Notes From The Red Team:
Why Perimeter Security Fails

Yossi Sassi

White h^t haɔker & Security Researcher

cyberart

The art of cyber security

What we’ll talk about

The Shift in APT Landscape

The New Perimeters

- Why Firewalls/AV/EDR fail
- Examples from our recent research

Whoami Y1nTh35h3ll

Security researcher, White h^t hacker (Finance, Military/Gov)

Co-Founder @ CyberArt, Board Member @ Javelin Networks

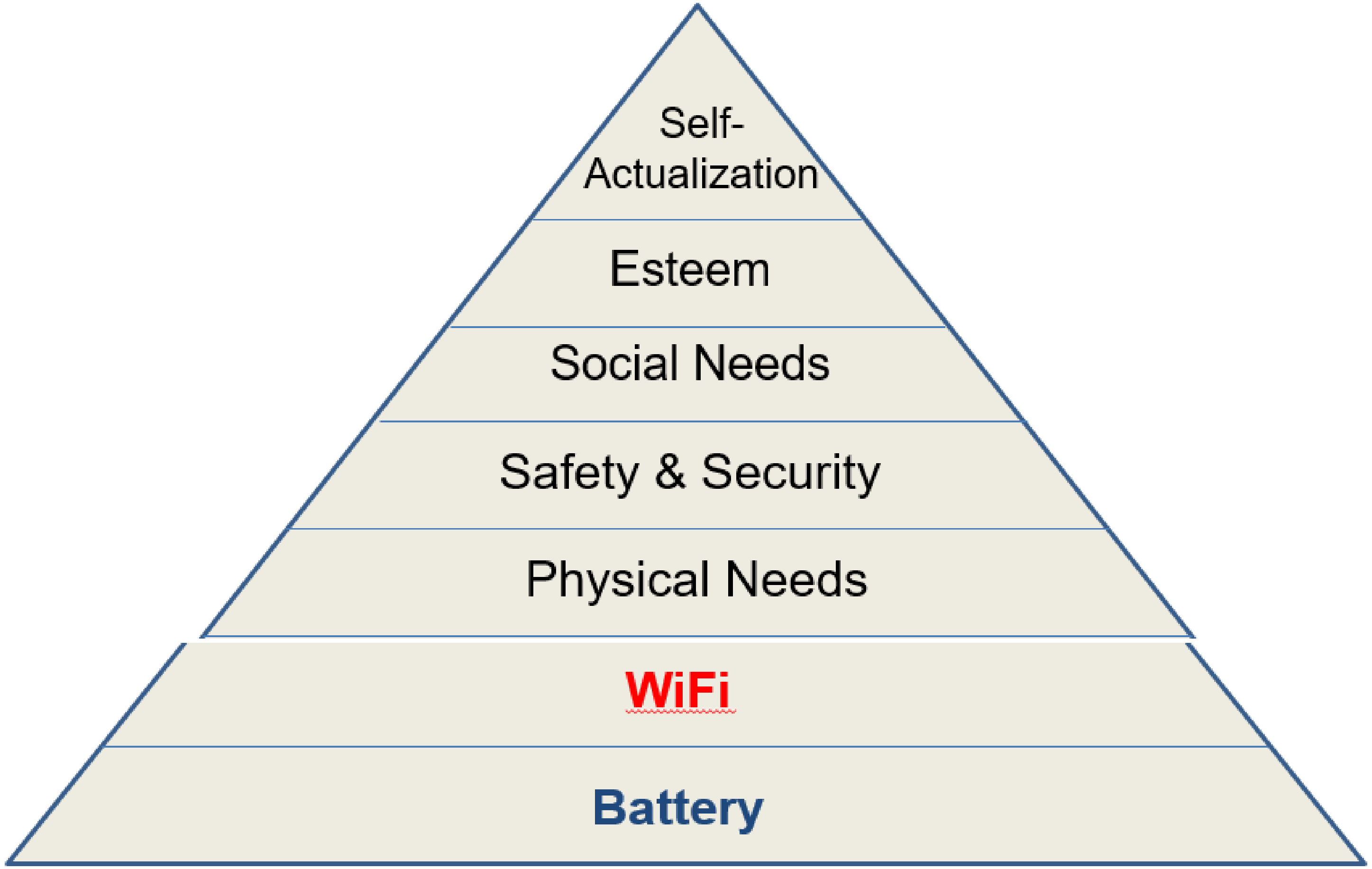
~30 years experience – Programming, NetComm, IT/System

Ex-Technology Group Manager @ Microsoft (~8 years), coded Windows Server Tools

Ex-CTO @ public companies, M.A Law

Certified CISSP, VMWare, NetApp, EMC, Netware etc

All you need is… Love?



