УДК 004.046

Керимкулова Гулсаат Кубатбековна, *e-mail: gulsaat@mail.ru*
Каримова Гульмира Токтомуратовна*, e-mail: k.gulpeace@kstu.kg*
КГТУ им. И.Раззакова,

ОБЗОР И ПРАКТИЧЕСКОЕ ЗНАЧЕНИЕ ТЕХНОЛОГИЙ OSINT

OSINT (Open-SourceIntelligence), или разведка на основе открытых источников, представляет собой методологию и процесс сбора, анализа и интерпретации информации, доступной из открытых источников. К таким источникам относятся интернет в целом, социальные сети, СМИ, публичные реестры, научные публикации и другие виды открытых источников. В отличие от закрытых или засекреченных данных информация, используемая в OSINT, доступна любому пользователю, что делает этот вид разведки легальным и этически допустимым при соблюдении соответствующих норм и правил.

Представим, что крупный банк или телекоммуникационная компания проводит мониторинг «внешнего» пространства на предмет утечек, имеющих к ним непосредственное отношение. Аналитики CTI (Cyber Threat Intelligence) могут использовать OSINT-методы для превентивного мониторинга специализированных форумов, где злоумышленники часто публикуют украденные данные. С помощью автоматизированных инструментов, в.т.ч. таких как Maltego, специалисты агрегируют, структурируют и анализируют найденную информацию, идентифицируют факт утечки либо отсутствия таковой и в случае необходимости переходят к дальнейшим мерам по усилению практик и внутрикорпоративной системы ИБ.Таким образом, сбор и анализ данных из открытых источников позволяют выявить потенциальные риски, связанные с контрагентами, клиентами или конкурентами.

Ключевые слова: OSINT,Maltego, публичные реестры, информационная безопасность

Введение

Для профессионального применения OSINT-методологий в рамках реальных кейсов существуют программные комплексы, включающие в себя возможности работы с разными источниками, например:

- Социальные сети и поисковые движки;
- Корпоративные источники;
- Сетевая инфраструктура;
- Onion/i2p/Freenet – то, что в бытовом сленге именуется “дарквебом”/”даркнетом”;
- Транспортные узлы и транспортные средства [1].

В тех случаях, когда работа отдельно взятого аналитика предполагает часто используемые «сценарии», можно внедрять элементы вторичной автоматизации запросов, т.е. первым слоем автоматизации может выступать программный комплекс, являющийся индустриальным стандартом (напр. Maltego, i2 AnalystNotebook, SpiderFoot, Lampyre), а второй слой – скриптинг последовательности запросов в рамках используемой среды представления данных [2].

Введение в Maltego

Maltego – программный комплекс, разработанный в 2007 году южноафриканской компанией Paterva и предназначенный для сбора данных из открытых источников с последующим анализом связей в рамках графовой среды представления [5].

Синтаксис MSL прост и интуитивно понятен для опытных программистов. При этом в силу очевидного фактора привязки к конкретному программному комплексу, пусть и имеющему большие возможности, MSL не предполагает ряда широко распространённых понятий, таких как, например, переменные, циклы и функции [6]. Основные элементы синтаксиса – пайплайны, фильтры и запуск запроса.

Пример создания сущности:

```
createEntity(maltego.Domain", "example.com");
```

Пример блока трансформаций:

```
paths {
run("paterva.v2.DomainToWebsite_DNS")
run("paterva.v2.DomainToDNSName_DNSBrute",slider:500)
run("paterva.v2.DomainToDNSName_ZT",slider:10000)
```

```
run("paterva.v2.DomainToSOAInformation")
run("paterva.v2.DomainToWebsiteDNS_SE",slider:255)
run("paterva.v2.DomainToDNSName_DB_interest")
run("paterva.v2.DomainToDNSName_DB","extra":"*",slider:500)
```

Написание скрипта вторичной автоматизации для последующего применения:

В первом блоке трансформаций проведём DNS-энумерацию. Далее настроим переход от DNS-записей к соответствующим IP-адресам (Maltego может работать как с IPv4, так и с IPv6) [7]. После чего добавляем две последующих блока – обогащение полученных IPv4-адресов при помощи Shodan, как показано на рисунке 1 (в.т.ч. с выявлением CVE), и запрос от полученных предыдущим блоком CVE в AlienVault OTX с дальнейшим выведением на граф ссылку на отчёт-первоисточник [8].

