Разработка методики тестирования на уязвимости сертифицированного межсетевого экрана для защиты объектов критической информационной инфраструктуры

Любименко Дмитрий Анатольевич
заместитель генерального директора АО «ПО «Аквамаш», г. Волгоград, Россия, d.lyubimenko@aquamash.ru

АННОТАЦИЯ

Введение: анализ работы межсетевого экрана нового поколения в качестве системы защиты периметра предприятия, являющегося субъектом критической информационной инфраструктуры, проверка программно-аппаратного комплекса на наличие уязвимостей является актуальной задачей. **Цель исследования**: разработка методики тестирования next generation firewall на наличие уязвимостей для злоумышленников, занимающихся кражей данных, шифрованием, шантажом. **Результаты**: в рамках тестирования развернута операционная система на базе Kali Linux укомплектованная в базовой конфигурации средствами для сканирования, поиска уязвимости в сетевом, серверном оборудовании. В качестве целевой системы для обследования выбран наиболее распространенный и часто используемый межсетевой экран нового поколения usergate версии 6.1.8. Для сканирования, тестирования и эксплуатации уязвимостей сформирован перечень типовых прикладных программ используемых большинством злоумышленников для проникновения внутрь периметра: nessus, netcat, Yersinia, THC Hydra, Metasploit Framework. Результатом проделанной работы стала разработка практической методики, позволяющей провести полноценное тестирование next generation firewall на наличие уязвимостей. Возможно применение не только для тестирования продукции компании usergate. Но также аналогичных технических решений от альтернативных производителей – Eltex, Ideco, других. Универсальность разработанной методики обеспечена использованием практически во всех решениях в качестве базовой системы Unix/Linux. **Практическая значимость**: Методика позволяет систематизировать процесс тестирования, сформировать контрольные точки, обеспечить комплексную проверку программно-аппаратного комплекса на наличие уязвимостей, «закладок» разработчика. Применение актуальных средства для проверки таких комплексов позволит смоделировать поведение злоумышленника целью которого является проникновение и закрепление внутри закрытого сетевого контура. Приведенная методика дает возможность своевременно обнаружить проблемные места, обеспечить их ликвидацию и ускорит выпуск обновлений для закрытия уязвимостей, дает возможность своевременно формировать бюллетень информационной безопасности.

КЛЮЧЕВЫЕ СЛОВА: система защиты периметра; межсетевой экран нового поколения; usergate; NGFW; закрытие уязвимостей.

Введение

Государственной думой ещё в 2017 был принят Федеральный закон №187-ФЗ «О безопасности критической информационной инфраструктуры». Нормативная документация этого типа предъявляет серьезные требования к техническим и организационным мерам, принятым на предприятиях, входящих в установленный перечень. В связи с началом специальной военной операции (СВО) пристальное внимание со стороны ФСТЭК и ФСБ уделяется именно предприятиям оборонно-промышленного комплекса. Вне зависимости от наличия значимых объектов критических объектов инфраструктуры, при отнесении предприятия к субъектам критической информационной инфраструктуры (КИИ), необходимо использовать сетевое оборудование только отечественного производства [1].

Требования к сетевому, коммутационному оборудованию устанавливаются Приказом ФСТЭК №235. Сетевой периметр обязательно должен быть защищен межсетевыми экранами, имеющими сертификат ФСТЭК с классом защиты не ниже требуемого. Устанавливаются требования к квалификации работников отдела информационной безопасности. В РФ существует несколько ключевых производителей межсетевых экранов нового поколения, имеющих сертификат ФСТЭК. Большинство оборонных предприятий используют Континент или Usergate.

В моей работе будет рассмотрен вопрос наличия уязвимостей межсетевого у экрана Usergate D200. В качестве тестовой машины задействуется виртуальный образ на базе vmware. Тестирование на наличие уязвимостей будет выполняться типовым программным обеспечением, предустановленным в Kali Linux. Сканирование выполняется из сети внутри периметра. Конфигурация межсетевого экрана – базовая, без предустановленных плагинов, «из коробки». Это позволит объективно оценить уровень защищенности межсетевого экрана [2].

Компоненты для тестирования методики сканирования уязвимостей

Для разработки методики тестирования выбраны следующие программно-аппаратные комплексы, условия построения сетевого периметра:

– целевая системы – ПАК Usergate d200 на базе операционной системы 6.1.8 (выпущен кандидат-релиз версии 7.0, но версия не является стабильной);

– операционная система Kali Linux на базе Debian – один из самых распространенных дистрибутивов для тестирования защищенных периметров на проникновение.

