**Questions & Answers:**

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

А) Прежде всего необходимо понять какая активность нормальна для нашей системы (какие ресурсы и по каким протоколам и портам должны быть доступны сервисы, какая нагрузка нормальна для наших сервисов в зависимости от дня недели и времени суток, активность из каких стран и регион нормальна для данных сервисов).

Б) Необходимо организовать автоматический централизованный сбор, нормализацию и корреляцию логов с файрволла. Это позволит быстрее и эффективнее анализировать логи.

В) На основании первых двух пунктов необходимо настроить механизм оповещения и блокировки подозрительной активности.

1. **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)?**

А) Проверка оповещения. Просмотр логов на IDS Web сервере для уточнения деталей SQL-инъекции. Если оповещение подтверждено, то необходимо немедленно заблокировать IP-адрес с которого осуществлялась атака.

Б) В ходе анализа логов необходимо обратить внимание на повторяющиеся специфические запросы, запросы, которые содержат специальные символы (‘ ; --), логи ошибок (анализ данных логов может дать лучшее понимание о характере SQL-атаки, а так же о ее цели).

В) Анализ содержимого инъекции, определение полей для ввода, проверка базы данных на наличие изменений (сравнение с бекапом).

Г) Анализ глубины проникновения злоумышленника в систему, проверка логов системы, на которой располагается web-сервер. Проверка на отсутствие попыток подключения либо сканирования сети с машины, подвергшейся нападению.

Д) После установления поверхности атаки, которой подверглась система необходимо исключить дальнейшую возможность распространения вглубь инфраструктуры путем отключения от сети активов, перешедших под контроль злоумышленника, смена паролей скомпрометированных аккаунтов. То есть предпринять все действия для сокращения рисков и ущерба связанных с атакой.

Е) Восстановление системы из бекапов, на момент нормального функционирования. Устранение уязвимостей, которые позволили провести успешную атаку (проверка и саницизания вводимой информации, использование заранее подготовленных запросов, чтобы ограничить пользователя в возможности для будущих инъекций, ограничение прав пользователей для работы с базой данных).

З) После восстановления работоспособности необходимо провести анализ действий злоумышленника и специалистов СОКа для выработки шагов и рекомендаций по недопущению подобных ситуаций впредь.

**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?**

А) Мониторинг логов аутентификации: отслеживание неудачные попытки входа, отслеживание горизонтального перемещения (использование украденных учетных данных для входа на другие машины в сети), попытки повышения привилегий (отслеживание доступа к важной информации и системам).

Б) Использование EDR, XDR и threat intelligence решений для анализа поведения пользователей в системе.

**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.**

A) VPN. Определение нехарактерных попыток подключения для пользователя (вне рабочего времени, много неудачных попыток подключения). Подключение из нехарактерных для пользователя местоположений. Несколько сессий пользователя с разных устройств.

Б) Firewall. Множественные оповещения о блокировке подключений или оповещения о попытке доступа к конфиденциальной информации. Повышенный исходящий трафик. Использование нестандартных протоколов, портов, доменов для подключения.

В) СКУД. Проход вне рабочего времени либо множественные неудачные попытки входа. Проход в разных удаленных друг от друга местах здания по одному пропуску за короткий промежуток времени. Попытки получить доступ в ограниченные для прохода помещения либо помещения без прав допуска для данного сотрудника

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

А) Определение деятельности ВПО, а также площади атаки на инфраструктуру.

Б) Анализ поведения пользователя после обнаружения угрозы.

В) Анализ сетевой активности в связи с обнаружением ВПО.

Г) Изучение логов аутентификации в связи с обнаружением угрозы.

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

* 1. **What immediate actions would you take to contain the spread?**

А) Вне рабочего времени – изоляции системы от корпоративной среды. В рабочее время – связаться с администратором/пользователем ответственным за данную систему и уточнить по поводу данной активности, а затем, при необходимости изолировать.

Б) Провести анализ логов и пользовательской активности

В) Провести сканирование системы на наличие ВПО.

Г) Сменить учетные данные пользователя от имени которого произошел запрос на вредоносный сайт либо заблокировать учетную запись.

* 1. **In which system you can try to get additional information?**

А) EDR/XDR/Антивирус

Б) SIEM

В) IPS/IDS

Г) Threat Intelligence Platforms

Д) Firewall

* 1. **Which stage of the “kill chain” attack this case is?**

А) Вероятнее всего это стадия доставки (delivery) ВПО, однако запросы на вредоносные домены может происходить и на стадии команды и контроля (command and control).

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

А) Данный лог скорее всего взят со службы DNS. Происходят попытки послать UDP-пакеты на домены типа mggw-at-f3f0c6e992b7562598d9865b6fe8b3a6.com, при этом возвращается ответ **NXDOMAIN**, что обозначает отсутствие записей о существовании данного домена. Так же станным является то, что обращение идет на порт 8081, а не 53 (DNS). Данная активность с большой долей вероятности является вредоносной, однако может свидетельствовать о неправильной настройке службы DNS.

**8. What is happening according to the following events?**

А) От имени пользователя kheirkhabarov (скорее всего администратор системы kheirkhabarov.avp.ru) через командную строку была выполнена команда на запуск утилиты procdupm64, которая расположена на рабочем столе пользователя, с повышенными привилегиями (от имени системы). Данная утилита служит для снятия дампа процессора. Вызываема команда ‘procdump64.exe lsass.exe’ говорит о том, что хотят снять дамп процесса LSASS (Local Security Authority Subsystem Service). Данный процесс отвечает за применение политик безопасности, хранения данных пользователя и управления изменений паролей.

