Demo: Why NTLM sucks

2013-01-24

by Mart & vn

Déroulement

- NTLMv1 en théorie
- Fonctionnement
- Faiblesse
- Scénario
- Stratégie d'attaque
- Schéma de l'infrastructure
- Démo

NTLMv1 en théorie

- Acronyme de: NT Lan Manager
- Successeur du protocole LM
- Prédécesseur du protocole NTLMv2
- Utilisation déconseillé par Microsoft depuis juillet 2010 [1]
- Encore beaucoup trop utilisé sur le marché...

[1] http://msdn.microsoft.com/en-us/library/cc236715.aspx

NTLMv1 en théorie

- NTLM et les réseaux Microsoft
  - Windows Integrated Authentication
    - Kerberos est d'abord utilisé
    - Si Kerberos échoue, NTLM est utilisé
  - Arrivé avec Windows 2000 SP4
  - Supporté jusqu'à Windows XP et Windows 2003

http://blogs.iss.net/archive/NTLMReflection.html

http://social.technet.microsoft.com/Forums/en/winservergen/thread/0a9d7c97-987e-4305-b95b-189c8c90837b

Fonctionnement

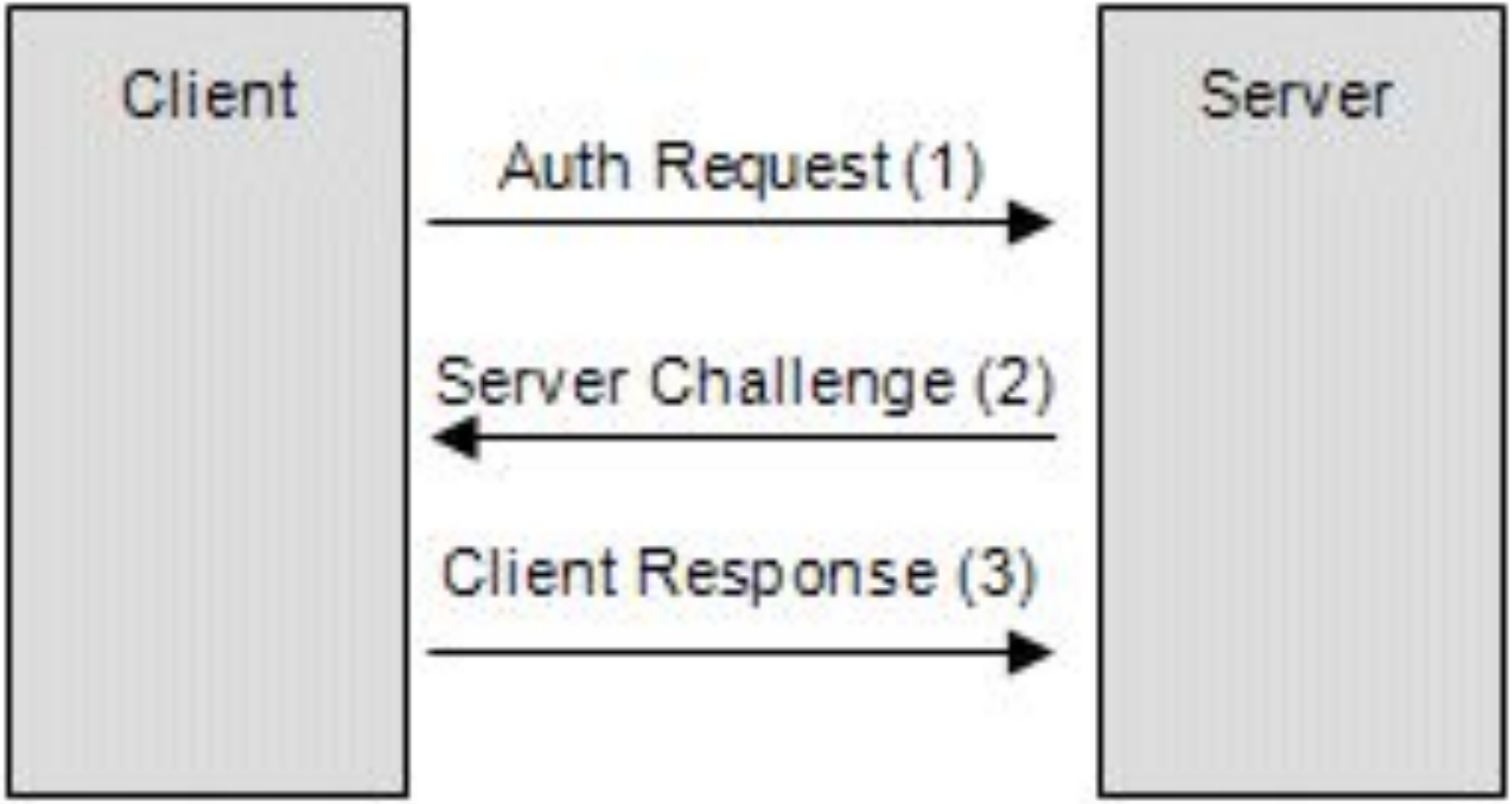
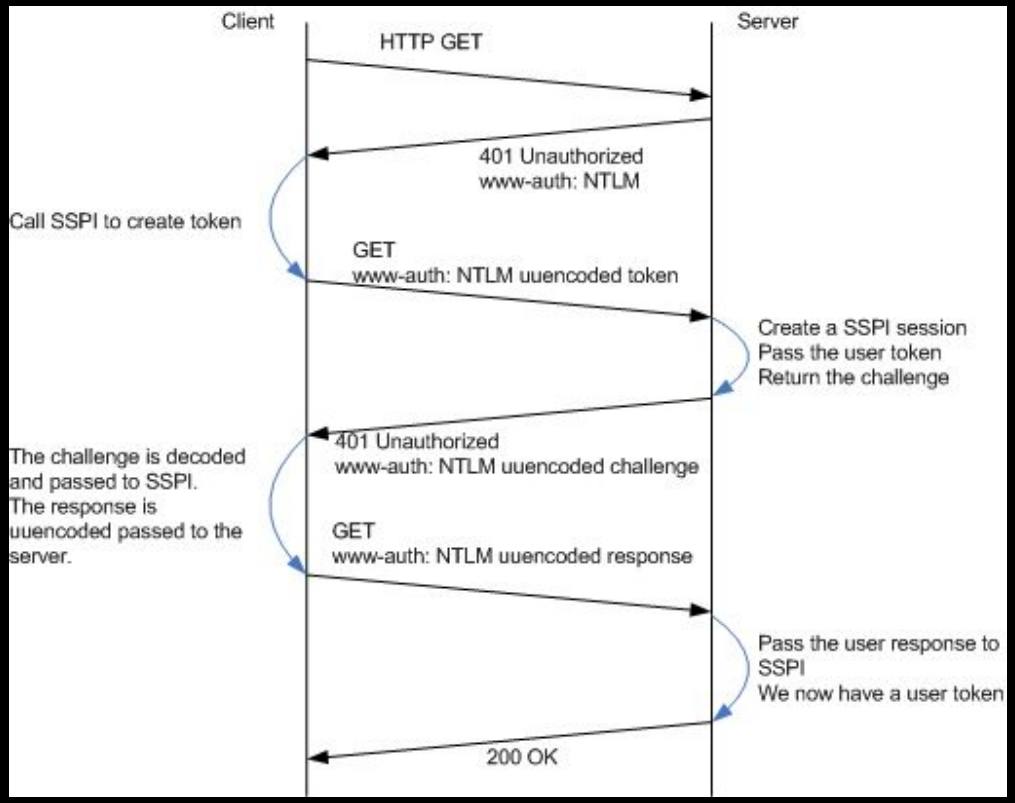


Figure 1. NTLM authentication.