Self-Actualization

Esteem

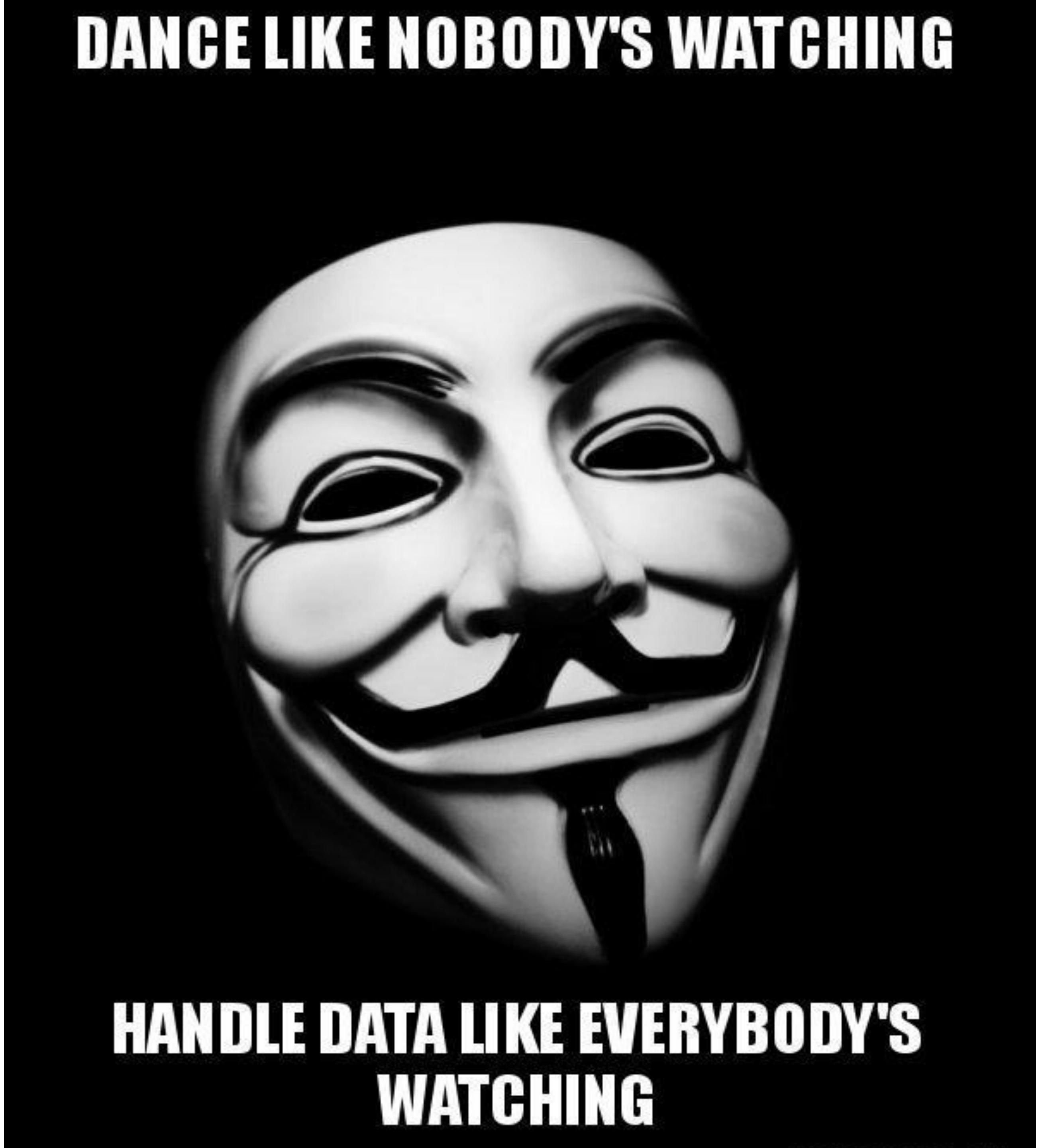
Social Needs

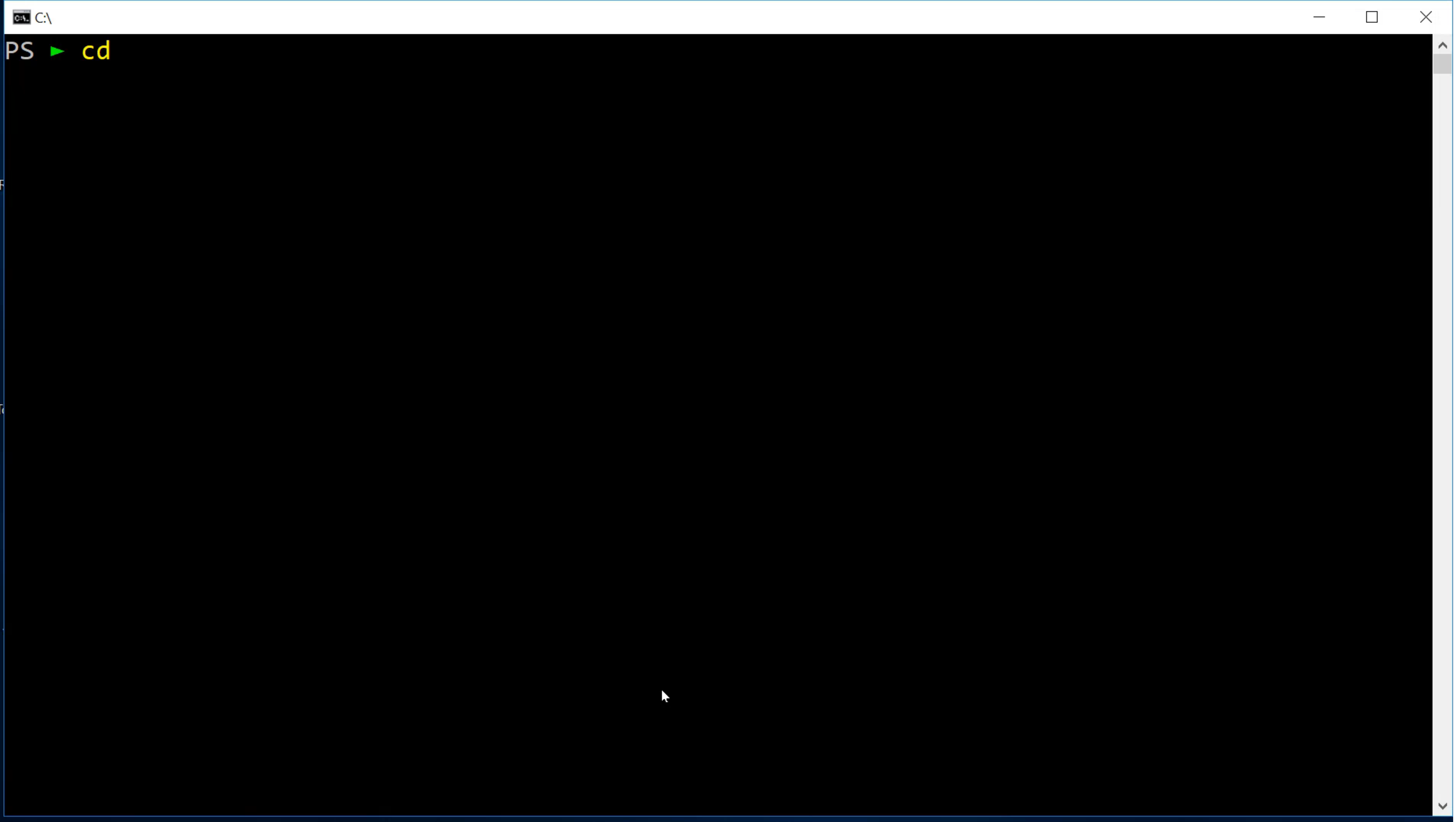
Safety & Security

Physical Needs

WiFi

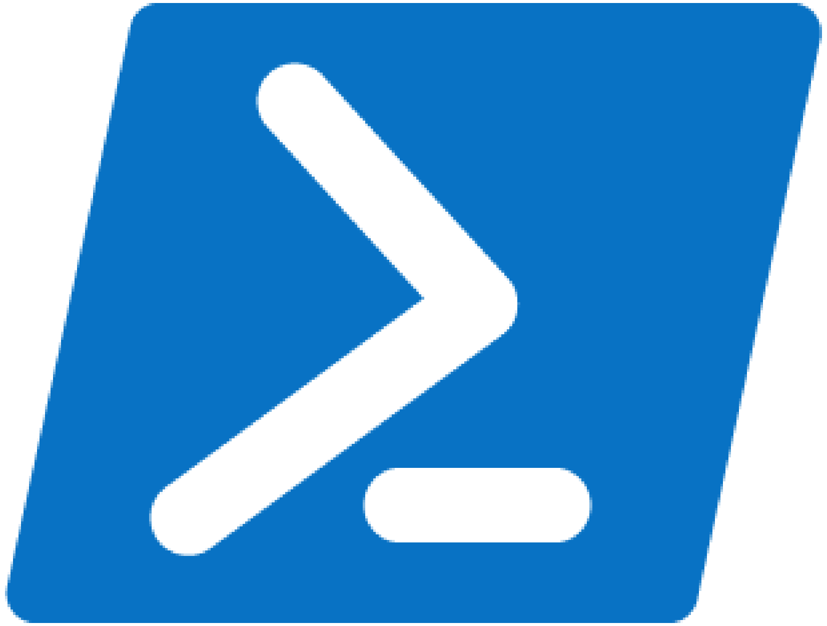
Battery


DANCE LIKE NOBODY'S WATCHING
HANDLE DATA LIKE EVERYBODY'S WATCHING

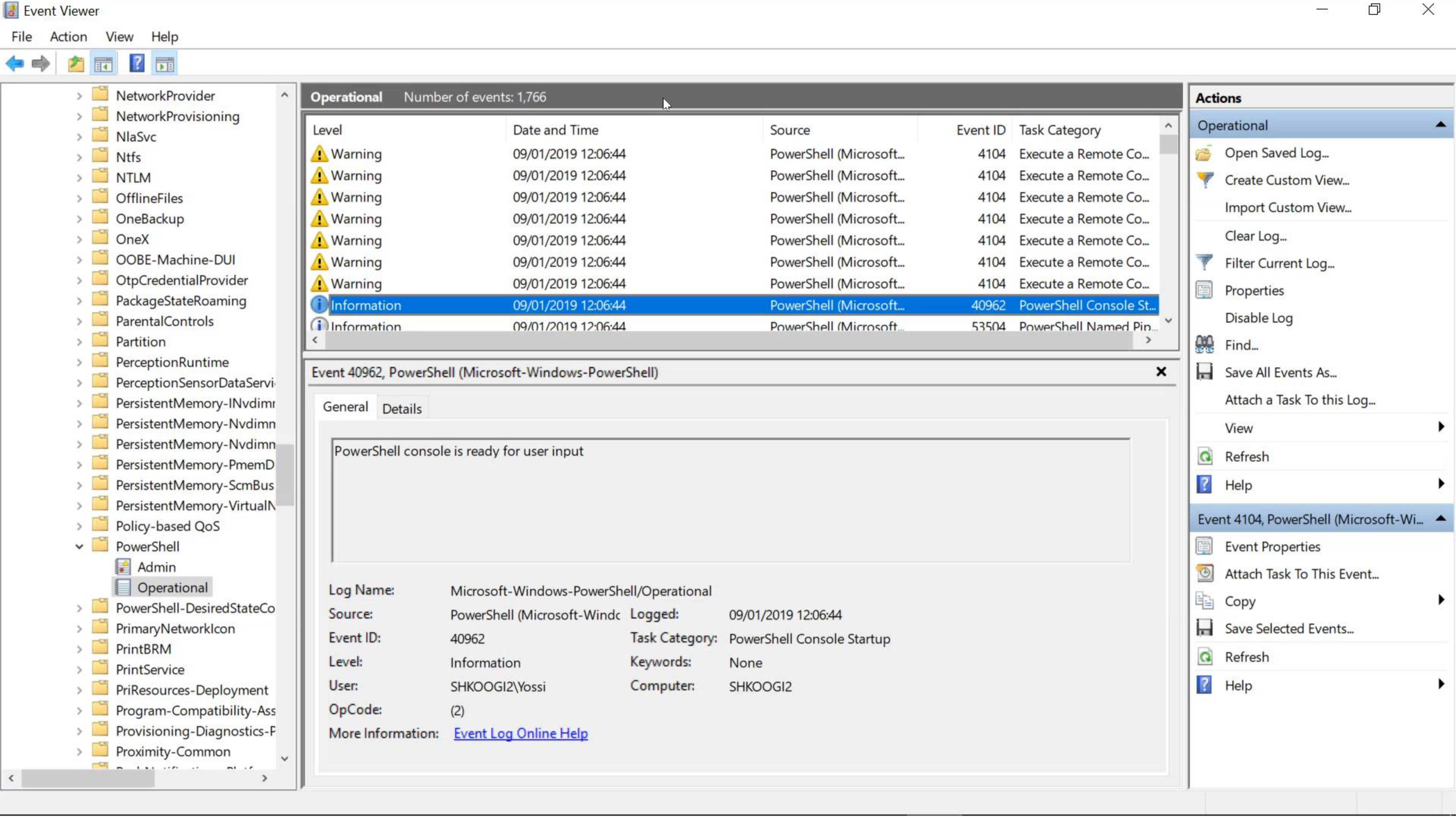


```
PS ► cd
```

ANY organization can be hacked.



