



Formation **Wireshark** *L'essentiel*



Hamza KONDAH

Une formation
Alphorm.com



Plan de la formation

Présentation de la formation

Manipuler les différentes fonctionnalités de Wireshark

Maîtriser l'analyse protocolaire avec Wireshark

Maîtriser l'analyse avancée de flux

Découvrir l'analyse forensique des réseaux avec Wireshark

Une formation
Alphorm.com



Plan de la formation

Identifier des attaques sur le réseau

Découvrir les outils complémentaires à Wireshark

Conclusion et perspectives

Une formation
Alphorm.com



Connaissances requises

Connaissances de base en systèmes d'exploitation et réseaux

Culture générale en cybersécurité

Optionnel : Expérience dans le domaine IT

Une formation
Alphorm.com

Formation Cisco ICND1/CCENT : Réussir l'examen 100-101

Découvrir les concepts essentiels de l'administration réseau et préparer la certification Cisco 100-101



Public concerné

Administrateurs réseaux et systèmes

Equipes opérationnelles SOC

Equipes de réponse d'incident

Pentesteurs

Auditeurs techniques, Analystes de sécurité

RSSI

AVERTISSEMENT

Le **formateur** n'est pas responsable de la mauvaise utilisation du contenu de cette formation

L'utilisation des outils, use cases et des malwares doit être réalisée uniquement au sein d'un environnement virtuelle



KEEP
CALM
AND
USE
WIRESHARK



Mettre en place le Lab



Hamza KONDAH

Une formation
Alphorm
com



Plan

Architecture du lab
Lab : Déployer le LAB

Une formation
Alphorm
com

WIRESHARK

L'essentiel

Architecture du lab

VMWare Workstation Pro 15+ ●



Windows 10



Kali Linux



CentOS

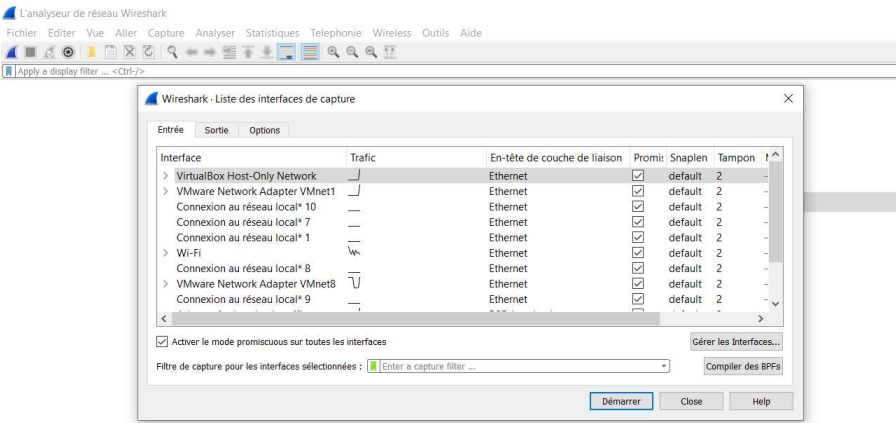


Une formation
Alphorm.com

WIRESHARK

L'essentiel

Lab : Déployer le LAB



Une formation
Alphorm.com



Découvrir Wireshark



Hamza KONDAH

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



Comprendre l'analyse réseau avec Wireshark



Hamza KONDAH

Une formation
Alphorm.com



Plan

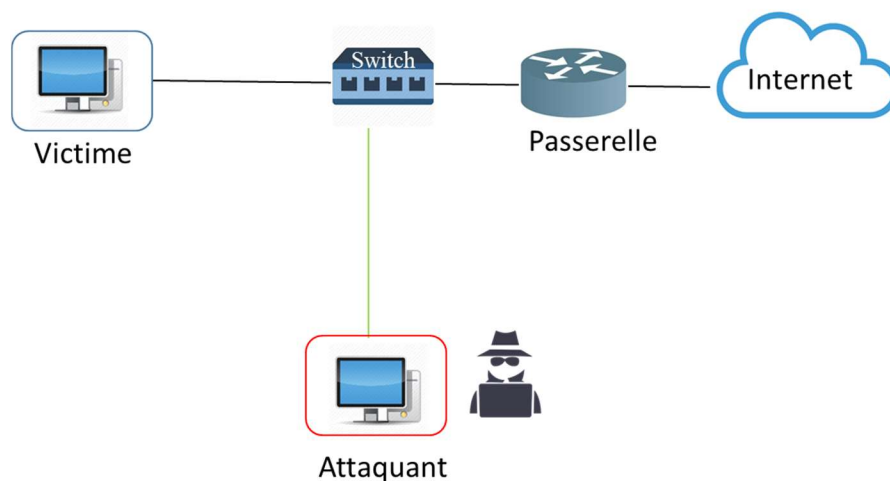
Le Sniffing Objectifs du Sniffing

Une formation
Alphorm.com



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



Apprendre les méthodologie et approches d'analyse



Hamza KONDAH

Une formation
Alphorm.com



Plan

Analyse dans le LAN
Méthodologie d'analyse

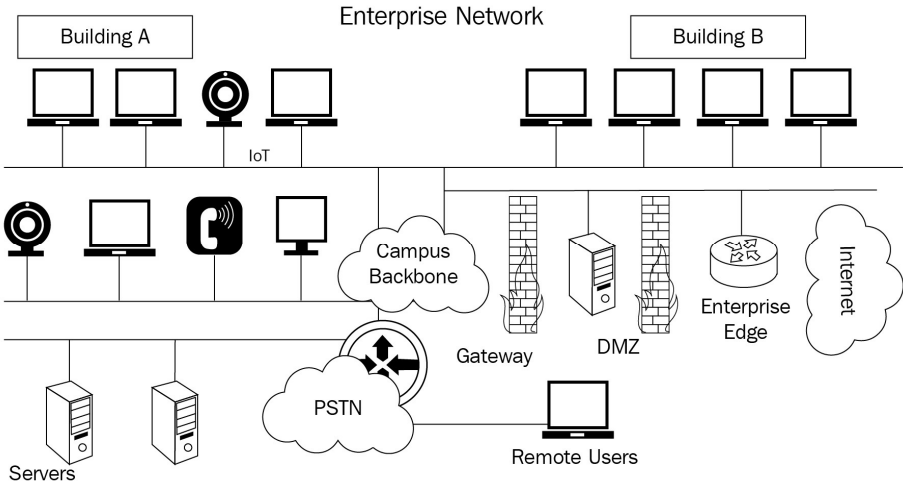
Une formation
Alphorm.com



L'essentiel

Une formation
Alphorm.com

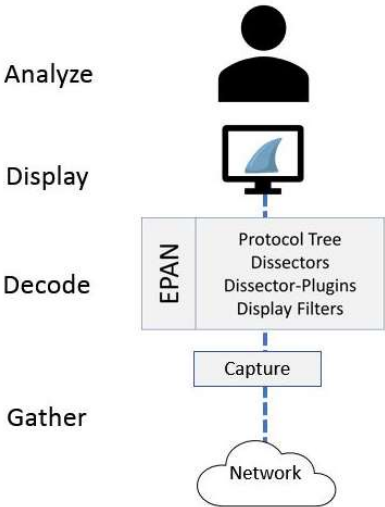
Analyse dans le LAN



L'essentiel

Une formation
Alphorm.com

Méthodologie d'analyse





Installer et configurer Wireshark sous différents environnements



Hamza KONDAH

Une formation
Alphorm.com



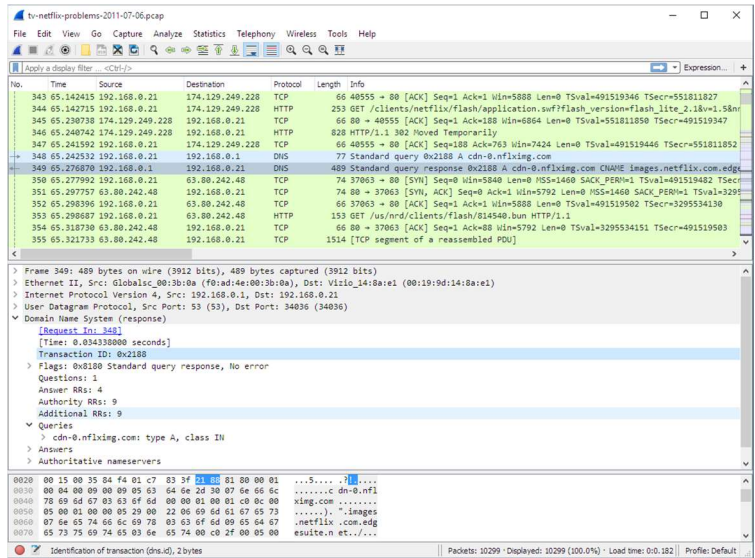
Plan

Installation sous Linux
Installation sous Windows

Une formation
Alphorm.com



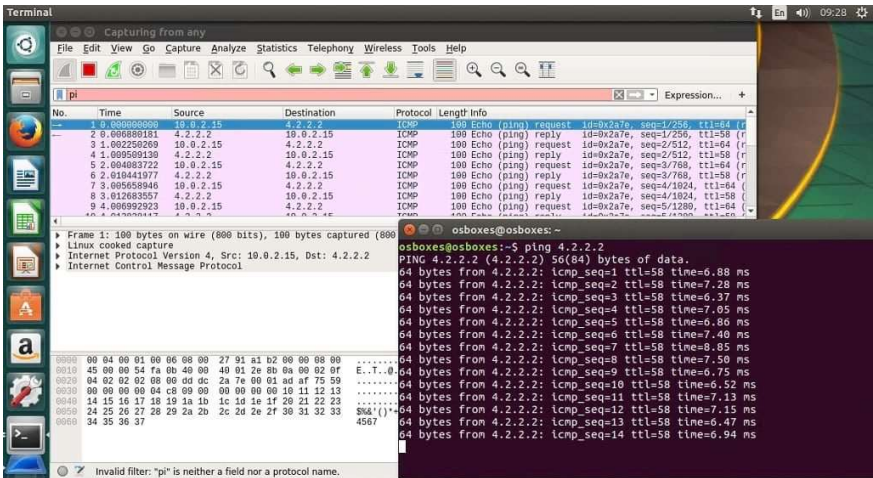
Installation sous Windows



Une formation
Alphorm.com



Installation sous Linux



Une formation
Alphorm.com



Effectuer du listing avec Capinfos



Hamza KONDAH

Une formation
Alphorm.com



Plan

Définition : capinfos

Sorties de capinfos

Options de Capinfos

Lab : Maîtriser capinfos

Une formation
Alphorm.com



Introduction à Capinfos

Capinfos est un programme qui lit un ou plusieurs fichiers de capture

Il retourne certaines ou toutes les statistiques disponibles (infos) de chaque <**fichier**> dans l'un des deux types de formats de sortie : **long ou table**

Une formation
Alphorm.com



Sorties de capinfos

La sortie long est interprétable

La sortie du tableau est utile pour générer un rapport qui peut être facilement importé dans une feuille de calcul ou une base de données

Une formation
Alphorm.com



Options de Capinfos

L'utilisateur spécifie quel type de sortie (**long ou table**) et quelles statistiques afficher en spécifiant des indicateurs (**options**) correspondant au type de rapport et aux informations souhaitées

Une formation
Alphorm.com



Options de capinfos

NB : *Si aucune option n'est spécifiée, Capinfos rendra compte de toutes les statistiques disponibles au format "long"*

Une formation
Alphorm.com



Une formation
Alphorm.com

Lab : Maîtriser capinfos

```
Windows PowerShell
PS C:\Program Files\Wireshark> .\capinfos.exe .\BackIT.pcapng
File name: .\BackIT.pcapng
File type: Wireshark/... - pcapng
File encapsulation: Ethernet
File timestamp precision: nanoseconds (9)
Packet size limit: file hdr: (not set)
Number of packets: 1038
File size: 710 kB
Data size: 675 kB
Capture duration: 146,17583394 second
First packet time: 2019-01-16 09:31:34,427920635
Last packet time: 2019-01-16 09:34:00,603504029
Data byte rate: 4621 bytes/s
Data bit rate: 36 kbps
Average packet size: 650,78 bytes
Average packet rate: 7 packets/s
SHA256: 114b8837568bcdaff9055405d660c2a42922a6e3f04830ac6c24cb464859e529
RIPEMD160: d8af61d3bbe0d1f528343771dad17557b69dc373
SHA1: b5f52d3c991241e4aa27a285d4dbd3d369c89c5c
Strict time order: False
Capture hardware: Intel(R) Core(TM) i7-7700HQ CPU @ 2.80GHz (with SSE4.2)
Capture oper-sys: Linux 4.18.0-kali2-amd64
Capture application: Dumpcap (Wireshark) 2.6.3 (Git v2.6.3 packaged as 2.6.3-1)
Number of interfaces in file: 1
Interface #0 info:
    Name = eth0
    Encapsulation = Ethernet (1 - ether)
    Capture length = 262144
    Time precision = nanoseconds (9)
    Time ticks per second = 1000000000
    Time resolution = 0x09
    Operating system = Linux 4.18.0-kali2-amd64
    Number of stat entries = 1
    Number of packets = 1038
PS C:\Program Files\Wireshark>
```



Une formation
Alphorm.com

Capturer le trafic avec Dumpcap et Mergecap



Hamza KONDAH



Plan

Présentation de Dumpcap
Fonctionnement de Dumpcap
Présentation de Mergecap
Fonctionnement de Mergecap

Une formation
Alphorm.com



Présentation de Dumpcap

Dumpcap est un outil de **dump** du trafic réseau

Il vous permet de **capturer** des données de paquets à partir d'un réseau en direct et **d'écrire** les paquets dans un fichier

Une formation
Alphorm.com



Fonctionnement de Dumpcap

Le format de fichier de capture par défaut de **Dumpcap** est le format **pcapng**

Lorsque l'option **-P** est spécifiée, le fichier de sortie est écrit au format pcap

Une formation
Alphorm.com



Fonctionnement de Dumpcap

Sans aucune option définie, il utilisera la bibliothèque **libpcap**, **Npcap** ou **WinPcap** pour capturer le trafic de la première interface réseau disponible et écrit les données brutes des paquets reçus, *ainsi que les horodatages des paquets dans un fichier pcap*

Une formation
Alphorm.com



Présentation de Dumpcap

Mergecap est un programme qui combine plusieurs fichiers de capture enregistrés dans un seul fichier de sortie spécifié par l'argument **-w**

Une formation
Alphorm.com



Fonctionnement de Mergecap

Mergecap sait lire les fichiers de capture **pcap** et **pcapng**, y compris ceux de **tcpdump**, Wireshark et d'autres outils qui écrivent des captures dans ces formats

Une formation
Alphorm.com



Fonctionnement de Mergecap

Par défaut, **Mergecap** écrit le fichier de capture au format **pcapng** et écrit tous les paquets des fichiers de capture d'entrée dans le fichier de sortie

Mergecap est capable de détecter, lire et écrire les mêmes fichiers de capture pris en charge par Wireshark