Входные данные:

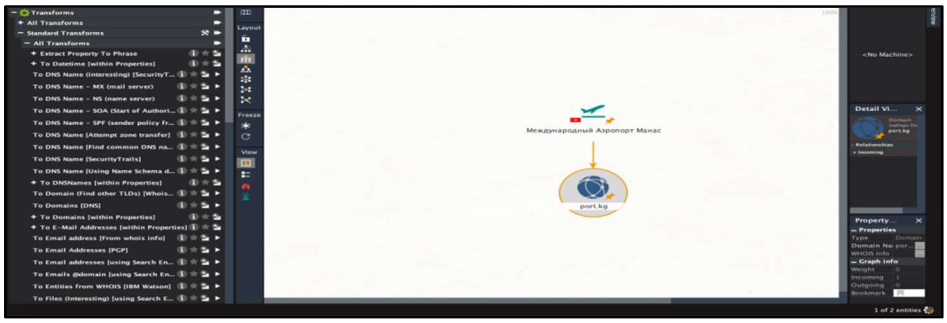


Рисунок 1– Входные данные

-Название (логическая сущность);

-Доменное имя port.kg.

В начале исследования создаём две сущности в графе, как показано на рисунке 2. Сущность доменного имени будет основной входной точкой запуска запросов.

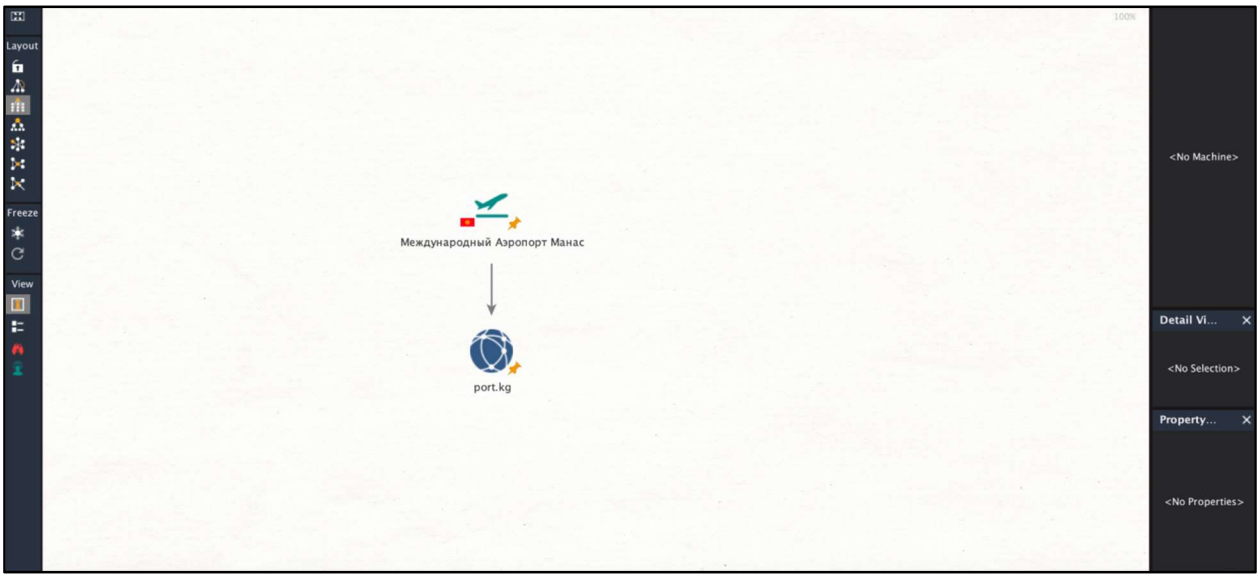


Рисунок 2 – Создание сущностей

Далее при выборе сущности домена мы видим в соответствующем окне доступные внешние поисковые запросы, как показано на рисунке 3, работающие для данного конкретного объекта.