Выполнение работы осуществляется с использованием тестового стенда, включающего в себя коммутатор доступа Eltex 2448b. Использование оборудования этого типа позволяет смоделировать ситуацию попытки проникновения с максимальной реалистичностью. Создано несколько тестовых vlan для размещения межсетевого экрана, атакующей системы [3]. Схема сетевого взаимодействия представлена на рис. №1. Таблица vlan, назначенных на интерфейсах программно-аппаратных комплексов, представлена в табл. №1.

Табл. 1. Таблица vlan тестируемого проекта

Наименование vlan	Адрес сети	Маска	Шлюз
Trusted	10.80.8.0	/24	10.80.8.1
Management	10.80.6.0	/24	10.80.6.1
Untasted	10.80.7.0	/24	10.80.7.1

Для симуляции условий, максимально приближенных к реальным, была построена схема из двух узлов Usergate. Первый выступает в качестве сервера. Второй – клиент. Между узлами поднят VPN туннель. Предполагается что злоумышленнику известны ip адреса публичного типа (зона untrasted). Внутренняя адресация неизвестна. Это позволит приблизить процесс построения вектора атаки к реальному, избежать «читерства». Для шифрования трафика используется IPSec. Атака будет выполняться последовательно на оба узла. Режим построения VPN между двумя межсетевыми экранами – Site-to-Site [5].

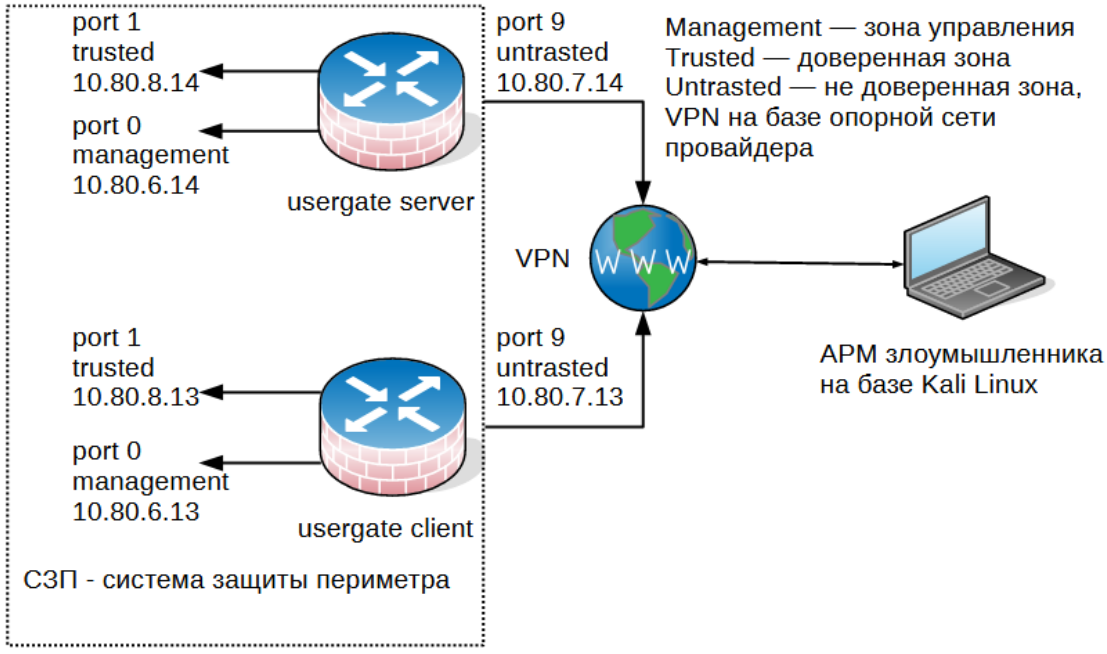

Рис. 1 Структурная схема системы защиты периметра и АРМ злоумышленника

Физическая коммутация выполняется через коммутатор L2 производства компании Eltex 1124. Все vlan являются тегированными. Причем номер vlan соответствует предпоследнему октету сети:

– Management – vlan 6;
– Trusted – vlan 8;
– Untrasted – vlan 7.

АРМ злоумышленника будет находиться в подсети untrusted – предполагается эмуляция атаки из зоны internet [6]. В зоне trusted и management разрешены все без исключения протоколы работы. Подробная информация представлена в табл. №2.