Faiblesse

- **Un seul challenge**
  - Celui du serveur
  - Vulnérable aux "Reflection attacks"



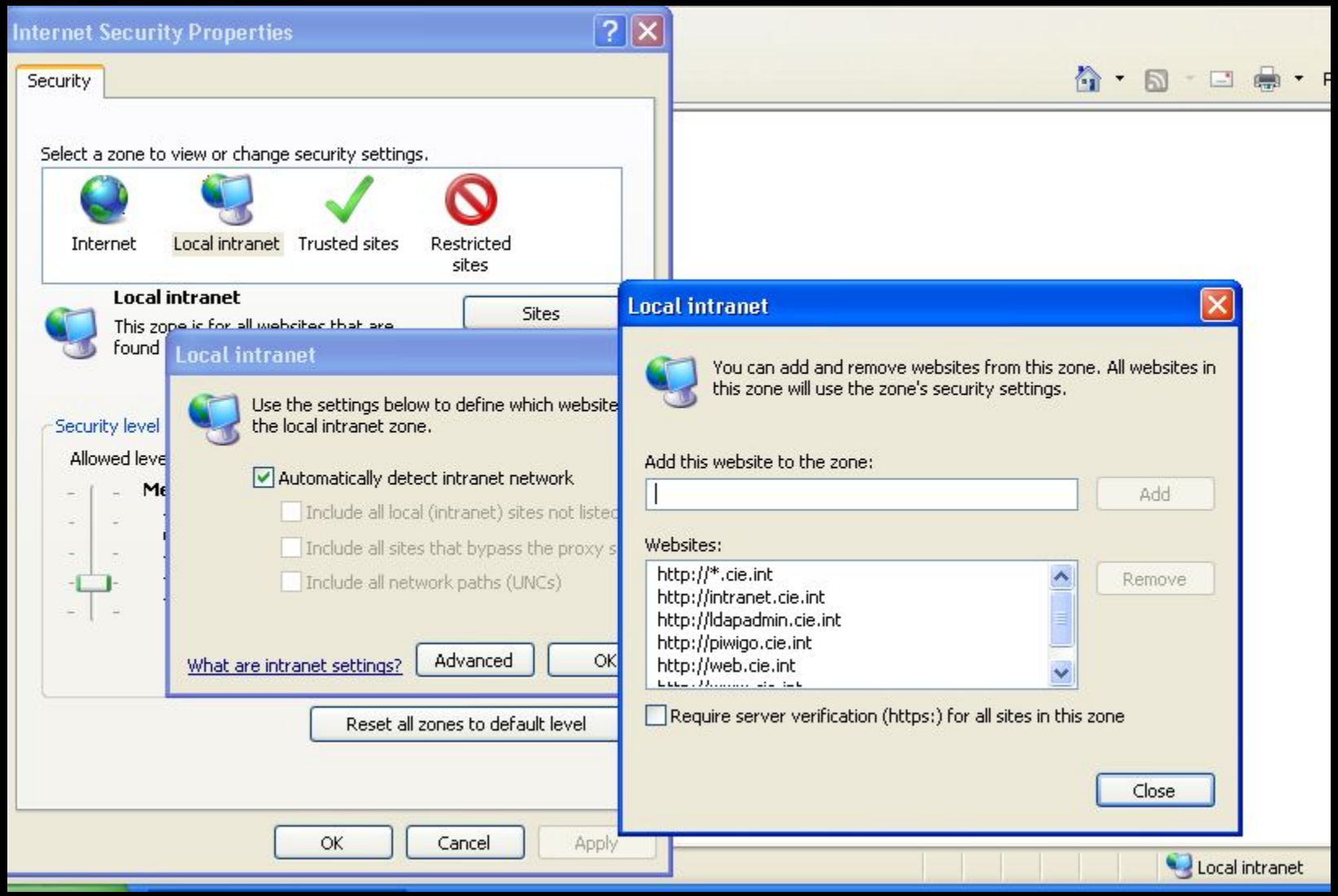
Scénario

- Nous sommes un développeur mal intentionné avec peu de privilèges (dev only).
  - Évaluation difficile avec le boss? Manque d'écoute? Manque d'accès? Frustré de quoi que ce soit?
- Nous avons un accès réseau
- Victime: Nicolas Duchesneau
  - Architecte ayant accès aux environnements de production et de développement
- Les environnements de dev et de prod partagent le même réseau et domaine

Stratégie

- Grandes étapes
  - Récupérer un hash NTLM ainsi que le challenge (nonce) associé de Nicolas Duchesneau
  - Cracker le hash
- Contraintes
  - Trouver un moyen qu'un individu s'authentifie sur une ressource contrôlé par nous.
  - IE s'authentifie en NTLM seulement sur des sites de catégorie "Local Intranet"
    - Le nom d'hôte de l'attaquant devra donc faire parti de la "white list" du navigateur

Stratégie


Internet Security Properties
Security
Select a zone to view or change security settings.
Internet
Local intranet
Trusted sites
Restricted sites
Local intranet
Sites
Security level
Reset all zones to default level
OK
Cancel
Apply
Local intranet
Use the settings below to define which website
the local intranet zone.
Automatically detect intranet network
Include all local (intranet) sites not listed
Include all sites that bypass the proxy s
Include all network paths (UNCs)
What are intranet settings?
Advanced
OK
Local intranet
You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.
Add this website to the zone:
Add
Websites:
http://*.cie.int
http://intranet.cie.int
http://ldapadmin.cie.int
http://piwigo.cie.int
http://web.cie.int
Remove
Require server verification (https:) for all sites in this zone
Close
Local intranet

Stratégie

1. MITM
   - Victime <-> DC + Victime <-> WEB
   - Script Scapy
2. DNS Spoofing
   - Il faut spoofer un nom valide afin que NTLM soit utilisé par le navigateur
3. WebScarab
   - Configuré en proxy transparent
   - Règle iptables qui forward le traffic HTTP
4. PokeHashBall
   - Outil qui simulera un échange NTLM avec la victime
   - nonce prédéfinit

Stratégie

5. Attendre que la victime accède la page
   - Ou l'inviter subtilement via un courriel...
6. Lors de l'appel, intercepter une requête http
   - Inclure une image afin que la victime effectue une requête vers le poste de l'attaquant
   - Pourrait être automatisé dans WebScarab (java)
7. Récupérer le hash
8. Effectuer des recherches sur l'individu
9. Monter un dictionnaire sur mesure
10. Cracker le mot de passe
11. W00t :-)

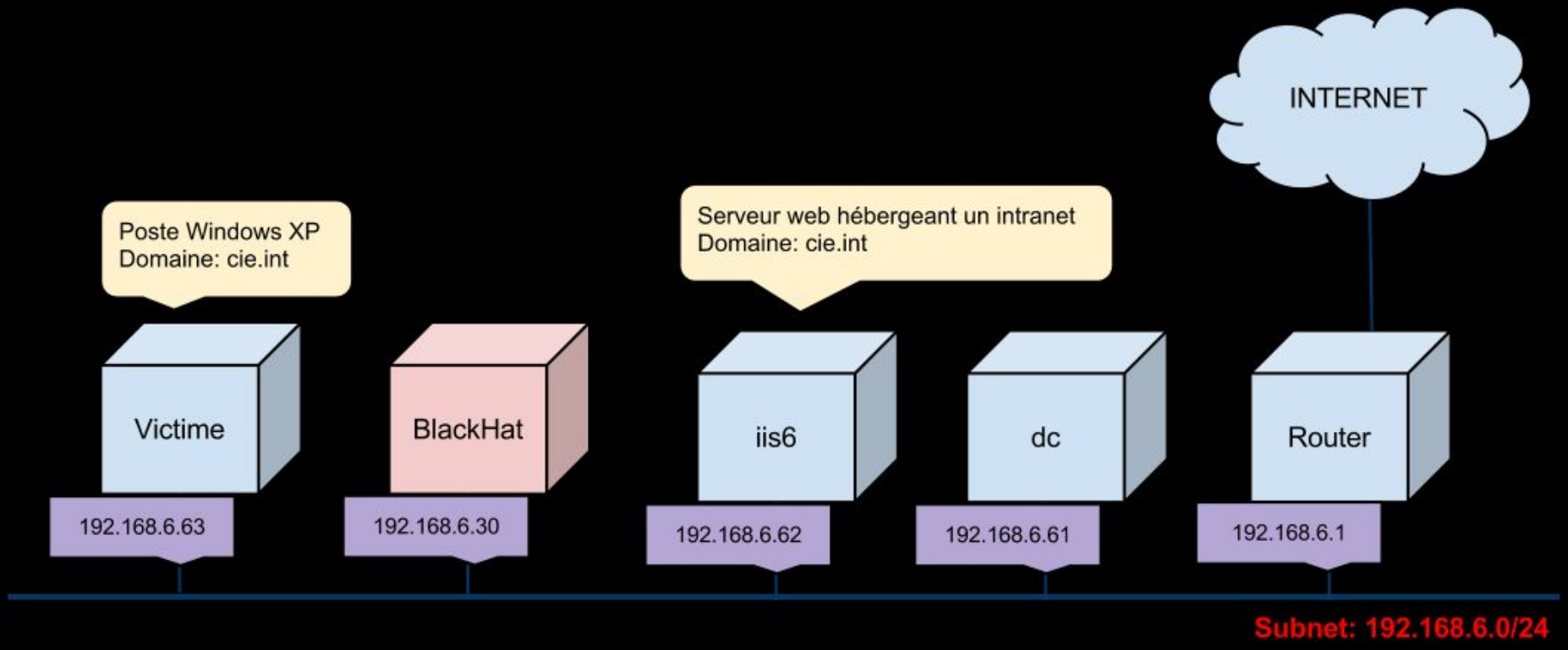
Stratégie

- Alternative
  - Pour être plus furtif au niveau du réseau et éviter le ARP Poisoning, les accès suivants sont suffisants:
    - créer une entrée dans les DNS
    - modifier la page web