Une formation
Alphorm.com



Lab : Dumpcap et Mergecap

```
ca. Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Andrew>cd c:\Program Files\Wireshark

c:\Program Files\Wireshark>mergecap -h
Mergecap (Wireshark) 2.2.2 (v2.2.2-0-g775fb08)
Merge two or more capture files into one.
See https://www.wireshark.org for more information.

Usage: mergecap [options] -w <outfile>[- <infile> [<infile> ...]

Output:
-a          concatenate rather than merge files.
            default is to merge based on frame timestamps.
-s <snaplen> truncate packets to <snaplen> bytes of data.
-w <outfile>[- set the output filename to <outfile> or '-' for stdout.
-F <capture type> set the output file type; default is pcapng.
            an empty "-F" option will list the file types.
-I <IDB merge mode> set the merge mode for Interface Description Blocks; default
            is 'all'.
            an empty "-I" option will list the merge modes.
```

Une formation
Alphorm.com



Découvrir l'outil tshark et Rawshark



Hamza KONDAH

Une formation
Alphorm.com



Plan

Introduction à Rawshark
Rawshark : Stdin
Raswshark : Stdout

Une formation
Alphorm.com



Introduction à Rawshark

Rawshark lit un flux de paquets à partir d'un fichier ou d'un canal et affiche une ligne décrivant sa sortie, suivi d'un ensemble de champs correspondant pour chaque paquet sur stdout

Une formation
Alphorm.com



RawShark : Stdin

```
struct rawshark_rec_s {  
    uint32_t ts_sec;      /* Time stamp (seconds) */  
    uint32_t ts_usec;    /* Time stamp (microseconds) */  
    uint32_t caplen;      /* Length of the packet buffer */  
    uint32_t len;         /* "On the wire" length of the packet */  
    uint8_t data[caplen]; /* Packet data */  
};
```

Une formation
Alphorm.com



Rawshark : Stdout

```
0 FT_IPv4 BASE_NONE - 1 FT_UINT16 BASE_HEX -  
1 1="1" 0="192.168.77.10" 1 -  
2 1="1" 0="192.168.77.250" 1 -  
3 0="192.168.77.10" 1 -  
4 0="74.125.19.104" 1 -
```

Une formation
Alphorm.com



TShark

TShark est un analyseur de protocole réseau

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

Une formation
Alphorm.com



TShark

Ou encore en affichant les informations sous une forme décodée de ces paquets sur la sortie standard, soit en écrivant les paquets dans un fichier

Une formation
Alphorm.com



TShark

Le format de fichier de capture natif de TShark est le format pcapng, qui est également le format utilisé par Wirehark et divers autres outils

Une formation
Alphorm.com



TShark

Sans aucune option définie, TShark fonctionnera un peu comme tcpdump

Il utilisera la bibliothèque pcap pour capturer le trafic de la première interface réseau disponible et affiche une ligne récapitulative sur la sortie standard pour chaque paquet reçu

Une formation
Alphorm.com



Lab : Tshark

```
Command Prompt
c:\Program Files\Wireshark>tshark -i Ethernet
Capturing on 'Ethernet'
 1  0.000000 12:da:43:22:ff:75 → Spanning-tree-(for-bridges)_00 60 STP  Conf. Root = 327
68/0/10:da:43:22:ff:75  Cost = 0  Port = 0x8003
 2  0.781891 192.168.1.116 → 204.11.192.22 46 UDP  65510→5080 Len=4
 3  0.791128 192.168.1.116 → 204.11.192.22 830 SIP  Request: REGISTER sip:callcentric.co
m (1 binding) |
 4  0.877988 204.11.192.22 → 192.168.1.116 457 SIP  Status: 200 Ok (1 binding) |
 5  0.998111 192.168.1.102 → 239.255.255.250 369 SSDP  NOTIFY * HTTP/1.1
 6  1.101586 192.168.1.102 → 239.255.255.250 369 SSDP  NOTIFY * HTTP/1.1
 7  1.205605 192.168.1.102 → 239.255.255.250 378 SSDP  NOTIFY * HTTP/1.1
 8  1.290135 52.71.182.200 → 192.168.1.123 66 TCP  1 443→53432 [ACK] Seq=1 Ack=1 Win=136
Len=0 TSval=554058558 TSecr=50151473
 9  1.319675 192.168.1.102 → 239.255.255.250 378 SSDP  NOTIFY * HTTP/1.1
10  1.421830 192.168.1.102 → 239.255.255.250 433 SSDP  NOTIFY * HTTP/1.1
11  1.531164 192.168.1.102 → 239.255.255.250 433 SSDP  NOTIFY * HTTP/1.1
12  1.626488 192.168.1.102 → 239.255.255.250 443 SSDP  NOTIFY * HTTP/1.1
13  1.630181 128.121.22.159 → 192.168.1.116 85 TLSv1.2 1 Application Data
14  1.631402 192.168.1.116 → 128.121.22.159 89 TLSv1.2 1 Application Data
15  1.682442 128.121.22.159 → 192.168.1.116 60 TCP  32 443→51752 [ACK] Seq=32 Ack=36 Win=
11 Len=0
16  1.726789 192.168.1.102 → 239.255.255.250 443 SSDP  NOTIFY * HTTP/1.1
17  1.962162 192.168.1.116 → 209.18.47.62 78 DNS  Standard query 0xbd9c A www.cellstream
.com
17 packets captured
c:\Program Files\Wireshark>
```

Une formation
Alphorm.com



Maîtriser l'analyse et le dépannage réseau à distance



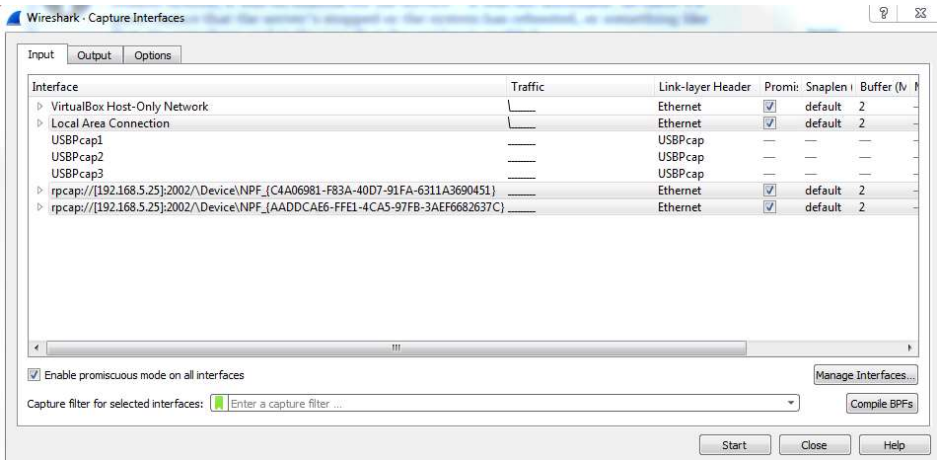
Hamza KONDAH

Une formation
Alphorm.com



Lab : Analyse en Remote

Une formation
Alphorm.com





Maîtriser les paramètres généraux et personnels



Hamza KONDAH

Une formation
Alphorm.com



Plan

Gestion des profils

Lab : Maitriser le Paramétrage

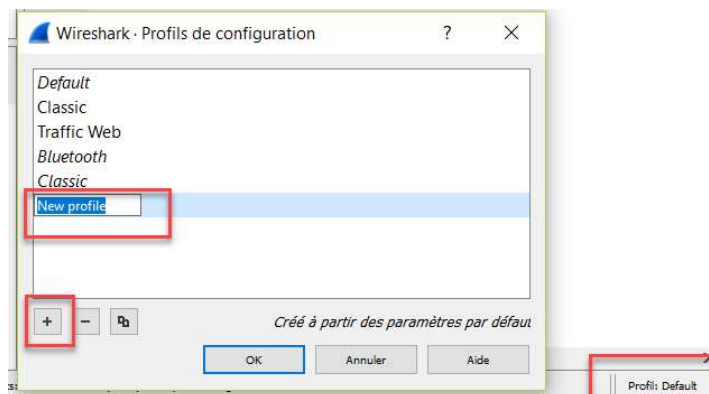
Une formation
Alphorm.com

Gestion des profils

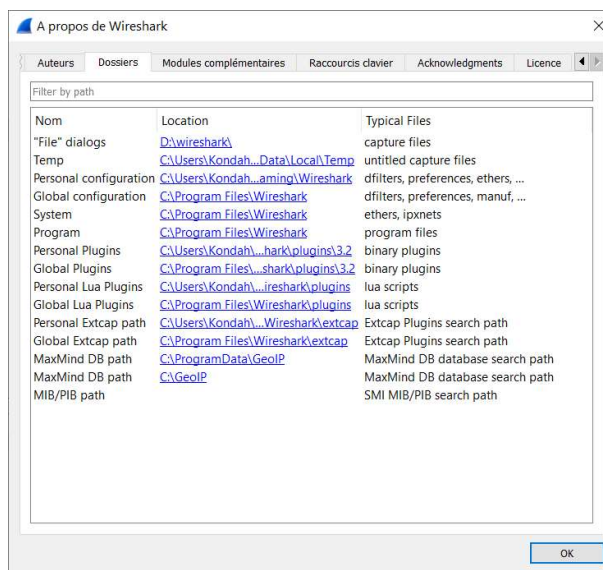
Wireshark permet de créer des profils à chaque scénario spécifique

On peut associer chaque profil peut être associé :

- Paramètres et réglages
- Des filtres de captures
- Des filtres d'affichage
- Règles de coloration



Lab : Maitriser le Paramétrage





Une formation
Alphorm.com

Maîtriser la création de filtres d'affichage et de capture



Hamza KONDAH



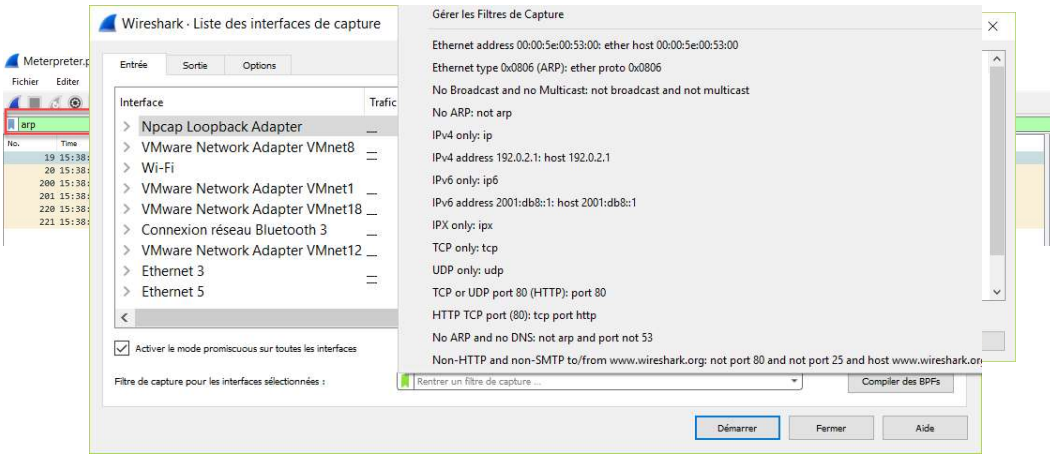
Une formation
Alphorm.com

Plan

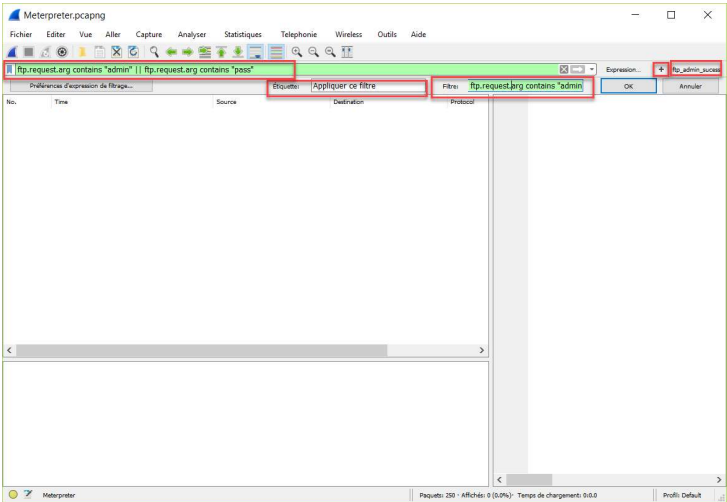
Les filtres Wireshark
Création de boutons
Lab : Gestion des filtres

Les filtres Wireshark

- Filtres d'affichage
- Filtres de captures



Création de boutons





Lab : Gestion des filtres

```
ca Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Andrew>cd c:\Program Files\Wireshark

c:\Program Files\Wireshark>mergcap -h
Mergcap (wireshark) 2.2.2 (v2.2.2-0-g775fb00)
Merge two or more capture files into one.
See https://www.wireshark.org for more information.

Usage: mergcap [options] -w <outfile>[- <infile> [<infile> ...]

Output:
-a          concatenate rather than merge files.
            default is to merge based on frame timestamps.
-s <snaplen> truncate packets to <snaplen> bytes of data.
-w <outfile>[- set the output filename to <outfile> or '-' for stdout.
-F <capture type> set the output file type; default is pcapng.
                an empty "-F" option will list the file types.
-I <IDB merge mode> set the merge mode for Interface Description Blocks; default
it is 'all'.
                an empty "-I" option will list the merge modes.
```

Une formation
Alphorm.com



Effectuer des suivis et du réassemblage de flux

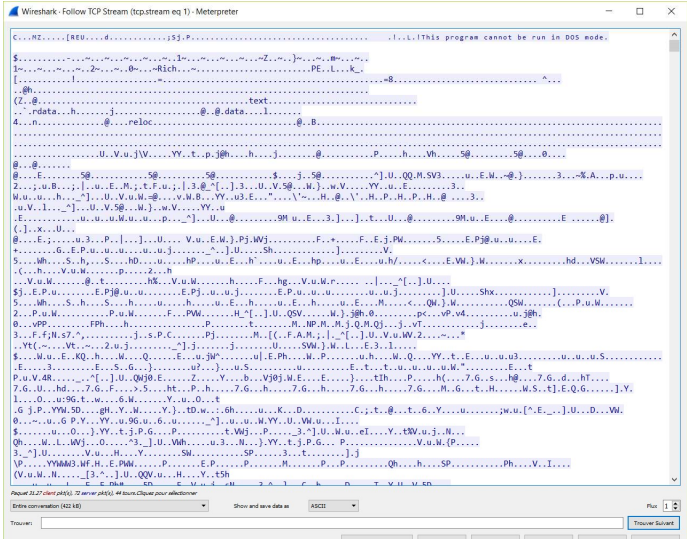


Hamza KONDAH

Une formation
Alphorm.com



Lab : Analyse de flux



Exploiter l'Expert Information de Wireshark



Hamza KONDAH



Lab : Expert Information

Wireshark - Expert Information - Internet's Noise 24 h 4 without ICMP destination unreachable

Severity	Summary	Group	Protocol	Count
> Error	Malformed Packet (Exception occurred)	Malformed	RTPproxy	1
> Error	Malformed Packet (Exception occurred)	Malformed	NTP	4
> Warning	Previous segment(s) not captured (common at capture start)	Sequence	TCP	3
> Warning	This frame is a (suspected) out-of-order segment	Sequence	TCP	1
> Warning	Connection reset (RST)	Sequence	TCP	7
> Warning	Header not terminated by empty line (CRLF)	Malformed	SIP	1
> Note	The urgent pointer field is nonzero while the URG flag is not set	Protocol	TCP	1
> Note	A new tcp session is started with the same ports as an earlier session in this trace	Sequence	TCP	18
> Note	"Time To Live" only 1	Sequence	IPv4	2
> Note	This frame is a (suspected) retransmission	Sequence	TCP	353
> Note	The acknowledgment number field is nonzero while the ACK flag is not set	Protocol	TCP	22
> Chat	M-SEARCH * HTTP/1.1\r\n	Sequence	SSDP	10
> Chat	Connection establish request (SYN): server port 2222	Sequence	TCP	1547
> Chat	Connection establish acknowledge (SYN+ACK): server port 80	Sequence	TCP	842

No display filter set.