Табл. 2. Таблица разрешенных сервисов тестируемого проекта

Наименование зоны	Наименование разрешенных сервисов
Management	ping, snmp, captive, cluster, vrrp, консоль администрирования, DNS, HTTP-прокси, консоль администрирования, SMTP, POP3, CLI SSH, VPN, SCADA, Reverse-прокси, веб-портал, log analayzer, ospf, bgp, rip, snmp-прокси, ssh-прокси, multicast, NTP-сервис
Trusted	ping, snmp, captive, cluster, vrrp, консоль администрирования, DNS, HTTP-прокси, консоль администрирования, SMTP, POP3, CLI SSH, VPN, SCADA, Reverse-прокси, веб-портал, log analayzer, ospf, bgp, rip, snmp-прокси, ssh-прокси, multicast, NTP-сервис
Untrusted	ping, snmp, DNS, HTTP(S)-прокси, агент авторизации, SNMP(S)-прокси, POP3(S)-прокси, VPN, Reverse-прокси, веб-портал, Log Analyzer, OSPF, BGP, RIP, SNMP-прокси, NTP-сервис

Тест на уязвимости, проникновение будет осуществляться со стороны зоны Untrusted. Для всех перечисленных в зоне Untrusted сервисов будут открыты соответствующие порты.

Выбор системы как инструмента для сканирования и поиска уязвимостей

Для выполнения пентеста существует широкий перечень ОС на базе Unix с предустановленным прикладным программным обеспечением. К наиболее распространенным можно отнести:

- Parrot Security Edition;
- BlackArch;
- Pentoo;
- Fedora Security Lab;
- Kali Linux.

Parrot Security Edition основан на Debian. Что по функционалу, перечню предустановленных утилит делает его близким к Kali Linux. Основное отличие Parrot – наличие приложений для использования в рабочей среде – не предусматривающей тестирование на уязвимость [7]. Преимуществом является запуск в криминалистическом режиме (отсутствие следов на запускаемом хосте после перезапуска).

BlackArch включает в себя более трех тысяч утилит для тестирования на проникновение, решения других задач. Что является преимуществом. Но эксплуатация ОС вызывает сложности у пользователей при отсутствии релевантного опыта. Сложность интерфейса, отсутствие подробной документации существенно усложняет работу [8].

Pentoo прост в настройке, присутствует минимум утилит. Большая часть из них предназначена для работы с беспроводными сетями. Базовая система - Gentoo Linux. Использование ОС позволит сделать возможным низкоуровневое компилирование Дистрибутив предназначен для академических исследований, проведения экспериментов. Для использования дистрибутив удобен лишь при тонкой предварительной настройке.

Основное преимущество Fedora Security Lab – наличие учебных материалов. Все без исключения приложения, утилиты, предустановленные и используемые для пентеста, задокументированы. Присутствуют подробные руководства упрощающие, ускоряющие работу. Но перечень предустановленного программного обеспечения ограничен [9].

Kali Linux – оптимальный вариант в качестве ОС для проведения тестирования на наличие уязвимостей. Использование предустановленного программного обеспечения позволит обнаружить все уязвимости актуальные на начало 2024 года.

Выбор прикладных программ для поиска и эксплуатации уязвимостей

Большинство злоумышленников используют типовые вектора атак на защищенные системы. Согласно статистике компании BI.ZONE (управление цифровыми рисками, одна из ведущих в отрасли) к наиболее часто используемым прикладным инструментам для тестирования можно отнести:

– Nessus;
– Netcat;
– Yersinina;
– THC Hydra;
– Metasploit Framework.

Использование всего пяти инструментов позволит выявить большую часть проблем присутствующих в оборудовании Usergate [10].

Изначально планировалось использовать Nmap для выполнения тестирования межсетевого экрана на наличие проблем безопасности. Но количество средств для поиска уязвимостей, обнаружения брешей в защите недостаточно. Основным конкурентом является Nessus. Использование по лицензии GPL позволяет применять его юридическим лицам, не отчисляя плату разработчику. При этом инструмент конкурирует на равных с различными платными решениями. Планируется использование специальных «опасных» сценариев. Например, rpc_endpoint mapper будет использоваться для симуляции DDos атаки.

Netcat будет использоваться для эксплуатации уязвимостей – если таковые будут обнаружены с помощью Nessus. Широкий функционал делает Netcat полноценным швейцарским ножом для «вскрытия» серверов, других типов хостов, находящихся за NAT. Сценарий использования будет зависеть от выбранного вектора атаки. Использование в режиме подключения позволит выполнить подключения по протоколам http, ftp, telnet и другим [11].

Yersinia используется для внедрения с использованием протоколов низкого уровня. Будет применяться для тестирования защищенности поддерживаемых Usergate сетевых технологий первых трех уровней OSI. К таковым относятся: STP (протокол связующего дерева), CDP (Cisco Discovery Protocol), VLAN (VTP), ISL (межсетевое взаимодействие), IEEE 802.1Q/IEEE 802.1X, DHCP (протокол динамической настройки хоста), DTP (протокол динамической транкинговой связи).

