

Litter,pcap(DNS 隧道)

Sherlock Scenario

Khalid has just logged onto a host that he and his team use as a testing host for many different purposes. It's off their corporate network but has access to lots of resources on the network. The host is used as a dumping ground for a lot of people at the company, but it's very useful, so no one has raised any issues. Little does Khalid know; the machine has been compromised and company information that should not have been on there has now been stolen – it's up to you to figure out what has happened and what data has been taken.

* * *

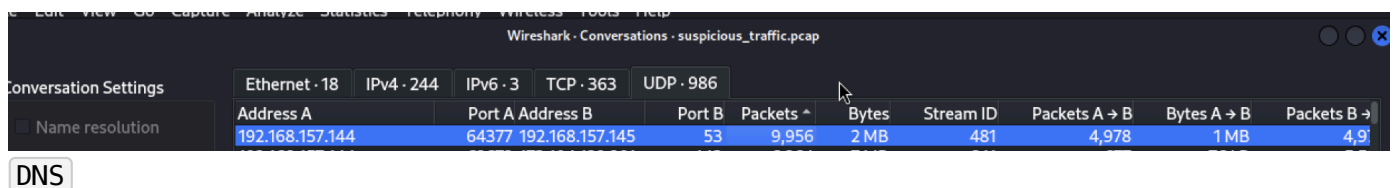
About Litter

A commonly used off-network host, which serves as a testing ground for various purposes, has been breached. The host, while not on the corporate network, has extensive access to numerous resources, making it a significant vulnerability point. It has come to light that company information, which should not have been on this host, has been stolen. As the forensic investigator, your mission is multi-fold: you must unearth how this breach occurred, what company data has been exfiltrated, and whether the attacker employed any form of tunneling for the intrusion or data theft. This task demands your advanced understanding of cybersecurity, particularly network tunneling techniques, and your ability to perform thorough digital forensics to restore security and prevent further data loss.

文件 : `suspicious_traffic.pcap`

Task 1

At a glance, what protocol seems to be suspect in this attack?



Task 2

There seems to be a lot of traffic between our host and another, what is the IP address of the suspect host?

同上

192.168.157.145

Task 3

What is the first command the attacker sends to the client?

設定 `udp.length > 200` 是因為 UDP 封包的負載部分需要超過 200 個位元組才能包含足夠的資料來顯示文字內容。

```
ip.src_host== 192.168.157.145 && ip.dst_host== 192.168.157.144 &&
udp.length >200
```