Full Bypass of
AV / EDR / Logging / Auditing
Using Invisi-Shell PoC



Operational Number of events: 1,766

Level	Date and Time	Source	Event ID	Task Category
Warning	09/01/2019 12:06:44	PowerShell (Microsoft...	4104	Execute a Remote Co...
Warning	09/01/2019 12:06:44	PowerShell (Microsoft...	4104	Execute a Remote Co...
Warning	09/01/2019 12:06:44	PowerShell (Microsoft...	4104	Execute a Remote Co...
Warning	09/01/2019 12:06:44	PowerShell (Microsoft...	4104	Execute a Remote Co...
Warning	09/01/2019 12:06:44	PowerShell (Microsoft...	4104	Execute a Remote Co...
Warning	09/01/2019 12:06:44	PowerShell (Microsoft...	4104	Execute a Remote Co...
Warning	09/01/2019 12:06:44	PowerShell (Microsoft...	4104	Execute a Remote Co...
Information	09/01/2019 12:06:44	PowerShell (Microsoft...	40962	PowerShell Console St...
Information	09/01/2019 12:06:44	PowerShell (Microsoft...	53504	PowerShell Named Pip...

Event 40962, PowerShell (Microsoft-Windows-PowerShell)

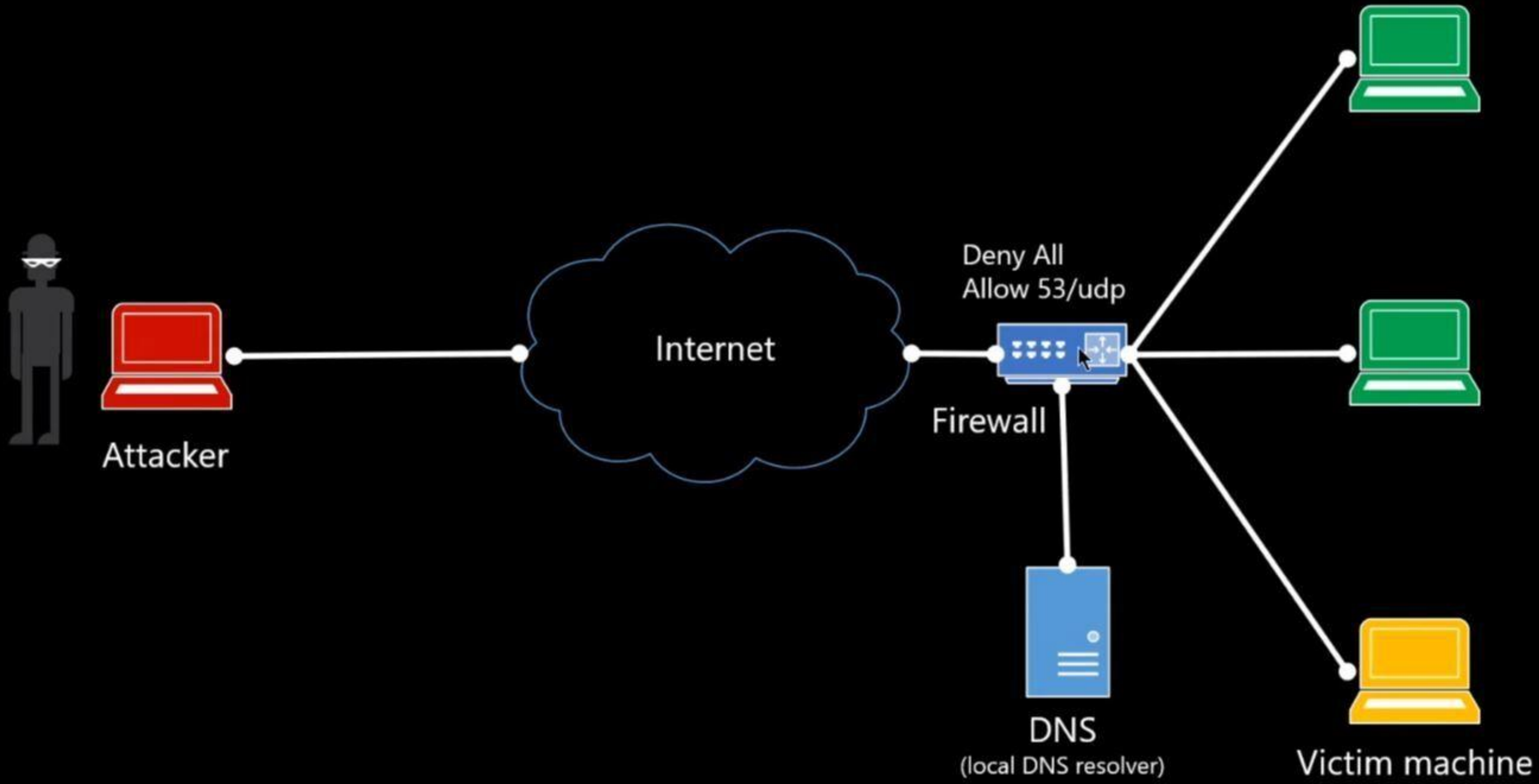
General Details

PowerShell console is ready for user input

Log Name:	Microsoft-Windows-PowerShell/Operational		
Source:	PowerShell (Microsoft-Windc	Logged:	09/01/2019 12:06:44
Event ID:	40962	Task Category:	PowerShell Console Startup
Level:	Information	Keywords:	None
User:	SHKOOGI2\Yossi	Computer:	SHKOOGI2
OpCode:	(2)		
More Information:	Event Log Online Help		