Stratégie

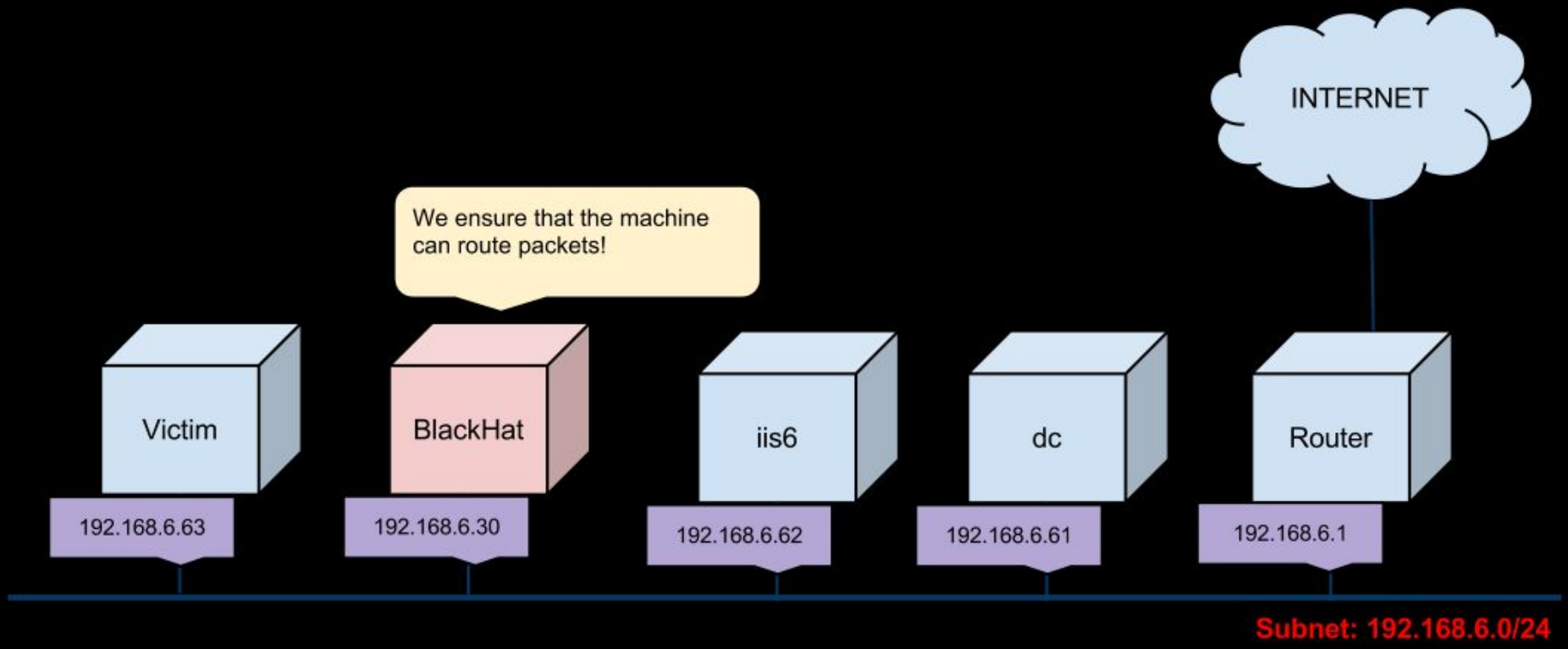
- L'imagination est votre limite...
  - Via un lien et un partage réseau
    - http://blog.spiderlabs.com/2012/12/you-down-with-lnk.html
  - Via un .doc
    - http://jedicorp.com/security/exploit-dev/stealing-netntlm-credentials-by-injecting-unc-path-into-docx
  - Via MSSQL
    - http://www.netspi.com/blog/2012/12/26/executing-smb-relay-attacks-via-sql-server-using-metasploit/