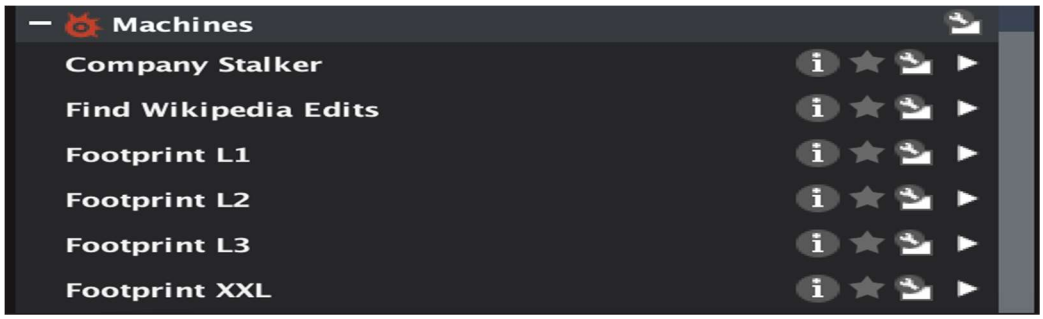


Рисунок 3 – Список поисковых запросов

Также мы видим доступные скрипты (рис. 3) запросов – т.н. «machines», именно они являются фокусом данной работы в контексте этого исследования. Поскольку выбранный нами в среде представления объект относится к категории сетевой инфраструктуры, доступные скрипты по умолчанию оперируют именно теми запросами, которые работают для данной категории[8].

Для начала исследования запустим доступный нам скрипт «Footprint L1». Данный сценарий запросов запускает процесс DNS-энумерации в рамках используемой среды представления, после чего «вытаскивает» из полученных DNS-записей полученные IP-адреса, после чего посредством них получает сетевые диапазоны, от которых в свою очередь переходит к ASN (номерам автономных систем) и далее от них к владеющим данными автономными системами организациям [8].

Это позволяет нам понять первичную картину исследования и выбрать дальнейшие фокусные направления, например, следующей отправной точкой могут быть IPv4-адреса, к которым относятся определённые сервисы и приложения, а следующей подзадачей исследования – выявление критических уязвимостей, получение их характеристик и более подробных сведений, для чего будут использоваться такие источники – IoT-сканер Shodan и открытая платформа аналитики киберугрозAlienVault OTX [9].

Использование Shodan

Shodan, часто называемый «поисковой системой для IoT», представляет собой эффективный ИБ-инструмент, который предоставляет исследователям и специалистам по информационной безопасности мощные возможности для обнаружения и анализа подключенных к интернету устройств[9]. Разработанный американским специалистом Джоном Матерли в 2009 году Shodan сканирует и индексирует устройства по всему миру, позволяя пользователям искать конкретные типы оборудования, обнаруживать уязвимости и анализировать глобальные тенденции в области ИБ.

Технические характеристики

Shodan осуществляет непрерывное сканирование интернета, собирая и индексируя данные о подключенных устройствах. Ключевые аспекты работы Shodan включают:

- **Сбор данных**: Shodan использует распределенную сеть сканеров, которые периодически «опрашивают» IP-адреса по всему миру, собирая информацию о баннерах сервисов, открытых портах и конфигурациях устройств.
- **Индексация**: Собранные данные обрабатываются и индексируются, что позволяет пользователям быстро находить устройства по ключевым параметрам, таким как тип устройства, используемое программное обеспечение, версия операционной системы и открытые порты.
- **Интерфейсы**: Shodan предоставляет веб-интерфейс, API и интеграции с другими инструментами, что позволяет осуществлять поисковые запросы, анализировать результаты и автоматизировать задачи [10].

Пример запроса в Shodan для поиска веб-камер, использующих определенную версию прошивки:

```
org:"Netwave" firmware:"2.0.3.0"
```

Примеры использования

Shodan широко используется в различных сценариях, включая:

- **Оценку безопасности инфраструктуры**: Организация может использовать Shodan для анализа своего сетевого периметра, обнаружения неправильно настроенных устройств и выявления потенциальных уязвимостей.
- **Исследования угроз**: Исследователи могут анализировать глобальные тенденции в области безопасности, отслеживать распространение той или иной уязвимости среди разных категорий устройств и изучать новые типы атак.
- **Инвентаризацию активов**: Организации могут проводить аудит подключенных устройств, отслеживая изменения и аномалии в своей инфраструктуре.
- **Тестирование на проникновение**: Пентестеры используют Shodan для предварительного сбора информации о целевых системах перед проведением более обдуманных атак [10].