16

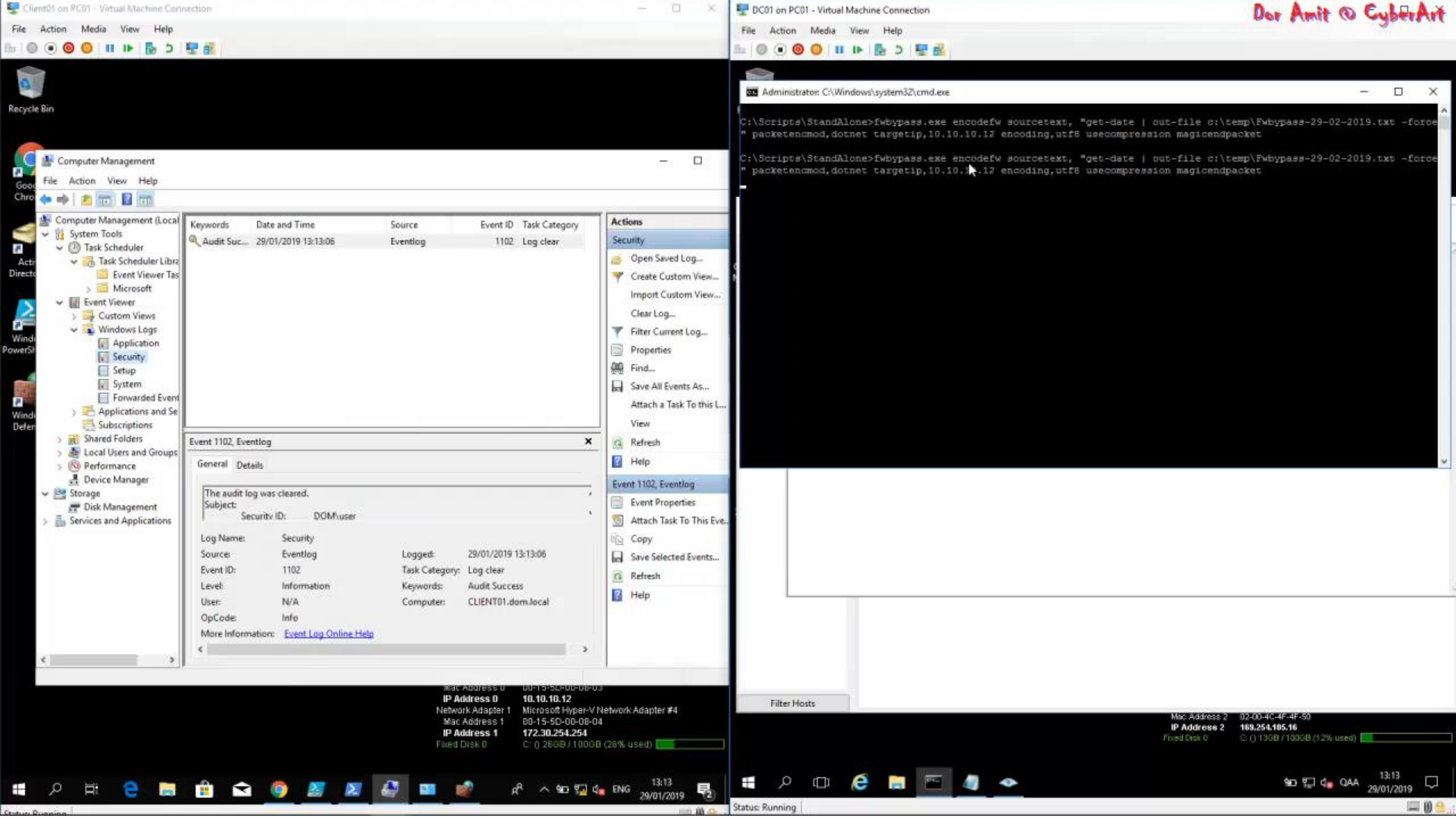
C2 Scenario with No Direct Internet Allowed



FWBypass: Crafted dropped packets C2

By Dor Amit

- In-direct bypass with a set of C&C techniques
- Transfer payload by manipulating the data captured by different audit mechanisms
- Consume it later by accessing the log and reconstruct it using pre-defined logic
- https://youtu.be/XkVSCATKzwU



Keywords	Date and Time	Source	Event ID	Task Category
Audit Suc...	29/01/2019 13:13:06	Eventlog	1102	Log clear

Event 1102, Eventlog

General Details

The audit log was cleared.
Subject:
Security ID: DOM\user

Log Name: Security
Source: Eventlog
Logged: 29/01/2019 13:13:06
Event ID: 1102
Task Category: Log clear
Level: Information
Keywords: Audit Success
User: N/A
Computer: CLIENT01.dom.local
OpCode: Info
More Information: Event Log Online Help

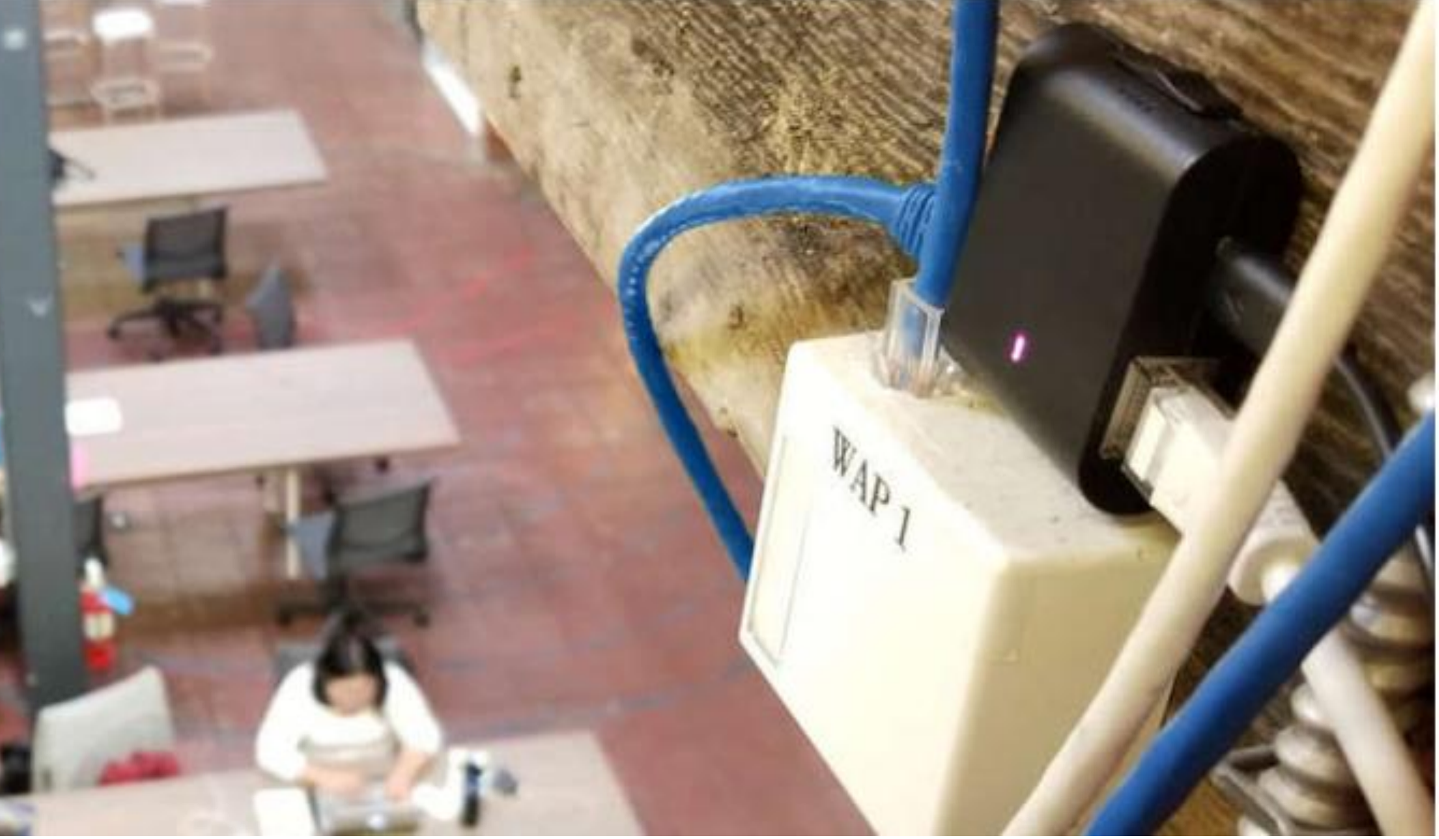
Administrator: C:\Windows\system32\cmd.exe