☐ Limit to Display Filter ☒ Group by summary Search: Show...



Introduire l'analyse protocolaire avec Wireshark



Hamza KONDAH



Plan

Interfaces supportées Liste des protocoles supportés

Une formation
Alphorm.com

Interfaces supportées

	AIX	FreeBSD	HP-UX	Irix	Linux	MacOSX	NetBSD	OpenBSD	Solaris	Tru64UNIX	Windows
Physical Interfaces											
ATM	Unknown	Unknown	Unknown	Unknown	Yes	No	Unknown	Unknown	Yes	Unknown	Unknown
Bluetooth	No	No	No	No	Yes ¹	No	No	No	No	No	No
CiscoHDLC	Unknown	Yes	Unknown	Unknown	Yes	Unknown	Yes	Yes	Unknown	Unknown	Unknown
Ethernet	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
FDDI	Unknown	Unknown	Unknown	Unknown	Yes	No	Unknown	Unknown	Yes	Unknown	Unknown
FrameRelay	Unknown	Unknown	No	No	Yes	No	Unknown	Unknown	No	No	No
IrDA	No	No	No	No	Yes	No	No	No	No	No	No
PPP ²	Unknown	Unknown	Unknown	Unknown	Yes	Yes	Unknown	Unknown	No	Unknown	Yes
TokenRing	Yes	Yes	Unknown	No	Yes	No	Yes	Yes	Yes	Unknown	Yes
USB	No	No	No	No	Yes ³	No	No	No	No	No	No
WLAN ⁴	Unknown	Yes	Unknown	Unknown	Yes	Yes	Yes	Yes	Unknown	Unknown	Yes
Virtual Interfaces											
Loopback	Unknown	Yes	No	Unknown	Yes	Yes	Yes	Yes	No	Yes	N/A ⁵
VLAN Tags	Yes	Yes	Yes	Unknown	Yes	Yes	Yes	Yes	Yes	Yes	Yes



Liste des protocoles supportés

Wireshark supporte plus de 1500 protocoles

➔ <https://wiki.wireshark.org/ProtocolReference>

Possibilité de développer des dissecteurs

Rétroingénierie à ne pas négliger

Une formation
Alphorm.com



Apprendre à analyser le trafic ARP



Hamza KONDAH

Une formation
Alphorm.com

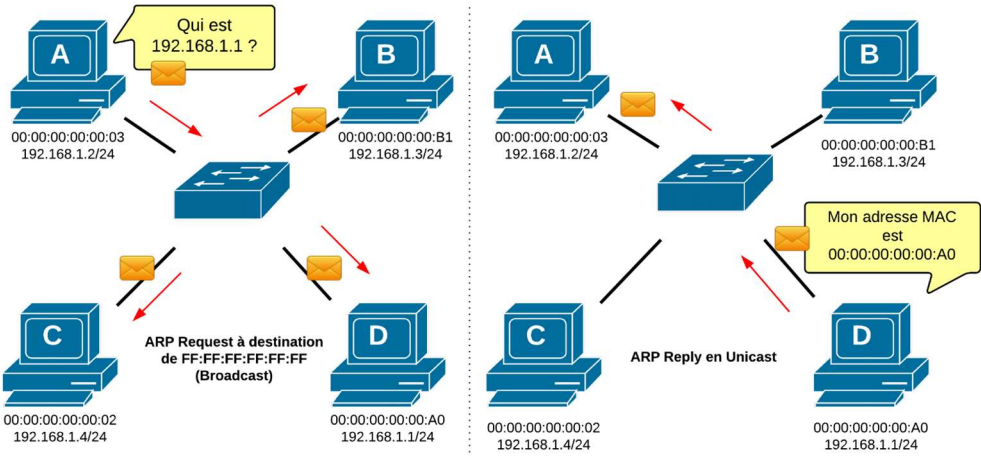


Plan

Rappel protocole ARP
Lab : Analyse ARP

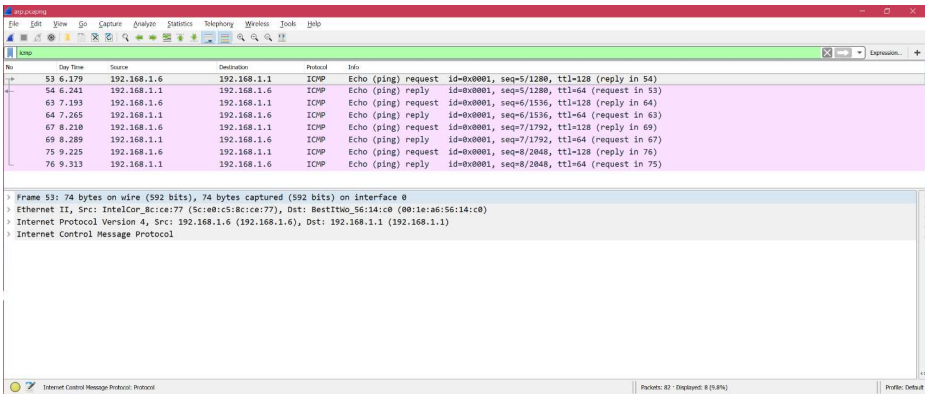


Rappel protocole ARP





Lab : Analyse ARP



Apprendre à analyser le trafic DHCP



Hamza KONDAH



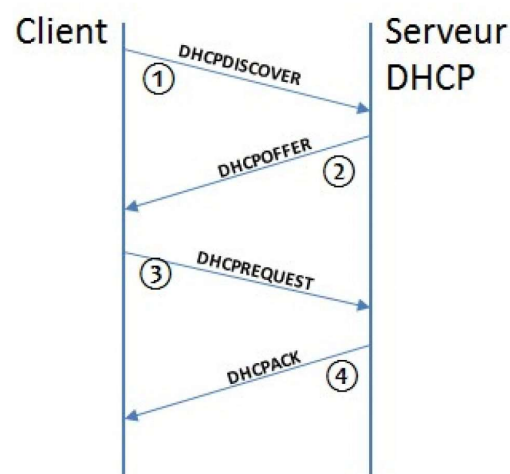
Plan

Rappel protocole DHCP LAB : Analyse DHCP

Une formation
Alphorm.com



Rappel protocole DHCP



Une formation
Alphorm.com



LAB : Analyse DHCP

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter:

Expression...

Clear

Apply

No.	Time	Source	Destination	Protocol	Info
10	35.322186	10.0.3.254	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0xb9983b
11	35.322279	VMware el:b3:10	10.0.3.130	ICMP	Echo (ping) request
12	36.323378	VMware el:b3:10	Broadcast	ARP	Who has 10.0.3.130? Tell 10.0.3.2
13	36.323621	10.0.3.254	255.255.255.255	DHCP	DHCP Offer - Transaction ID 0xb9983b
14	36.332000	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0xb9983b
15	36.376251	10.0.3.254	255.255.255.255	DHCP	DHCP ACK - Transaction ID 0xb9983b
16	36.379567	cc:02:0a:9e:00:00	Broadcast	ARP	Gratuitous ARP for 10.0.3.130 (Reply)

Hops: 0

Transaction ID: 0xb9983b

Seconds elapsed: 0

Bootp flags: 0x0000 (Broadcast)

Client IP address: 0.0.0.0 (0.0.0.0)

Your (client) IP address: 0.0.0.0 (0.0.0.0)

Next server IP address: 0.0.0.0 (0.0.0.0)

Relay agent IP address: 0.0.0.0 (0.0.0.0)

Client MAC address: cc:02:0a:9e:00:00 (cc:02:0a:9e:00:00)

Client hardware address padding: 00000000000000000000

Server host name not given

Boot file name not given

Magic cookie: (OK)

Option: (t=53,l=1) DHCP Message Type = DHCP Discover

Option: (t=57,l=2) Maximum DHCP Message Size = 1152

Option: (t=61,l=27) Client identifier

Option: (t=12,l=5) Host Name = "R3DMZ"

Option: (t=55,l=8) Parameter Request List

Option: (t=52,l=1) Option Overload = Boot file and server host names hold options

Boot file name option overload

Padding (128 bytes)