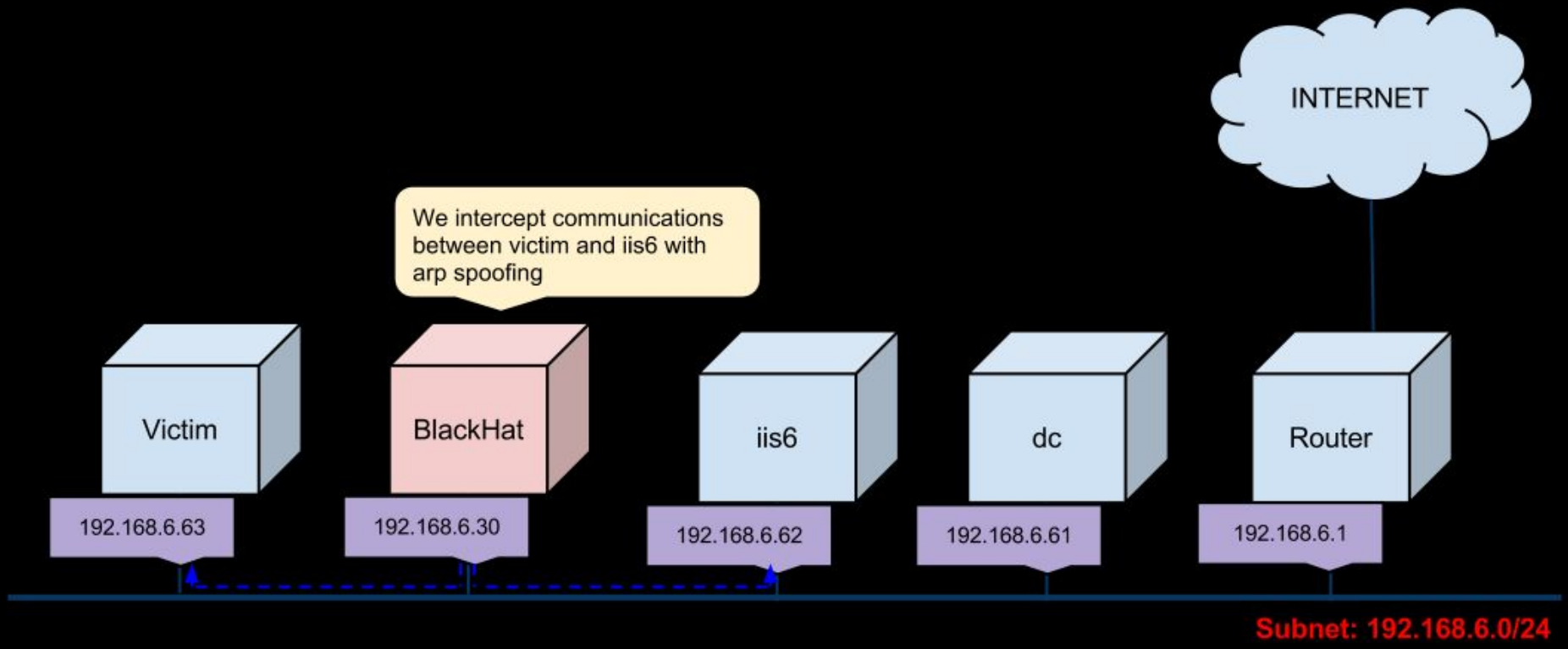
Schéma de l'infrastructure

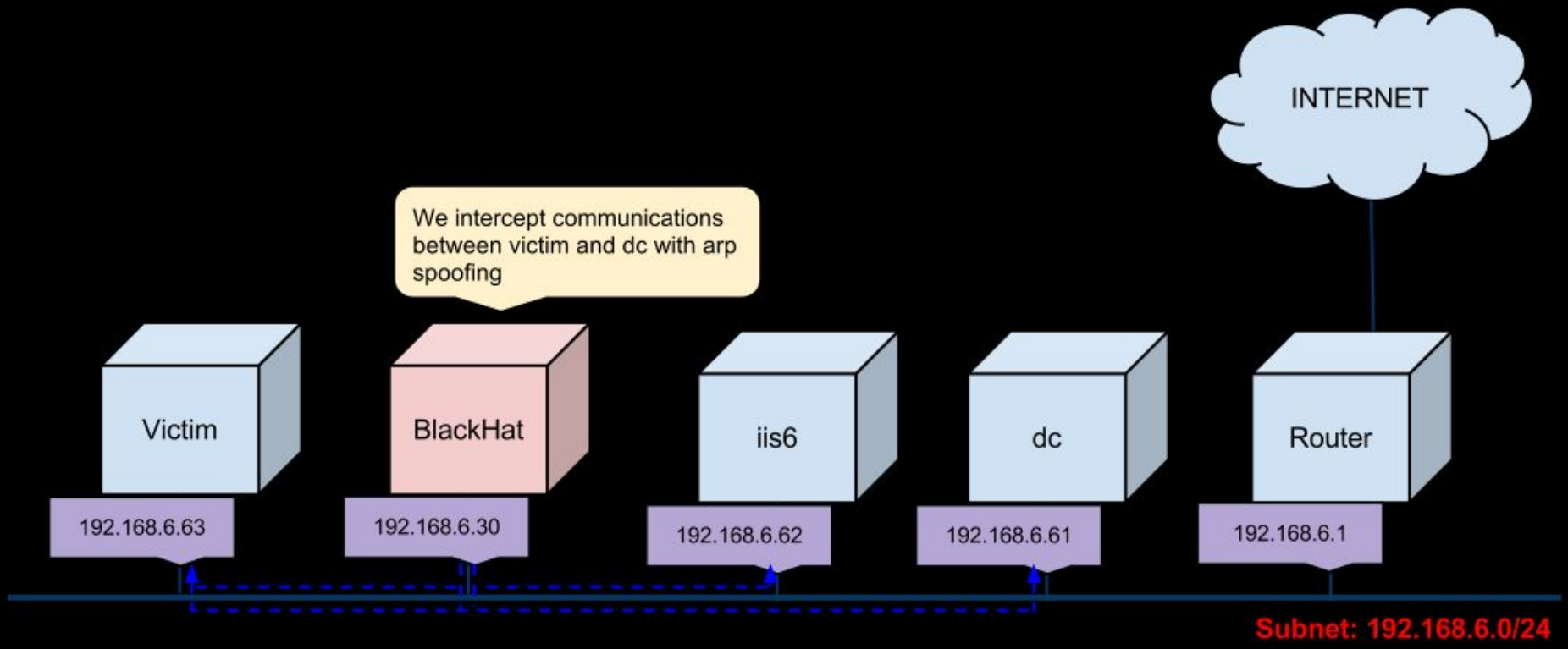


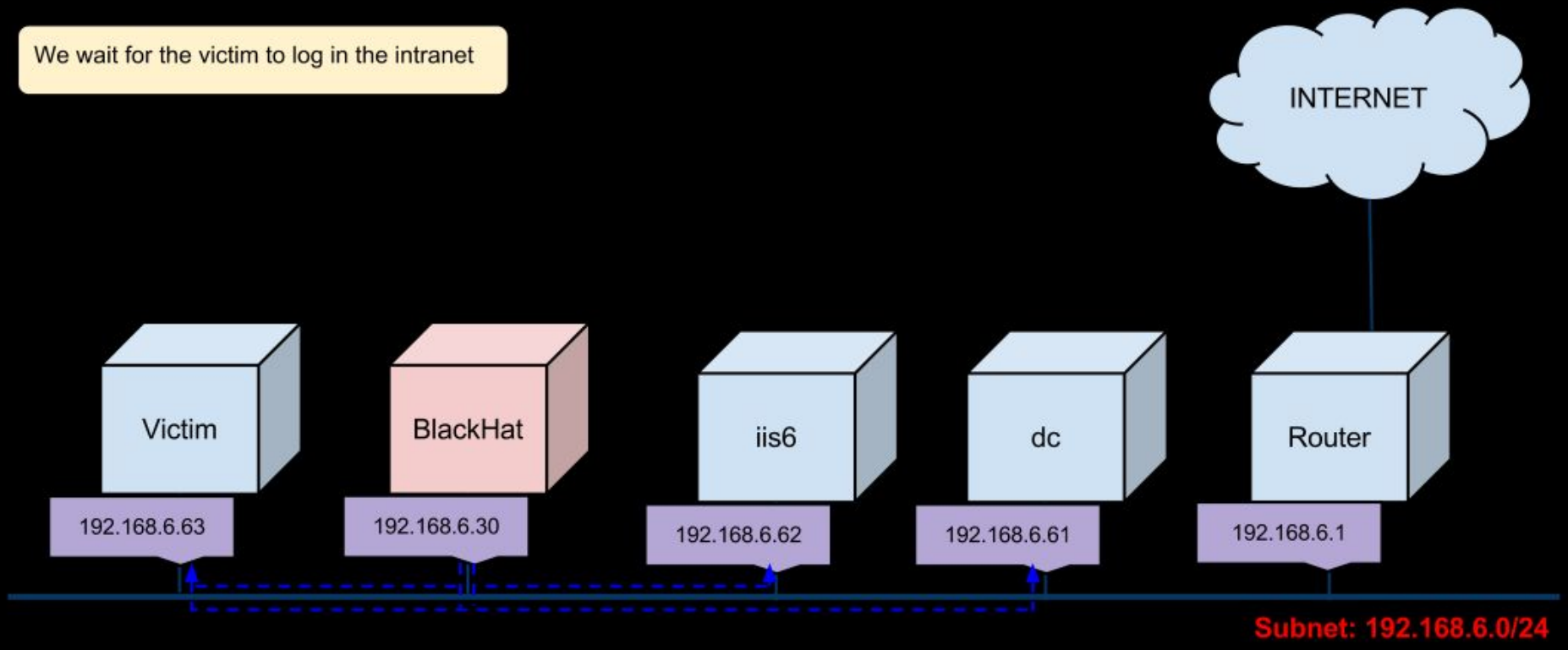
Demo

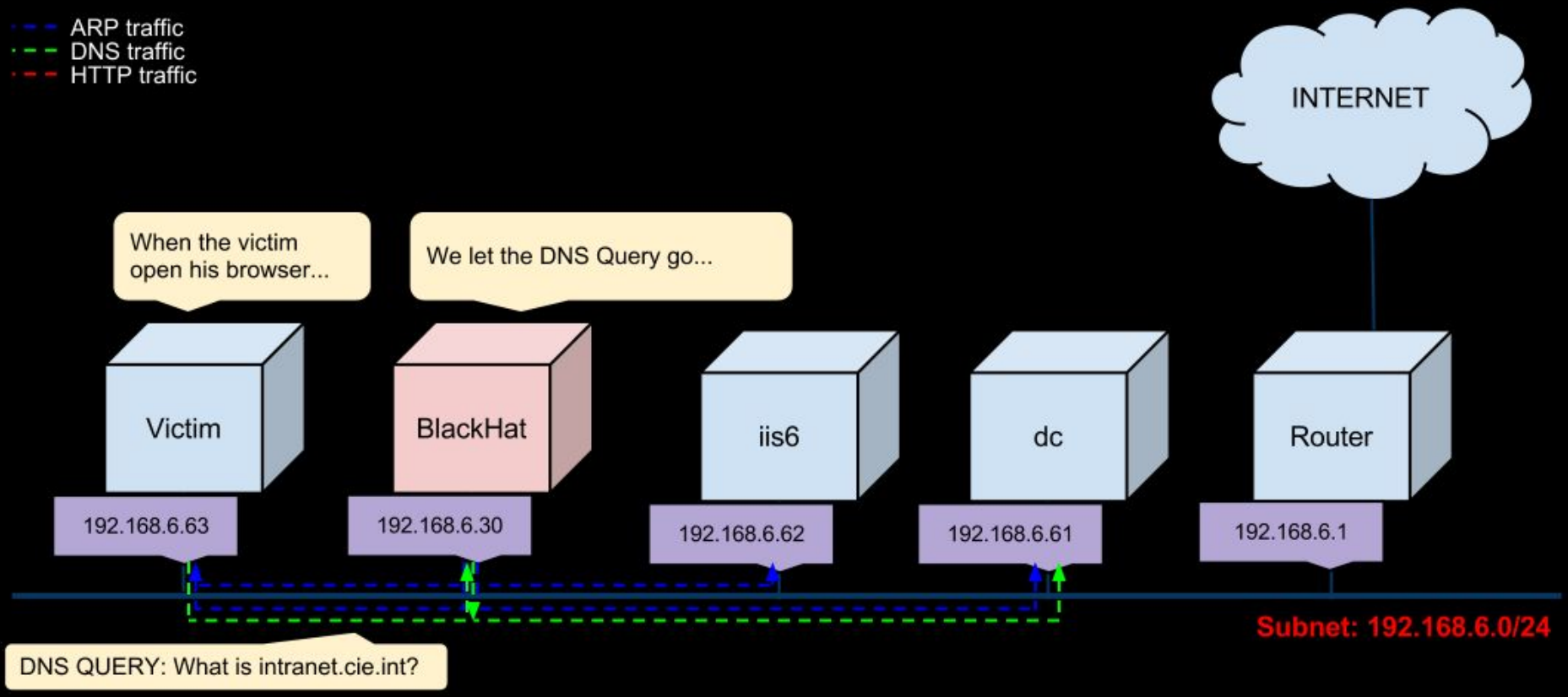
AIright, gimme my precious!