Сравнение с другими инструментами

Shodan уникален в своем подходе к сбору и анализу данных об устройствах, подключенных к интернету. Однако существуют и другие инструменты, которые можно использовать для аналогичных целей:

- **Censys**: Инструмент для анализа IoT, который собирает и индексирует данные об устройствах и сервисах, предоставляя детальную информацию – наиболее близкий аналог.
- **ZoomEye**: Китайский аналог Shodan, который также осуществляет сканирование и индексирование устройств в интернете, но с акцентом на азиатский рынок.
- **BinaryEdge**: Платформа, которая осуществляет массовое сканирование и анализ интернета, предоставляя API для доступа к собранным данным.

В отличие от NMap, который требует ручного сканирования и анализа, Shodan предоставляет готовую базу исторических (но регулярно обновляющихся) данных, что может значительно упростить процесс выявления рисков [11].

Юридические и этические вопросы

В использовании Shodan стоит не забывать о юридических и этических нормах. Хотя Shodan осуществляет сканирование публичных IP-адресов, использование его данных для несанкционированного доступа или атак на устройства является незаконным. Специалисты по безопасности должны:

- **Соблюдать законы**: Убедиться, что использование Shodan соответствует местным законам о компьютерной информации.
- **Этические принципы**: Уважать конфиденциальность и права владельцев устройств, не осуществлять несанкционированные действия.
- **Получать разрешения**: Получать разрешение от владельцев устройств и сетей перед проведением каких-либо действий, основанных на данных Shodan – данный сценарий актуален для коммерческого пентеста [13].

Введение в AlienVault OTX

Платформа AlienVaultOpenThreatExchange (OTX) является одной из ведущих платформ для обмена информацией об угрозах (CyberThreatIntelligence, CTI). Она разработана компанией AlienVault (ныне часть AT&T Cybersecurity) и предоставляет исследователям и специалистам по информационной безопасности доступ к коллективным данным об угрозах, собранным со всего мира [14]. OTX позволяет пользователям обмениваться индикаторами компрометации (IndicatorsofCompromise, IoCs), анализировать текущие киберугрозы и интегрировать эти данные в свои системы защиты.

Технические характеристики

1. **Архитектура и компоненты**:
    - **OTX Server**: Центральный сервер, который собирает, анализирует и распределяет данные об угрозах.
    - **OTX Endpoint**: Клиентские устройства и системы, которые отправляют данные об