Server host name option overload

Text item (1), 3 bytes

Packets: 22 Displayed: 22 Marked: 0 Dropped: 0

Profile: Default



Apprendre à analyser le trafic DNS



Hamza KONDAH



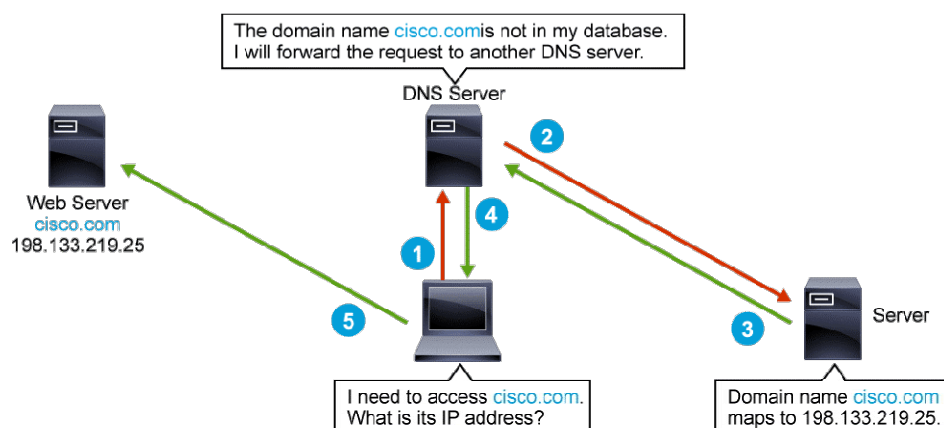
Plan

Rappel DNS LAB : Analyse DNS

Une formation
Alphorm.com



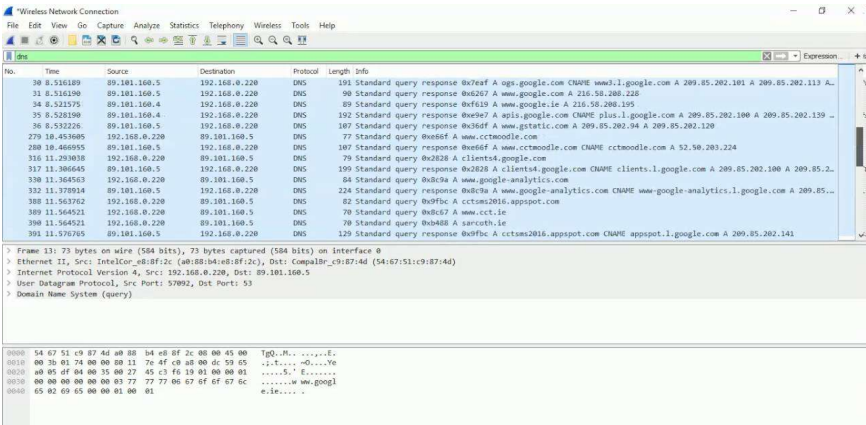
Rappel DNS



Une formation
Alphorm.com



LAB : Analyse DNS



Apprendre à analyser le trafic HTTP



Hamza KONDAH



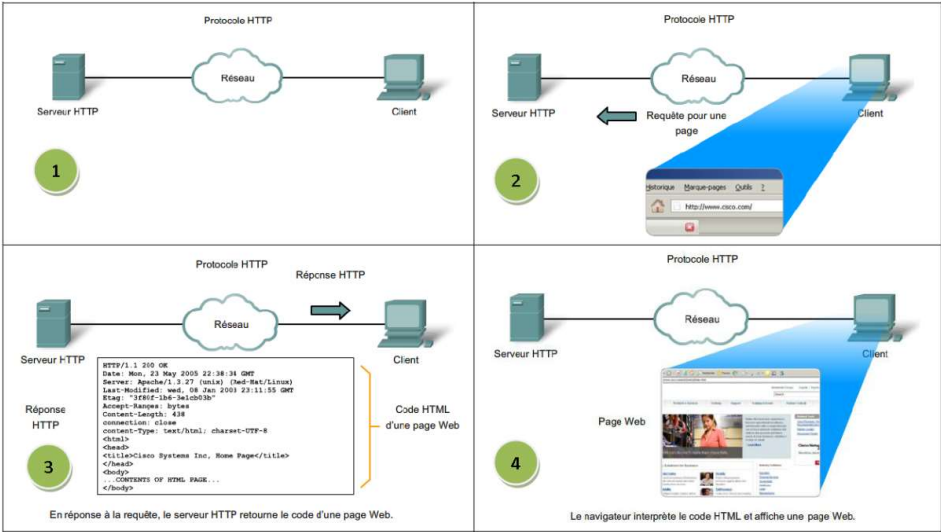
Plan

Rappel HTTP

Lab : Analyse HTTP

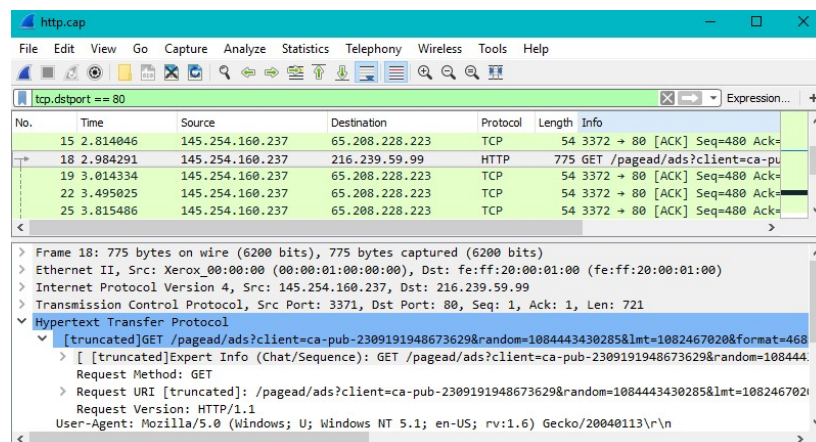


Rappel HTTP





Lab : Analyse HTTP



Une formation
Alphorm.com



Apprendre à analyser le trafic VoIP



Hamza KONDAH

Une formation
Alphorm.com



Plan

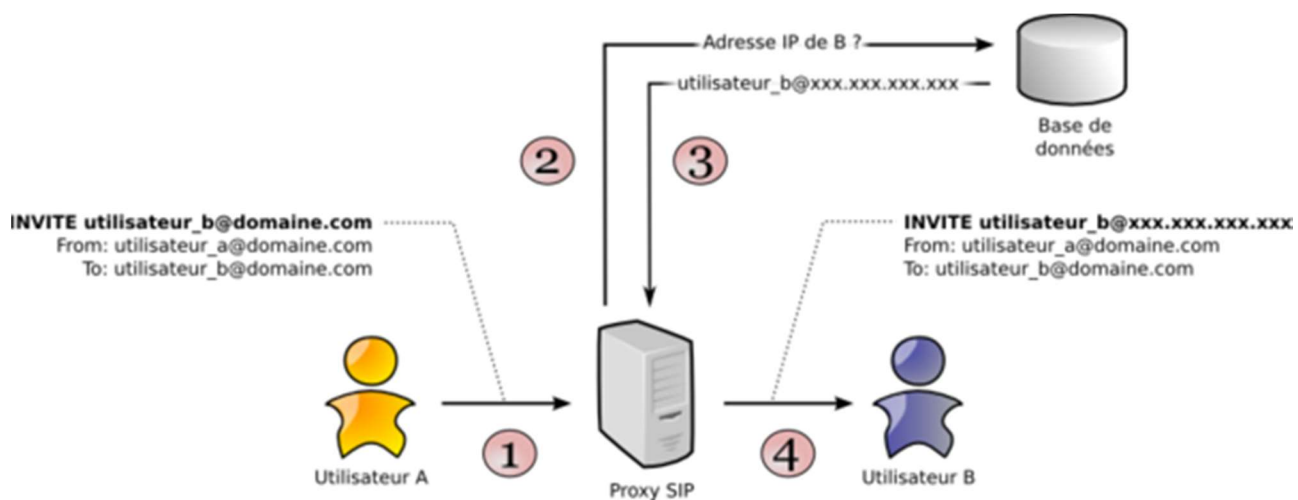
Introduction au SIP

Préparation du lab

Lab : à analyser le trafic VoIP

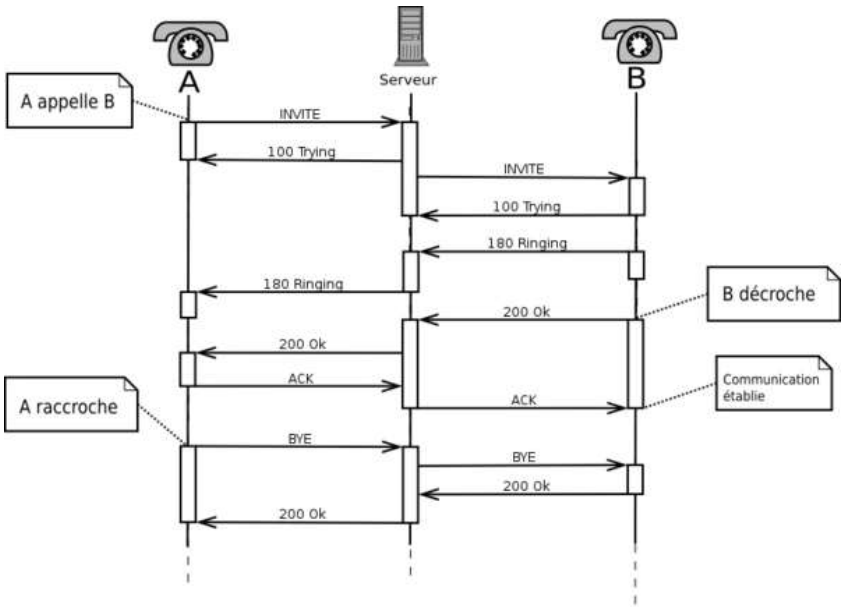
Une formation
Alphorm
com

Introduction au SIP





Introduction au SIP



Préparation du lab

SampleCaptures - The Wi x

Secure | https://wiki.wireshark.org/SampleCaptures#SIP_and_RTP

[lpmb.multi.packets.pcap](#) (libpcap), IPMB interface capture file, include multiple request and response packets.

SIP and RTP

[aaa.pcap](#) Sample SIP and RTP traffic.

[SIP_CALL RTP_G711](#) Sample SIP call with RTP in G711.

[SIP_DTMF2.cup](#) Sample SIP call with RFC 2833 DTMF

[DTMFsipinfo.pcap](#) Sample SIP call with SIP INFO DTMF

[h223-over-rtp.pcap.gz](#) (libpcap) A sample of H.223 running over RTP, following negotiation over SIP.

[h263-over-rtp.pcap](#) (libpcap) A sample of RFC 2190 H.263 over RTP, following negotiation over SIP.

[metasploit-sip-invite-spoof.pcap](#) Metasploit 3.0 SIP Invite spoof capture.

[FAX-Call-t38-CA-TDM-SIP-FB-1.pcap](#) Fax call from TDM to SIP over Mediatgateway with declined T38 request, megaco H.248.

[Asterisk_ZFONE_XLITE.pcap](#) Sample SIP call with ZRTP protected media.

MagiJack+ Power On sequence SIP and RTP traffic generated by power on the MagiJack+

MagiJack+ short test call A complete telephone call example

SIP calls between SIPp ([scenario file](#)) and FreeSWITCH 1.6.12, playing [ivr-on_hold_indefinitely.wav](#) in one direction using various codecs:



Lab : à analyser le trafic VoIP

```
Message Header
  Via: SIP/2.0/UDP 192.168.0.10:59205;branch=z9hG4bKc0a8000a052182706faf2cbf3d;rport=59205;received=206.248.161.77
  Contact: <sip:4165551212@216.234.64.8:5070>
  To: <sip:9055551212@talk4free.com>;tag=30da0aed-co12170-IN5015
  From: "unknown"<sip:E646657195201@talk4free.com>;tag=2afc8c735218176
  Call-ID: C5570127C1A6A1ABF7ED9DB9AD608CE00xc0a8000a
  CSeq: 2 INVITE
    Sequence Number: 2
    Method: INVITE
  Content-Type: application/sdp
  Date: Thu, 12 Apr 2012 15:40:21 GMT
  User-Agent: ENSR3.2.21.22-IS15-RMRG5002-RG900-EP-CPI15-CP025791
  Content-Length: 236
  X-Number-Type: 9055551212;type=off-net
    [Expert Info (Note/Undecoded): Unrecognised SIP header (x-number-type)]
    [Unrecognised SIP header (x-number-type)]
    [Severity level: Note]
    [Group: Undecoded]
```

Une formation
Alphorm.com



Apprendre à effectuer une analyse du trafic WLAN



Hamza KONDAH

Une formation
Alphorm.com



Une formation
Alphorm.com

Plan

Standards

Trames wlan

Trames de management

Associations et états

Trames de contrôle

Lab : Analyse WLAN



Une formation
Alphorm.com

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)

Standards

Le terme IEEE 802.11 est également utilisé pour désigner la norme d'origine 802.11

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.

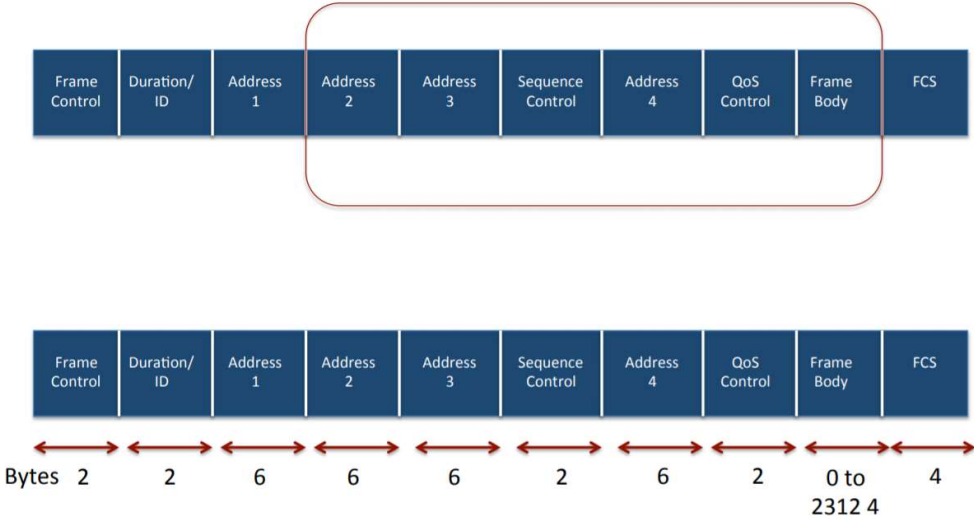


Standards

Standard	Frequency Band	Bandwidth	Modulation Scheme	Channel Arch.	Maximum Data Rate	Range	Max Transmit Power
802.11	2.4 GHz	20 MHz	BPSK to 256-QAM	DSSS, FHSS	2 Mbps	20 m	100 mW
b	2.4 GHz	21 MHz	BPSK to 256-QAM	CCK, DSSS	11 Mbps	35 m	100 mW
a	5 GHz	22 MHz	BPSK to 256-QAM	OFDM	54 Mbps	35 m	100 mW
g	2.4 GHz	23 MHz	BPSK to 256-QAM	DSSS, OFDM	54 Mbps	70 m	100 mW
n	2.4 GHz, 5 GHz	24 MHz and 40 MHz	BPSK to 256-QAM	OFDM	600 Mbps	70 m	100 mW
ac	5 GHz	20, 40, 80, 80+80=160 MHz	BPSK to 256-QAM	OFDM	6.93 Gbps	35 m	160 mW
ad	60 GHz	2.16 GHz	BPSK to 64-QAM	SC, OFDM	6.76 Gbps	10 m	10 mW
af	54-790 MHz	6, 7, and 8 MHz	BPSK to 256-QAM	SC, OFDM	26.7 Mbps	>1km ?	100 mW
ah	900 MHz	1, 2, 4, 8, and 16 MHz	BPSK to 256-QAM	SC, OFDM	40 Mbps	1 km	100 mW



Frames wlan



Frames wlan

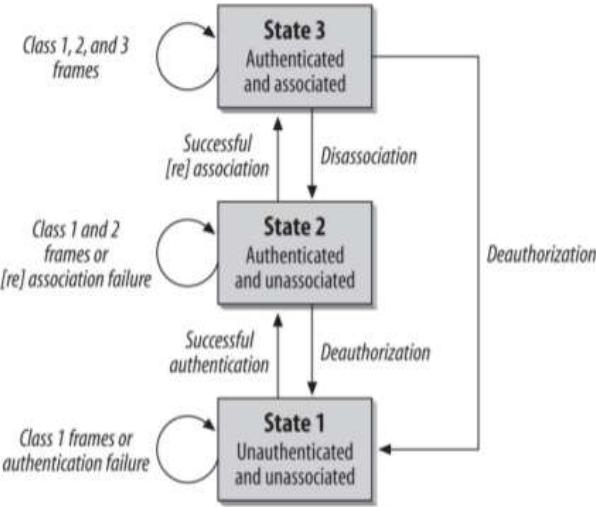


Trames de management

Authentification	Désauthentification	Demande d'association	Réponse de l'association	Demande de réassociation
Réponse de réassociation	Dissociation	Balise	Demande de sonde	Réponse de la sonde



Associations et états





Trames de contrôle

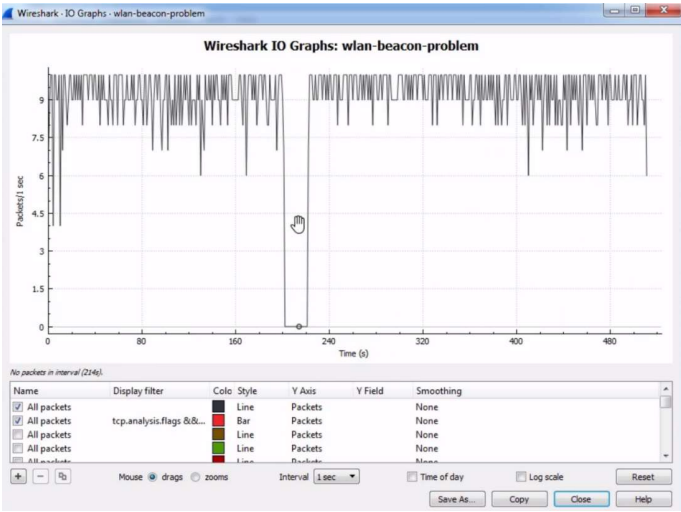
Demande d'envoi (RTS)

Effacer pour envoyer (CTS)

Accusé de réception (ACK)



Lab : Analyse WLAN





Appréhender les IoC d'infection réseau



Hamza KONDAH

Une formation
Alphorm.com



Plan

Introduction

Classification

Spear phishing / phishing

Les serveurs C&C

Lab : les IoC d'infection réseau

Une formation
Alphorm.com



Introduction

APT : *Advanced Persistant Threat*

Furtivité

Exfiltration de données

Malwares assez sophistiqués

Etats, hacktivistes....