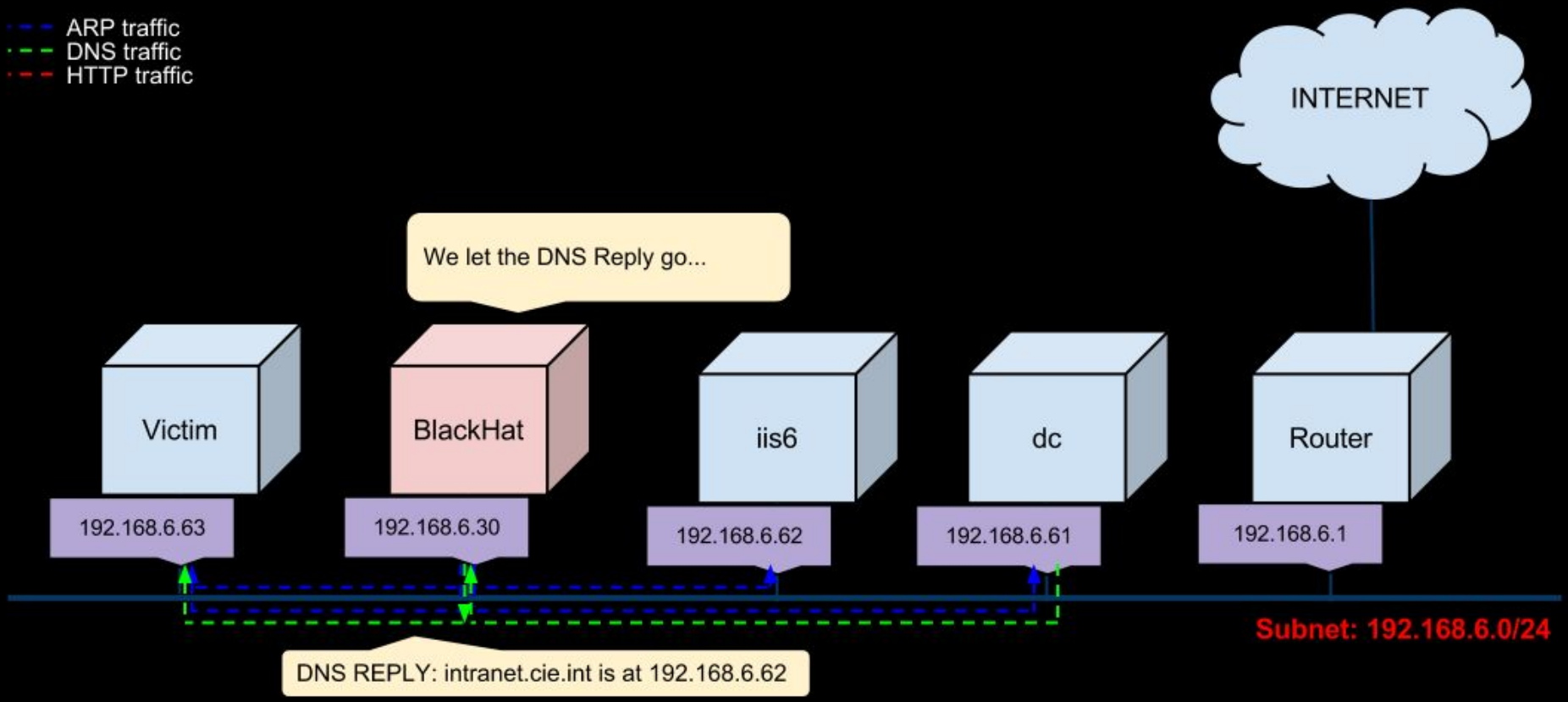

INTERNET
We ensure that the machine can route packets!
Victim
BlackHat
iis6
dc
Router
192.168.6.63
192.168.6.30
192.168.6.62
192.168.6.61
192.168.6.1
Subnet: 192.168.6.0/24

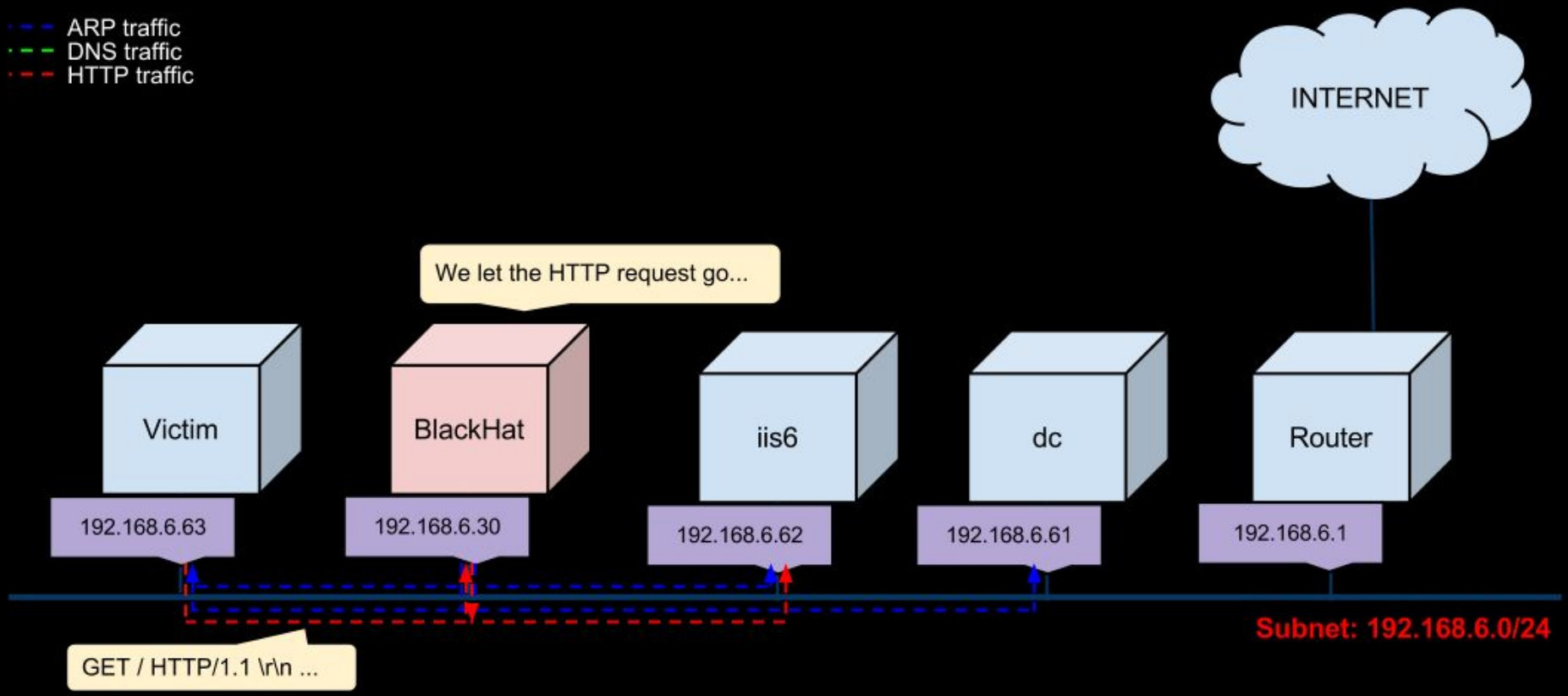

INTERNET
We intercept communications between victim and iis6 with arp spoofing
Victim
BlackHat
iis6
dc
Router
192.168.6.63
192.168.6.30
192.168.6.62
192.168.6.61
192.168.6.1
Subnet: 192.168.6.0/24