進行時間排序，我找到第二個開始出入指令

No.	Time	Source	Destination	Protocol	Length	Info
13777	2023-04-30 10:31:01.271225	192.168.157.145	192.168.157.144	DNS	339	Standard query response 0x0940 CNAME
13939	2023-04-30 10:31:17.797493	192.168.157.145	192.168.157.144	DNS	239	Standard query response 0x650c TXT 3
13969	2023-04-30 10:31:21.581279	192.168.157.145	192.168.157.144	DNS	341	Standard query response 0x54fa MX 70
13971	2023-04-30 10:31:21.690795	192.168.157.145	192.168.157.144	DNS	341	Standard query response 0x6fa3 MX 10
13973	2023-04-30 10:31:21.800093	192.168.157.145	192.168.157.144	DNS	341	Standard query response 0x6f5b MX 30
13981	2023-04-30 10:31:21.925784	192.168.157.145	192.168.157.144	DNS	341	Standard query response 0x3242 MX 20
13983	2023-04-30 10:31:22.032577	192.168.157.145	192.168.157.144	DNS	341	Standard query response 0x31b9 MX 51
13987	2023-04-30 10:31:22.141619	192.168.157.145	192.168.157.144	DNS	341	Standard query response 0x3555 MX 50
13989	2023-04-30 10:31:22.255545	192.168.157.145	192.168.157.144	DNS	320	Standard query response 0x41e4 TXT 1
13991	2023-04-30 10:31:22.362094	192.168.157.145	192.168.157.144	DNS	320	Standard query response 0x79bd TXT 6
13995	2023-04-30 10:31:22.470742	192.168.157.145	192.168.157.144	DNS	320	Standard query response 0x24a3 TXT 7
13997	2023-04-30 10:31:22.581378	192.168.157.145	192.168.157.144	DNS	341	Standard query response 0x2850 MX 61
13999	2023-04-30 10:31:22.688644	192.168.157.145	192.168.157.144	DNS	339	Standard query response 0x4104 CNAME
14001	2023-04-30 10:31:22.801698	192.168.157.145	192.168.157.144	DNS	320	Standard query response 0x1264 TXT 2
14003	2023-04-30 10:31:22.908653	192.168.157.145	192.168.157.144	DNS	341	Standard query response 0x2d62 MX 15
14009	2023-04-30 10:31:23.017340	192.168.157.145	192.168.157.144	DNS	341	Standard query response 0x7dd4 MX 30
14011	2023-04-30 10:31:23.128046	192.168.157.145	192.168.157.144	DNS	320	Standard query response 0x7569 TXT 5
14013	2023-04-30 10:31:23.253758	192.168.157.145	192.168.157.144	DNS	320	Standard query response 0x7007 TXT 2
14015	2023-04-30 10:31:23.377109	192.168.157.145	192.168.157.144	DNS	341	Standard query response 0x3bc3 MX 60
14017	2023-04-30 10:31:23.501475	192.168.157.145	192.168.157.144	DNS	341	Standard query response 0x4cdb MX 50
14019	2023-04-30 10:31:23.610317	192.168.157.145	192.168.157.144	DNS	337	Standard query response 0x2db2 MX 54
14619	2023-04-30 10:32:52.040515	192.168.157.145	192.168.157.144	DNS	341	Standard query response 0x0703 MX 30
14758	2023-04-30 10:33:03.911567	192.168.157.145	192.168.157.144	DNS	239	Standard query response 0x40eb TXT 5
14780	2023-04-30 10:33:05.427170	192.168.157.145	192.168.157.144	DNS	339	Standard query response 0x5bfa CNAME

需使用 `gchq.github.io` 轉換

Recipe

From Hex

Delimiter
Auto

Input

1eca012ec7305cb1f877686f616d690a6465736b746f702d756d6e636265.375c746573740d0a0d0a433a5c55736572735c746573745c446f776e6c6f.6164733e.microsofto365.com: type TXT, class IN