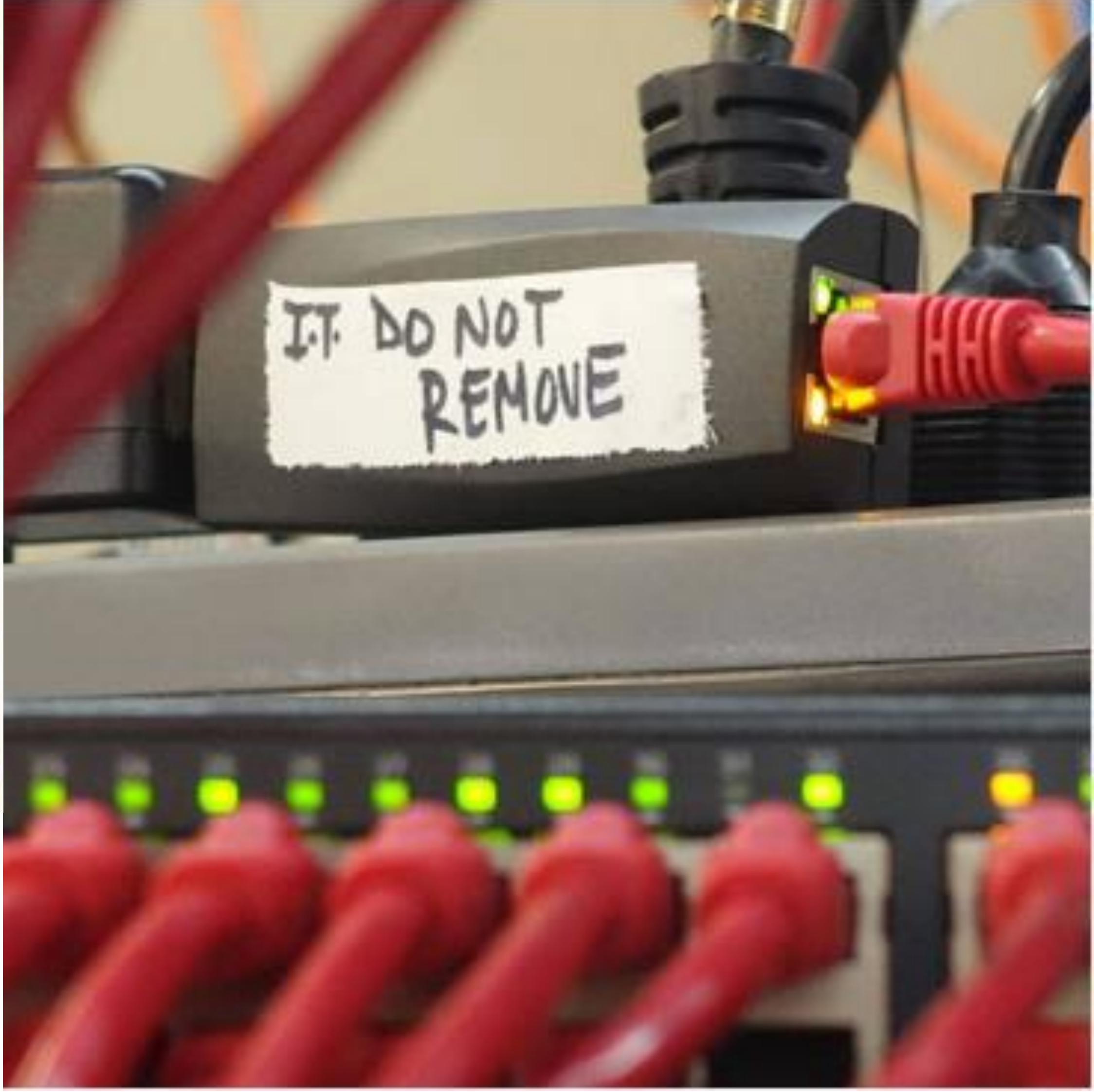
```
C:\Scripts\StandAlone>fwbypass.exe encodefw sourcetext, "get-date | out-file c:\temp\Fwbypass-29-02-2019.txt -force
" packetencmod,dotnet targetip,10.10.10.12 encoding,utf8 usecompression magicendpacket

C:\Scripts\StandAlone>fwbypass.exe encodefw sourcetext, "get-date | out-file c:\temp\Fwbypass-29-02-2019.txt -force
" packetencmod,dotnet targetip,10.10.10.12 encoding,utf8 usecompression magicendpacket
```

IP Address 0 10.10.10.12
Network Adapter 1 Microsoft Hyper-V Network Adapter #4
Mac Address 1 00-15-5D-00-08-04
IP Address 1 172.30.254.254
Fixed Disk 0 C: () 26GB / 100GB (26% used)

Mac Address 2 02-00-4C-4F-4F-50
IP Address 2 169.254.105.16
Fixed Disk 0 C: () 13GB / 100GB (12% used)