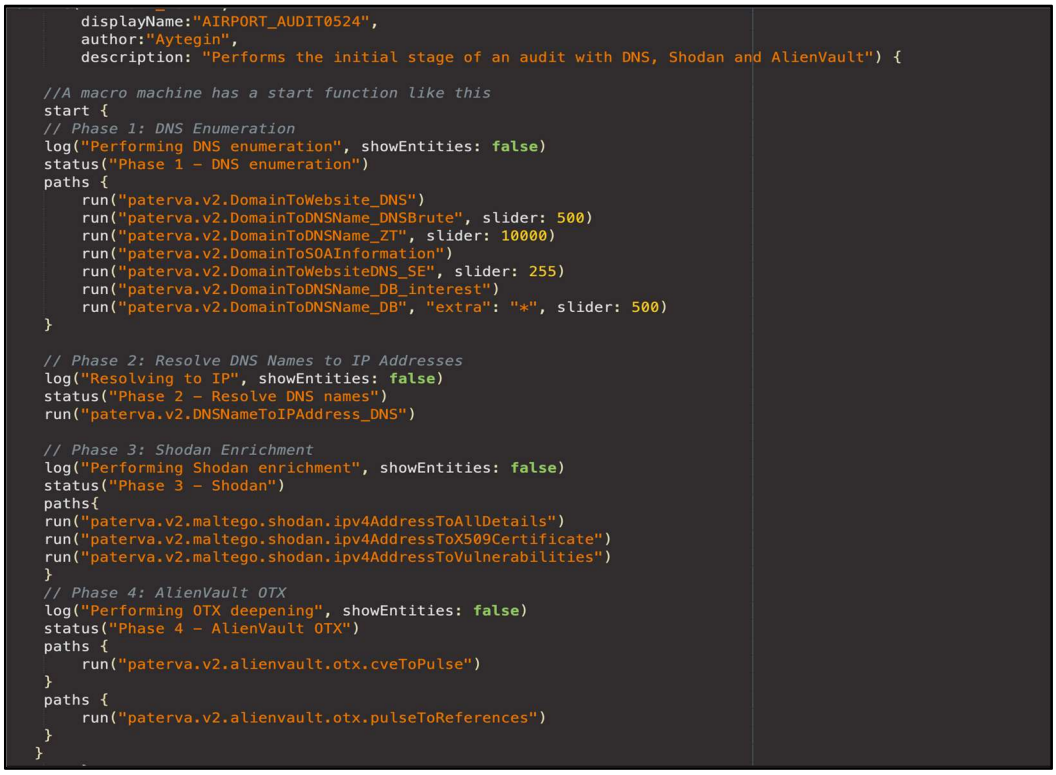
угрозах на сервер и получают обновления в реальном времени.
    - **OTX API**: Программный интерфейс, который позволяет пользователям интегрировать данные OTX в свои собственные системы и приложения [16].
2. **Типы данных**:
    - **Индикаторы компрометации (IoCs)**: IP-адреса, доменные имена, URL-адреса, хэши файлов и другие данные, указывающие на потенциальную угрозу.
    - **Пульсы (Pulses)**: Наборы связанных IoCs, сгруппированные в зависимости от конкретной угрозы или кампании.
    - **Аналитика и отчеты**: Подробные анализы и отчеты о выявленных угрозах, предоставляемые как самой платформой, так и пользователями.
3. **Интеграция и автоматизация**:
    - **SIEM**: Интеграция с системами управления информацией и событиями безопасности (SIEM), такими как AlienVault USM, для автоматического получения и обработки данных об угрозах.
    - **SOAR**: Возможность интеграции с платформами для оркестрации, автоматизации и реакции на инциденты (SOAR).
    - **Разработчики**: API для разработчиков позволяет создавать кастомные решения и интеграции [16].

Примеры использования

1. **Обнаружение и реагирование на инциденты**:
    - Исследователи используют данные OTX для выявления новых угроз и создания правил для своих систем безопасности.
    - Платформа позволяет автоматизировать процесс реагирования на инциденты, сокращая время обнаружения и устранения угроз.
2. **Анализ угроз**:
    - Специалисты по ИБ могут анализировать данные о текущих угрозах, используя пульсы, чтобы понять контекст и тактику, техники и процедуры (TTP’s) злоумышленников.
    - Возможность объединения данных, полученных из других платформ и источников для получения более полной картины.
3. **Обмен информацией**:
    - Пользователи могут делиться своими собственными данными об угрозах с сообществом OTX, создавая и обогащая таким образом «коллективную базу знаний».
    - Платформа поддерживает создание частных групп для обмена данными внутри организации или между доверенными партнерами.

