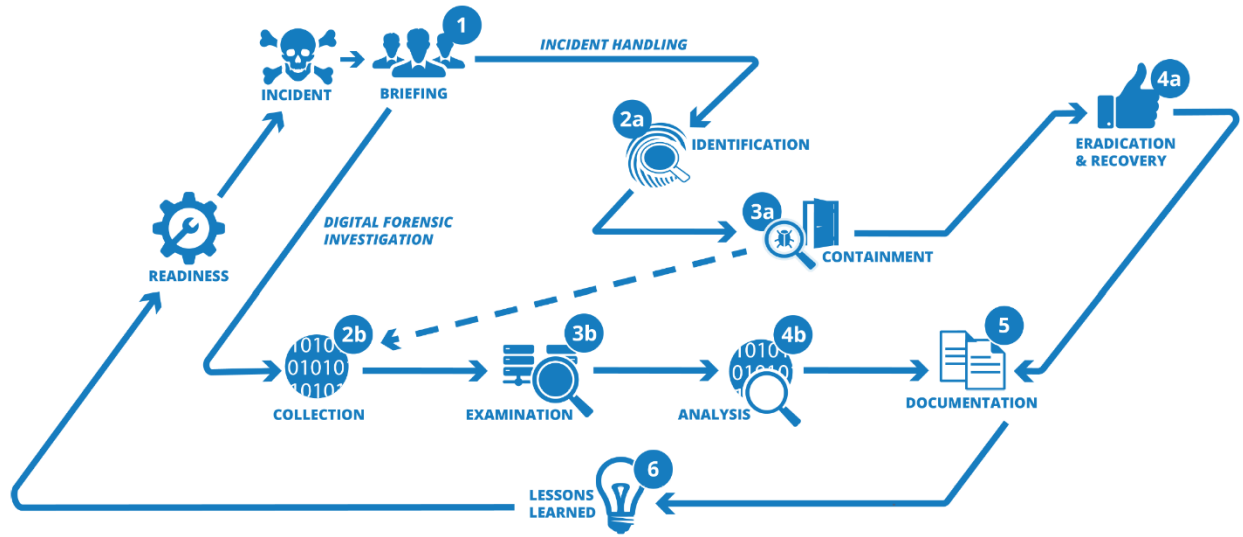


Incident Response [الاستجابة للحوادث]



IT-FORENSIK READINESS

>

Rechtlich

Gesetze, private oder öffentliche Untersuchung, SLAs, Do's & Don'ts

>

Technisch

Logging, Monitoring, Tools

>

Organisatorisch

Team/CSIRT, Prozesse, Checklisten, Ressourcenbereitstellung, Training

ملخص :

في هذا الملف سوف نتكلم عن الأشياء الأساسية للدخول في عالم التحقيق الجنائي الرقمي وماهي الأشياء التي تحتاجها كمحقق وأين تبحث بشكل رئيسي لن نتحدث عن كل شيء سوف نتكلم فقط عن الأساسيات.

جدول المحتوى

2.....	كيف تقوم بعمل خطة للاستجابة للحوادث (How to create Incident Response Plan)
5.....	المهام المجدولة (Scheduled Tasks):
6.....	السجلات (Registry):
7.....	العمليات (Process)
8.....	عمليات التشغيل (Startup)
9.....	المنافذ النشطة (Active ports)
10	المستخدمين (Active ports)

كيف تقوم بعمل خطة للاستجابة للحوادث (How to create Incident Response Plan)

ماهي عملية الاستجابة للحوادث؟

الاستجابة للحوادث هي طريقة لإدارة عملية الاستجابة للحوادث. خطة الاستجابة للحوادث تساعد في عملية احتواء أي حادثة من خلال 6 خطوات رئيسية:

- التحضير [Preparation]
- التحقق [Identification]
- المجال/النطاق [Scope]
- الاستئصال [Eradication]
- التعافي/العودة لما قبل الحادثة [Recovery]
- ما تم تعلمه خلال الحادثة [Lessons Learned]

1- التحضير [Preparation]

إنشاء نظام تسجيل مركزي
من المهم من حيث توفير الوقت أن يتم فحص جميع البيانات من نقطة واحدة باستخدام نظام تجميع السجلات المركزي الذي يمكنه إدارة الملفات الكبيرة.