THC Hydra будет использоваться для последовательного перебора паролей. Многие специалисты считают концепцию брутфорса устаревшей. Большинство современного оборудования ещё на этапе проектирования включает в себя защиту от подобных атак. Но этап тестирования на наличие уязвимостей к базовому перебору по типовым словарям обязателен в любой методике. THC Hydra предустановлена в системе Kali Linux. Она эффективна, не вызывает затруднений при использовании.

Metasploit Framework – бесплатная, проприетарная версия с базовым набором функций, консольным управлением. Структура фреймворка проста, позволяет оперативно

сформировать сценарии для обнаружения уязвимостей. Для построения вектора атаки будут использованы типовые модули. Единственная сложность, связанная с эксплуатацией инструмента Metasploit Framework – использование базы данных. Предварительно потребуется установить postgresql [12].

Формирование перечня тестов применительно к ПАК usergate 6.1.8: практическое применение разработанной методики

Для начала тестирования просканируем Usergate выступающий в роли сервера с помощью приложения Nessus (адрес – 10.80.7.14 согласно приведенной схеме). В результате сканирования было выявлено всего 2 открытых порта: 53 и 8090. Согласно открытой на сайте производителя документации порт 53 используется для службы DNS. 8090 – выступает как порт для подключения к прокси-серверу. Именно через порт 8090 планируется в дальнейшем развивать вектор атаки.

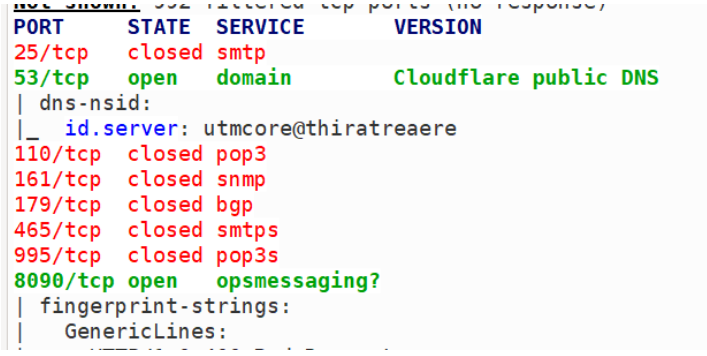

Рис. 2 Перечень открытых портов интерфейса, задействованного для работы VPN

Злоумышленник зачастую имеет информацию о внутренней сетевой адресации за NAT. Потому просканируем внутренний адрес, используемый для транспорта данных между зоной Trusted и Untrusted. На приведенной выше схеме внутри сети (не для управления) используется адрес 10.80.6.14 (серверная часть). Результат сканирования внутренней части сети более продуктивен – в стандартной конфигурации открыто более восьми различных портов. Что позволяет получить больше вариантов для атаки на сервер VPN [13]. Перечень открытых портов позволяет с помощью сканера определить сервисы и версии:

– 53 – DNS;

– 80 – http (nextgen_0.5);

– 443 – https (веб-сервер позволяет получить подробную информацию о ключе RSA, поддерживаемых методах);

– 2200 – ssh (версия 2.0);

– 8001 – веб-сервер управления межсетевым экранов (отображается перечень поддерживаемых методов);

– 8002 - teradataordbms?;

– 9002 - dynamid?.

Сразу обращает на себя внимание открытый порт 9002. Существует уязвимость CVE-2011-2738 свойственная устройствам, изготовленным Cisco. Уязвимость данного типа предполагает возможность выполнения произвольного кода с помощью обработанных пакетов [14].

Полученных результатов достаточно для использования инструмента netcat позволяющего выполнять подключения. Одной из обнаруженных в результате сканирования межсетевого экрана уязвимостью является CWE-79. Предполагает эксплуатацию неправильной нейтрализации ввода при генерации веб-страницы. Используя межсайтовый скриптинг (XSS). В нашем случае возможно использование первого типа XSS – отраженный. Достаточно с помощью ncat правильно подобрать запрос типа HTTP и сервер отобразит необходимые данные в HTTP-ответе. Опасность уязвимости этого типа кроется в возможности модификации страницы. При попытке авторизоваться через веб-интерфейс допускаются перенаправления пользователя методом социальной инженерии на сторонний сайт где будут введены учетные данные (логин, пароль). Что приводит к их компрометации. Данная уязвимость присутствовала в более ранней версии usergate – 5.0 [15].