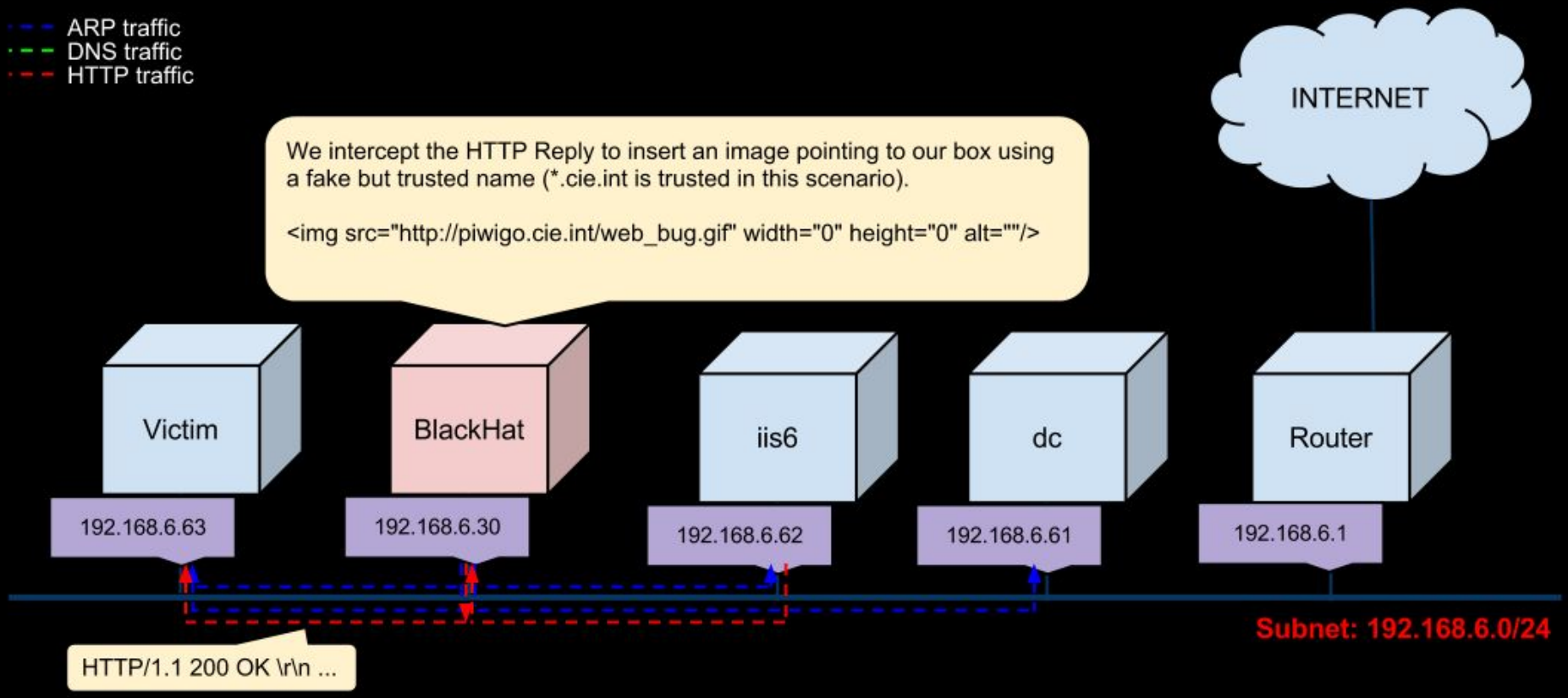

INTERNET
We intercept communications between victim and dc with arp spoofing
Victim
BlackHat
iis6
dc
Router
192.168.6.63
192.168.6.30
192.168.6.62
192.168.6.61
192.168.6.1
Subnet: 192.168.6.0/24


We wait for the victim to log in the intranet
INTERNET
Victim
BlackHat
iis6
dc
Router
192.168.6.63
192.168.6.30
192.168.6.62
192.168.6.61
192.168.6.1
Subnet: 192.168.6.0/24

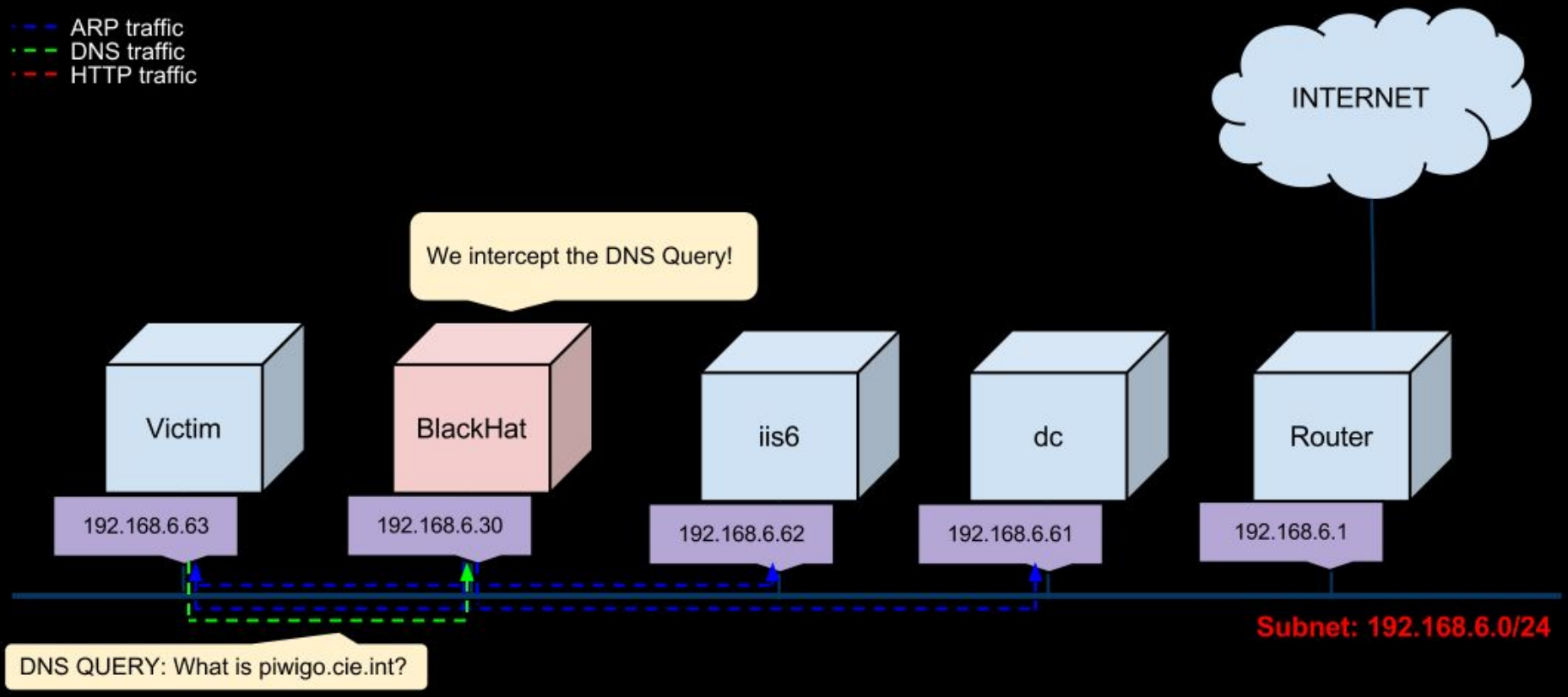

ARP traffic
DNS traffic
HTTP traffic
INTERNET
When the victim open his browser...
We let the DNS Query go...
Victim
BlackHat
iis6
dc
Router
192.168.6.63
192.168.6.30
192.168.6.62
192.168.6.61
192.168.6.1
Subnet: 192.168.6.0/24
DNS QUERY: What is intranet.cie.int?

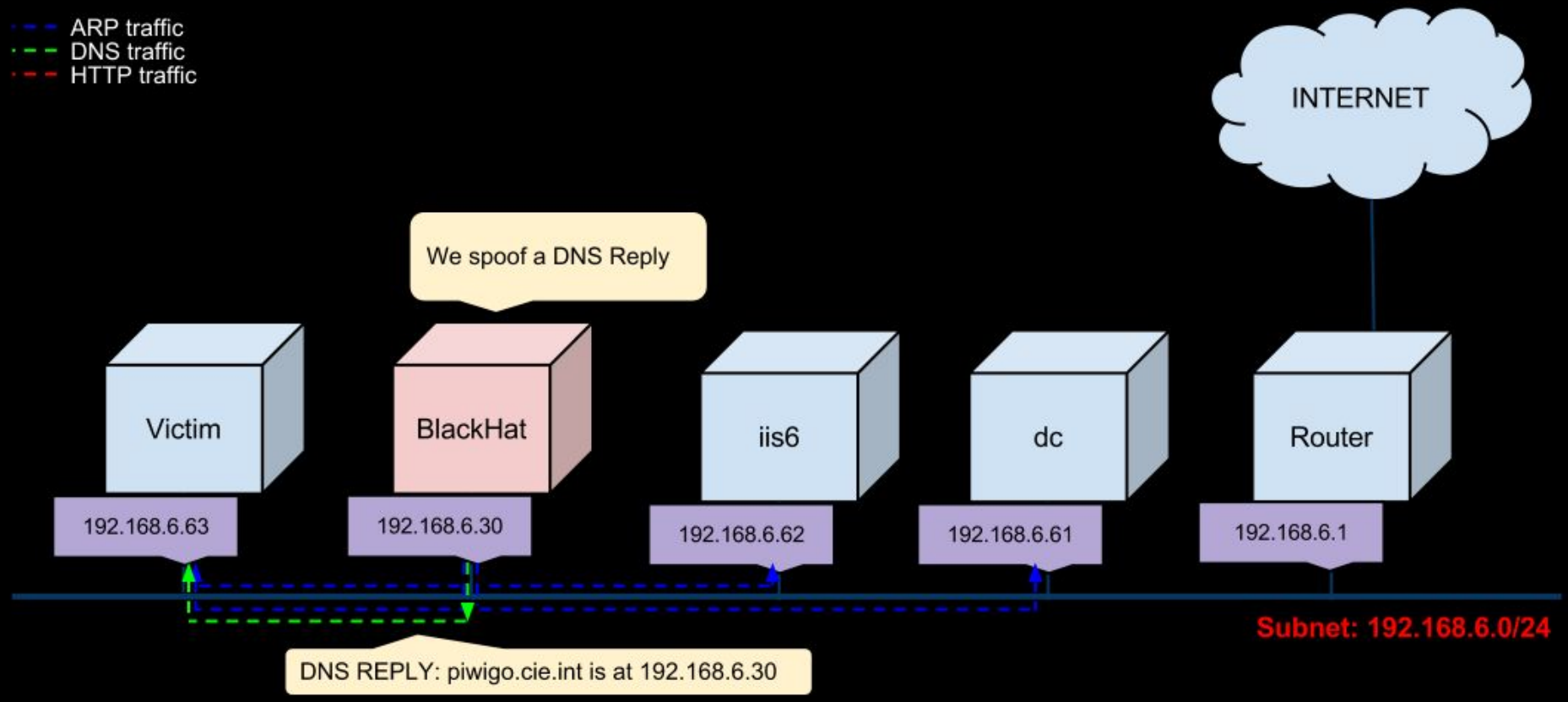

ARP traffic
DNS traffic
HTTP traffic
INTERNET
We let the DNS Reply go...
Victim
BlackHat
iis6
dc
Router
192.168.6.63
192.168.6.30
192.168.6.62
192.168.6.61
192.168.6.1
Subnet: 192.168.6.0/24
DNS REPLY: intranet.cie.int is at 192.168.6.62