مزامنة الوقت

يعد تمكين NTP على جميع الأجهزة في الشبكة أمرًا مهمًا لمطابقة معلومات الوقت الخاصة بالسجلات التي تم جمعها.

إدارة حساب المستخدم

حقيقة أن أسماء المستخدمين للحسابات المختلفة التابعة للموظفين هي نفسها ومختلفة عن الموظفين الآخرين تجعل من السهل مراقبة أنشطة المستخدم في حالة وقوع حدث.

إدارة حسابات النظام والخدمة

يجب تعيين مديري الخدمات والأنظمة المستخدمة وإنشاء وثيقة حول كيفية الوصول إلى هؤلاء المديرين إذا لزم الأمر.

إدارة الأصول

يجب أن يتوفر الوصول الفوري إلى المعلومات مثل الأجهزة وأنظمة التشغيل وإصدارات التصحيح والحالة الحرجة.

اتصال آمن

إذا لزم الأمر ، قد يحتاج الفريق إلى التواصل بشكل مستقل عن الشبكة الداخلية ، في مثل هذه الحالات يمكن استخدام الهاتف المحمول أو رسائل البريد الإلكتروني الثانوية.

المعاملات القانونية

طريقة من سببها الإجراءات القضائية وفي أي الحالات يجب تحديدها قبل وقوع الحادث.

2- التحقق [Identification]

إعادة النظر (Review)

بالنسبة لحادث مشبوه محتمل ، يجب جمع معلومات أولية عن الحادث. ثم يجب تقرير ما إذا كان الموقف حدثًا مشبوهًا أم لا.

تكليف (Assignment)

يجب تحديد أول شخص يفحص الحادث. يجب على الشخص تدوين ملاحظات حول المراجعة.

استخدام قائمة التحقق (Using the Checklist)

يجب أن تكون هناك قوائم مرجعية للتحليل من أجل ضمان استجابات متنسقة للحوادث.

3- المجال/النطاق [Scope]

تميز الحدث (Characterize the event)

نظرًا لأن تحديد الحدث سيحدد الإجراءات الواجب اتخاذها ، فمن المهم تحديد نوع الحدث القادم. مثال DDoS :، الإصابة بالبرامج الضارة ، تسرب البيانات...

تصرف (Taking Action)

يجب اتخاذ الإجراء وفقًا للتقنية المستخدمة لاعتراض طريقة المهاجم بسرعة. إذا كان هناك حساب تم الاستيلاء عليه ، فيجب اتخاذ إجراءات بسيطة مثل إلغاء تنشيط الحساب وحظر IP بسرعة .

جمع البيانات (Data collecting)

سنكون هناك حاجة إلى صورة الذاكرة المتقلبة جنبًا إلى جنب مع جدار الحماية وحركة مرور الشبكة والسجلات الأخرى للتحقيق

العزل (Isolation)

يمكن أن يكون فصل النظام المخترق حلاً ، وعزله هو حل أكثر قابلية للتطبيق بعد تحديد الأنظمة المتأثرة بالحدث ، يتم قطع إمكانية انتشار المهاجم في الشبكة ويتم جمع المعلومات المتقلبة ، ويمكن اجتياز الخطوة التالية.

4- الاستئصال [Eradication]

تحديد السبب الجذري (Identifying the Root Cause)

مع المعلومات التي تم الحصول عليها في المرحلتين الثانية والثالثة ، يجب تحديد السبب الجذري للحدث. يجب بعد ذلك طرد المهاجم تمامًا.