Имеющейся информации достаточно для выполнения атаки на протоколы низкого уровня. Например, L2. При сканировании портов внимание к себе привлекает порт 80 http nextgen 0.5. Изначально была предпринята попытка использования эксплойта WordPress Plugin WP Business Intelligence Lite File Read Vulnerability. При внешнем сканировании веб-сервер выглядит похожим на WordPress. Воспользуемся готовым скриптом для эксплуатации уязвимости позволяющей сканировать содержимое каталога системы со стандартными реквизитами для подключения: Admin/utm. Как продуктивный порт используется 8001 – через него осуществляется подключение к веб-консоли управления.

```
msf6 auxiliary(scanner/http/wp_nextgen_galley_file_read) > RHOSTS 10.80.6.14 PORT 80
[-] Unknown command: RHOSTS
msf6 auxiliary(scanner/http/wp_nextgen_galley_file_read) > RHOSTS 10.80.6.14
[-] Unknown command: RHOSTS
msf6 auxiliary(scanner/http/wp_nextgen_galley_file_read) > set RHOSTS 10.80.6.14
RHOSTS => 10.80.6.14
msf6 auxiliary(scanner/http/wp_nextgen_galley_file_read) > exploit
```

Рис. 3 Перечень открытых портов интерфейса, задействованного для работы VPN

После запуска аргумента run получаем результат – нет возможности подключения. Можно сделать вывод – от базовых эксплойтов веб-сервер usergate защищено. Но лишь при поверхностном сканировании.

Для перебора атаки по словарю либо иным способом используется штатное приложение Kali Linux THC Hydra. Инструмент включает поддержку нескольких десятков самых популярных протоколов. Для примера использовался стандартный порт 2200. Базовая конфигурация Usergate предполагает его использование для работы через cli. Стандартная комбинация логина и пароля (Admin/utm) показывает положительный результат при попытке авторизации. Соответственно, позволит проверить валидность учетных данных [16].

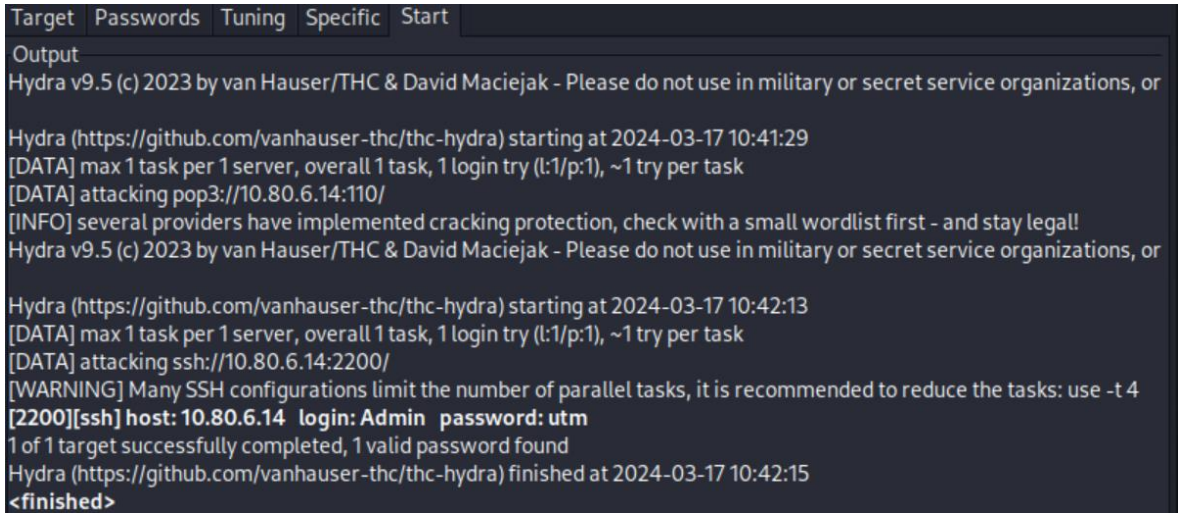

Рис. 4 Запуск перебора по словарю для стандартного порта ssh

Для выполнения атаки на протокол DHCP воспользуемся утилитой Yersinina. Попытка выполнения работы с протоколом L2 при его использовании внутри канала VPN не дала положительного результата. Тестирование остальных протоколов, поддерживаемых Yersinia (cdp, dtp, mpls, stp), не проводилось [17].

Анализ выявленных уязвимостей и типовые рекомендации по устранению

Поверхностное тестирование операционной системы Usergate позволило сформировать несколько базовых рекомендаций обязательных к выполнению при интеграции межсетевого экрана в систему защиты периметра.