13:13 29/01/2019



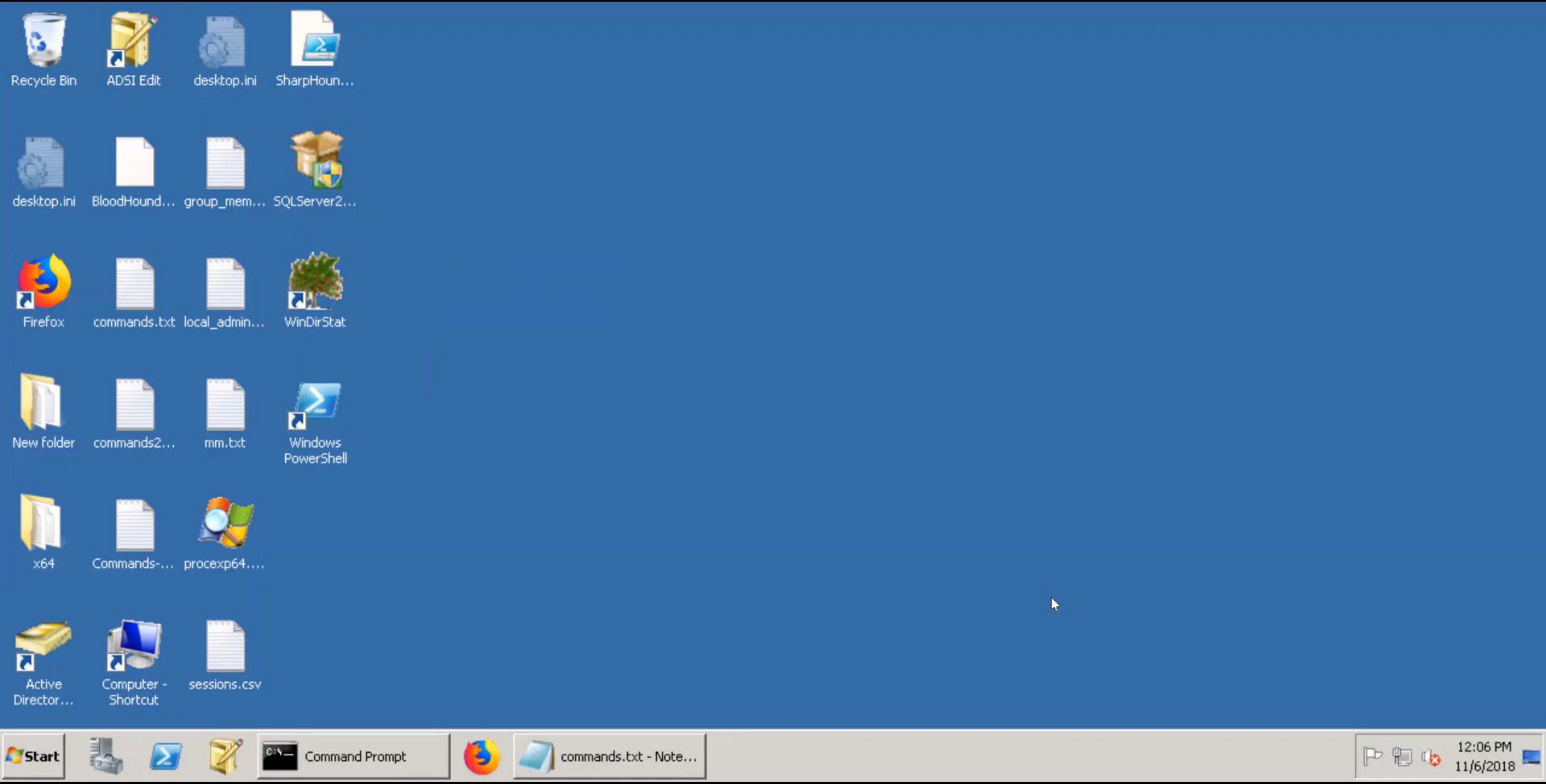


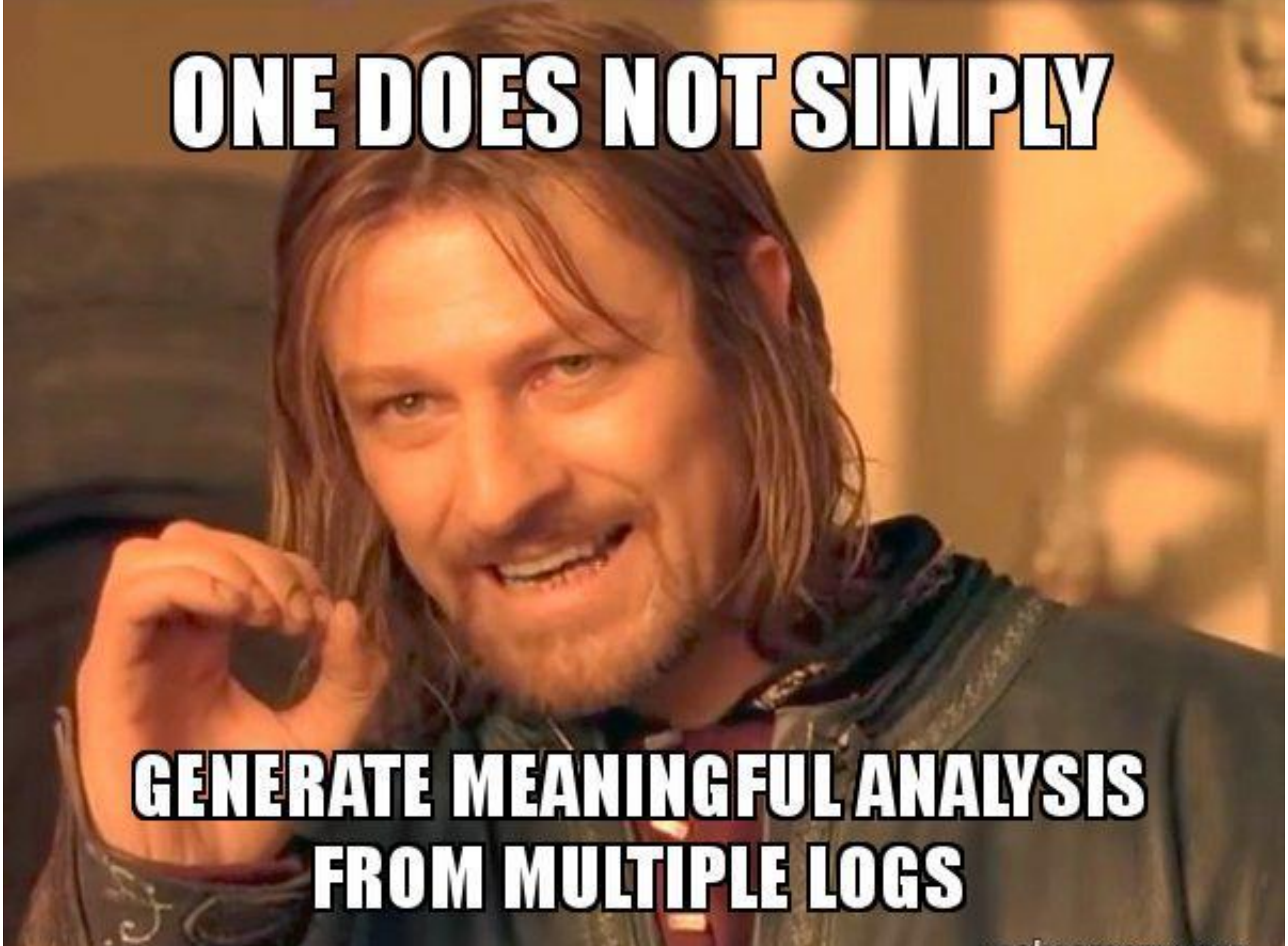
How adversaries bypass your perimeter defenses

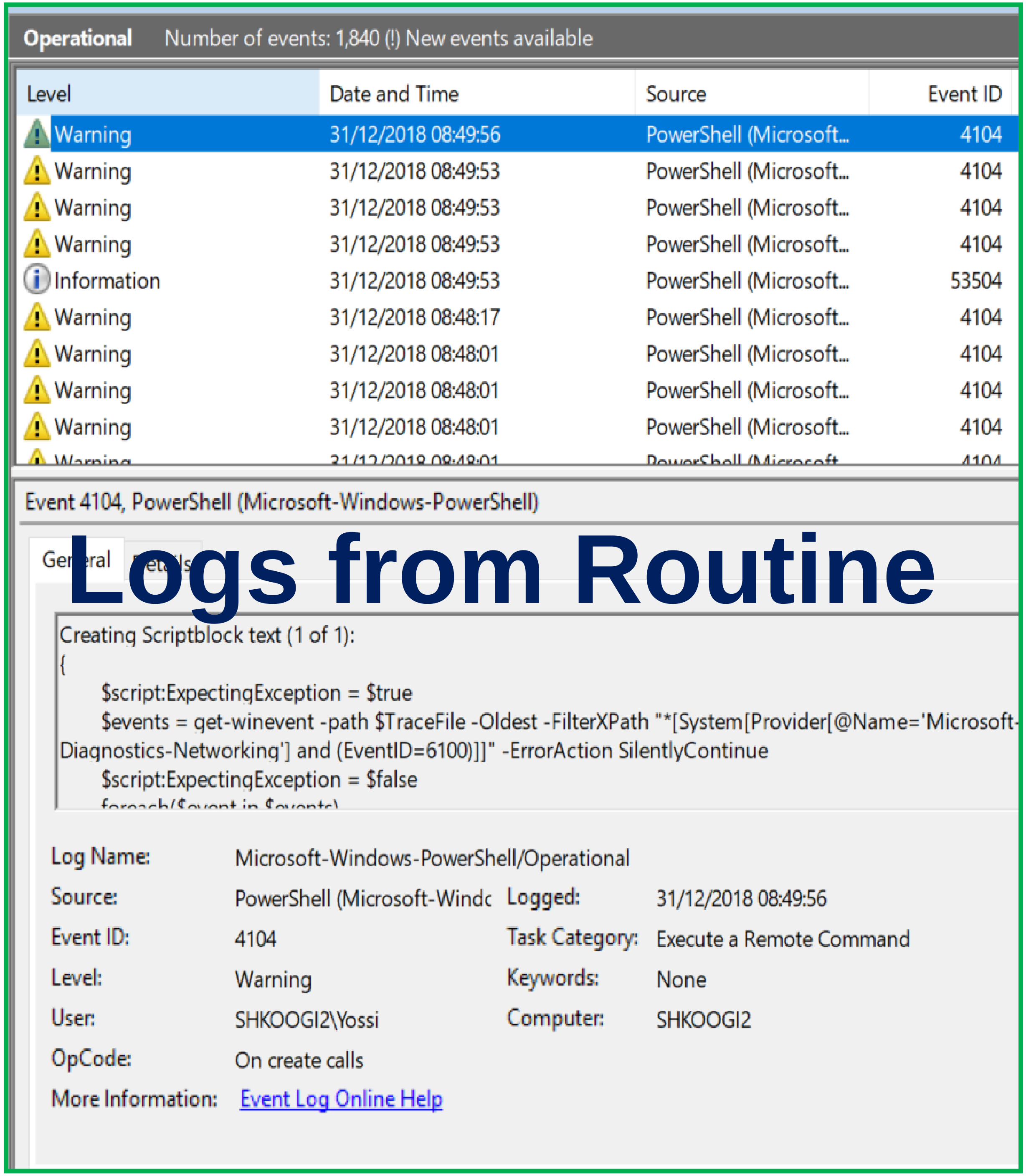
(H)Ac(k)tive Directory

AD DATABASE
IS EXPOSED BY DESIGN FROM EVERY ENDPOINT

Active Directory Reconnaissance


Recycle Bin
ADSI Edit
desktop.ini
SharpHoun…
desktop.ini
BloodHound…
group_mem…
SQLServer2…
Firefox
commands.txt
local_admin…
WinDirStat
New folder
commands2…
mm.txt
Windows PowerShell
x64
Commands-…
procexp64.…
Active Director…
Computer - Shortcut
sessions.csv
Start
Command Prompt
commands.txt - Note…
12:06 PM
11/6/2018


ONE DOES NOT SIMPLY
GENERATE MEANINGFUL ANALYSIS
FROM MULTIPLE LOGS



Logs from Routine

Operational Number of events: 1,840 (!) New events available

Level	Date and Time	Source	Event ID
Warning	31/12/2018 08:49:56	PowerShell (Microsoft...	4104
Warning	31/12/2018 08:49:53	PowerShell (Microsoft...	4104
Warning	31/12/2018 08:49:53	PowerShell (Microsoft...	4104
Warning	31/12/2018 08:49:53	PowerShell (Microsoft...	4104
Information	31/12/2018 08:49:53	PowerShell (Microsoft...	53504
Warning	31/12/2018 08:48:17	PowerShell (Microsoft...	4104
Warning	31/12/2018 08:48:01	PowerShell (Microsoft...	4104
Warning	31/12/2018 08:48:01	PowerShell (Microsoft...	4104
Warning	31/12/2018 08:48:01	PowerShell (Microsoft...	4104
Warning	31/12/2018 08:48:01	PowerShell (Microsoft...	4104

Event 4104, PowerShell (Microsoft-Windows-PowerShell)

General Details

```
Creating Scriptblock text (1 of 1):
{
      $script:ExpectingException = $true
      $events = get-winevent -path $TraceFile -Oldest -FilterXPath "*[System[Provider[@Name='Microsoft-
Diagnostics-Networking'] and (EventID=6100)]]" -ErrorAction SilentlyContinue
      $script:ExpectingException = $false
      foreach($event in $events)
```