Output

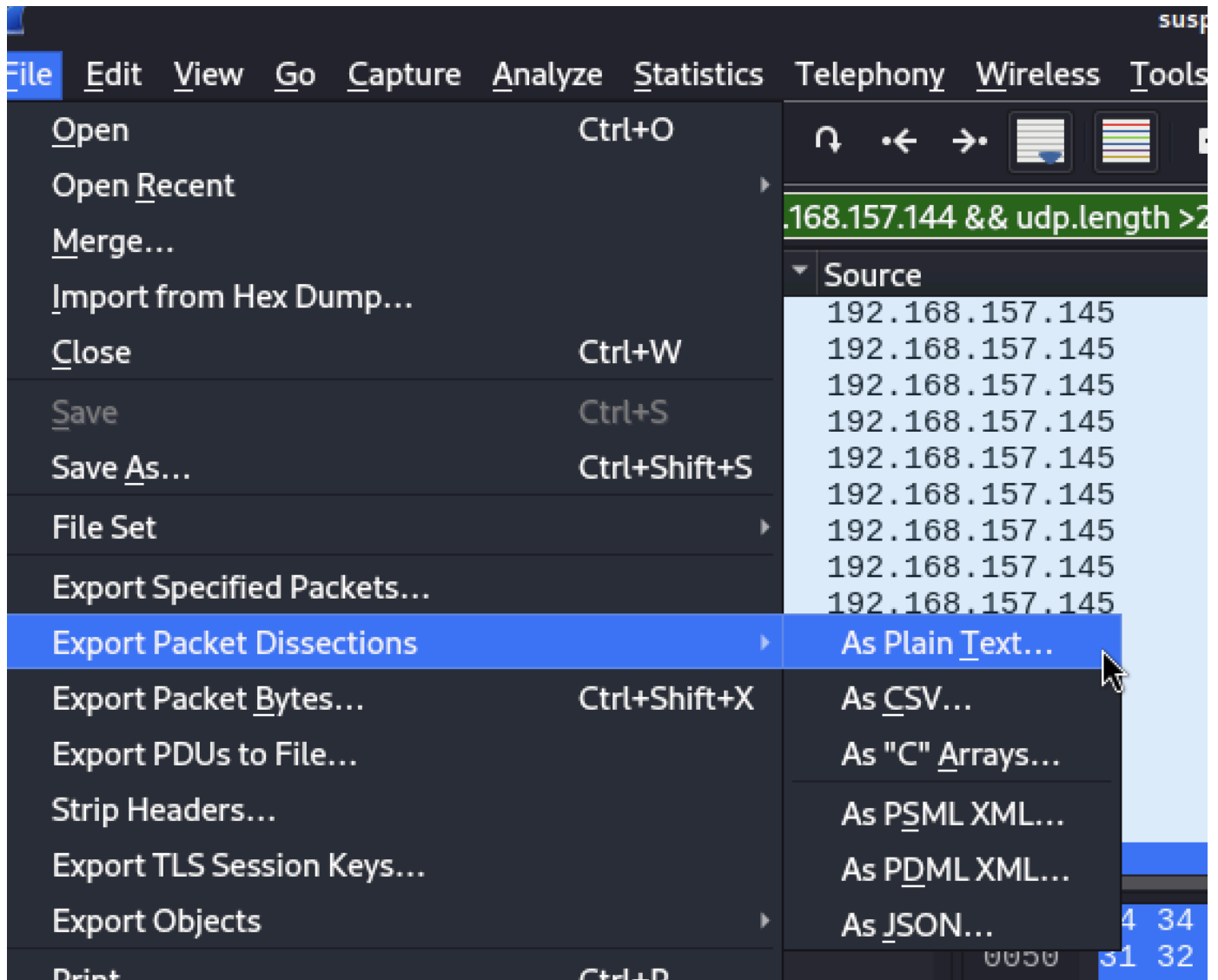
== Ê == .Ç0\±øwhoami
desktop-umncbe7\test
C:\Users\test\Downloads> 6 == 6 == 6 == 6

whoami

Task 4

What is the version of the DNS tunneling tool the attacker is using?

同上，使用另一個方式，存為文字



做法一：

腳本：https://github.com/a6232283/HTB/blob/main/Sherlocks/wireshark_DNS.py

查詢DNS

```
(root@kali)-[/home/kali/Desktop]
# cat 2.txt | grep dns
28/05/2016 21:38 142,336 dnscat2-v0.07-clientB.Browser.for.SQLite-3.12.2-win64.msi
28/05/2016 21:38 142,336 dnscat2-v0.07-client-win32.exe
28/05/2016 21:38 142,336 dnscat2-v0.07-clientB.Browser.for.SQLite-3.12.2-win64.msi
28/05/2016 21:38 142,336 dnscat2-v0.07-client-win32.exe
C:\Users\test\Downloads>ren dnscat2-v0.07-client-win32.exe
C:\Users\tren ren dnscat2-v0.07-client-win32.exe
C:\Users\tren ren 'dnscat2-v0.07-client-win32.exe' 'win_install.exe'
The syntax of the command is incorrect.
28/05/2016 21:38 142,336 dnscat2-v0.07-clientB.Browser.for.SQLite-3.12.2-win64.msi
28/05/2016 21:38 142,336 dnscat2-v0.07-client-win32.exe
C:\Users\test\Downloads>ren dnscat2-v0.07-client-win32.exe win_installer.exe
C:\Users\test\Downloads>ren dnscat2-v0.07-client-win32.exe win_installer.exe
```