Сравнение с другими инструментами

AlienVault OTX выделяется среди других CTI-платформ своей открытостью и акценту на коллективном обмене данными. В отличие от коммерческих платформ, таких как Fire Eye Threat Intelligence, Recorded Future или Kaspersky CTI, OTX предоставляет доступ к своим данным бесплатно, что делает его привлекательным для небольших компаний и независимых исследователей [17]. Кроме того, интеграция с решениями AT&T Cybersecurity расширяет возможности платформы, позволяя пользователям получать более комплексную защиту.



```
    displayName:"AIRPORT_AUDIT0524",
    author:"Aytegin",
    description: "Performs the initial stage of an audit with DNS, Shodan and AlienVault") {

//A macro machine has a start function like this
start {
// Phase 1: DNS Enumeration
log("Performing DNS enumeration", showEntities: false)
status("Phase 1 - DNS enumeration")
paths {
    run("paterva.v2.DomainToWebsite_DNS")
    run("paterva.v2.DomainToDNSName_DNSBrute", slider: 500)
    run("paterva.v2.DomainToDNSName_ZT", slider: 10000)
    run("paterva.v2.DomainToSOAInformation")
    run("paterva.v2.DomainToWebsiteDNS_SE", slider: 255)
    run("paterva.v2.DomainToDNSName_DB_interest")
    run("paterva.v2.DomainToDNSName_DB", "extra": "*", slider: 500)
}

// Phase 2: Resolve DNS Names to IP Addresses
log("Resolving to IP", showEntities: false)
status("Phase 2 - Resolve DNS names")
run("paterva.v2.DNSNameToIPAddress_DNS")

// Phase 3: Shodan Enrichment
log("Performing Shodan enrichment", showEntities: false)
status("Phase 3 - Shodan")
paths{
run("paterva.v2.maltego.shodan.ipv4AddressToAllDetails")
run("paterva.v2.maltego.shodan.ipv4AddressToX509Certificate")
run("paterva.v2.maltego.shodan.ipv4AddressToVulnerabilities")
}
// Phase 4: AlienVault OTX
log("Performing OTX deepening", showEntities: false)
status("Phase 4 - AlienVault OTX")
paths {
    run("paterva.v2.alienvault.otx.cveToPulse")
}
paths {
    run("paterva.v2.alienvault.otx.pulseToReferences")
}
}
```

Рисунок 4 – Создание нового документа

Для начала создадим в Maltego свежий документ с первоначальными входными данными, т.е. аэропортом и доменным именем, как показано на рисунке 4.

Используем написанный нами в рамках работы скрипт рисунок 4. Данная программа начинается с DNS-энумерации, после чего переходит к запуску трансформаций Shodan для получения доступных деталей об IPv4-адресах, в.т.ч. о критических уязвимостях [17]. После блока Shodan начинается блок AlienVault OTX, в рамках которого осуществляется запрос в базу киберугроз от полученных в графе критических уязвимостях, от которых уже в свою очередь осуществляется запрос, возвращающий в графу ссылки на первоисточник. После выполнения скрипта применяем по очереди оба варианта условного форматирования, чтобы увидеть, какие уязвимости затрагивают элементы CISCO, а какие – элементы ORACLE, что позволит нам более информировано подойти к гипотетической следующей стадии исследования [18]. В статье приведены результаты работы кода программы, приведенной на рисунке 4, и полный результат её выполнения и некоторые спецификации в приближении и выводы по возможным дальнейшим действиям от полученного результата с логическим переходом к следующей стадии исследования.

Введение в NMap

NMap (NetworkMapper) является одним из наиболее широко используемых инструментов для анализа сетевой безопасности. Он был разработан Гордоном Лион (известным также под псевдонимом Fyodor) и впервые представлен общественности в 1997 году. NMap предоставляет исследователям и специалистам по информационной безопасности мощные возможности для сканирования и анализа сетевых структур, выявления активных хостов, определения открытых портов, идентификации служб и обнаружения уязвимостей [19].

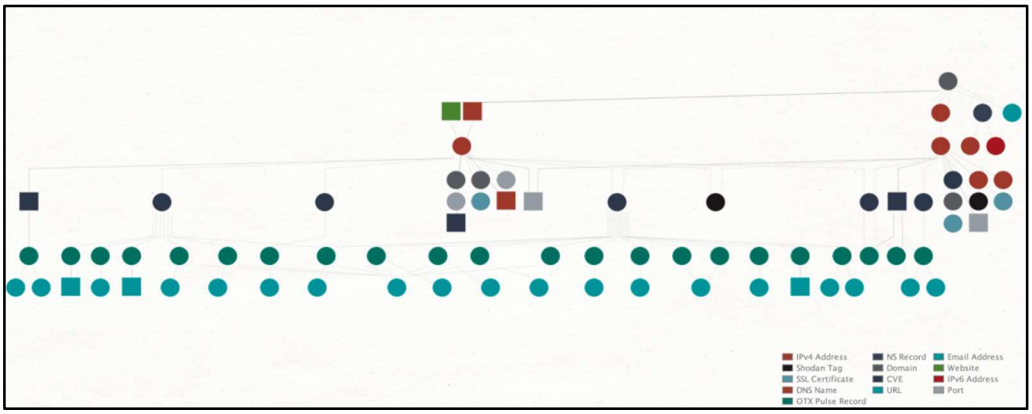


Рисунок 5 – Результаты анализа сетевых структур

UNIX-подобные операционные системы. С момента своего создания инструмент прошел значительный путь развития, включая добавление поддержки для Windows, улучшение производительности и интеграцию с другими системами безопасности. Сегодня NMap поддерживает широкий спектр операционных систем, включая Linux, Windows, macOS и другие.