Log Name: Microsoft-Windows-PowerShell/Operational

Source: PowerShell (Microsoft-Windc Logged: 31/12/2018 08:49:56

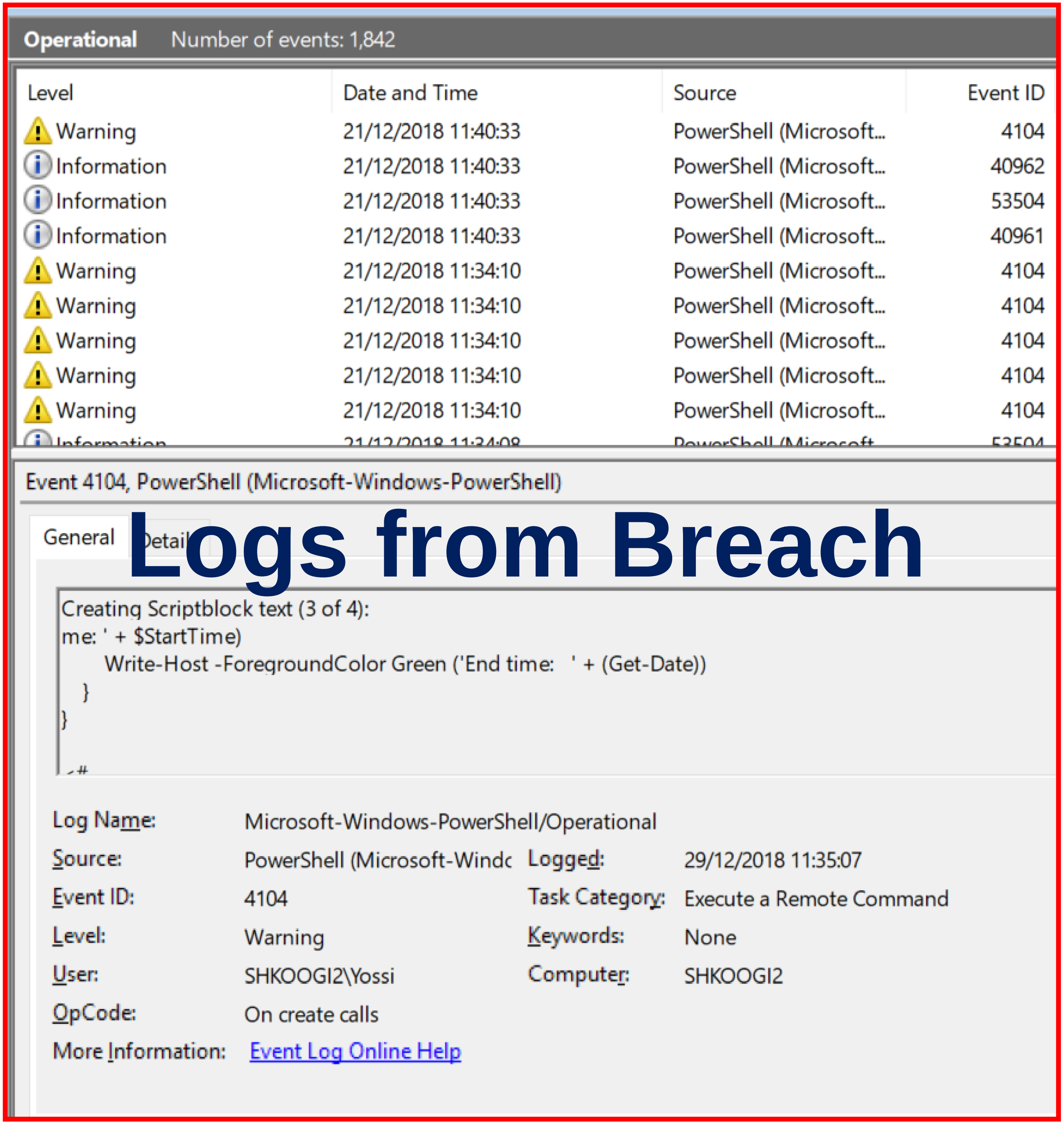
Event ID: 4104 Task Category: Execute a Remote Command

Level: Warning Keywords: None

User: SHKOOGI2\Yossi Computer: SHKOOGI2

OpCode: On create calls

More Information: Event Log Online Help



Logs from Breach

Operational Number of events: 1,842

Level	Date and Time	Source	Event ID
Warning	21/12/2018 11:40:33	PowerShell (Microsoft...	4104
Information	21/12/2018 11:40:33	PowerShell (Microsoft...	40962
Information	21/12/2018 11:40:33	PowerShell (Microsoft...	53504
Information	21/12/2018 11:40:33	PowerShell (Microsoft...	40961
Warning	21/12/2018 11:34:10	PowerShell (Microsoft...	4104
Warning	21/12/2018 11:34:10	PowerShell (Microsoft...	4104
Warning	21/12/2018 11:34:10	PowerShell (Microsoft...	4104
Warning	21/12/2018 11:34:10	PowerShell (Microsoft...	4104
Warning	21/12/2018 11:34:10	PowerShell (Microsoft...	4104
Information	21/12/2018 11:34:08	PowerShell (Microsoft...	53504

Event 4104, PowerShell (Microsoft-Windows-PowerShell)

General Details

```
Creating Scriptblock text (3 of 4):
me: ' + $StartTime)
      Write-Host -ForegroundColor Green ('End time:   ' + (Get-Date))
   }
}

<#
```