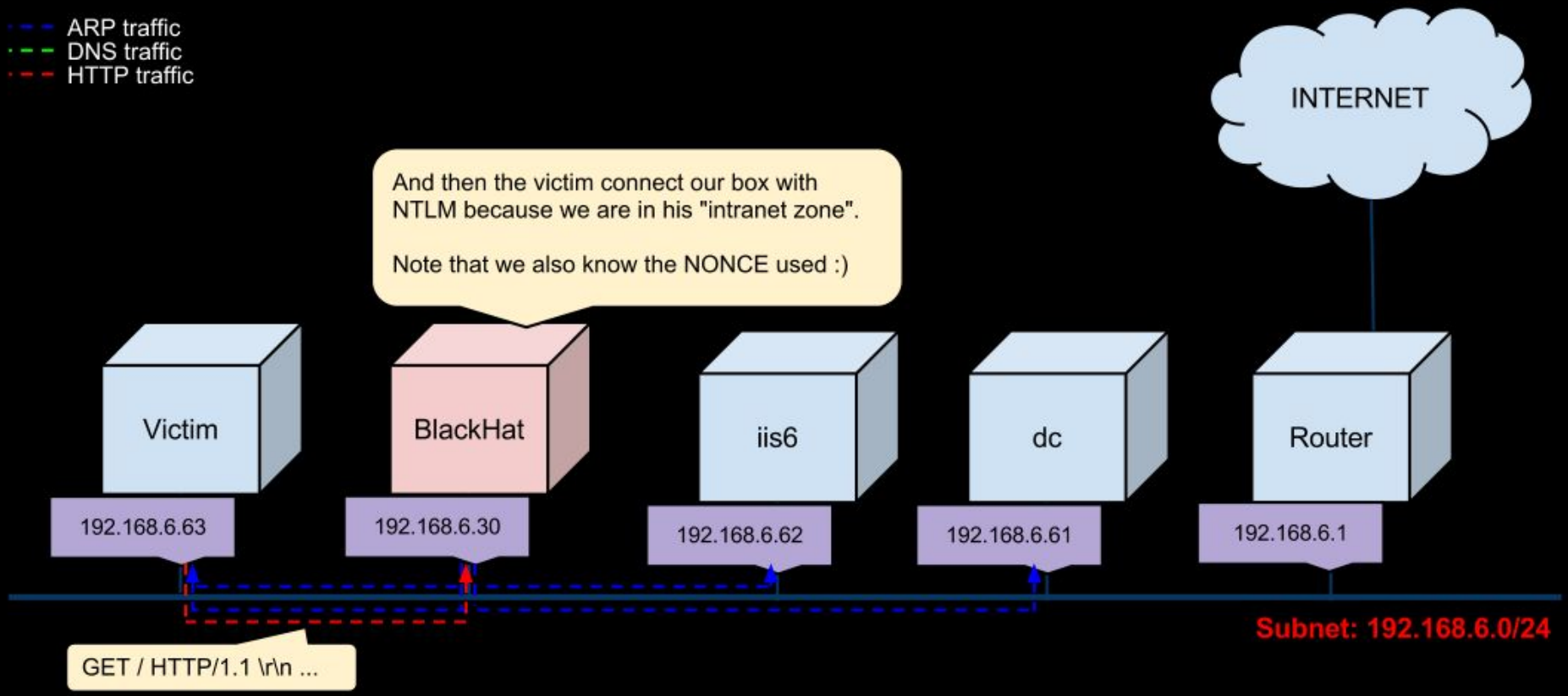

ARP traffic
DNS traffic
HTTP traffic
INTERNET
We let the HTTP request go...
Victim
BlackHat
iis6
dc
Router
192.168.6.63
192.168.6.30
192.168.6.62
192.168.6.61
192.168.6.1
Subnet: 192.168.6.0/24
GET / HTTP/1.1 \r\n ...


ARP traffic
DNS traffic
HTTP traffic
INTERNET
We intercept the HTTP Reply to insert an image pointing to our box using a fake but trusted name (*.cie.int is trusted in this scenario).

Victim
BlackHat
iis6
dc
Router
192.168.6.63
192.168.6.30
192.168.6.62
192.168.6.61
192.168.6.1
Subnet: 192.168.6.0/24
HTTP/1.1 200 OK \r\n ...


ARP traffic
DNS traffic
HTTP traffic
INTERNET
We intercept the DNS Query!
Victim
BlackHat
iis6
dc
Router
192.168.6.63
192.168.6.30
192.168.6.62
192.168.6.61
192.168.6.1
Subnet: 192.168.6.0/24
DNS QUERY: What is piwigo.cie.int?


ARP traffic
DNS traffic
HTTP traffic
INTERNET
We spoof a DNS Reply
Victim
BlackHat
iis6
dc
Router
192.168.6.63
192.168.6.30
192.168.6.62
192.168.6.61
192.168.6.1
Subnet: 192.168.6.0/24
DNS REPLY: piwigo.cie.int is at 192.168.6.30


ARP traffic
DNS traffic
HTTP traffic
INTERNET
And then the victim connect our box with NTLM because we are in his "intranet zone".
Note that we also know the NONCE used :)
Victim
BlackHat
iis6
dc
Router
192.168.6.63
192.168.6.30
192.168.6.62
192.168.6.61
192.168.6.1
GET / HTTP/1.1 \r\n ...
Subnet: 192.168.6.0/24

Profiling

ou coller des morceaux...

Intel

Pour ramasser de l'intelligence, il s'agit surtout d'avoir plusieurs sources, mais avant tout d'obtenir des informations de base :

- Nickname
- Nom
- Ville
- # de téléphone ou adresse
- Nom de l'employeur
- Infos sur la famille
- Infos sur les loisirs
- ...anything related

Sources d'intel

Bien évidemment, la meilleure place pour obtenir l'intel de base...est à la même place qu'on a obtenu cette dernière, sinon...

- Google
- Facebook/Twitter/LinkedIn
- Whois
- NEQ
- *Dumpster Diving*
- Social Engineering
- ...

Ramassage de déchets...euh d'intel

- Objectif : cracker un mot de passe qui n'a pas fonctionné avec des *wordlists* traditionnelles (rockyou, myspace, wikipedia, john.txt ou cain.txt)
- http://360percents.com/posts/wordlist-by-scraping/
- Permet de construire une *wordlist* en se basant sur une page Web
- Nous allons donc bâtir de l'intel à partir de la page Intranet!

Ce que le script fait?

- Extrait les mots/chiffres contenus dans la page Web et les rend uniques
- Les classe en ordre alphabétique
- Le script original ne permet pas de récupérer des chiffres/années...on modifie la regexp
  - sed '/[^a-zA-Z]/d' ===> sed '/[^a-zA-Z0-9]/d'
- Il y a une version plus avancée qui *scrape* récursivement...un peu trop
  - Tout dépendant si vous voulez *scraper* style.css!

Après ./scrape.sh wtf we doin'?

- Étudier la liste résultante et apporter des changements au besoin
  - Casse
  - Abbréviations
  - Accents
  - Attaque table-lookup manuelle
    - Pour chars peu communs
      - ex: hackfest ==> H@¢k£3§t
- Ajouter des résultats d'intel et leurs variantes
  - Apporter les changements susmentionnés

Manual intel avec notre exemple

- On recherche des noms uniques
- avril = avr, apr, 04
- Google
  - duchesneau+nicolas+camaro
  - duchesneau+nicolas+ver-mac
  - duchesneau+nicolas+"carrés rouges"
  - Varknar
    - On voit clairement que ça joue à WoW...on pourrait scraper WoWWiki juste pour ça...SKIP.
  - nicolas+duchesneau+alexis OR maria
  - camaro+rs/ss+1967 (genre pour avoir le model ID du moteur)
  - "acton vale"+"cayo coco"

