
- peut générer des alertes
- laisse des traces

Exemple : scanning de ports (1/3)

L'outil

http://nmap.org/

Un outil versatile

- options de découverte
- types de scans
- timing
- détection de service et de version
- option de furtivité

Exemple : scanning (2/3)

Le scan TCP/IP : comportement (limite)

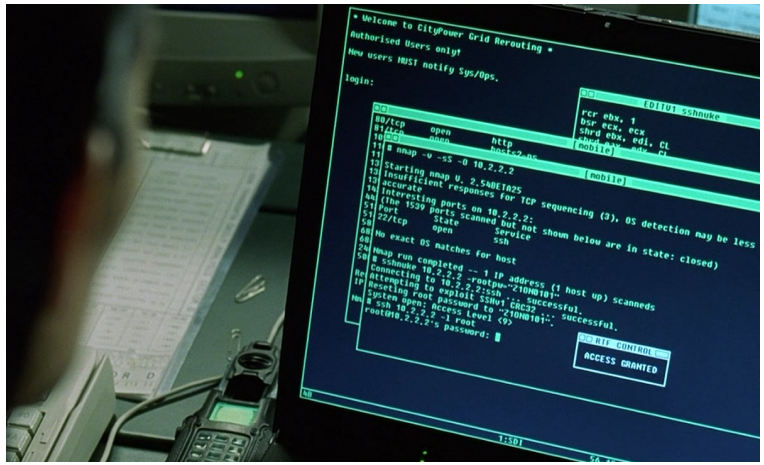
- RFC 791 : IP
- RFC 792 : ICMP
- RFC 793 : TCP
- RFC 768 : UDP
- RFC 826 : ARP

La détection d'OS

- variation dans les implémentations
- RFC non-respectées
- base d'empreintes `/usr/share/nmap/nmap-os-db`

Exemple : scanning (3/3)

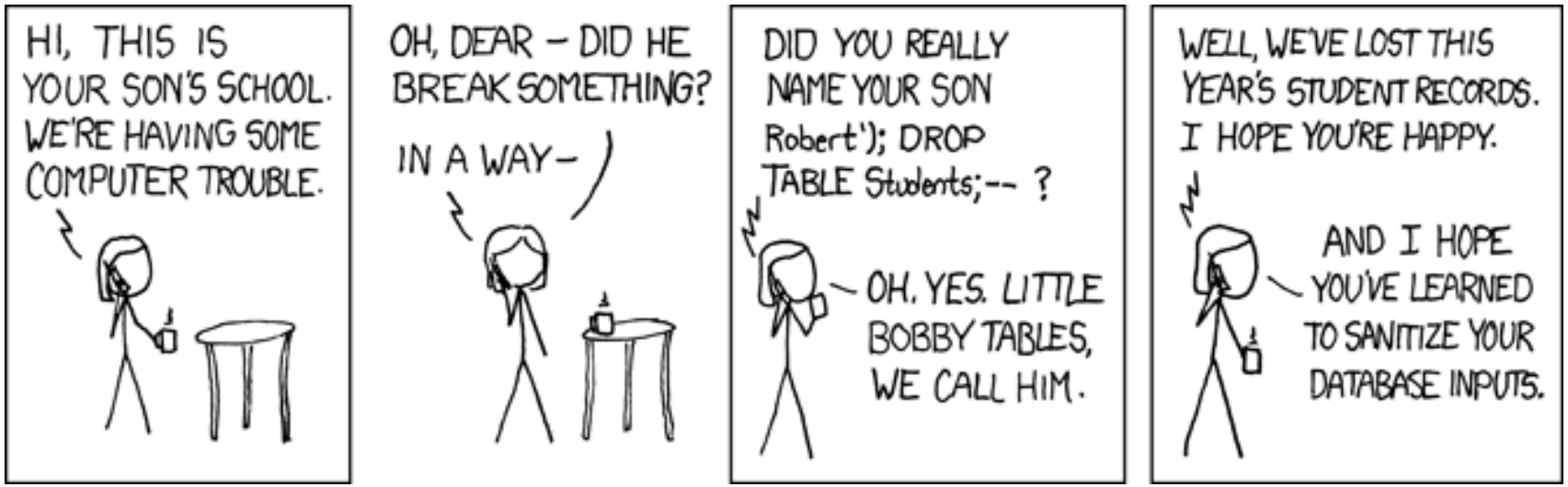
- Outil standard d'administration
- Illégal sans consentement
- Incontournable
- Permet de comprendre le réseau !