Log Name: Microsoft-Windows-PowerShell/Operational

Source: PowerShell (Microsoft-Windc Logged: 29/12/2018 11:35:07

Event ID: 4104 Task Category: Execute a Remote Command

Level: Warning Keywords: None

User: SHKOOGI2\Yossi Computer: SHKOOGI2

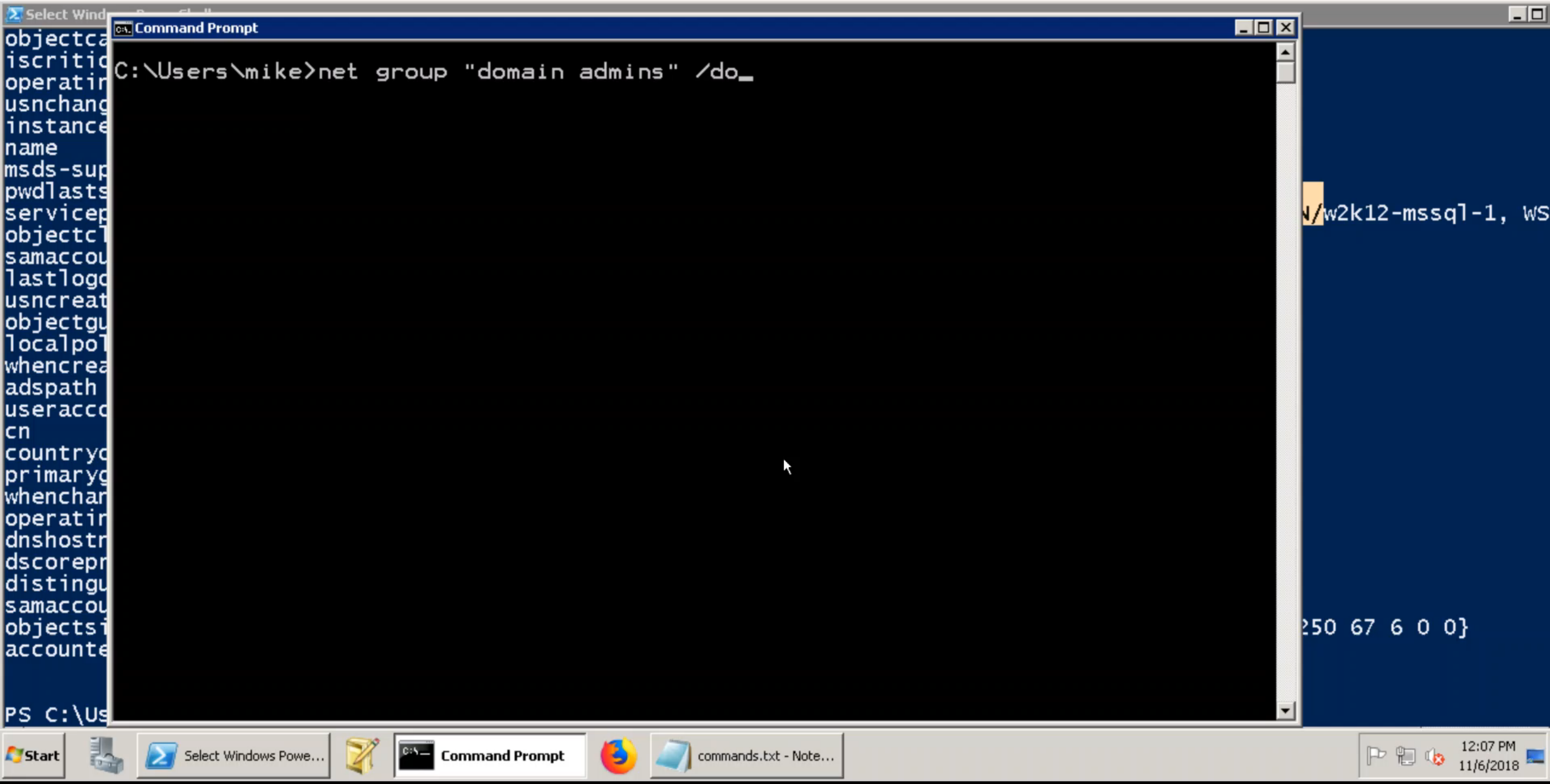
OpCode: On create calls

More Information: Event Log Online Help

Logging is *Not* Detecting

Detecting is *Not* Mitigating

Active Directory Reconnaissance With Javelin ‘ADProtect’ (aka Threat Defense for AD)



```
C:\Users\mike>net group "domain admins" /do_
```

```
objectca
iscritic
operatin
usnchang
instance
name
msds-sup
pwdlasts
servicep                                    N/w2k12-mssql-1, WS
objectcl
samaccou
lastlogo
usncreat
objectgu
localpol
whencrea
adspath
useracco
cn
countryc
primaryg
whenchar
operatin
dnshostn
dscorepr
distingu
samaccou
objectsi                                    250 67 6 0 0}
accounte

PS C:\Us
```

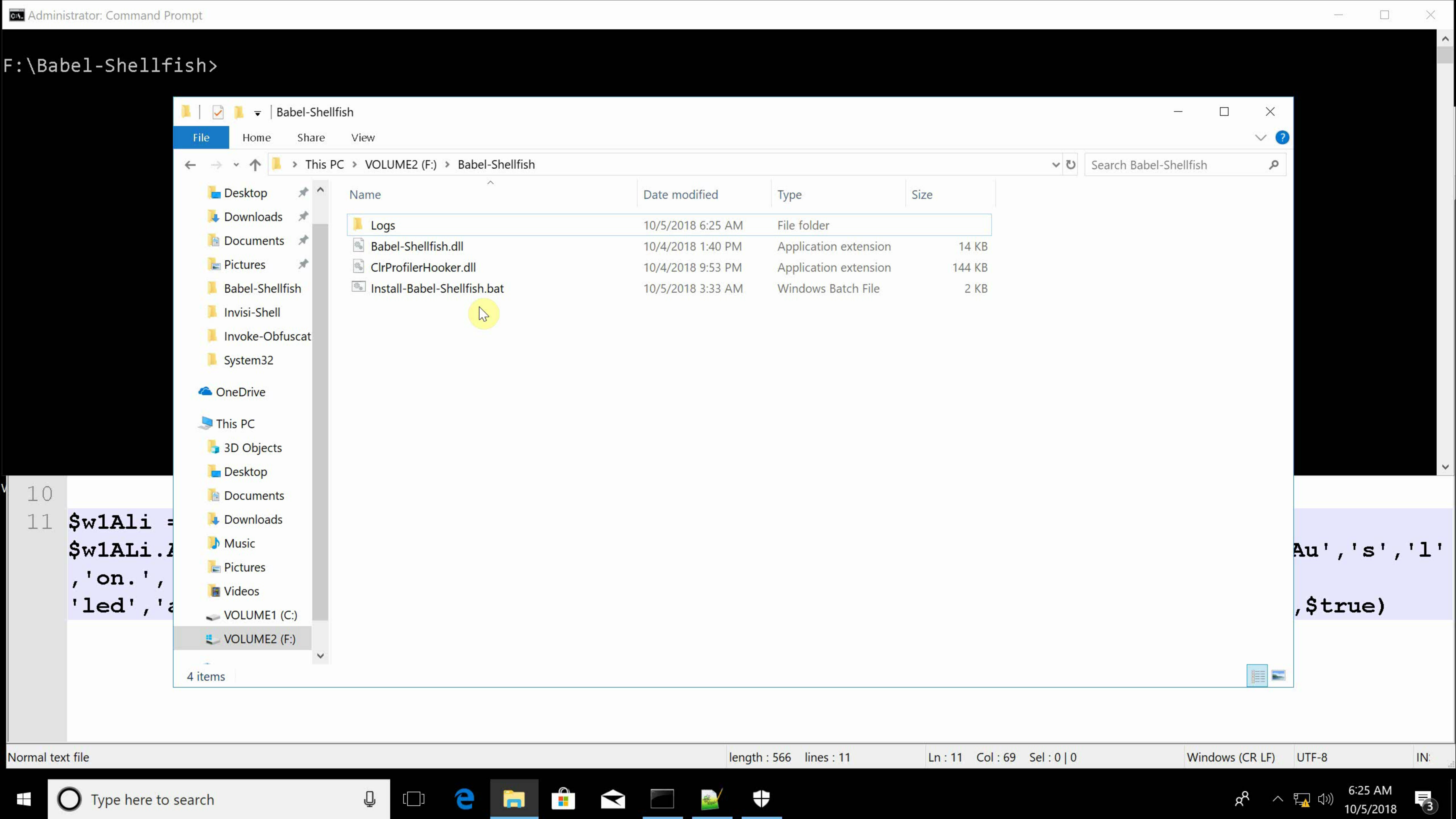
Symantec TDAD (Threat Defense for AD)
<Previously Javelin ADProtect>

- No agent. No installations.
- Up to 10x scale for Perception Control.
- No fake stuff, not a honeypot - instead unique hooking with memory manipulation (Patented)
- Unique presence allows for Forensics and Containment opportunity.
- Ongoing Attack Simulations for Active Directory.

De-obfuscate any command~

with **Babel-Shellfish**

By Omer Yair



Administrator: Command Prompt

```
F:\Babel-Shellfish>
```

Babel-Shellfish

This PC > VOLUME2 (F:) > Babel-Shellfish

Name	Date modified	Type	Size
Logs	10/5/2018 6:25 AM	File folder	
Babel-Shellfish.dll	10/4/2018 1:40 PM	Application extension	14 KB
ClrProfilerHooker.dll	10/4/2018 9:53 PM	Application extension	144 KB
Install-Babel-Shellfish.bat	10/5/2018 3:33 AM	Windows Batch File	2 KB

4 items

```
$w1Ali =
$w1ALi.A                                                              Au','s','l'
,'on.',
'led','a                                                              ,$true)
```

Normal text file   length : 566   lines : 11   Ln : 11   Col : 69   Sel : 0 | 0   Windows (CR LF)   UTF-8   INS

Key Takeaways

Motivation & time are all it takes to hack ANY organization

- Easy to get in
- Easy to bypass perimeter defenses
- Easy to do reconnaissance on identities & data assets

Perimeters are *trivially bypassed* by skilled adversaries.

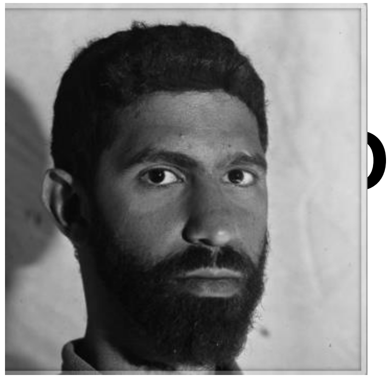
Your SIEM can easily increase your Time To Resolve.

Physical Security & Meaningful Logging (with High-Fidelity Signals, Detection & Mitigation) probably last controls to get fair chance in unfair battle field.

Do you haɔk a question?

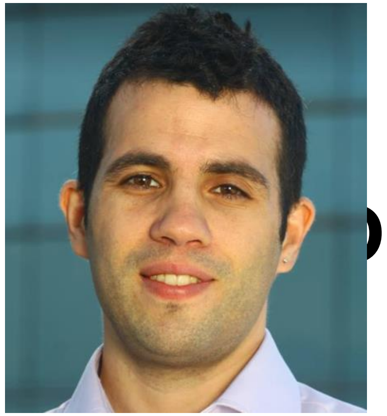
Links & THANKS!

My Git: https://github.com/YossiSassi



Omer Yair

https://github.com/OmerYa



Dor Amit

The Gang :-)

Th^nK Yoo

Yossi **S**assi

Yossi@**C**yber**A**rt**S**ecurity.com