Amélioration du dictionnaire

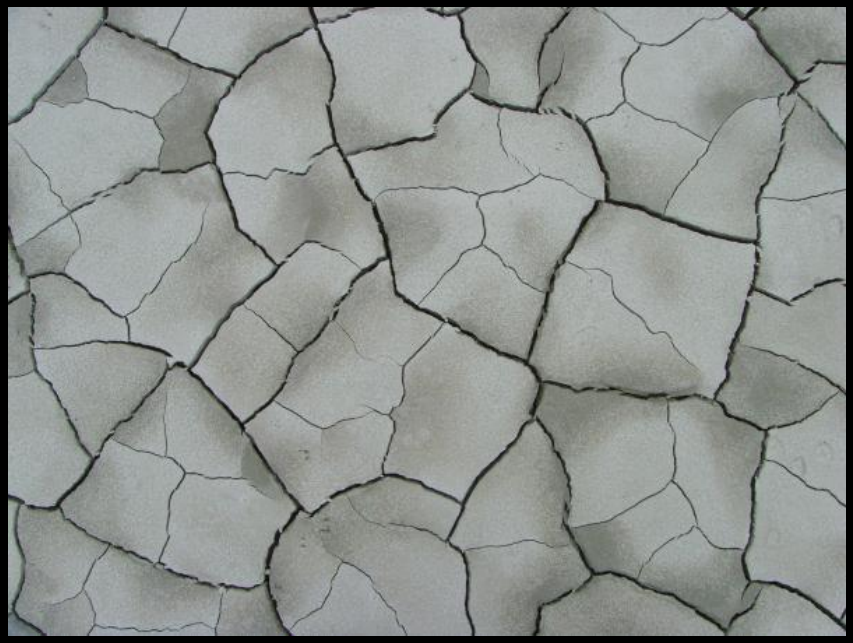
- On a tous tendance à faire des *patterns* de passwords :
  - $word1##$word2#
  - $word1$word2
  - ##$word
  - ...
- On peut créer des *rules* dans notre outil de *cracking* pour automatiser les *combination attacks*
- On peut faire le *table-lookup* manuellement avec un sed -e...ou laisser les rules faire la job ou encore établir manuellement les variantes

Amélioration du dictionnaire

Utilisation de hashcat-utils

- http://hashcat.net/wiki/doku.php?id=hashcat_utils
- Disponible sur BackTrack
- Pour l'exemple, on va se contenter de *combinator*
- ./combinator.bin $wordlist $wordlist > ~/cbwl1
- ./combinator.bin $wordlist ~/cbwl1 > ~/cbwl21
- On peut faire de multiples combinaisons

Cracking time



Choix de l'outil de *cracking*

- Le choix ne manque pas...
  - *hashcat*
  - John the Ripper (JtR)
  - hashkill
  - CloudCracker ($)
  - Logiciels d'ElcomSoft ($)
  - CryptoHaze
  - ...
- Ils ne supportent pas tous les mêmes types de hashes
- Certains ont des clones...

Choix de l'outil de *cracking*

- Au début je regardais les tools qui supportaient NTLM ET LM...
  - JtR
  - hashkill
  - Rainbow Tables @ max 8/9-char length
  - CloudCracker
- Je me suis bien rendu compte que rien marchait et que le hash fittait pas avec le contexte
- En fait le bon *hashtype* c'est netNTLMv1

Choix de l'outil de *cracking*

- Un Google rapide nous indique que la version -jumbo de JtR fait le netntlmv1
- Un exemple avec *password* réussit
- L'étape suivante fut de savoir dans quel format disposer le data.
  - user::WORKGROUP:5237496CFCBD3C0CB0B1D6E0D579FE9977C173BC9AA997EF:A37C5C9316D9175589FDC21F260993DAF3644F1AAE2A3DFE:1122334455667788
  - domain\user:::5237496CFCBD3C0CB0B1D6E0D579FE9977C173BC9AA997EF:A37C5C9316D9175589FDC21F260993DAF3644F1AAE2A3DFE:1122334455667788

Cracking time...

- Pourtant le résultat final...
  - $NETNTLM$1122334455667788$727b4e35f947129ea52b9cdedae86934bb23ef89f50fc595:password
- Donc, le format en entrée :
  - user::WORKGROUP:5237496CFCBD3C0CB0B1D6E0D579FE9977C173BC9AA997EF:A37C5C9316D9175589FDC21F260993DAF3644F1AAE2A3DFE:1122334455667788
  - OU
  - DOMAIN\user:::5237496CFCBD3C0CB0B1D6E0D579FE9977C173BC9AA997EF:A37C5C9316D9175589FDC21F260993DAF3644F1AAE2A3DFE:1122334455667788
  - OU
  - DOMAIN\user:5237496CFCBD3C0CB0B1D6E0D579FE9977C173BC9AA997EF:A37C5C9316D9175589FDC21F260993DAF3644F1AAE2A3DFE:1122334455667788
  - Enfin on avançait avec celui-là...mais le *nonce* semblait me poser problème

L'heure est arrivée...

```
# cat ~/cbwl1 ~/cbwl21 $wordlist > ~/wordlist.txt
# cat john.conf|grep Wordlist
# Wordlist file name, to be used in batch mode
#Wordlist = $JOHN/password.lst
#Wordlist =
/pentest/passwords/wordlists/rockyou.txt
Wordlist = /root/wordlist.txt
```

- root@bt:~/john-copy/run# ./john --wordlist --format=netntlm tocrack.txt

Résultat

root@bt:~/john-copy/run# ./john --wordlist --format=netntlm tocrack.txt

Loaded 7 password hashes with 3 different salts (NTLMv1 C/R MD4 DES (ESS MD5) [32/64])

Cricket88! (user)

82Varknar67 (LABO\nicduc2404)

82Varknar67 (LABO\nicduc2404)

camaro82Varknar (LABO\nicduc2404)

guesses: 4 time: 0:00:00:01 DONE (Wed Jan 23 02:19:07 2013) c/s: 2927K trying: wowwowcamaro - wowwowwow

Use the "--show" option to display all of the cracked passwords reliably

Résultat

root@bt:~/john-copy/run# cat john.pot

$NETNTLM$1122334455667788$a37c5c9316d9175589fdc21f260993daf3644f1aae2a3dfe:Cricket88!

$NETNTLM$1122334455667788$6fa23b67cdb418c8c766ea9beb3e275e37ef7637ec213c4b:82Varknar67

$NETNTLM$21893754907832 54$41888686e9823f598f726c631eaac42a320305582e5a45bb:82Varknar67

$NETNTLM$21893754907832 54$67e4196eb5323bb864fc144e152cb61d726779db69434782:camaro82Varknar

Autres techniques de *cracking*

- Mask attack
  - $word#### ou ####$word
- Bruteforce
  - -1 ?d?l?s -2 ?u?l?d?s ??2?1?1?1?1?1?1?1
- Bruteforce avec rules
  - Doubler lettres
  - table-lookup
  - jouer avec la casse
  - 31337
- Permutation
  - abc = bac = cab
- Toggle case
  - chocolate = cHoColaTE

Applications potentielles

- *Privilege escalation*
- Espionnage professionnel
  - Peut-être personnel...sachant que certains ne changent pas leurs mots de passe!
- Abus de confiance
  - Le facteur humain est trop souvent négligé
- ...

Conclusion et développement

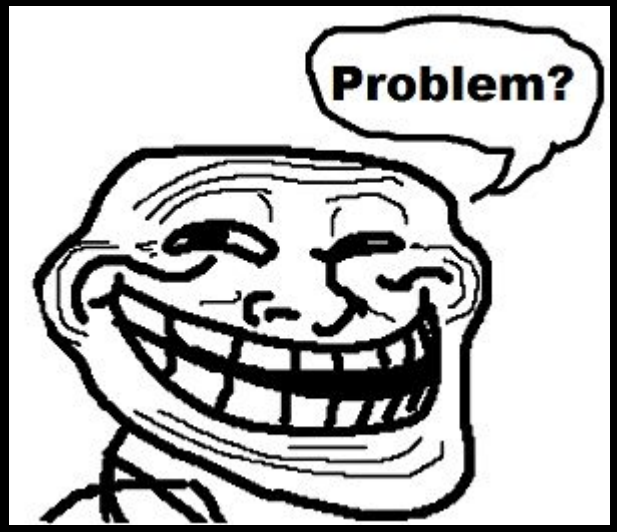
- NTLMv1 sucks!
- IWA c'est bien beau et pratique mais...
  - Il faut bien configurer
  - S'assurer que les mécanismes entourant IWA sont solides par *design* et bien structurés
- Avoir une politique de mots de passes solide aiderait grandement
  - Blacklister des *strings* ou des parties, en se basant
    - Sur des variables, genre $nom, $annéenaissance
    - Des mots contenus dans des *wordlists* populaires
  - Limiter la validité et la possibilité de répétition des

Conclusion et développement

- Utiliser des protocoles sécuritaires
  - Kerberos
  - NTLMv2
- Segmentation des environnements
  - 2x Réseau
  - 2x domaines

Depuis la présentation...

- atom de hashcat a intégré netntlmv1 en CPU
  - Prévoit l'intégration GPU
  - Implémente une meilleure attaque
- Meilleure performance+++++
  - jtr CPU = 14M hashes/s sur un AMD FX-8120
  - hashcat CPU = 76M hashes/s sur un AMD FX-8120
  - oclHashcat+ = 8B hashes/s sur une Radeon 7970



Questions?

martin.dube@hackfest.ca
vn@hackfest.ca