Une formation
Alphorm.com

Introduction

Internationalisation de la
cybercriminalité

Rejoint le monde réel en élargissant
les domaines d'activité

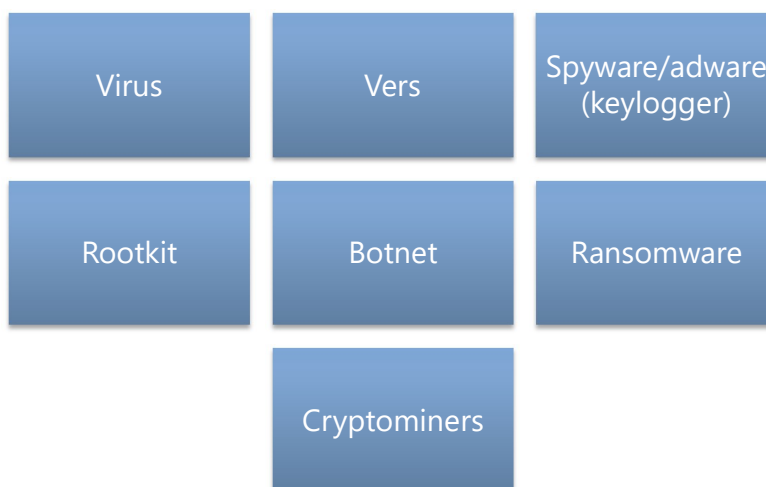
Cyber-espionnage très actif

APT21, collecte des teras octets de
plus de 140 entreprises

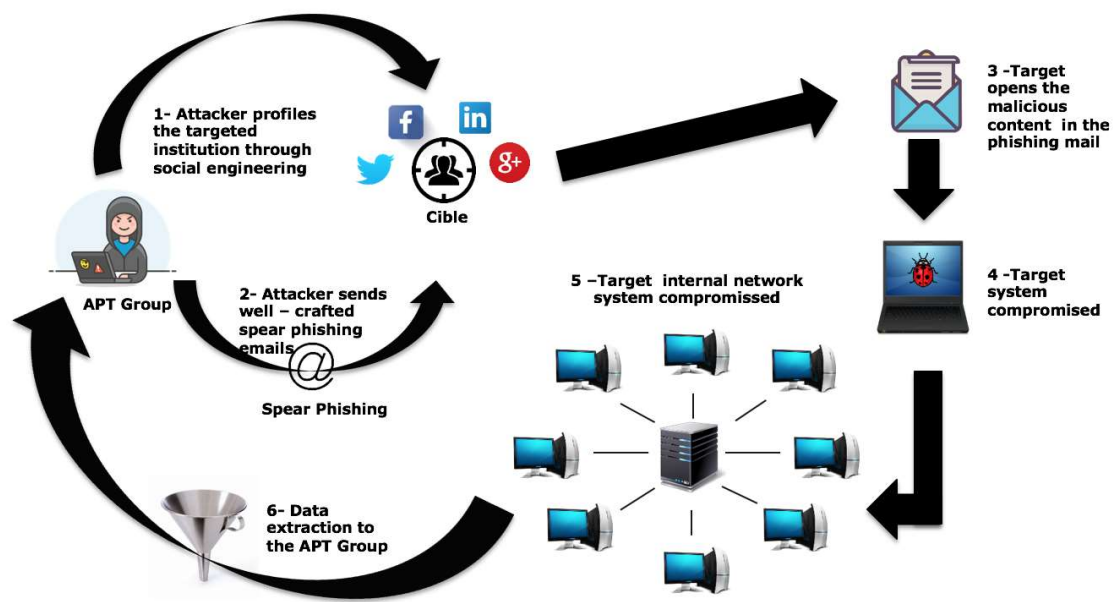


Une formation
Alphorm.com

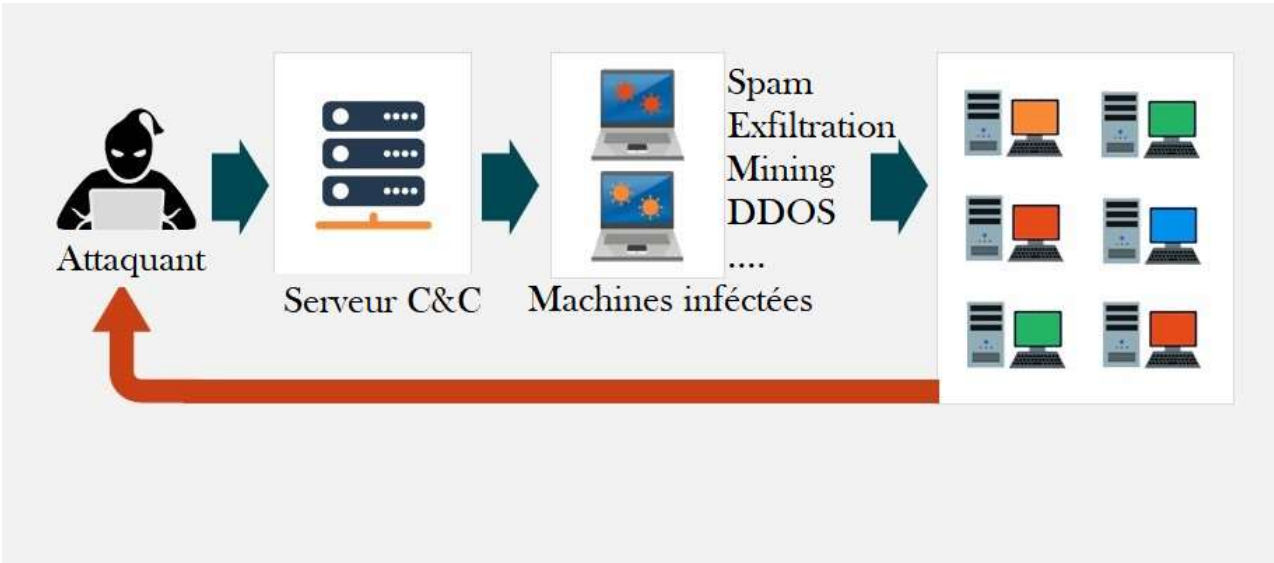
Classification



Spear phishing / phishing



Les serveurs C&C





Une formation
Alphorm.com

Lab : les IoC d'infection réseau

```
Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Andrew>cd c:\Program Files\Wireshark

c:\Program Files\Wireshark>mergcap -h
Mergcap (Wireshark) 2.2.2 (v2.2.2-0-g775fb08)
Merge two or more capture files into one.
See https://www.wireshark.org for more information.

Usage: mergcap [options] -w <outfile>[- <infile> [<infile> ...]

Output:
-a          concatenate rather than merge files.
            default is to merge based on frame timestamps.
-s <snaplen> truncate packets to <snaplen> bytes of data.
-w <outfile>|- set the output filename to <outfile> or '-' for stdout.
-F <capture type> set the output file type; default is pcapng.
            an empty "-F" option will list the file types.
-I <IDB merge mode> set the merge mode for Interface Description Blocks; default
            is 'all'.
            an empty "-I" option will list the merge modes.
```



Une formation
Alphorm.com

Apprendre à exploiter les graphes



Hamza KONDAH



Apprendre à extraire des mots de passes d'une capture réseau



Hamza KONDAH

Une formation
Alphorm.com



Introduire la notion de forensique réseaux



Hamza KONDAH

Une formation
Alphorm.com



Plan

Qu'est ce que le DFIR ?
Forensics vs Incident Response
Remarque !

Une formation
Alphorm.com



Qu'est ce que le DFIR ?

**Digital Forensics and Incident
Reponse** : Forensique digitale et
réponse aux incidents

Une formation
Alphorm.com



Qu'est ce que le DFIR ?

Le Cyber Forensics est alors l'enquête sur l'interface homme-machine à un degré ***d'intégrité et de certitude qui convient à un tribunal***

Une formation
Alphorm.com



Qu'est ce que le DFIR ?

La forensique désigne l'ensemble des sciences appliquées utilisées dans la collecte, l'analyse et l'interprétation des traces dans le but d'établir des faits devant être présentés devant une cour de justice

Une formation
Alphorm.com

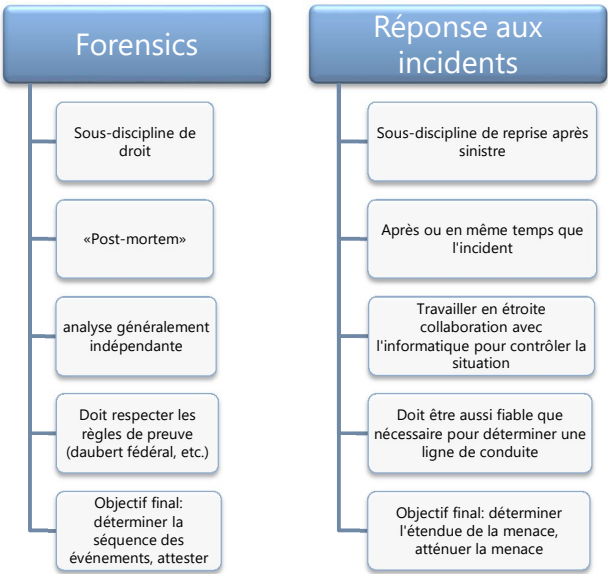


Qu'est ce que le DFIR ?

Réponse aux incidents : préparation et réponse à une menace d'urgence ou émergente



Forensics vs Incident Response





Remarque

La nature transitoire des Forencics de réseau signifie que, souvent, il n'est pas possible d'effectuer une acquisition de preuves conforme aux normes de preuve actuelles

Une formation
Alphorm.com



Remarque

À ce titre, nous examinerons également les choses pertinentes à la réponse à incidents

Une formation
Alphorm.com



Découvrir la méthodologie d'analyse forensique dans les réseaux informatiques



Hamza KONDAH

Une formation
Alphorm.com



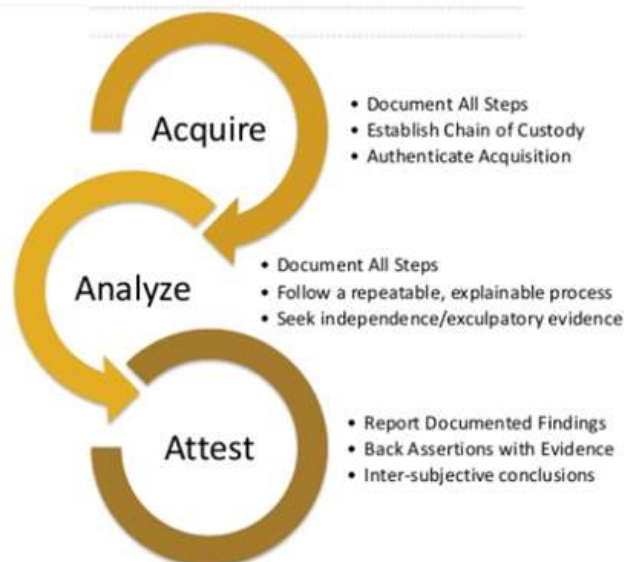
Plan

Méthodologie forensics
Notion de preuve
Notre mission
Où retrouver nos preuves ?

Une formation
Alphorm.com



Méthodologie forensics



Une formation
Alphorm.com



Notion de preuve

Règles de preuve - des normes établissent des lignes directrices concernant la recevabilité

Ces «normes» varient à tous les niveaux de gouvernement et de nombreuses normes disparates existent

Une formation
Alphorm.com



Notre mission

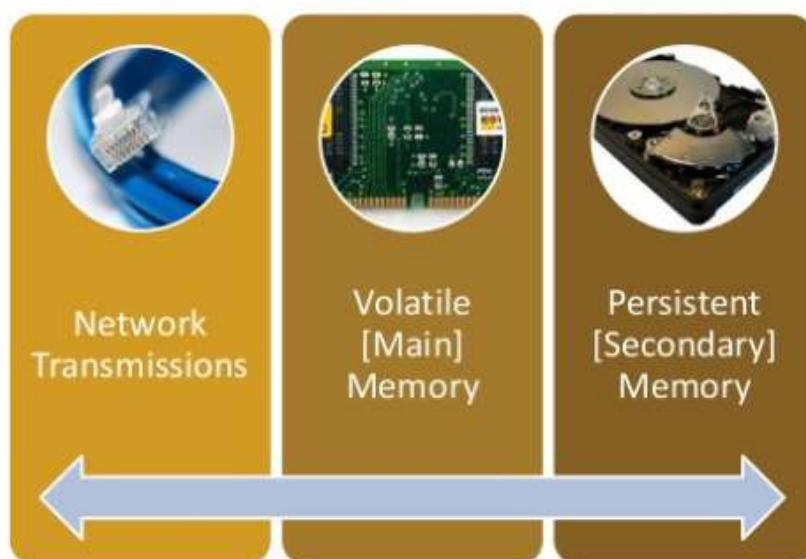
Comprendre et décrire un événement, un ensemble d'événements ou un système de la manière la plus précise et détaillée possible compte tenu de toutes les informations disponibles.

Maintenir l'intégrité de la preuve et de la scène pour garantir cette précision.

Une formation
Alphorm.com



Où retrouver nos preuves ?



Une formation
Alphorm.com



Démystifier les mesures anti forensique réseau avec Wireshark



Hamza KONDAH

Une formation
Alphorm.com



Obscurcissement

Usurpation d'identité : chaînes
d'agent utilisateur IP / MAC ou de pile
IP pour masquer le type de système
d'exploitation ou navigateur

Cryptage : y compris TLS, Tor,
personnalisés...

Une formation
Alphorm.com



Mesures anti forensics

Compression d'exécutables / fichiers

Stéganographie :(

Canaux secrets (IP over DNS est un dérivé populaire, également projet **Telex**)

Fragmentation / fuzzing des commandes (outils comme **SniffJoke**)

Une formation
Alphorm.com



Exploitation

Attaques contre les outils d'enquête / IDS (à la *CVE-2011-1591*)

Détection active de la surveillance du réseau

Une formation
Alphorm.com



Apprendre à effectuer du forensique réseau



Hamza KONDAH

Une formation
Alphorm.com



Comprendre le déroulé d'une killchain



Hamza KONDAH

Une formation
Alphorm.com



Plan

Notion de Killchain
Phishing : Kill Chain (Avancée)

Une formation
Alphorm.com



Notion de killchain

«**Kill chain**» est un terme utilisé à l'origine par les militaires pour définir les étapes qu'un ennemi utilise pour attaquer une cible

En **2011**, **Lockheed Martin** a publié un article définissant une Cyber Kill Chain

Une formation
Alphorm.com



Notion de killchain

Similaire dans son concept au modèle militaire, il définit les étapes utilisées par les cyber-attaquants dans les cyber-attaques d'aujourd'hui

Une formation
Alphorm.com



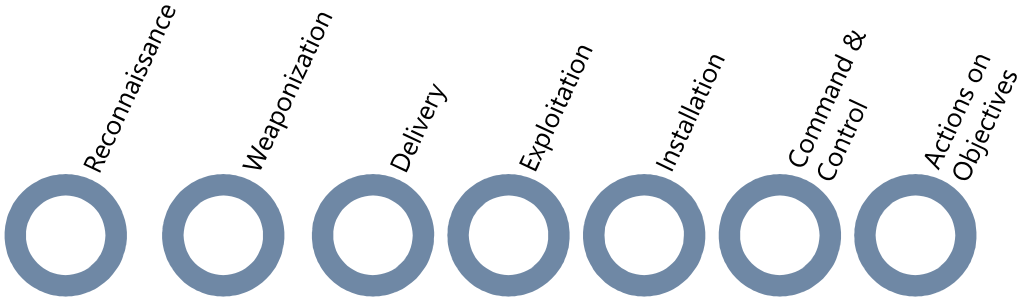
Notion de killchain

Plus vous pouvez intercepter les méchants, plus vous avez des chances de les refuser de leur objectif ou de les forcer à faire suffisamment de bruit où vous pouvez plus facilement les détecter

Une formation
Alphorm.com



Phishing : Kill Chain (Avancée)