做法二：

存為文字後，只接將文字轉換明文

Recipe

From Hex

Delimiter
Auto

Input

5/3b5/2/35C/4b5/3/45C44bTb3/5b0b5.be/4/35C63bcb9b5be/420b4b1/4b120bT/0/4b9b0b9/3b1/4b9bTbe3e.micr0s
ofto365.com: type MX, class IN, preferen
Name:
104d011ccd4c0d781b77686f616d690a6465736b746f702d756d6e636265.375c746573740d0a0d0a433a5c55736572735c
746573745c446f63756d65.6e74735c636c69656e742064617461206f7074696d69736174696f6e3e.microsoft365.com
Type: MX (15) (Mail eXchange)
Class: IN (0x0001)
Time to live: 60 (1 minute)
Data length: 40
Preference: 10
Mail Exchange: 6ef4011ccd781b4c5d.microsoft365.com
[Request In: 60123]
[Time: 0.001119000 seconds]

rec 6783764 92156

Raw Bytes

Output

dns

next previous all

☐ match case
☐ regexp
☐ by word

```

$0(
Srd7
X
I
.
.
U
.
.
EÍI0 ID0u,B.Browser.for.SQLite-3.12.2-win64.msi
28/05/2016 21:38 142,336 dnscat2-v0.07-client 6

```

STEP

BAKE!

Auto Bake

0.07

Task 5

The attackers attempts to rename the tool they accidentally left on the clients host. What do they name it to?

因為是windows所以指令為 `ren`，前面一開始：`win_install.exe`是錯誤...

re

next previous all

☐ match case
☒ regexp
☐ by word

```

i
6
qq
F
F
NUL SOH SO SO ` SOH SO U
SO DC4 BEL i SO SO I DLE
SO F
SO NAK = SOH FS Íu•Peren dnscat2-v0.07-clie çBxv•ã3"æW•R BEL v•åö•ç7F SYN ÆÆW"æW•P
F SI 6 ENQ F SO SO CAN p ACK SO NUL NUL DC2 Y NUL NUL iR SO Ip
F SO SI CAN p # EOT 0 DLE 4 DC3 F CAN F EM STX SYN BS NAK BEL DC4 ENQ EM STX SYN BS NAK BEL DC4 EOT R0 ACK
UR SO SO SO XáF
SO ^ý SOH FS ÍPouÆren dnscat2-v0.07-client-win32.exe win_installer.exe
C:\Users\test\Downloads>
win_installer.exe

```

Task 6

The attacker attempts to enumerate the users cloud storage. How many files do they locate in their cloud storage directory?

查詢各大公司、OneDrive都找不到

0

Task 7

What is the full location of the PII file that was stolen?

pii檔用途：儲存已編譯的函數或物件。
用查看 type 方式來尋找

Output

type

next

previous

all

☐ match case

☐ regexp

☐ by word

SO F

SO ' a SOH FS I•8wb F S1 6 ENQ F

SO SO 6<< SO F ETX SO F

SO ENQ ÊÊ

SO S1

F

NUL SOH

SO ÊÍ ' a SOH FS I•8wb F S1 6 ENQ F SO F

SO F

F

SO \$

SOH FS Iwb•8type "C:\Users\test\Do ACK 7VÖVçG5Æ6Æ•VçB ACK F ETB F DC2 ACK ÷ BEL F•Ö•6 ETB F•ö SO \user details.cs BEL

SO ' a SOH FS I•8wb F S1 6 ENQ F SO F

SO ENQ ÊÊ

SO S1

F

NUL SOH SO SO SO SOH SO Ú

SO CAN ACK F

SO \$

SOH FS Iwb•8type "C:\Users\test\Do ACK 7VÖVçG5Æ6Æ•VçB ACK F ETB F DC2 ACK ÷ BEL F•Ö•6 ETB F•ö SO \user details.csv"