تحديد إمكانات الجذور الخفية (Determining Rootkit Potential)

في حالة الاشتباه في وجود أدوات rootkits في النظام ، يجب تنظيف القرص وتثبيت نسخة احتياطية نظيفة. بعد التثبيت ، يجب تثبيت آخر تحديثات التطبيقات والأنظمة الحالية

تحسين الدفاع (Improve Defense)

أنظمة التشغيل والتطبيقات المستخدمة والشبكة والمنطقة منزوعة السلاح وما إلى ذلك. يجب تحديد أوجه القصور في الدفاع في المناطق والعمل على كيفية إجراء التحسين

فحص الضعف (Vulnerability Scan)

يجب تحديد نقاط الهجوم المحتملة على الشبكات والأنظمة وتصحيحها عن طريق إجراء عمليات فحص الثغرات الأمنية . عندما يتم إعداد الترتيبات اللازمة لمنع تكرار الحدث ، يمكن بدء مرحلة الاسترداد.

5- التعافي/العودة لما قبل الحادثة [Recovery]

تحقق (Verification)

تحقق من أن التسجيل والأنظمة والتطبيقات وقواعد البيانات والعمليات الأخرى تعمل بشكل صحيح .

يعيد (Restore)

في هذه المرحلة ، يتم تنسيق عملية الاستعادة .

يراقب (Monitoring)

يجب مراقبة الأنظمة للأحداث المتكررة . عندما لا يكون هناك موقف ضار متكرر أو نشاط غير عادي ، يتم اتخاذ الخطوة التالية.

6- ما تم تعلمه خلال الحادثة/الدروس المستفادة [Lessons Learned]

كتابة تقرير متابعة (Writing a Follow-up Report)
ويتضمن التقرير الاختبارات مع الخبير والسلطة التنفيذية ، ومراحل العمل الجيد والسيئ في خطة التدخل ، والتوصيات المتعلقة بالعملية.
يجب كتابة التقرير بطريقة يتأكد المدير من إغلاق الحدث.

المهام المجدولة (Scheduled Tasks):

غالبًا ما يستخدم المتسللون المهام المجدولة للاستمرار. مع "جدولة المهام" ، يمكن إدراج المهام المجدولة.



Task Scheduler
App

أو يمكنك استخدام الأمر "schtasks" عبر cmd.

```
Administrator: cmd
PS C:\Windows\system32> exit

C:\Windows\system32>schtasks.exe

Folder: \
TaskName                Next Run Time           Status
=====
GoogleUpdateTaskMachineCore 5/31/2021 12:27:07 AM Ready
GoogleUpdateTaskMachineUA 5/30/2021 6:27:07 PM Ready
npcapwatchdog N/A Ready
OneDrive Standalone Update Task-S-1-5-21 5/31/2021 11:23:48 AM Ready
TaskbarX N/A Ready

Folder: \Microsoft
TaskName                Next Run Time           Status
=====
INFO: There are no scheduled tasks presently available at your access level.
```

إذا كنت تريد الوصول إلى السجلات المرتبطة ببرنامج جدولة المهام ، فيمكنك الوصول إليها من

" Applications and Services Logs-Microsoft-Windows-TaskScheduler%4Operational.evtx"

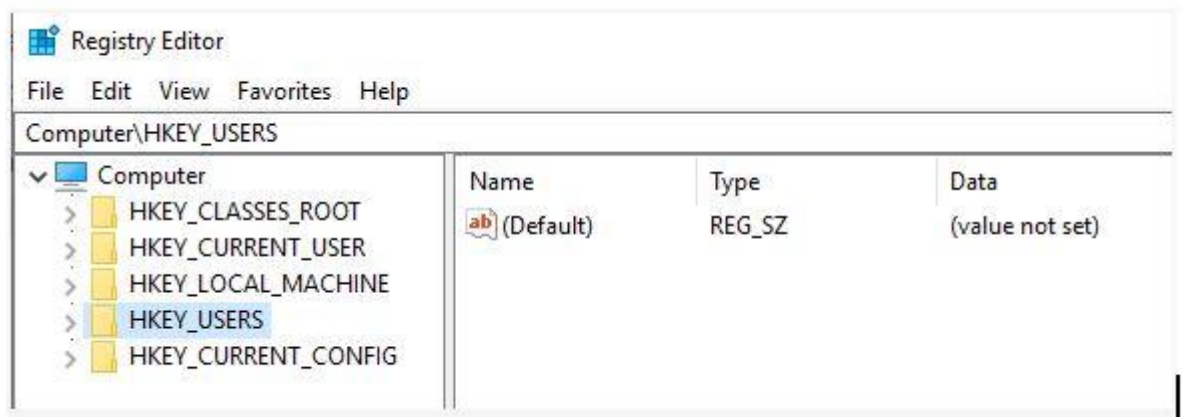
في عارض الأحداث.