Outils complémentaires

- `netcat` (ou `ncat`)
- `hping3` (ou `nping`)
- `tcpdump`, `wireshark` (GUI)
- `zenmap`

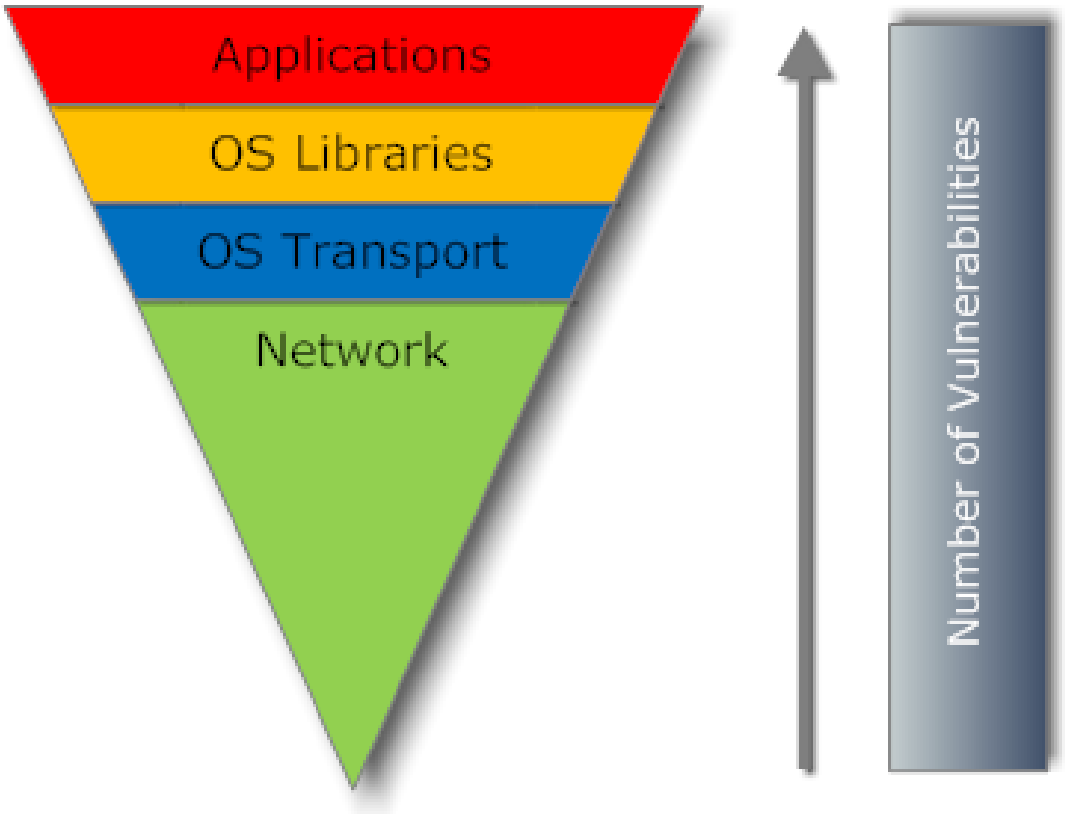
SQLi



https://xkcd.com/327/

Exploiter

Concrétiser une menace à l'aide d'une (ou plusieurs) vulnérabilités



Exploiter

Canal de communication : « Master SRIV »