Une formation
Alphorm.com



Lab : le MITRE - ATT&CK

MITRE ATTACK™ Navigator										
Layer										
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 items	31 items	56 items	28 items	59 items	20 items	19 items	17 items	13 items	8 items	21 items
Drive-by Compromise	AppletControl	Run profile and launch	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Window Discovery	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	Command-Line Interface	Accessibility Features	Accessibility Features	Binary Padding	Batch History	Blade Forge	Browser Bookmarks	Clipboard Data	Data Compressed	Communication Through Removable Media
Hardware Addition	Control Panel Items	AppCert DLLs	AppCert DLLs	BITS Jobs	Credential Dumping	Credential Discovery	Distributed Component Object Model	Data from Information Repositories	Data Transfer Size Limits	Connection Proxy
Replication Through Removable Media	Dynamic Data Exchange	Application Shimming	Application Shimming	Clear Command History	Credentials in Files	Credentials in Registry	Exploitation of Remote Services	Data from Local System	Exfiltration Over Command and Control Channel	Custom Command and Control Protocol
Seaphishing Attachment	Execution through API	Authentication Package	Bypass User Account Control	Code Signing	Application for Credential Access	Network Share Discovery	Exploitation of Remote Services	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Seaphishing Link	Exploitation through Module Load	BitLocker	DLL Search Order Hijacking	Component Firmware	Forced Authentication	Password Policy Discovery	Pass the Hash	Remote Desktop Protocol	Exfiltration Over Other Network Medium	Data Encoding
Seaphishing via Service	Graphical User Interface	Browser Extensions	DLL Search Order Hijacking	Component Object Model Hijacking	Hooking	Peripheral Device Discovery	Pass the Ticket	Data from Removable Media	Domain Fronting	Data Obfuscation
Supply Chain Compromise	Trustful Relationship	Change Default File Association	Dynamic Data Exchange	Control Panel Items	Input Capture	Remote File Copy	Remote File Copy	Data Staged	Fallback Channels	
Valid Accounts	Launchd	Component Object Model Hijacking	Extra Window Memory Injection	Deobfuscate/Decode Files or Information	Input Prompt	Permission Groups Discovery	Remote Services	Email Collection	Exfiltration Over Physical Medium	Multi-Stage Attack
	Local Job Scheduling	Create Account	Disabling Security Tools	Disabling Security Tools	Input Prompt	Process Discovery	Input Capture	Scheduled Transfer	Scheduled Transfer	Multi-Stage Channels
	LSASS Driver	DLL Search Order Hijacking	File System Permissions	DLL Search Order Hijacking	LLMNR/NB-NS Poisoning	Quota Registry	Shared Webroot	Screen Capture	Multi-Stage Communication	Multi-Stage Encryption
	PowerShell	DLL Hijacking	Image File Execution Options Injection	DLL Side-Loading	Network Sniffing	System Software Discovery	Shared Webroot	Video Capture	Port Knocking	Remote Access Tools
	Regsvr32	External Remote Services	Launch Daemon	Exploitation for Defense Evasion	Network Sniffing	System Software Discovery	Shared Webroot	Video Capture	Port Knocking	Remote File Copy
	Rundll32	File System Permissions	Launch Daemon	Exploitation for Defense Evasion	Network Sniffing	System Software Discovery	Shared Webroot	Video Capture	Port Knocking	Remote File Copy
	Scheduled Task	Hidden Files and Directories	Path Interception	File Deletion	Application Through Removable Media	System Network Configuration	Shared Webroot	Video Capture	Port Knocking	Remote File Copy
	Service Execution	Hidden Files and Directories	Path Interception	File Deletion	Application Through Removable Media	System Network Configuration	Shared Webroot	Video Capture	Port Knocking	Remote File Copy
	Signed Binary Proxy Execution	Hooking	Port Monitors	Hidden Files and Directories	Application Through Removable Media	System Network Configuration	Shared Webroot	Video Capture	Port Knocking	Remote File Copy
	Signed Script Proxy Execution	Hypervisor	Process Injection	Hidden Users	Application Through Removable Media	System Network Configuration	Shared Webroot	Video Capture	Port Knocking	Remote File Copy
	Source	Kernel Modules and Extensions	Service Registry Permissions	Hidden Windows	Application Through Removable Media	System Network Configuration	Shared Webroot	Video Capture	Port Knocking	Remote File Copy
	Space after Filename	Launch Agent	Weakness	HISTCONTROL	Application Through Removable Media	System Network Configuration	Shared Webroot	Video Capture	Port Knocking	Remote File Copy
	Third-party Software	Launch Daemon	Setuid and Setgid	Image File Execution Options Injection	Application Through Removable Media	System Network Configuration	Shared Webroot	Video Capture	Port Knocking	Remote File Copy
	Trap	Launchd	Setuid and Setgid	Indicator Blocking	Application Through Removable Media	System Network Configuration	Shared Webroot	Video Capture	Port Knocking	Remote File Copy
	Trusted Developer	Launchd	Setuid and Setgid	Indicator Blocking	Application Through Removable Media	System Network Configuration	Shared Webroot	Video Capture	Port Knocking	Remote File Copy

Une formation
Alphorm.com



Appréhender le reporting



Hamza KONDAH

Une formation
Alphorm.com



Plan

Notion de Killchain
Phishing : Kill Chain (Avancée)
Lab : MITRE - ATT&CK

Une formation
Alphorm.com



Notion de killchain

«**Kill chain**» est un terme utilisé à l'origine par les militaires pour définir les étapes qu'un ennemi utilise pour attaquer une cible

En **2011**, **Lockheed Martin** a publié un article définissant une Cyber Kill Chain



Notion de killchain

Similaire dans son concept au modèle militaire, il définit les étapes utilisées par les cyber-attaquants dans les cyber-attaques d'aujourd'hui



Notion de killchain

Plus vous pouvez intercepter les méchants, plus vous avez des chances de les refuser de leur objectif ou de les forcer à faire suffisamment de bruit où vous pouvez plus facilement les détecter

Une formation
Alphorm.com



Phishing : Kill Chain (Avancée)



Une formation
Alphorm.com



Lab : le MITRE - ATT&CK

Layer											Technique controls										
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control											
10 items	31 items	56 items	28 items	59 items	20 items	19 items	17 items	13 items	9 items	21 items											
Drive-by Compromise	AppletScript	Task profile and history	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppletScript	Audio Capture	Automated Exfiltration	Commonly Used Port											
Exploit Public-Facing Application	CMSTP	Accessibility Features	Binary Padding	Binary Padding	Batch History	Batch History	Batch History	Clipboard Data	Data Compressed	Encryption Through Removable Media											
Hardware Addition	Control Panel Items	AppCert DLLs	AppCert DLLs	AppCert DLLs	BITS Jobs	BITS Jobs	BITS Jobs	Data from Information Repositories	Data Encrypted	Connection Proxy											
Replication Through Removable Media	Dynamic Data Exchange	Application Shim	Application Shim	Application Shim	Credential Dumping	Credential Dumping	Credential Dumping	Data from Local System	Custom Command and Control Protocol	Custom Cryptographic Protocol											
Spearinghoning Attachment	Execution through API	Authentication Package	Authentication Package	Authentication Package	Clear Command History	Clear Command History	Clear Command History	Exfiltration Over Alternative Protocol	Exfiltration Over Alternative Protocol	Exfiltration Over Alternative Protocol											
Spearinghoning Link	Execution through Modules Load	BITS Jobs	BITS Jobs	BITS Jobs	Code Signing	Code Signing	Code Signing	Exfiltration Over Network Share	Exfiltration Over Network Share	Exfiltration Over Network Share											
Spearinghoning via Service	Exploitation for Client Execution	Browser Extensions	Browser Extensions	Browser Extensions	Component Object Model Hacking	Component Object Model Hacking	Component Object Model Hacking	Exfiltration Over Remote Desktop Protocol	Exfiltration Over Remote Desktop Protocol	Exfiltration Over Remote Desktop Protocol											
Supply Chain Compromise	Graphical User Interface	Change Default File Association	Change Default File Association	Change Default File Association	Control Panel Items	Control Panel Items	Control Panel Items	Exfiltration Over Other Network Medium	Exfiltration Over Other Network Medium	Exfiltration Over Other Network Medium											
Trusted Relationship	Invalidity	Component Object Model Hacking	Component Object Model Hacking	Component Object Model Hacking	Disabling Security Tools	Disabling Security Tools	Disabling Security Tools	Exfiltration Over Physical Medium	Exfiltration Over Physical Medium	Exfiltration Over Physical Medium											
Valid Accounts	Launch	Create Account	Create Account	Create Account	Extra Window Memory Injection	Extra Window Memory Injection	Extra Window Memory Injection	Exfiltration Over Scheduled Transfer	Exfiltration Over Scheduled Transfer	Exfiltration Over Scheduled Transfer											
	Local Job Scheduling	LSASS Driver	LSASS Driver	LSASS Driver	File System Permissions	File System Permissions	File System Permissions	Exfiltration Over Shared Webroot	Exfiltration Over Shared Webroot	Exfiltration Over Shared Webroot											
	PowerShell	Registry/Regasm	Registry/Regasm	Registry/Regasm	Image File Execution Options	Image File Execution Options	Image File Execution Options	Exfiltration Over Third-party Software	Exfiltration Over Third-party Software	Exfiltration Over Third-party Software											
	Regedit32	External Remote Services	External Remote Services	External Remote Services	Launch Daemon	Launch Daemon	Launch Daemon	Exfiltration Over Windows Admin Shares	Exfiltration Over Windows Admin Shares	Exfiltration Over Windows Admin Shares											
	Rundll32	File System Permissions	File System Permissions	File System Permissions	Path Interception	Path Interception	Path Interception	Exfiltration Over System Network Connections	Exfiltration Over System Network Connections	Exfiltration Over System Network Connections											
	Scheduled Task	Hidden Files and Directories	Hidden Files and Directories	Hidden Files and Directories	Process Injection	Process Injection	Process Injection	Exfiltration Over System Service Discovery	Exfiltration Over System Service Discovery	Exfiltration Over System Service Discovery											
	Scripting	Hidden Files and Directories	Hidden Files and Directories	Hidden Files and Directories	Service Registry	Service Registry	Service Registry	Exfiltration Over System Time Discovery	Exfiltration Over System Time Discovery	Exfiltration Over System Time Discovery											
	Service Execution	Hooking	Hooking	Hooking	System Logical Offsets	System Logical Offsets	System Logical Offsets	Exfiltration Over Web Service	Exfiltration Over Web Service	Exfiltration Over Web Service											
	Signal Binary Proxy Execution	Hypervisor	Hypervisor	Hypervisor	System Time Discovery	System Time Discovery	System Time Discovery	Exfiltration Over Web Service	Exfiltration Over Web Service	Exfiltration Over Web Service											
	Signed Script Proxy Execution	Image File Execution Options Injection	Image File Execution Options Injection	Image File Execution Options Injection	System Time Discovery	System Time Discovery	System Time Discovery	Exfiltration Over Web Service	Exfiltration Over Web Service	Exfiltration Over Web Service											
	Source	Kernel Modules and Extensions	Kernel Modules and Extensions	Kernel Modules and Extensions	System Time Discovery	System Time Discovery	System Time Discovery	Exfiltration Over Web Service	Exfiltration Over Web Service	Exfiltration Over Web Service											
	Space after Filename	Launch Agent	Launch Agent	Launch Agent	System Time Discovery	System Time Discovery	System Time Discovery	Exfiltration Over Web Service	Exfiltration Over Web Service	Exfiltration Over Web Service											
	Third-party Software Trap	Launch Daemon	Launch Daemon	Launch Daemon	System Time Discovery	System Time Discovery	System Time Discovery	Exfiltration Over Web Service	Exfiltration Over Web Service	Exfiltration Over Web Service											
	Trusted Developer	Launch	Launch	Launch	System Time Discovery	System Time Discovery	System Time Discovery	Exfiltration Over Web Service	Exfiltration Over Web Service	Exfiltration Over Web Service											