Технические характеристики

NMap использует различные методы сканирования для определения состояния сетевых хостов и портов. Основные методы включают:

- **SYN-сканирование** (полуоткрытое сканирование), которое является быстрым и малозаметным для систем детекции.
- **TCP-сканирование**, которое устанавливает полное TCP-соединение с целевым хостом.
- **UDP-сканирование**, используемое для проверки открытых UDP-портов.
- **ICMP-сканирование**, позволяющее определить активные хосты на основе ответов на ICMP-запросы [21].

Функционал NMap также в себя включает мощный скриптовый движок NSE (Nmap Scripting Engine), который позволяет автоматизировать задачи по обнаружению уязвимостей, выполнению сложных сетевых аудитов и сбору информации. Скрипты NSE пишутся на языке программирования Lua, что делает их гибкими и расширяемыми.

Примеры использования

Исследователи и специалисты по информационной безопасности используют NMap для различных задач, включая:

- **Картирование сети**: Определение топологии сети, активных хостов и маршрутов.
- **Аудит безопасности**: Обнаружение уязвимостей в сетевых службах и приложениях.
- **Мониторинг доступности**: Проверка доступности критически важных сетевых ресурсов.
- **Тестирование на проникновение**: Сканирование целевых систем для выявления потенциальных векторов атаки в полноценной симуляции реального сценария поведения злоумышленников.

Пример команды для сканирования сети на наличие активных хостов и открытых портов:

```
nmap -sP 192.168.1.0/24
```

Сравнение с другими инструментами

NMap часто сравнивается с другими инструментами для сканирования и аудита сетей, такими как:

- **OpenVAS**: Более специализированный инструмент для анализа уязвимостей, который включает в себя управление уязвимостями и создание отчетов.
- **Nessus**: Коммерческий инструмент для сканирования на уязвимости, предлагающий обширную базу данных уязвимостей и удобный интерфейс.
- **Masscan**: Инструмент для очень быстрого сканирования, способный сканировать весь интернет за считанные минуты, но с меньшей функциональностью в сравнении с NMap.

NMap выделяется своей гибкостью, подверженностью индивидуальной пользовательской кастомизации и мощными возможностями скриптинга, что делает его предпочтительным выбором для многих профессионалов в области ИБ [22].

При использовании NMap важно не забывать о юридической стороне вопроса – несанкционированное сканирование сетей без разрешения может привести к юридическим последствиям. Специалисты должны всегда получать согласие владельцев сетей и ресурсов перед проведением сканирования. Кроме того, результаты сканирования должны обрабатываться с соблюдением конфиденциальности и защиты данных [24].

NMap остается важным инструментом для исследователей и ИБ-специалистов, предоставляя эффективные средства для анализа и аудита компьютерных сетей. Его гибкость, расширяемость и широкие возможности делают его незаменимым в арсенале ИБ-профессионала.