- protocoles
- médium de communication
- interconnexions

Logiciels : « Master TIW »

- systèmes d'exploitation
- applications
- composants

Aucun bien support n'est exempt de vulnérabilités

CWE TOP 25 Most Dangerous Software Errors

Une référence !

http://cwe.mitre.org/top25/archive/2019/2019_cwe_top25.html

https://www.sans.org/top25-software-errors/
(comparaison 2009/2010)

CWE TOP 25 Most Dangerous Software Errors

Remarques

- mise-à-jour régulièrement : évolution des menaces ;
- prédominance des vulnérabilités web ;
- beaucoup d'erreurs de conception et de configuration ;
- mauvaise pratiques de programmation ;

Fiche MITRE CWE (Common Weakness Enumeration)

- Exemple pour Cross-site Scripting (CWE#79)
- `http://cwe.mitre.org/data/definitions/79.html`
- voir OWASP

Comparaisons OWASP versus CWE/SANS

OWASP Top Ten Most Critical Web Application Security Risks (2017)

OWASP Top 10 compared to SANS CWE 25

Sur les failles logicielles

Il y en aura toujours

- indénombrables, nouvelles (0-days)
- potentiellement très dangereuses
  e.g. exécution de code arbitraire à distance
- vecteurs d'attaques à tous les niveaux de la pile logicielle

S'en prémunir

- bonnes pratiques de code et vérification formelle (e.g., code critique)
- gestion du logiciel (e.g., patchs de sécurité, mise-à-jour)
- mesures de sécurité redondantes (*defense in depth*)
- langages avec propriétés de sécurité (e.g., vérif statique)
- . . . *liste à compléter !*

Best practices

https://cheatsheetseries.owasp.org/

Plateforme de TP

Audit et exploitation des applications Web

- VM (même IP que TP précédent)
- mardi 14/01 PM : 1reséance TP (biref annulé)
- mercredi 15/01 PM 2 : ^{e}séance TP et débrief avec intervenant pen-tester pro