Une formation
Alphorm.com



Détecter les attaques par dénis de service et bruteforcing



Hamza KONDAH

Une formation
Alphorm.com



Plan

Le dénis de service

Le dénis de service distribué

SYN FLOODING

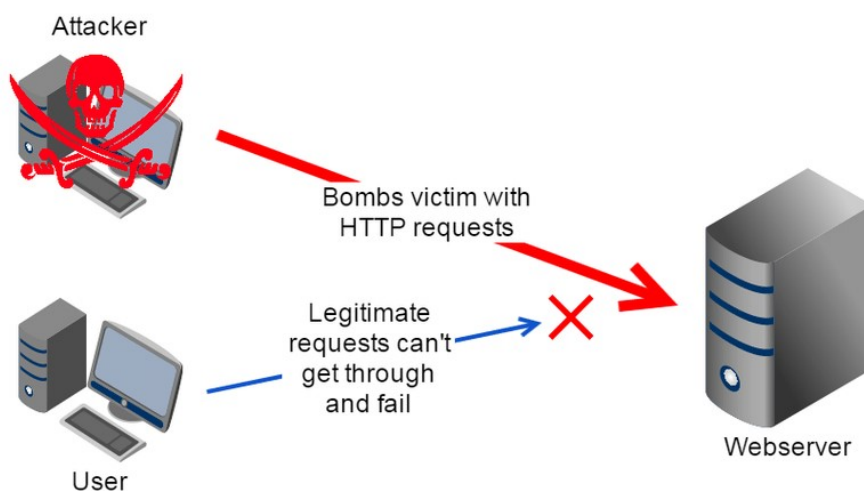
Le bruteforcing

Lab : Dos et bruteforcing

Une formation
Alphorm.com



Le dénis de service



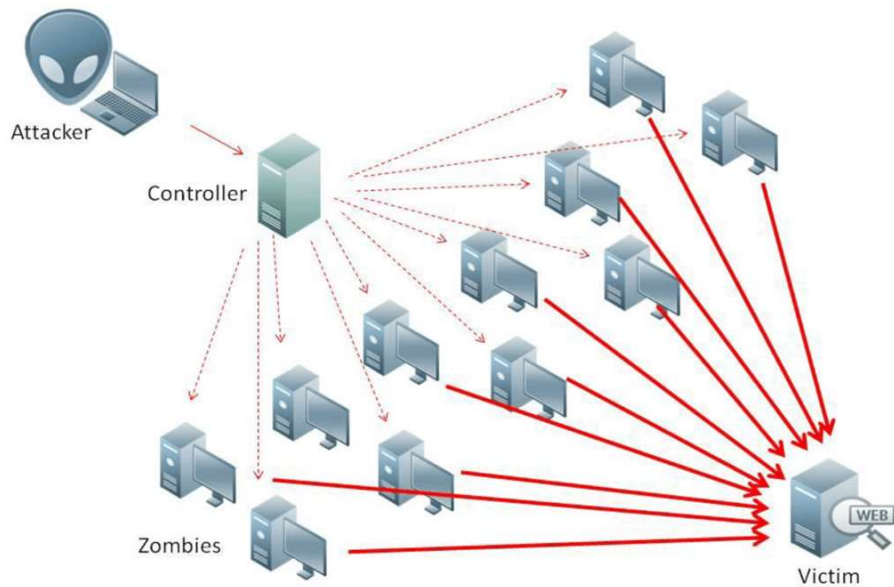
Une formation
Alphorm.com

WIRESHARK

L'essentiel

Une formation
Alphorm.com

Le dénis de service distribué

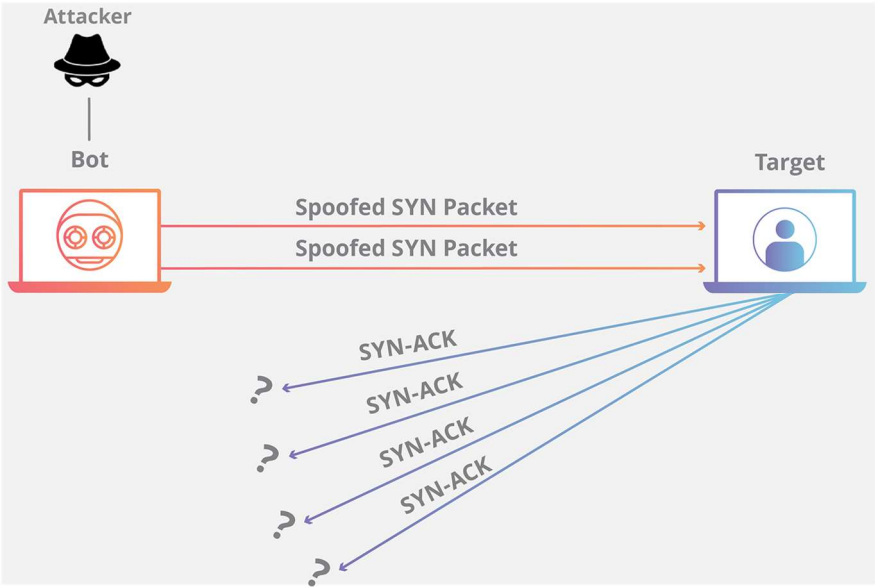


WIRESHARK

L'essentiel

Une formation
Alphorm.com

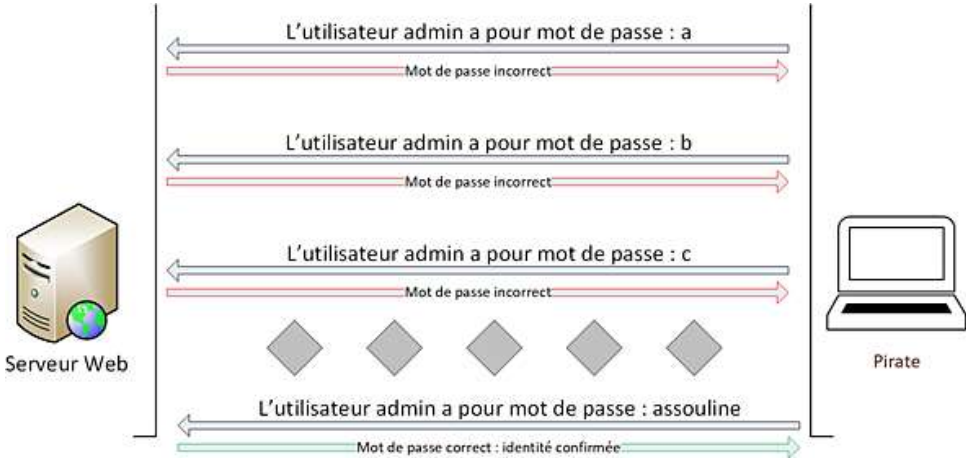
SYN FLOODING





L'essentiel

Le bruteforcing



Une formation
Alphorm.com



L'essentiel

Lab : Dos et bruteforcing

Filter: ftp.request.command						Expression...	Clear	Apply	Save
No.	Time	Source	Destination	Protocol	Info				
25	*REF*	192.168.10.129	192.168.10.133	FTP	Request: USER admin				
28	0.003557	192.168.10.129	192.168.10.133	FTP	Request: PASS anonymous				
30	0.006026	192.168.10.129	192.168.10.133	FTP	Request: USER admin				
32	0.009513	192.168.10.129	192.168.10.133	FTP	Request: PASS PACKT				
34	0.021116	192.168.10.129	192.168.10.133	FTP	Request: USER admin				
36	0.031096	192.168.10.129	192.168.10.133	FTP	Request: PASS packtpub				
39	0.032572	192.168.10.129	192.168.10.133	FTP	Request: USER admin				
48	0.048233	192.168.10.129	192.168.10.133	FTP	Request: USER admin				
51	0.060492	192.168.10.129	192.168.10.133	FTP	Request: PASS ftppassword				

Une formation
Alphorm.com



Une formation
Alphorm.com

Détecter les attaques DHCP Starvation



Hamza KONDAH



Une formation
Alphorm.com

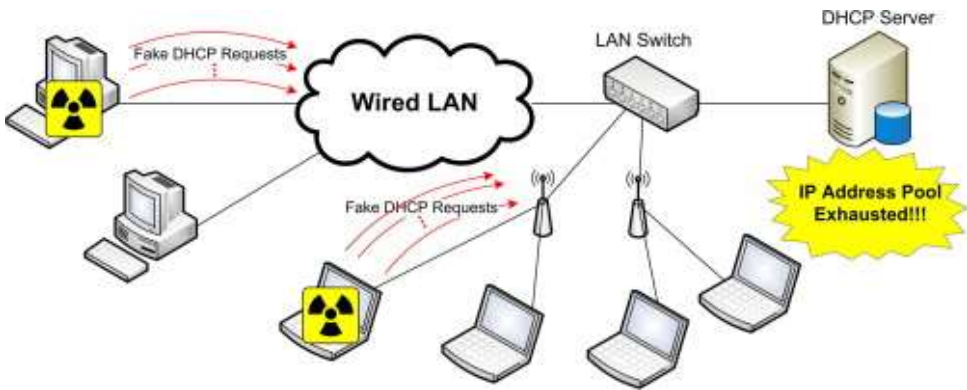
Plan

DHCP Starvation

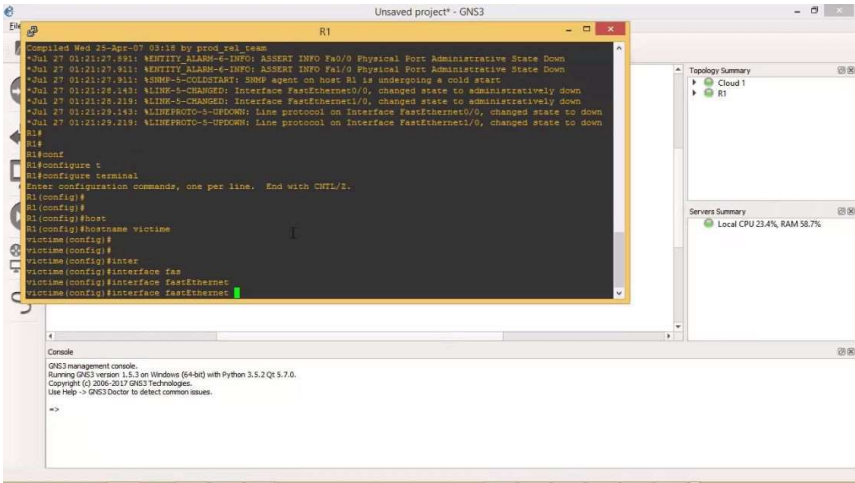
Lab : DHCP Starvation



DHCP Starvation



Lab : DHCP Starvation





Détecter les attaques ARP spoofing



Hamza KONDAH

Une formation
Alphorm.com



Plan

L' ARP spoofing

Le MiTM

Lab : ARP spoofing

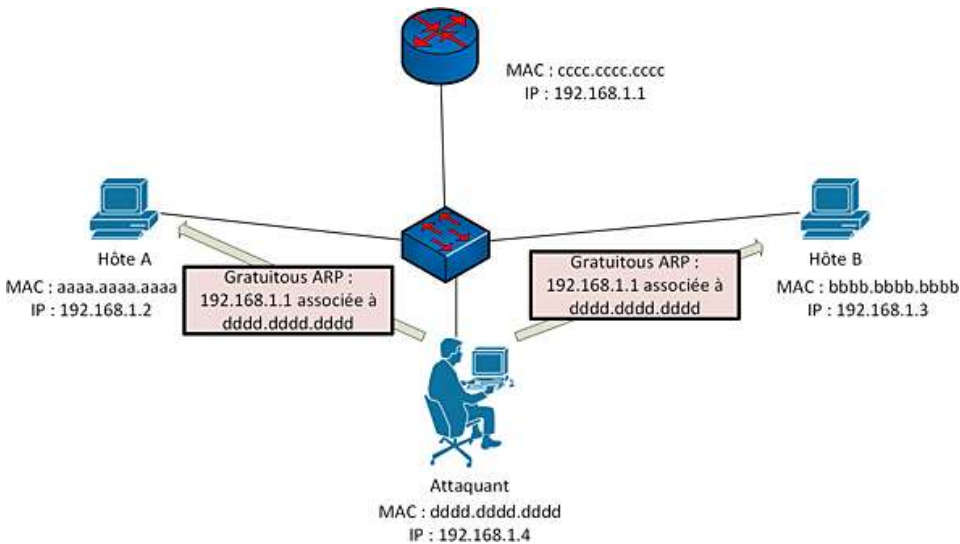
Une formation
Alphorm.com



L'essentiel

Une formation
Alphorm.com

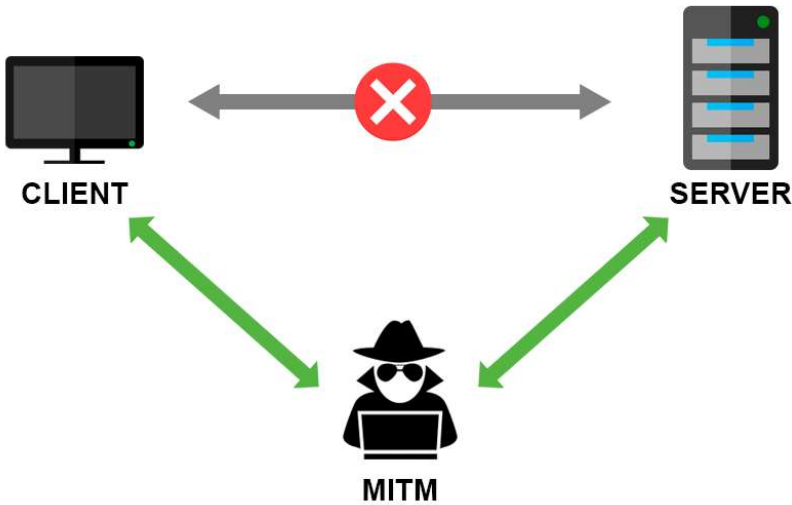
L' ARP spoofing



L'essentiel

Une formation
Alphorm.com

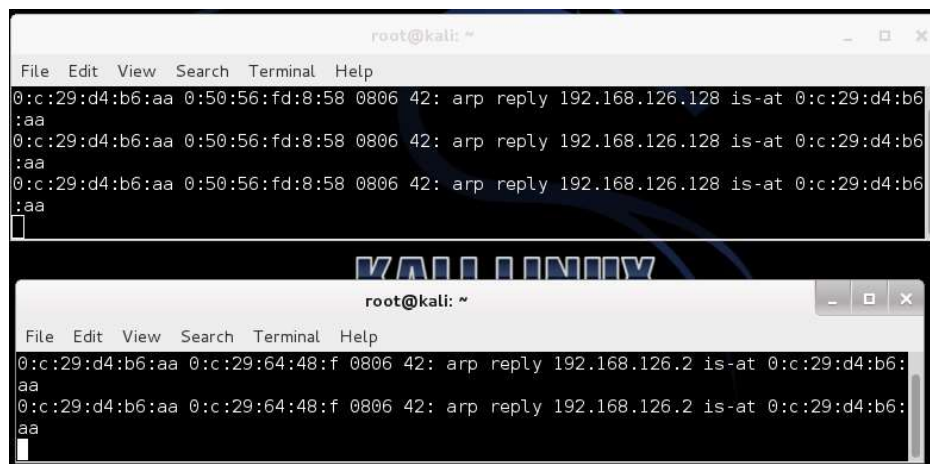
Le MiTM



WIRESHARK

L'essentiel

Lab : ARP spoofing



```
root@kali: ~  
File Edit View Search Terminal Help  
0:c:29:d4:b6:aa 0:50:56:fd:8:58 0806 42: arp reply 192.168.126.128 is-at 0:c:29:d4:b6:aa  
0:c:29:d4:b6:aa 0:50:56:fd:8:58 0806 42: arp reply 192.168.126.128 is-at 0:c:29:d4:b6:aa  
0:c:29:d4:b6:aa 0:50:56:fd:8:58 0806 42: arp reply 192.168.126.128 is-at 0:c:29:d4:b6:aa  
[ ]  
KALI LINUX  
root@kali: ~  
File Edit View Search Terminal Help  
0:c:29:d4:b6:aa 0:c:29:64:48:f 0806 42: arp reply 192.168.126.2 is-at 0:c:29:d4:b6:aa  
0:c:29:d4:b6:aa 0:c:29:64:48:f 0806 42: arp reply 192.168.126.2 is-at 0:c:29:d4:b6:aa  
[ ]
```

Une formation
Alphorm.com

WIRESHARK

L'essentiel

Détecter les attaques les exfiltrations de data



Hamza KONDAH

Une formation
Alphorm.com



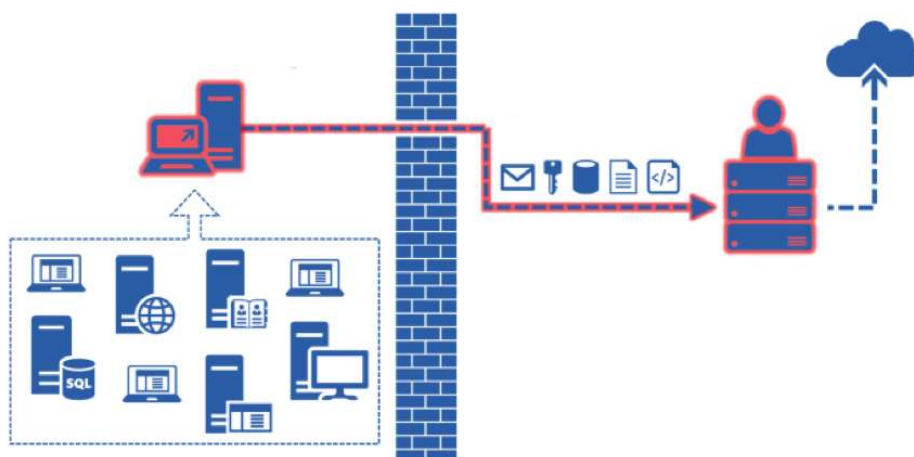
Plan

L'exfiltration de données Lab : L'exfiltration de data

Une formation
Alphorm.com



L'exfiltration de données



Une formation
Alphorm.com



Méthodes ouvertes

Téléchargements

Téléchargements HTTP / HTTPS

FTP

Email

Messagerie instantanée

Partage de fichiers P2P

Une formation
Alphorm.com



Méthodes cachées

SSH

VPN

Tunnellisation de protocole

Téléchargements de stockage
dans le cloud

Stéganographie

Chaîne de Timing

Une formation
Alphorm.com



Lab : L'exfiltration de data

analysis.pcap									
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help									
Apply a display filter ... <Ctrl>F									
No.	Time	Source	Destination	Protocol	Length	Info			
1	0.000000	192.168.1.24	192.168.1.16	ICMP	542	Echo (ping) request id=0xdd7a, seq=0/0, ttl=64 (reply in 2)			
2	0.000290	192.168.1.16	192.168.1.24	ICMP	542	Echo (ping) reply id=0xdd7a, seq=0/0, ttl=64 (request in 1)			
3	1.000291	192.168.1.24	192.168.1.16	ICMP	542	Echo (ping) request id=0xdd7a, seq=256/1, ttl=64 (reply in 4)			
4	1.000593	192.168.1.16	192.168.1.24	ICMP	542	Echo (ping) reply id=0xdd7a, seq=256/1, ttl=64 (request in 3)			
5	2.000882	192.168.1.24	192.168.1.16	ICMP	542	Echo (ping) request id=0xdd7a, seq=512/2, ttl=64 (reply in 6)			
6	2.001200	192.168.1.16	192.168.1.24	ICMP	542	Echo (ping) reply id=0xdd7a, seq=512/2, ttl=64 (request in 5)			
7	3.001253	192.168.1.24	192.168.1.16	ICMP	542	Echo (ping) request id=0xdd7a, seq=768/3, ttl=64 (reply in 8)			
8	3.001566	192.168.1.16	192.168.1.24	ICMP	542	Echo (ping) reply id=0xdd7a, seq=768/3, ttl=64 (request in 7)			
9	4.001422	192.168.1.24	192.168.1.16	ICMP	542	Echo (ping) request id=0xdd7a, seq=1024/4, ttl=64 (reply in 10)			
10	4.001669	192.168.1.16	192.168.1.24	ICMP	542	Echo (ping) reply id=0xdd7a, seq=1024/4, ttl=64 (request in 9)			
11	5.001553	192.168.1.24	192.168.1.16	ICMP	542	Echo (ping) request id=0xdd7a, seq=1280/5, ttl=64 (reply in 12)			
12	5.001878	192.168.1.16	192.168.1.24	ICMP	542	Echo (ping) reply id=0xdd7a, seq=1280/5, ttl=64 (request in 11)			
13	6.077653	192.168.1.24	192.168.1.16	ICMP	542	Echo (ping) request id=0xdd7a, seq=1536/6, ttl=64 (reply in 14)			
14	6.078037	192.168.1.16	192.168.1.24	ICMP	542	Echo (ping) reply id=0xdd7a, seq=1536/6, ttl=64 (request in 13)			
15	7.078260	192.168.1.24	192.168.1.16	ICMP	542	Echo (ping) request id=0xdd7a, seq=1792/7, ttl=64 (reply in 16)			
16	7.078532	192.168.1.16	192.168.1.24	ICMP	542	Echo (ping) reply id=0xdd7a, seq=1792/7, ttl=64 (request in 15)			
17	8.078866	192.168.1.24	192.168.1.16	ICMP	542	Echo (ping) request id=0xdd7a, seq=2048/8, ttl=64 (reply in 18)			