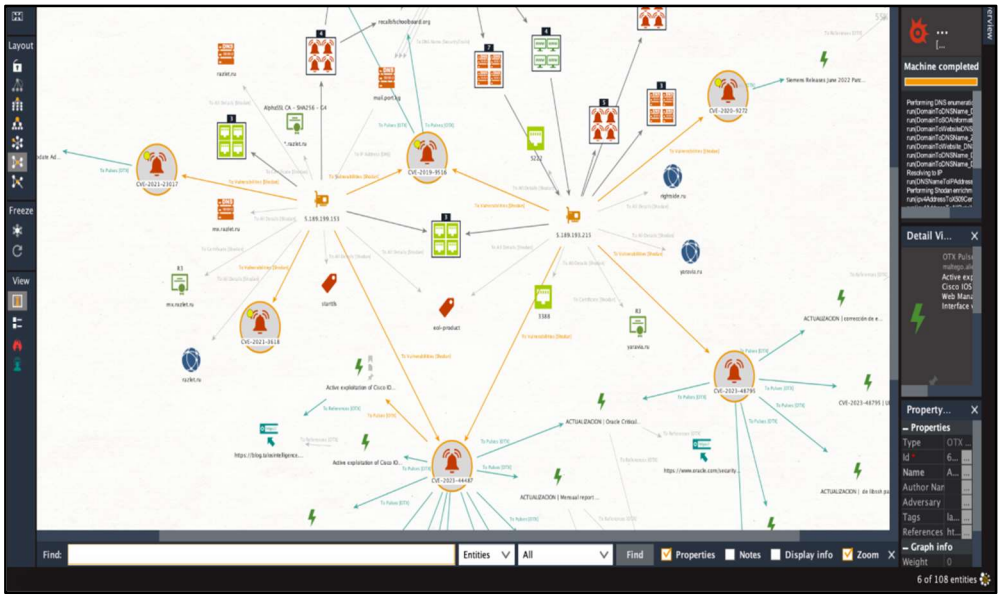


Рисунок 6 – Результаты сканирования NMap

Заключение

Итак, в рамках данной статьи:

- Было дано определение и примеры применения методологии OSINT;
- Было проведено рассмотрение индустриальных инструментов применительно к конкретному виду задач;
- Были написаны и протестированы скрипты внутренней автоматизации данных инструментов, также применительно к конкретному виду задач;
- Была рассмотрена проблематика транспортной кибербезопасности и отдельных элементов в подходах к её обеспечению.

Литература

1. https://www.tandfonline.com/doi/pdf/10.1080/16161262.2023.2224091
2. https://osintframework.com/
3. https://www.gutenberg.org/ebooks/34815
4. https://www.recordedfuture.com/threat-intelligence-101/intelligence-sources-collection/osint-framework
5. https://docs.maltego.com/support/solutions/articles/15000019249-machines-transform-macros-#overview-0-0
6. https://scalar.usc.edu/works/conducting-surface-web-based-research-with-maltego-carbon/what-is-a-macro-what-is-pseudo-code
7. https://docplayer.net/32830503-11-25-2012-maltego-scripting-language-1-1.html
8. https://www.shodan.io/

9. https://irjaes.com/wp-content/uploads/2021/12/IRJAES-V6N4P275Y21.pdf
10. https://otx.alienvault.com/
11. https://cybersecurity.att.com/documentation/resources/pdf/otx-user-guide.pdf
12. https://nmap.org/book/nse.html
13. https://www.lua.org/spe.html
14. https://www.lua.org/gems/lpg.pdf
15. https://scilua.org/
16. https://eluaproject.net/overview/
17. https://crp.trb.org/acrpwebresource2/wp-content/themes/acrp-child/documents/188/original/acrp_r140.pdf
18. https://www.uaa.aero/docs/The_Nextgen_Cybersecurity_for_U.S._Airports.pdf
19. https://www.securityvision.ru/blog/kii-chto-eto/
20. https://mail.wjaets.com/sites/default/files/WJAETS-2024-0024.pdf
21. https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf
22. https://www.researchgate.net/figure/Power-grid-cyberattack-scenarios_fig2_355122168
23. https://jestec.taylors.edu.my/Special%20Issue%20ICCSIT%202018/ICCSIT18_03.pdf
24. https://securityaffairs.com/43196/hacking/railroad-systems-vulnerabilities.html
25. https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf
26. https://www.todaysmedicaldevelopments.com/news/cybersecurity-increase-ransomware-hospitals-attacks/
27. https://www.inss.org.il/wp-content/uploads/2024/02/Part-4.pdf
28. https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-040.pdf
29. https://www.kaspersky.ru/about/press-releases/2014_stuxnet-v-detaliakh
30. https://www.sipa.columbia.edu/sites/default/files/2022-11/NotPetya%20Final.pdf
31. https://grahamcluley.com/the-inside-story-of-the-maersk-notpetya-ransomware-attack/
32. https://www.doj.nh.gov/consumer/security-breaches/documents/air-canada-20180831.pdf