TODO : préparation du TP

Lire/parcourir les CWE Web du TOP 25 et les cheatsheet OWASP

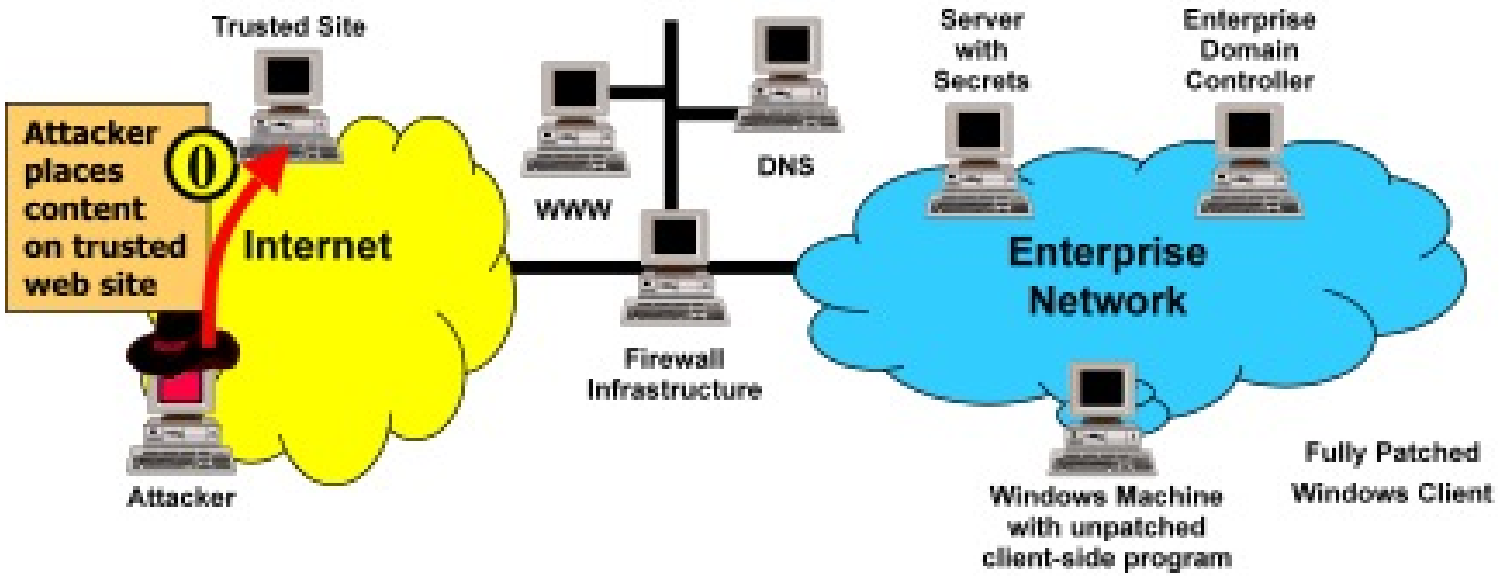
Rappel

Articles 323-1 et suivants du code pénal

5 Scenario HTTP Client-Side Exploit

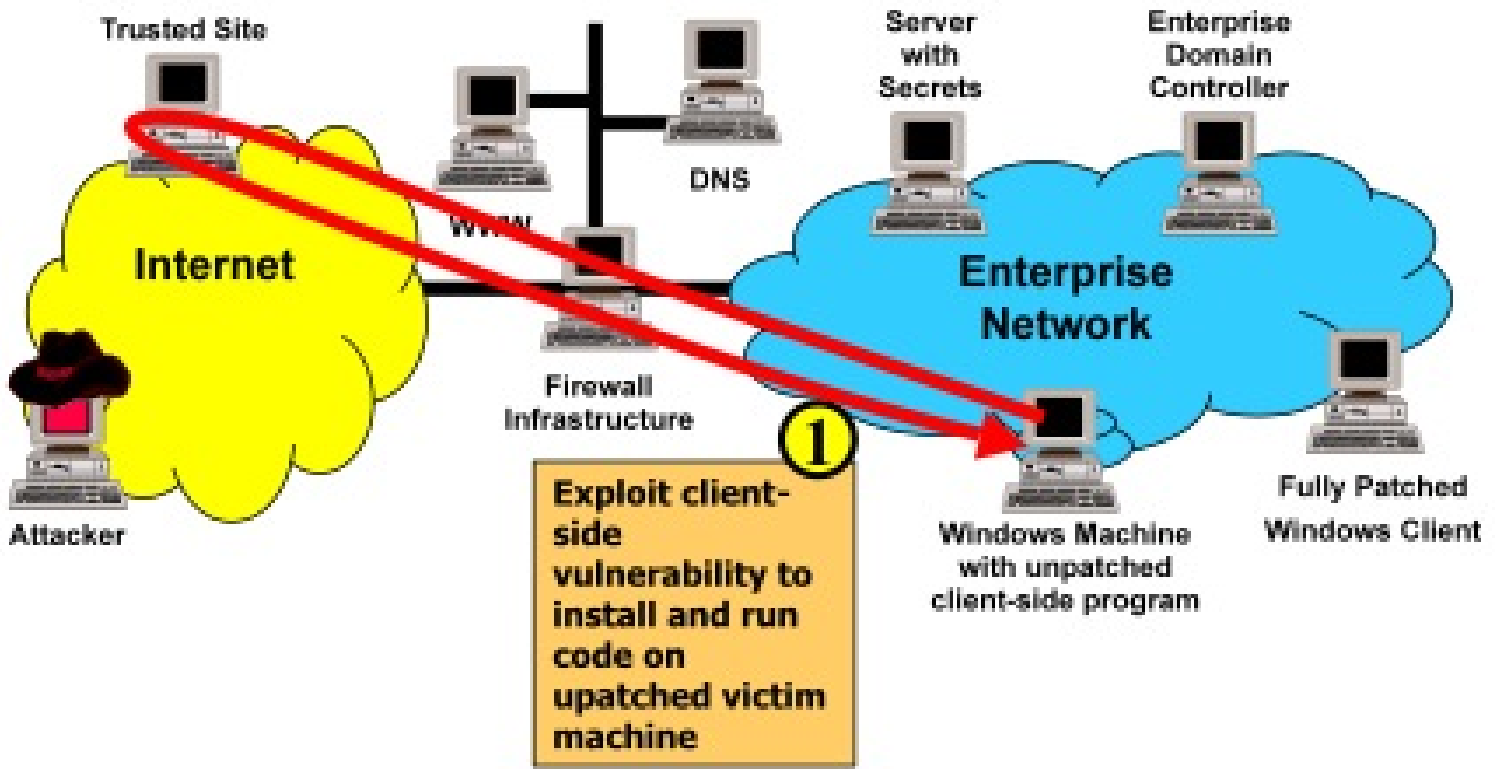
(1/5)