F 6 ENQ F SO SO G CAN BEL SO NUL NUL ' NUL NUL iC R SO ÎP

F S1 S1 G EM STX # 0 DLE @ DCI t ACK EM STX SYN BS NAK BEL DC4 ENQ EM STX SYN BS NAK BEL DC4 EOT CR4 SOH

ÚC R SO SO SO ;½qp SOH FS I•8w«type "C:\Users\test\Documents\client data optimisation\user details.csv"

,job,company,ssn,resid F S1 6 ENQ F DLE • C SOH FS Iw«•• F S1 6 ENQ F S1

SO G EM STX A SOH V_ SO SO ' (V_ A SOH V_ SO ÊÍ ' (V_ SO SO SO F

C:\Users\test\Documents\client data optimisation\user details.csv

Task 8

Exactly how many customer PII records were stolen?

同上，開始第一數字為0最後為720
開始

,job,company,ssn,resid^{F SO} ^{SOH FS} Í•8w«type "C:\Users\test\Documents\client data optimisation\user details.csv"
 ,job,company,ssn,resid^{F SO} ^{SI 6 ENQ F SO NAK}
 ^{SO F}
 ^{SO F}
 ^{NUL SOH SO SO SOH SO} Ú
 ^{SO} @i ^{SO SO} ^{SI DLE} Î
 ^{SO F}
 ^{SO • C SOH FS} Íw«••^{F SO} ^{SI 6 ENQ F SO} ^{SO G EM SOH SO NUL NUL DC4} I ^{NUL NUL} i^{C SO} ^{SI} Îp
 ^{F SO} ^{SI G EM ACK} # ^{EOT 0 DLE} @ ^{DC1 •} ^{STX EM STX SYN BS NAK BEL DC4 ENQ EM STX SYN BS NAK BEL DC4 EOT} ^{C 2 NUL}
 ^{Ú C SO} ^{SO SO} .D5à ^{SOH FS} ^{SI ••w\$ C}
 0,Chief Tec^{F SO} ^{SI 6 ENQ F SI}
 ^{SO G EM ACK 2 NUL V SO} ^{SO %`V 2 NUL V SO} Êí%`V ^{SO SO SO F}
 ^{SO m SOH Û NUL F} m ^{SOH Û C}
 ^{SO} ¥Ö(^{NUL F})¥Ö(^{SO SO F SO EOT F EM STX SYN BS NAK BEL DC4 ENQ C EM STX SYN BS NAK BEL DC4 EOT SO} Úzz

 ^{F F S C R} d7 ^{BEL C}

 ^{SO SO SO SO}
 -^{C R} .D ^{SI}
 • •
 ^{Ú C SO} ^{SO SO SO SO SO SOH}
 ^{SO SOH}
 ^{NUL • C}
 ^{NUL SO SO} Êí5à ^{SOH FS} ^{SI ••\$ C}
 0,Chief Tec^{F SO} ^{SI 6 ENQ F}
 ^{SO} 5à ^{SOH FS} ^{SI ••w«ence,current_location,blood_group,website,username,name,sex,address,mail,birthdate} ^C
 0,Chief Tec^{F SO} ^{SI 6 ENQ F}
 ^{SO SO "} ^{SO SO F ACK SO SYN SO F}
 ^{NUL SOH}
 ^{SO} Êí5à ^{SOH FS} ^{SI ••w«ence.current_location.blood aroup.website.username.name.sex.address.mail.birthdate} ^C
 最後
 ^F
 ^{SO F}
 ^{NUL SOH}
 ^{SO} ÊíW? ^{SOH FS} ^{SI -`w«",maria11@yahoo.com,1992-01-12} ^C
 720,Ambulance person,"Smith, Collins and Brown",524-80-5753,"22^{F SO} ^{SI 6 ENQ F}
 ^{SO W? SOH FS} ^{SI -`w«",maria11@yahoo.com,1992-01-12} ^C
 720,Ambulance person,"Smith, Collins and Brown",524-80-5753,"22^{F SO} ^{SI 6 ENQ F SO NAK}
 ^{SO F}
 ^{SO F}