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

А) На данной системе при помощи утилиты PSEXEC удаленно была выполнена какая-то команда. Об этом говорит создание службы PSEXECSVC. Так как данная служба была создана в 1:05 это является крайне подозрительным событием, которое требует отдельного внимания.

10. **What can you tell about logs below?**

А) Создан скрипт на скачивание файла misa2.bin в папку с профилем пользователя и переименованием в случайное число от 10000 до 999999.exe и его запуск.

Б) Скрытно выполняется скрипт на получение значений из реестра, замена знаков с ~ на А, конвертация строки из кодировки Base 64. На основании данной информации скачивание файла из сети и его запуск.

В) Скрытно выполняется скрипт на скачивание файла encrypted.exe по пути c:\Users\Abby\AppData\Roaming.exe и запуск этого процесса.

Г) Во всех приведенных логах происходит сокрытие факта скачивания ВПО и его запуск при помощи Powershell.

1. **What can you tell about this script?**

А) Этот скрипт проверяет версию powershell в системе (версия 3 и выше). Отключает логирование вызова скриптов. Отключает антивирусное сканирование. Открывает веб-клиент и подключается к удаленному сайту. Загружает данные с указанного URL, расшифровывает их и преобразует их в powershell-скрипт.

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

А) Модификация реестра - ID 4657

Б) Установка службы - ID 7045. Ошибка службы - ID 7031 – 7034.

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

А) .chm – файл справки формата HTML. Может содержать вредоносные скрипты, а также при использовании уязвимостей злоумышленник может выполнить вредоносный код.

Б) При использовании в социальной инженерии, так как файлы со справкой о продукте вызывает меньше подозрений, а значит размещенные там фишинговые ссылки могут сработать с большей вероятностью.

В) Обход инструментов безопасности.

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

А) Большое количество AXFR запросов с внешнего IP может представлять угрозу так как это является одним из индикаторов приводящейся разведки для последующей атаки на инфраструктуру.

1. **How can you detect Golden Ticket attack?**

А) Использование SIEM и XDRМониторинг эскалации привилегий. Аномальное поведение аккаунтов с административными привилегиями (например доступ к ресурсам, которые обычно не используются).

Б) Мониторинг событий 4769 и 4768, на наличие аномалий в запросах к TGS.

В) Мониторинг конфиденциальной информации и сервисов, особенно если доступ осуществляется впервые либо вне рабочего времени или разрешенного доступа.

Г) Мониторинг эскалации привилегий. Аномальное поведение аккаунтов с административными привилегиями (например доступ к ресурсам, которые обычно не используются).

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

А) Изолирование системы и оценка объема компрометации. Анализ логов и определение затронутых в компрометации аккаунтов. Сброс и смена учетных данных, перевыпуск сертификатов. Отключение скомпрометированных аккаунтов. Восстановление контроллера домена из бэкапа, если есть вероятность утечки backup\_secret\_key, то ребилд контроллера. Просмотр и усиление политик безопасности. Аудит выданных привилегий. Мониторинг контроллера домена на наличие подозрительной активности после восстановления. Анализ цепочки атаки и выработка рекомендаций для предотвращения подобных инцидентов. Разработка рекомендаций и обучение персонала.

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

А) Script block logging

**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?**

А) Запущен процесс flashhelperservice.exe на базе ОС Windows с идентификатором процесса 6508. Adobe завершил поддержку Flash Player 31 декабря 2020 г., поэтому скорее всего это ВПО которое маскируется под легитимное.

1. **During the investigation you see this information: **

А) Это строка в кодировке Base 64, здесь зашифровано выполнение скрипта. Скрипт получает информацию и декодирует в UTF-8. Вывод перенаправляется в null, чтобы он не отобразился пользователю, для скрытия выполнения скрипта. Затем собирает выход из паплайна и преобразует в строку. Эта строка содержит в себе 2 части, которые разделены между собой четырьмя нулями. Пустые строки после разделения строки отбрасываются. Затем скрипт проверяет, что в результате разделения получено ровне 2 части. Вторая часть содержит какую-то полезную нагрузку в формате JSON. Первая часть содержит powershell скрипт и запускает. Это позволяет динамически выполнять код, который был передан в качестве части входных данных.

1. **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?**

А) Это крайне подозрительно, так как обычно services.exe запускается wininit.exe, а не explorer.exe. Это является признаком компрометации системы. Какое-то ВПО пытается замаскировать под легитимный процесс.

1. **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?**

А) На стороне сервера наш IP или диапазон IP, характерный для нашего региона, заблокирован. Файрволл блокирует сетевую активность приложения. Приложение не имеет необходимых прав доступа. Приложение получило повреждения файлов и не может выйти в сеть.

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

А) Данное доменное имя выглядит как случайно сгенерированное. Если такой адрес был получен в письме, то переходить по этой ссылке крайне нежелателен, так как с большой долей вероятности это сайт, который используется для фишинговой рассылки. Так же с данного домена может осуществляется разведка либо атака на инфраструктуру.

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

А) На ресурсе установлен OpenSSh 7.2p2 и Apache 1.1. ОС Ubuntu (16.04 или более поздней). 80 порт защищен файерволом. Для подключения по ssh используются криптографические ключи, однако ключи RSA должны быть достаточно длинными, чтобы обеспечивать должный уровень криптографии.

OpenSSh 7.2p2 имеет уязвимость CVE-2016-6210 (username enumeration), CVE-2023-38408

Apache Struts имеет уязвимость CVE-2011-1772 (XSS).

1. **Восстановите пароль из хеша fmarket.stf\admin:1337:aad3b435b51404eeaad3b435b51404ee:bebaecb23aa18f5375628541ff3fb3b8:::**

А) У этого пользователя пустой пароль LM-hash - *aad3b435b51404eeaad3b435b51404ee*hash пустого пароля