http://www.sans.org/top-cyber-security-risks/tutorial.php



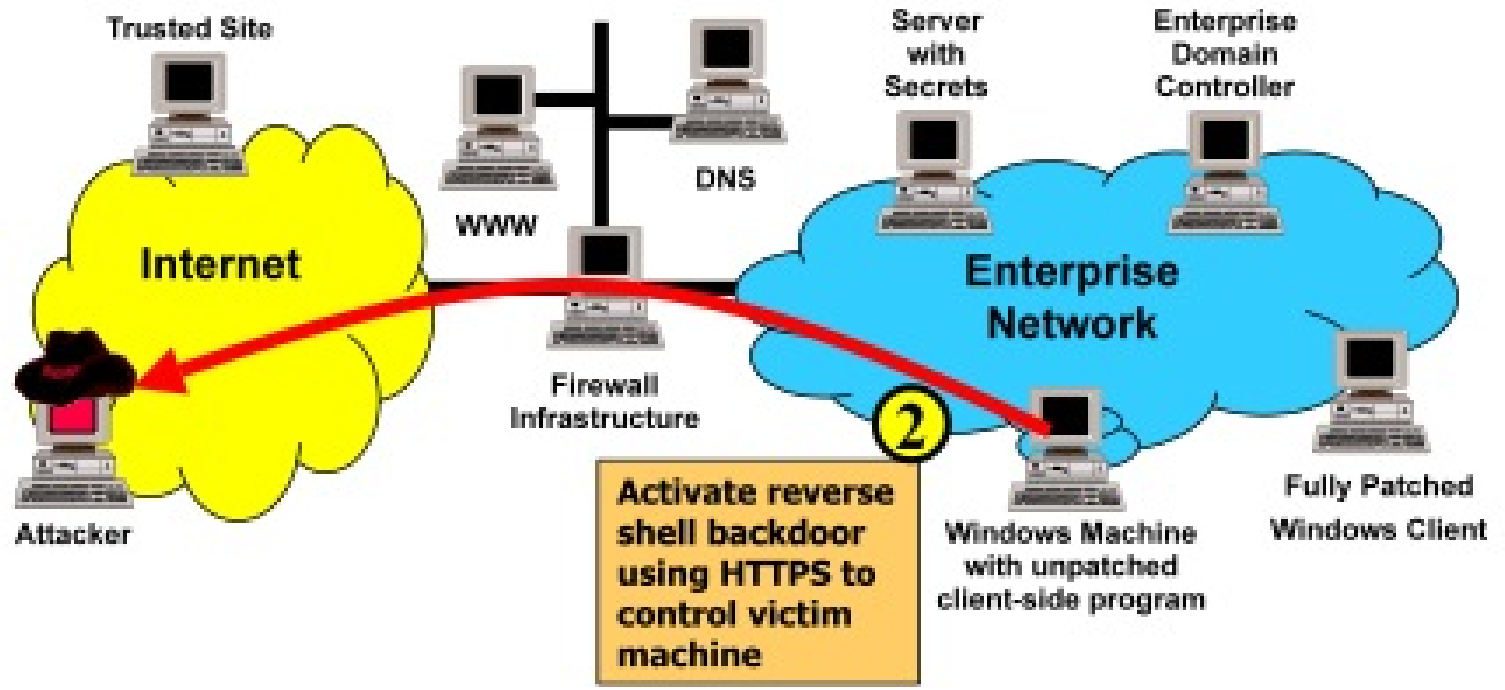
Step 0 : Attacker Places Content on Trusted Site