أو يمكنك متابعة سجلات "الأمان" مثل:

- معرف الحدث 4698 - تم إنشاء مهمة مجدولة.
- معرف الحدث 4702 - تم تحديث مهمة مجدولة.

السجلات (Registry):

غالبًا ما يغير المهاجمون قيم التسجيل لضمان الاستقرار. كلما تغيرت قيمة التسجيل ، يتم إنشاء سجل **Windows EventID 4657**. يمكنك الاستمرار في تسجيل قيم التسجيل المستخدمة للاستمرار ، أو يمكنك التحقق من هذه القيم بعد الحدث.



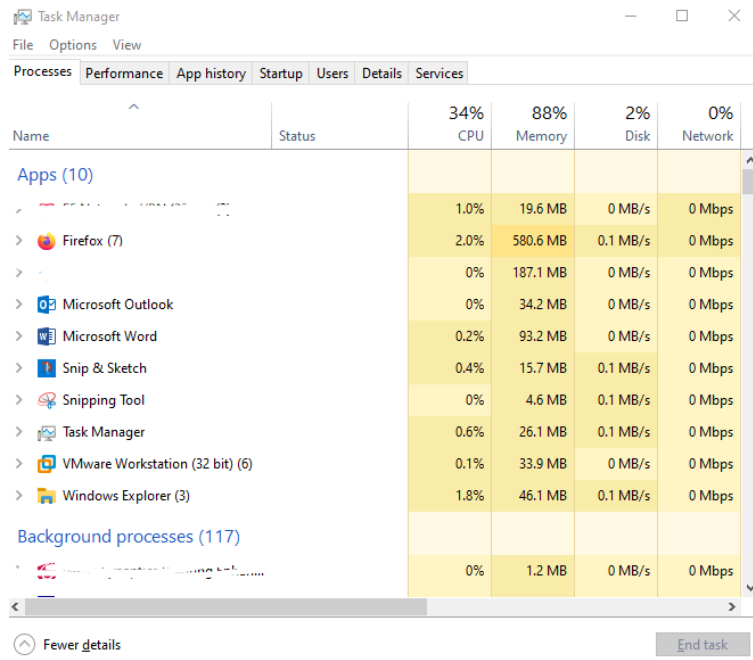
كثيرا ما تستخدم السجلات (Frequently used registries)

```
"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run"  
"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce"  
"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices"  
"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce"  
"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\0001"  
"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\0001\Depend"  
  
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run"  
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce"  
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices"  
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce"
```

من خلال التحقق من هذه السجلات ، يمكنك التحقق مما إذا كان المهاجم قد أسقط بابًا خلفيًا.

العمليات (Process)

يمكن التحقق من وجود أي برامج ضارة عن طريق فحص العمليات النشطة. يمكن الوصول إلى القائمة من علامة تبويب عملية "إدارة المهام"



The screenshot shows the Windows Task Manager window with the 'Performance' tab selected. The window title is 'Task Manager' and it has a menu bar with 'File', 'Options', and 'View'. Below the menu bar are tabs for 'Processes', 'Performance', 'App history', 'Startup', 'Users', 'Details', and 'Services'. The 'Performance' tab displays a summary of system resource usage: CPU at 34%, Memory at 88%, Disk at 2%, and Network at 0%. Below this summary is a table with columns for 'Name', 'Status', 'CPU', 'Memory', 'Disk', and 'Network'. The table is divided into two sections: 'Apps (10)' and 'Background processes (117)'. The 'Apps (10)' section lists various applications with their respective resource usage. The 'Background processes (117)' section shows a single entry for 'System Idle Process'.