Требуется обязательно выполнить закрытие портов, отключить сервисы – если они не используются в этой зоне. Это снизит вероятность эксплуатации уязвимостей, позволит избежать проникновения злоумышленника внутрь сетевого периметра. Использование преднастроенных зон по умолчанию предполагает предварительную их настройку. Если для удаленной настройки не используется web-интерфейс, ssh – необходимо его обязательно отключить. Это позволит избежать подбора паролей. От такой методики с помощью элементарных инструментов, входящих в базовый набор Kali Linux, межсетевой экран не защищен.

Защита низкоуровневых протоколов присутствует, применение утилит для сканирования внутреннего периметра сети не позволяет определить перечень IP адресов, подсетей, масок. Утилита Yersinina, предназначенная для работы с уровнем L2, не смогла справиться с возложенной на неё задачей. Что положительно характеризует межсетевой экран с операционной системой 6.1.8.

Необходимо использовать СОВ – систему обнаружения вторжений. Желательно применение сканеров IDS/IPS. Это позволит вовремя определить начало развития вектора атаки. Сканирование утилитами nmap, Nessus, аналогами. До начала специальной военной операции хорошим решением было использование Rapid 7, продуктов McAfee (IPS, ERC). Но сегодня компания McAfee не работает на территории России [18].

Желательно отключить стандартного пользователя Admin, выбрать для административной учетной записи нестандартное наименование. Сложность пароля должна составлять не менее 12 символов, включать в себя прописные и строчные буквы, цифры, специальные символы [19]. Это снизит вероятность подбора пароля по словарю.

Заключение

Использование межсетевого экрана Usergate позволит повысить защищенность сети передачи данных, сервисов, выполнить требования, сформированные ФСТЭК, ФСБ к субъектам КИИ. На момент написания статьи оборудование рассматриваемого производителя отличается стабильностью, высокой степенью защищенности. Usergate внесен в реестр российского программного обеспечения.

На 2024 год в официальном БДУ ФСТЭК присутствует всего три обнаруженные уязвимости для межсетевых экранов модели D500 (публикация выполнена 2021 году). Важно помнить: отсутствие опубликованных уязвимостей не означает их отсутствие. Потому необходимо обязательно соблюдать меры безопасности, рекомендованные субъектам КИИ. Это позволит избежать нарушений законодательства, административной и уголовной ответственности [20] для руководителя организации, системного администратора.

Литература

1. *Lei, Yunsen*; Lanson, Julian; Kaldawy, Remy; Estrada, Jeffrey; Shue, Craig (11 November 2020). "Can Host-Based SDNs Rival the Traffic Engineering Abilities of Switch-Based SDNs?". IEEE Network of the Future Conference: 91–99. doi:10.1109/NoF50125.2020.9249110.

2. *Будко П. А., Кулешов И. А., Курносов В. И., Мирошников В. И.* Инфокоммуникационные сети: энциклопедия. Кн. 4. Гетерогенные сети связи: принципы построения, методы синтеза, эффективность, цена, качество /под ред. проф. В. И. Мирошникова. М.: Наука, 2020. 683 с.

3. *Родичев Ю. А.* Нормативная база и стандарты в области информационной безопасности. Санкт-Петербург: Питер, 2018. 256 с.

4. *Сычев К. И.* Многокритериальное проектирование мультисервисных сетей связи. СПб.: Изд-во Политехи, ун-та, 2018. 272 с.

5. Nencioni G. Impact of SDN Controllers Deployment / Nencioni G., Helvik B.E., Gonzalezy A.J., Heegaard P.E., Kamisinski A. // on Network Availability — Cornell University Library [URL accessed on 20 Sept. 2022].

6. *Власенко А.В.* Событийное реагирование на инциденты информационной безопасности // Цифровая трансформация науки и образования. НАЛЬЧИК, 2021. С. 230-236.

7. *Виноградeнко А. М.* Методология интеллектуального контроля технического состояния автоматизированной системы связи специального назначения. СПб.: Наукоемкие технологии, 2020. 80с.

8. *Николаенко Е.П.* Управление инцидентами информационной безопасности // ЭМПИ: экономика, менеджмент, прикладная информатика. Брянск: Брянский государственный технический университет, 2019. С. 207-210.

9. *Porsev K. I., Sorokin A. V.* Management of Innovations and Knowledge in the Structure of the Enterprise Integrated Information Environment, In: Proceedings of the 2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS), 2020. Pp. 283–285.

10. *Singh,* S. A survey on Software Defined Networking: Architecture for next generation network /Singh, S., Jha, R. K. // In: Journal of Network and Systems Management, vol. 25 no. 2, pp. 321374 (2017). doi:10.1007/s10922-016-9393-9.

11. *Budko P. A., Vinogradenko A. M., Mezhenov A. V., Zhuravlyova N. G.* Method of adaptive control of technical states of radioelectronic systems // Advances in Signal Processing. Theories, Algorithms, and System Control. Intelligens Systems Reference Library. Springer-Verlag 2020. Vol. 184. Chapter 11. Pp. 137-151.