(2/5)



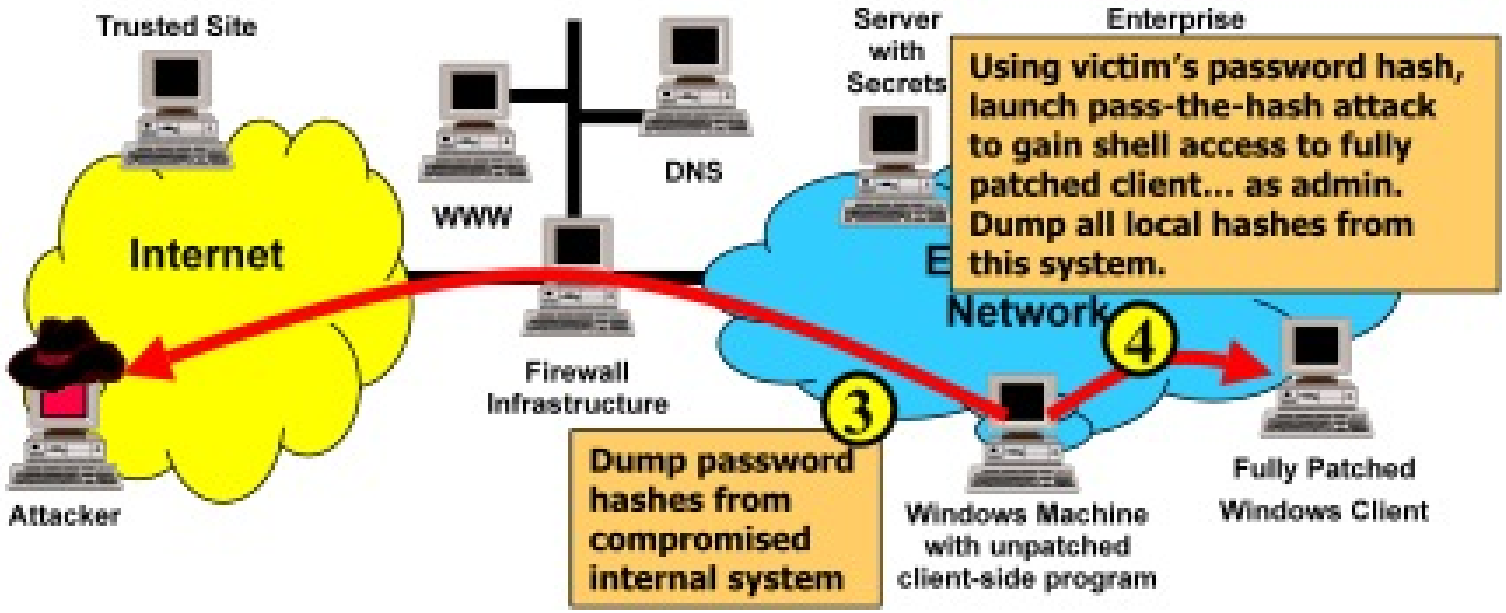
Step 1 : Client-Side Exploitation

(3/5)