Name	Status	34% CPU	88% Memory	2% Disk	0% Network
Apps (10)					
System Idle Process		1.0%	19.6 MB	0 MB/s	0 Mbps
Firefox (7)		2.0%	580.6 MB	0.1 MB/s	0 Mbps
Microsoft Outlook		0%	187.1 MB	0 MB/s	0 Mbps
Microsoft Word		0%	34.2 MB	0 MB/s	0 Mbps
Snip & Sketch		0.2%	93.2 MB	0 MB/s	0 Mbps
Snipping Tool		0.4%	15.7 MB	0.1 MB/s	0 Mbps
Task Manager		0%	4.6 MB	0.1 MB/s	0 Mbps
VMware Workstation (32 bit) (6)		0.6%	26.1 MB	0.1 MB/s	0 Mbps
Windows Explorer (3)		0.1%	33.9 MB	0 MB/s	0 Mbps
		1.8%	46.1 MB	0.1 MB/s	0 Mbps
Background processes (117)					
System Idle Process		0%	1.2 MB	0 MB/s	0 Mbps

إذا كنت تريد إنشاء قائمة باستخدام `cmd` ، يمكنك استخدام الأمر `Tasklist`.

```

Select Command Prompt

Microsoft Windows [Version 10.0.19041.928]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Halsulami>tasklist

Image Name                    PID Session Name        Session#    Mem Usage
-----
System Idle Process           0 Services             0             8 K
System                        4 Services             0          2,640 K
Registry                     124 Services            0         84,316 K
smss.exe                      536 Services            0          1,068 K
csrss.exe                     864 Services            0          5,408 K
wininit.exe                   964 Services            0          5,984 K
csrss.exe                     972 Console              1          5,776 K
services.exe                  628 Services            0         14,864 K
lsass.exe                     740 Services            0          26,148 K
svchost.exe                   1120 Services            0          35,748 K
WUDFHost.exe                  1152 Services            0          9,192 K
fontdrvhost.exe              1172 Services            0          4,260 K
svchost.exe                   1252 Services            0         20,920 K
svchost.exe                   1308 Services            0          10,364 K
WUDFHost.exe                  1344 Services            0         19,304 K
winlogon.exe                  1476 Console              1         12,496 K
fontdrvhost.exe              1548 Console              1         11,252 K
svchost.exe                   1672 Services            0         10,680 K
svchost.exe                   1692 Services            0          8,952 K
svchost.exe                   1704 Services            0          9,768 K
svchost.exe                   1744 Services            0         13,144 K
svchost.exe                   1772 Services            0         12,796 K
svchost.exe                   1896 Services            0         11,632 K
svchost.exe                   1904 Services            0         13,392 K
svchost.exe                   1936 Services            0          9,608 K
dwm.exe                       1984 Console              1        244,588 K
svchost.exe                   1996 Services            0         19,188 K
svchost.exe                   1860 Services            0         11,876 K
svchost.exe                   2056 Services            0         9,980 K
svchost.exe                   2164 Services            0         7,736 K

```

أثناء الاستجابة للحدث ، نحتاج عادةً إلى معلومات أكثر تفصيلاً. على سبيل المثال: العملية الأم (Parent Process) ، معلومات العملية الفرعية (child process) ، أنشطة الشبكة التي تقوم بها العملية ، تفريغ الذاكرة (Memory dump) وما إلى ذلك. يمكن استخدام أداة "Process Hacker" للحصول على مثل هذه البيانات الإضافية.