12. *Виноградeнко А. М., Будко Н. П.* Адаптивный контроль технического состояния сложных технических объектов на основе интеллектуальных технологий // T-Comm: Телекоммуникации и транспорт. 2020. Т. 14. № 1. С. 25–35. DOI: 10.36724/2072-8735-2020-14-1-25-35.

13. *Turskis Z., Goranin N., Nurusheva A., Boranbayev S.* Information Security Risk Assessment in Critical Infrastructure: A Hybrid MCDM Approach // Informatica. 2019. Vol. 30(1). Pp. 187–211. DOI:10.15388/Informatica.2019.203.

14. *A.M. Koushika,* S.T. Selvi. "Load balancing Using Software Defined Networking in cloud environment" Recent Trends in Information Technology (ICRTIT), 2014 International Conference on. IEEE, (2019), pp. 1.

15. *Кузьмина Н. А.* Системы фиксации и распознавания несанкционированного проникновения в охраняемую зону как элемент эффективной безопасности объекта транспортной инфраструктуры //T-Comm: Телекоммуникации и транспорт. 2018. Т. 12, № 5. С. 47-52. doi:10.24411/20728735201810086.

16. *Сухих С. Н., Николаев В. А., Кротов А. Ю.* О развитии технических средств охраны с применением Единого специализированного объектового протокола // Материалы международной научно-технической конференции «Системы безопасности». Москва, 2020. С. 240-244.

17. *Климов А. В., Николаев В. А., Кротов А. Ю.* О создании технических средств охраны нового поколения, работающих с использованием Единого специализированного объектового протокола // Академический вестник войск национальной гвардии Российской Федерации. 2020. № 3. С. 40-43.

18. *Свиридов В. В.* Применение робототехнических комплексов охраны и обороны критически важных объектов Ракетных войск стратегического назначения // Военная мысль. 2021. № 6. С. 57-64.

19. *Исхаков А. Ю., Исхаков С.Ю.* Модели нормализации данных в системах управления событиями безопасности РТК. М.: Институт проблем управления им. В.А. Трапезникова РАН, 2020. С. 1390 – 1399.

20. *Крыжановский А.В.* Управление инцидентами информационной безопасности. Волгоград: Волгоградский государственный университет, 2019. С. 30-33.

DEVELOPMENT OF A VULNERABILITY TESTING METHODOLOGY FOR A FSTEC CERTIFIED FIREWALL TO PROTECT SECURITY FACILITIES

DMITRY A. LYUBIMENKO
Deputy Director General for Information Security
of Akvamash Software LLC, Volgograd, Russia,
d.lyubimenko@aquamash.ru

ABSTRACT

Introduction: analysis of the work of a new generation firewall as a perimeter protection system for an enterprise that is a subject of CII, checking the hardware and software complex for vulnerabilities. **The purpose of the study:** to develop a methodology for testing the next generation firewall for vulnerabilities for intruders engaged in data theft, encryption and blackmail. **Results:** As part of the testing, a Kali Linux-based operating system was deployed, equipped in the basic configuration with tools for scanning, searching for vulnerabilities in network and server equipment. The most common and frequently used new generation firewall (usergate version 6.1.8) was selected as the target system for the survey. For scanning, testing and exploiting vulnerabilities, a list of typical application programs used by most attackers to penetrate the perimeter was formed: nessus, netcat, Yersinia, THC Hydra, Metasploit Framework. The result of the work done was the development of a practical methodology that allows for full-fledged testing of the next generation firewall for vulnerabilities. It can be used not only for testing usergate products. But also similar technical solutions from other manufacturers – Eltex, Ideko, others. The versatility of the developed methodology is ensured by the use of almost all solutions as a basic Unix/Linux system. **Practical significance:** The technique allows you to systematize the testing process, form control points, provide a comprehensive check of the hardware and software complex for vulnerabilities, "bookmarks" of the developer. The use of up-to-date means for checking the packet will allow you to simulate the behavior of an attacker whose purpose is to penetrate and consolidate inside a closed network circuit. The above methodology makes it possible to detect problem areas in a timely manner, ensure their elimination and accelerate the release of security updates, makes it possible to form an information security bulletin in a timely manner.

Keywords: perimeter protection system; new generation firewall; usergate; NGFW; vulnerability closure.