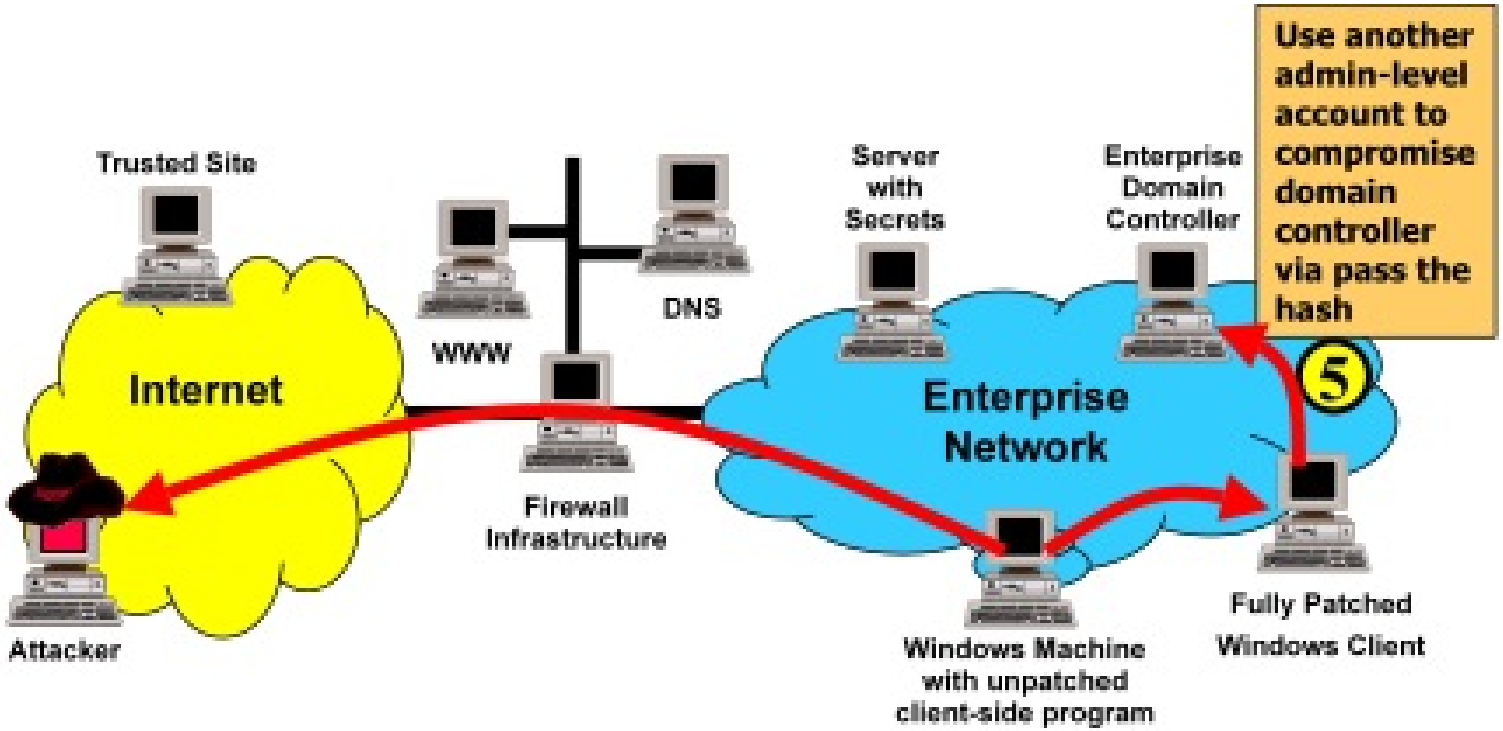
Step 2 : Establish Reverse Shell Backdoor Using HTTPS

(4/5)



Steps 3 & 4 : Escalation, Dump Hashes and Use Pass-the-Hash Attack to Pivot

(5/5)



Step 5 : Pass the Hash to Compromise Domain Controller