Process Hacker [DFIR\dfir]						
Hacker View Tools Users Help						
Refresh Options Find handles or DLLs System information						
Processes Services Network Disk						
Name	PID	CPU	I/O total ...	Private b...	User name	Description
SystemSettings.exe	2520			17.32 MB	DFIR\dfir	Settings
ProcessHacker.exe	3260	0.21		16.81 MB	DFIR\dfir	Process Hacker
TaskbarX.exe	3788	0.29	2.37 kB/s	23.41 MB	DFIR\dfir	TaskbarX
ctfmon.exe	5176			4.06 MB	DFIR\dfir	CTF Loader
explorer.exe	5480	0.37	40 B/s	93.58 MB	DFIR\dfir	Windows Explorer
sihost.exe	5780			5.96 MB	DFIR\dfir	Shell Infrastructure Host
openvpn-gui.exe	5792			3.56 MB	DFIR\dfir	
svchost.exe	5796			6.71 MB	DFIR\dfir	Host Process for Windows Ser...
svchost.exe	5856			6.87 MB	DFIR\dfir	Host Process for Windows Ser...
taskhostw.exe	6008			6.27 MB	DFIR\dfir	Host Process for Windows Tas...
StartMenu.exe	6216			2.86 MB	DFIR\dfir	Open-Shell Menu
svchost.exe	6244			6.57 MB	DFIR\dfir	Host Process for Windows Ser...
ShellExperienceHost.exe	6536			27.24 MB	DFIR\dfir	Windows Shell Experience Host
LockApp.exe	6676			11.48 MB	DFIR\dfir	LockApp.exe
SearchUI.exe	6704			65.73 MB	DFIR\dfir	Search and Cortana application
RuntimeBroker.exe	6868			4.13 MB	DFIR\dfir	Runtime Broker
RuntimeBroker.exe	6916			5.17 MB	DFIR\dfir	Runtime Broker
dllhost.exe	7292	0.16	2.52 kB/s	10.01 MB	DFIR\dfir	COM Surrogate
svchost.exe	7632			2.84 MB	DFIR\dfir	Host Process for Windows Ser...
ApplicationFrameHost.exe	7768			8.75 MB	DFIR\dfir	Application Frame Host
smartscreen.exe	8492			8.68 MB	DFIR\dfir	Windows Defender SmartScre...
SecurityHealthSystray.exe	8584			1.79 MB	DFIR\dfir	Windows Security notification...
vmtoolsd.exe	8724			1.41 MB	DFIR\dfir	

CPU Usage: 16% Physical memory: 76 GB (26.89%) Processes: 143

عمليات التشغيل (Startup)

تسرد علامة التبويب "Task Manager" الخاصة بـ "إدارة المهام" البرامج التي سيتم تشغيلها تلقائيًا عند بدء الجلسة.

Task Manager

File Options View

Processes Performance App history Startup Users Details Services

Name	Publisher	Status	Startup impact
Everything	voidtools	Enabled	High
Fluent Terminal	FS Apps	Disabled	None
Java Update Scheduler	Oracle Corporation	Enabled	Low
MLWapp2-1		Enabled	Not measured
Nimi Places		Enabled	Not measured
Open-Shell Menu	Open-Shell	Enabled	Medium
OpenVPN GUI for Windows	OpenVPN GUI	Enabled	Low
TightVNC Server	GlavSoft LLC.	Enabled	Low
Update		Enabled	Not measured
Update		Enabled	Not measured
vm3dservice.exe		Enabled	Low
VMware Tools Core Service	VMware, Inc.	Enabled	High
Windows Security notificati...	Microsoft Corporation	Enabled	Low

يمكن تقديم القائمة عبر CMD بالأمر التالي.

"wmic startup get"

المنافذ النشطة (Active ports)

يمكنك الكشف عن الباب الخلفي المحتمل عن طريق فحص المنافذ النشطة. للتحقق من المنافذ المفتوحة عبر CMD:

"netstat -ano"

```
Select Administrator: cmd
Microsoft Windows [Version 10.0.17763.1879]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>NETSTAT.EXE -ano

Active Connections

Proto Local Address          Foreign Address         State       PID
TCP    0.0.0.0:22              0.0.0.0:0               LISTENING   3456
TCP    0.0.0.0:80              0.0.0.0:0               LISTENING    4
TCP    0.0.0.0:135             0.0.0.0:0               LISTENING   996
TCP    0.0.0.0:445             0.0.0.0:0               LISTENING    4
TCP    0.0.0.0:3389            0.0.0.0:0               LISTENING  1064
TCP    0.0.0.0:5040            0.0.0.0:0               LISTENING  5248
TCP    0.0.0.0:5800            0.0.0.0:0               LISTENING  3492
TCP    0.0.0.0:5900            0.0.0.0:0               LISTENING  3492
TCP    0.0.0.0:7680            0.0.0.0:0               LISTENING  9556
TCP    0.0.0.0:49664           0.0.0.0:0               LISTENING   552
TCP    0.0.0.0:49665           0.0.0.0:0               LISTENING  1640
TCP    0.0.0.0:49667           0.0.0.0:0               LISTENING  2620
TCP    0.0.0.0:49670           0.0.0.0:0               LISTENING  2340
TCP    0.0.0.0:49671           0.0.0.0:0               LISTENING   716
TCP    0.0.0.0:49709           0.0.0.0:0               LISTENING  2992
TCP    0.0.0.0:62016           0.0.0.0:0               LISTENING   716
```

يمكن استخدام أداة "Process Hacker" للحصول على بيانات أكثر تفصيلاً تتعلق بالعملية. رابط التنزيل:

<https://processhacker.sourceforge.io/downloads.php>

يمكنك الوصول إلى البيانات من علامة التبويب "الشبكة".

المستخدمين (Active ports)

أثناء وقوع حادث إلكتروني ، يمكن للمهاجم إنشاء مستخدم جديد على النظام للاختباء أو الحصول على امتيازات أعلى. يمكنك التحقق من مستخدم مشبوه من خلال سرد المستخدمين الحاليين أثناء الاستجابة للحدث. تحقق عبر CMD:

“net user”

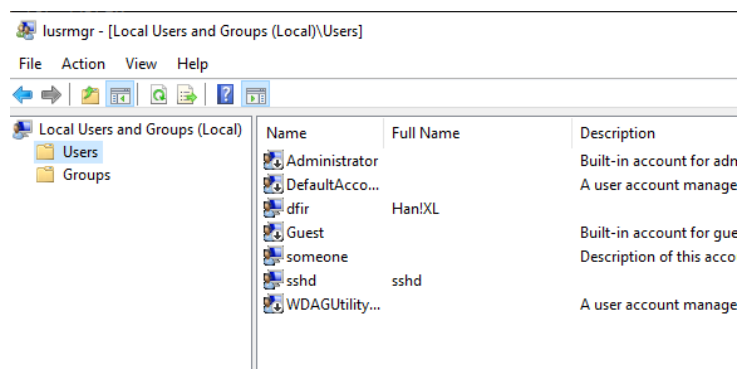
```
C:\Windows\system32>net user

User accounts for \\DFIR

-----
Administrator      DefaultAccount      dfir
Guest               someone             sshd
WDAGUtilityAccount
The command completed successfully.

C:\Windows\system32>
```

تحقق عبر "lusrmgr.msc"



كما ترى يوجد مستخدم اسمه "someone". يمكن استخدام الأمر التالي للحصول على مزيد من التفاصيل حول هذا المستخدم.

"net user {username}"

```
-----
Administrator      DefaultAccount      dfir
Guest               someone             sshd
WDAGUtilityAccount
The command completed successfully.

C:\Windows\system32>lusmgr
'lusmgr' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>net user someone
User name           someone
Full Name
Comment
User's comment
Country/region code 000 (System Default)
Account active       Yes
Account expires      Never

Password last set    5/31/2021 5:34:29 PM
Password expires      7/12/2021 5:34:29 PM
Password changeable   6/1/2021 5:34:29 PM
Password required     No
User may change password Yes

Workstations allowed  All
Logon script
User profile
Home directory
Last logon           Never
Logon hours allowed   All

Local Group Memberships
Global Group memberships *None
The command completed successfully.
```

باستخدام "Event ID 4720 - A user account was created"، يمكنك متابعة إنشاء المستخدم من سجلات الأحداث.