REFERENCES

1. Lei, Yunsen; Lanson, Julian; Kaldawy, Remy; Estrada, Jeffrey; Shue, Craig (11 November 2020)."Can Host-Based SDNs Rival the Traffic Engineering Abilities of Switch-Based SDNs?". IEEE Network of the Future Conference: 91-99. doi:10.1109/NoF50125.2020.9249110.
2. Budko P. A., Kuleshov I. A., Kurnosov V. I., Miroshnikov V. I. Infocommunication networks: encyclopedia. Book 4. Heterogeneous communication networks: principles of construction, synthesis methods, efficiency, price, quality. edited by prof. V. I. Miroshnikov. M.: Nauka, 2020. 683 p. (In Rus)
3. Rodichev Yu. A. Regulatory framework and standards in the field of information security. St. Petersburg: Peter, 2018. 256 p. (In Rus)
4. Sychev K. I. Multicriteria design of multiservice communication networks. St. Petersburg: Polytechnic Publishing House, University, 2018. 272 p. (In Rus)
5. Nencioni G. Impact of SDN Controllers Deployment. Nencioni G., Helvik B.E., Gonzalezy A.J., Heegaard P.E., Kamisinski A. on Network Availability — Cornell University Library [URL accessed on 20 Sept. 2022].
6. Vlasenko A.V. Event-based response to information security incidents //The digital transformation of science and education. NALCHIK, 2021. Pp. 230-236. (In Rus)
7. Vinogradenko A.M. Methodology of intelligent control of the technical condition of an automated special-purpose communication system. St. Petersburg: High-tech technologies, 2020. 80 p. (In Rus)
8. Nikolaenko E.P. Information security incident management. EMPI: economics, management, applied informatics. Bryansk: Bryansk State Technical University, 2019. Pp. 207-210.
9. Porsev K. I., Sorokin A. V. Management of Innovations and Knowledge in the Structure of the Enterprise Integrated Information Environment, In: Proceedings of the 2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS), 2020. Pp. 283–285.
10. Singh, S. A survey on Software Defined Networking: Architecture for next generation network.Singh, S., Jha, R. K. In: Journal of Network and Systems Management, vol. 25 no. 2, Pp. 321374 (2017). doi:10.1007/s10922-016-9393-9.
11. Budko P. A., Vinogradenko A. M., Mezhenov A. V., Zhuravlyova N. G. Method of adaptive control of technical states of radioelectronic systems. Advances in Signal Processing. Theories, Algorithms, and System Control. Intelligens Systems Reference Library. Springer-Verlag 2020. Vol. 184. Chapter 11. Pp. 137-151. (In Rus)
12. Vinogradenko A.M., Budko N. P. Adaptive control of the technical condition of complex technical objects based on intelligent technologies. T-Comm: Telecommunications and Transport. 2020. Vol. 14. No. 1. Pp. 25-35. DOI: 10.36724/2072-8735-2020-14-1-25-35. (In Rus)
13. Turskis Z., Goranin N., Nurusheva A., Boranbayev S. Information Security Risk Assessment in Critical Infrastructure: A Hybrid MCDM Approach. Informatica. 2019. Vol. 30(1). Pp. 187–211. DOI:10.15388/Informatica.2019.203.
14. A.M. Koushika, S.T. Selvi. "Load balancing Using Software Defined Networking in cloud environment" Recent Trends in Information Technology (ICRTIT), 2014 International Conference on. IEEE, (2019), Pp. 1.
15. Kuzmina N. A. Systems for fixing and recognizing unauthorized entry into a protected area as an element of effective security of a transport infrastructure facility. T-Comm: Telecommunications and transport. 2018. Vol. 12, No. 5. Pp. 47-52. doi:10.24411/20728735201810086. (In Rus)
16. Sukhoi S. N., Nikolaev V. A., Krotov A. Yu. On the development of technical means of protection using a single specialized object protocol. Materials of the international scientific and technical conference "Security Systems". Moscow, 2020. Pp. 240-244. (In Rus)
17. Klimov A.V., Nikolaev V. A., Krotov A. Yu. On the creation of new generation security equipment operating using a single specialized object protocol. Academic Bulletin of the National Guard troops of the Russian Federation. 2020. No. 3. Pp. 40-43. (In Rus)

18. Sviridov V. V. Application of robotic complexes for the protection and defense of critical facilities of strategic Missile forces. Military thought. 2021. No. 6. Pp. 57-64. (In Rus)

19. Iskhakov A. Yu., Iskhakov S.Yu. Data normalization models in RTK security event management systems. Moscow: V.A. Trapeznikov Institute of Management Problems of the Russian Academy of Sciences, 2020. Pp. 1390-1399. (In Rus)

20. Kryzhanovsky A.V. Information Security Incident Management. Volgograd: Volgograd State University, 2019. Pp. 30-33. (In Rus)