Détecter des trafics inconnus



Hamza KONDAH



Une formation
Alphorm.com

Détecter les Scans et attaques réseau



Hamza KONDAH



Une formation
Alphorm.com

Plan

- Détection Ping sweep
- Détection ARP SWEEP
- Détection MAC Flooding
- Détection de scans
- Reconnaissance passive d'os



L'essentiel

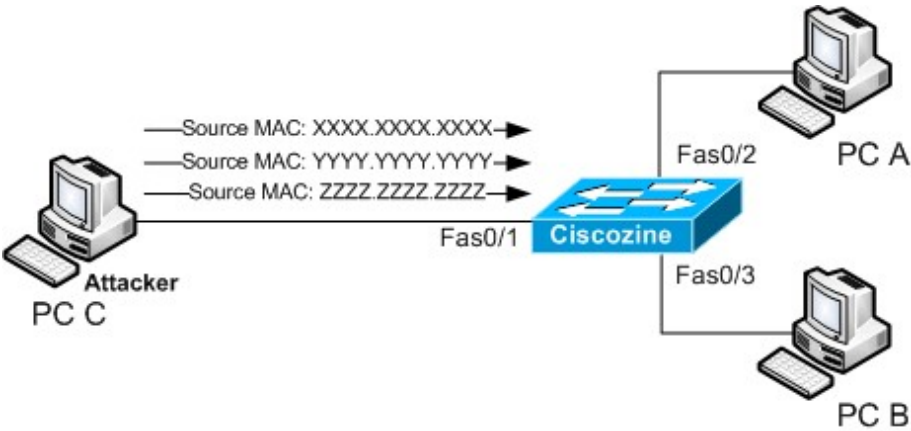
Détection Ping sweep

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	Apple_b9:53:ec	Broadcast	ARP	42	Who has 192.168.1.110? Tell 192.168.1.106
2	0.004128000	Apple_b9:53:ec	Broadcast	ARP	42	Who has 192.168.1.109? Tell 192.168.1.106
3	0.008476000	Apple_b9:53:ec	Broadcast	ARP	42	Who has 192.168.1.108? Tell 192.168.1.106
4	0.012705000	Apple_b9:53:ec	Broadcast	ARP	42	Who has 192.168.1.107? Tell 192.168.1.106
5	0.023785000	192.168.1.106	192.168.1.105	ICMP	98	Echo (ping) request id=0x11a8, seq=1/256, ttl=64
6	0.027774000	192.168.1.104	192.168.1.106	ICMP	98	Echo (ping) reply id=0x11a3, seq=1/256, ttl=64
7	0.031652000	Apple_b9:53:ec	Broadcast	ARP	42	Who has 192.168.1.103? Tell 192.168.1.106
8	0.035462000	192.168.1.106	192.168.1.102	ICMP	98	Echo (ping) request id=0x1199, seq=1/256, ttl=64
9	0.040423000	192.168.1.106	192.168.1.101	ICMP	98	Echo (ping) request id=0x1194, seq=1/256, ttl=64
10	0.047374000	192.168.1.106	192.168.1.100	ICMP	98	Echo (ping) request id=0x118f, seq=1/256, ttl=64
11	0.122601000	LiteonTe_fa:5e:b4	Broadcast	ARP	42	Who has 192.168.1.106? Tell 192.168.1.105
12	0.124979000	Apple_b9:53:ec	LiteonTe_fa:5e:b4	ARP	42	192.168.1.106 is at d8:bb:2c:b9:53:ec
13	0.125118000	192.168.1.100	192.168.1.106	ICMP	98	Echo (ping) reply id=0x118f, seq=1/256, ttl=64
14	0.126606000	192.168.1.105	192.168.1.106	ICMP	98	Echo (ping) reply id=0x11a8, seq=1/256, ttl=64
15	0.131304000	192.168.1.101	192.168.1.106	ICMP	98	Echo (ping) reply id=0x1194, seq=1/256, ttl=64
16	0.438404000	Apple_b9:53:ec	Zte_07:73:6c	ARP	42	Who has 192.168.1.1? Tell 192.168.1.106
17	0.528177000	Zte_07:73:6c	Apple_b9:53:ec	ARP	42	192.168.1.1 is at d0:5b:a8:07:73:6c



L'essentiel

Détection MAC flooding





Reconnaissance passive d'os

Protocol Header	Field	Default Value	Operating System
IP	Initial Time to Live	64	Nmap, BSD, Mac OS 10, Linux
		128	Novell, Windows
		255	CISCO IOS, Palm OS, Solaris
IP	Don't Fragment Flag	Set	BSD, Mac OS 10, Linux, Novell, Windows, Palm OS, Solaris
		Not set	Nmap, CISCO IOS
TCP	Maximum Segment Size	0	Nmap
		1440	Windows, Novell
		1460	BSD, Mac OS 10, Linux, Solaris
TCP	Window Size	1024-4096	Nmap
		65535	BSD, Mac OS 10
		2920-5840	Linux
		16384	Novell
		4128	Cisco IOS
		24820	Solaris
		Variable	Windows
TCP	Sack OK	Set	Linux, Windows. Open BSD
		Not set	Nmap, FreeBSD, MacOS 10, Novell,Cisco IOS, Solaris

Une formation
Alphorm.com

Détection de scans



Une formation
Alphorm.com

Maîtriser les NIDS : **use case Snort**



Hamza KONDAH



Une formation
Alphorm.com

Plan

IDS : Présentation et définition

IPS : Définition

Les faux-positifs & faux négatifs

Terminologie

Les NIDS

Snort : présentation générale



IDS: Présentation

Il existe trois types de systèmes de détection ou de prévention d'intrusion

HIDS (*Host Intrusion Detection System*)

NIDS (*Network Intrusion Detection System*)

IDS hybrides

KIDS/KIPS : IPS noyau

IPS (Système de Prévention d'Intrusion)

Une formation
Alphorm.com



IDS : Définition

IDS = *Système de Détection d'Intrusion* (en anglais IDS = Intrusion Detection System)

Mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte).

Une formation
Alphorm.com



IPS : Définition

IPS = *Système de Prévention d'Intrusion* (en anglais IPS : Intrusion Prevention System) :
Ensemble de composants logiciels et matériels dont la fonction principale est d'empêcher toute activité suspecte détectée au sein d'un système



Les faux-positifs & faux négatifs

Fausse alerte levée par l'ids
*Détection en absence d'attaque,
alarme générée par un IDS pour
un évènement légal*



Les faux-positifs

Attaque qui n'a pas été repérée par l'ids

Absence de détection en présence d'attaque, non génération d'alarme par un IDS pour un évènement illégal

Une formation
Alphorm.com



Terminologie

Evasion

Technique utilisée pour dissimuler une attaque et faire en sorte qu'elle ne soit pas décelée par l'IDS

Sonde

Composant de l'architecture IDS qui collecte les informations brutes

Une formation
Alphorm.com



Une formation
Alphorm.com

Terminologie

Log

Ligne d'un fichier d'un logiciel qui enregistre les données transitant sur un système pour surveiller ou faire des statistiques

Fichier log

Contient les événements produits sur un système



Une formation
Alphorm.com

Terminologie

Signature d'attaque

Une signature d'attaque est un motif (patron de comportement) représentant toute l'information concernant une attaque connue



Les NIDS

NIDS (*Network Intrusion Detection System*)

Le rôle essentiel d'un NIDS est l'analyse et l'interprétation des paquets circulant sur ce réseau

Une formation
Alphorm.com



Les NIDS

Il peut détecter en temps réel une attaque s'effectuant sur l'une de vos machines

Il contient une base de données avec tous les codes malicieux et peut détecter leurs envois sur une des machines

Une formation
Alphorm.com



Snort : présentation générale

Snort est un NIDS écrit par Martin Roesch, disponible sous licence GNU, son code source est accessible et modifiable à partir de l'URL :

<http://www.snort.org>

Une formation
Alphorm.com



Snort : Présentation générale

SNORT permet d'analyser le trafic réseau de type IP, compare ce trafic à des règles déjà définies par l'utilisateur et établit des actions à exécuter

Une formation
Alphorm.com





Maîtriser le NIDS Snort



Hamza KONDAH

Une formation
Alphorm.com



Plan

- Commandes Snort
- Options Snort
- Structure de règles Snort
- Les règles Snort
- Actions Snort
- Options de règles

Une formation
Alphorm.com



Commandes Snort

```
# snort -v
```

```
# snort -vd
```

```
# snort -vde
```

```
# snort -f
```

Une formation
Alphorm.com



Commandes Snort

```
# snort -de -l /var/log/too.log
```

(stockage de la capture dans le fichier too.log)

```
# snort -de -l /var/log/today.log -  
h 192.168.1.0/24
```

(spécification du réseau concerné)

Une formation
Alphorm.com



Commandes Snort

Détection d'intrusion en réseau (IDS)

```
# snort -D -i le0 -c /etc/snort.rules -A fast
```

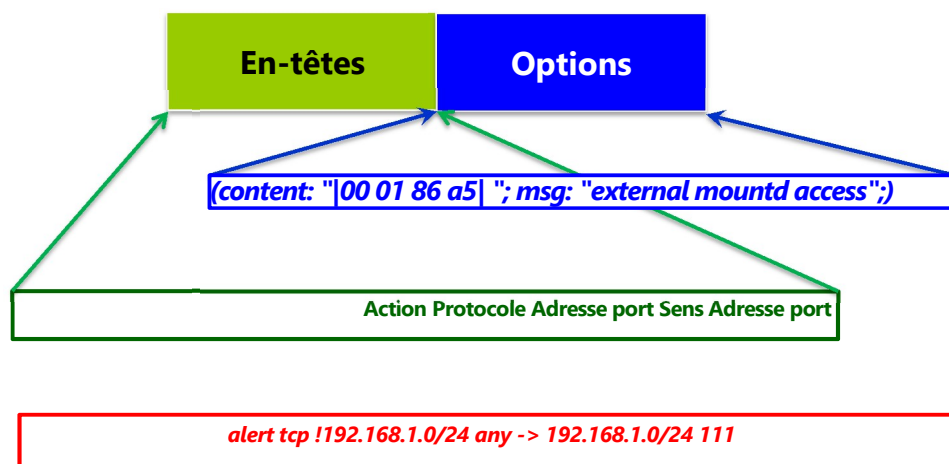


Options Snort

-D	lancement en mode daemon	-S	génère les alertes vers syslog
-i	pour désigner l'interface	-l	suivi du fichier pour les logs
-c	suivi du fichier des règles	-b	format binaire
-A	mode d'alerte (fast, full, none)		



Structure de règles Snort



Une formation
Alphorm.com



Snort : exemples de règles

Pour détecter les tentatives de login sous l'utilisateur **root**, pour le protocole ftp (port 21) :

```
alert tcp any any -> 192.168.1.0/24 21  
(content: "USER root"; nocase; msg: "FTP  
root user access attempt");
```

Une formation
Alphorm.com



Les règles Snort

Les en-têtes de règles
Contiennent les informations sur les paquets à surveiller et que faire s'ils se présenteraient
L'action de règle



Les règles Snort

Alert	Génère une alerte en utilisant la méthode d'alerte sélectionnée, et alors journalise le paquet
Log	Journalise le paquet
Pass	Ignore le paquet
Activate	Alerte et alors active une autre règle dynamic
Dynamic	Reste passive jusqu'à être activée par une règle activée, alors agit comme une règle log



Une formation
Alphorm.com

Les règles Snort

Trois actions supplémentaires disponibles en mode in-line :

Drop	Indique à iptables de rejeter le paquet et de le loguer
Reject	Indique à iptables de rejeter le paquet, de le loguer et d'envoyer un TCP reset si le protocole est TCP, ou un ICMP port unreachable si le protocole est UDP
Sdrop	Indique à iptables de rejeter le paquet et de ne pas le loguer



Une formation
Alphorm.com

Actions Snort

Il existe 5 actions dans Snort :

Alert	Génère une alerte en utilisant la méthode d'alerte sélectionnée, et alors journalise le paquet
Log	Journalise le paquet
Pass	Ignore le paquet
Activate	Alerte et alors active une autre règle dynamique
Dynamic	Reste passive jusqu'à être activée par une règle activée, alors agit comme une règle log

Options de règles

MSG	Affiche un message dans les alertes et journalise les paquets
LOGTO	Journalise le paquet dans un fichier nommé par l'utilisateur au lieu de la sortie standard
CONTENT	Recherche un motif dans la charge d'un packet
OFFSET	Modifie l'option content , fixe le décalage du début de la tentative de correspondance de motif
SESSION	Affiche l'information de la couche applicative pour la session donnée
FLOW	Permet de fixer le sens d'un flux , l'état de la connexion , ...
REACT	Réponse active (bloque les site web)
IP_PROTO	Permet de définir un protocole au dessus de l' IP
DEPTH	Modifie l'option content, fixe la profondeur maximale de recherche pour la tentative de correspondance de motif
CLASSTYPE	Assigne un classification à l'attaque (virus, cheval de troie, ...)
NOCASE	Correspond à la procédure de chaîne de contenus sans sensibilité aux différences majuscules / minuscules



Maîtriser l'analyse à grande échelle : **use case moloch et Wireshark**



Hamza KONDAH



Une formation
Alphorm.com

Conclusion et perspectives de la formation



Hamza KONDAH



Une formation
Alphorm.com

Bilan

Manipuler les différentes fonctionnalités
Maîtriser l'analyse protocolaire
Maîtriser l'analyse avancé de flux réseaux
Découvrir l'analyse forensique des réseaux
Identifier des attaques sur le réseau
Découvrir les outils complémentaires



Prochaines formations

SIEM

IoT et systèmes embarqués

Pentest Active Directory

Sécurisation d'infrastructures

Pentest des réseaux sans fils

Une formation
Alphorm.com



Prochainement



PENTESTING
ACTIVE DIRECTORY

Une formation
Alphorm.com