

УДК 004.056.5

И. Д. БОРЕКО, Н. И. ВАВУЛО (ЭМ-31)

Научные руководители: старшие преподаватели *С. В. КИСЕЛЕВА,*
В. Е. МИНИН

ТЕСТИРОВАНИЕ И МОНИТОРИНГ СЕТЕВОЙ БЕЗОПАСНОСТИ

Рассмотрены методология и практика тестирования безопасности локальной сети. На основе реального сценария атаки ARP-спуфинг с использованием инструментов Nmap, Wireshark, tcpdump и Metasploit проанализированы типичные уязвимости сетевой инфраструктуры. Предложены контрмеры по каждому классу угроз в соответствии с принципом Defense in Depth.

Обеспечение безопасности локальной сети предполагает, прежде всего, четкое понимание актуальной модели угроз. Атаки на сетевую инфраструктуру охватывают все уровни модели OSI: от физического несанкционированного доступа до эксплуатации уязвимостей прикладных протоколов [1].

На канальном уровне (L2) наибольшую опасность представляет протокол ARP, не предусматривающий механизмы аутентификации [2]. Это позволяет любому узлу сети декларировать принадлежность произвольного IP-адреса, что является основой атаки «человек посередине» (MitM). На транспортном уровне угрозу формируют незащищенные сервисы и открытые порты. На прикладном уровне критическим фактором остается использование устаревших протоколов, передающих данные в открытом виде.

Атака VLAN hopping – несанкционированный доступ к изолированным сегментам сети посредством манипуляций с тегами 802.1Q либо эксплуатации протокола DTP, активного по умолчанию на коммутаторах Cisco. Данная техника систематически фигурирует в отчетах о взломах корпоративных инфраструктур.

Тестирование на проникновение (penetration testing) – это структурированная верификация инфраструктуры методами реального атакующего, проводимая с явного разрешения владельца. В соответствии с методологией PTES [3] процесс включает пять последовательных этапов (рисунок 1).

1 *Разведка.* Сбор сведений об инфраструктуре: активные хосты, открытые порты, версии сервисов. Применяются Nmap [4], Masscan, OSINT-инструменты.

2 *Сканирование и перечисление.* Детальный анализ обнаруженных сервисов: версии ПО, конфигурации, SMB-ресурсы, SNMP-дерево.

3 *Эксплуатация.* Проверка уязвимостей на практике с применением Metasploit Framework [3] и ручных техник.

4 *Пост-эксплуатация*. Оценка возможного ущерба: горизонтальное перемещение (pivoting), повышение привилегий.

5 *Отчетность*. Документирование результатов с CVSS-оценками и рекомендациями по устранению.



Рисунок 1 – Этапы тестирования на проникновение

В ходе тестирования на одном из узлов исследуемой сети был обнаружен Telnet-сервис – протокол удаленного управления 1983 года, не предусматривающий шифрования передаваемых данных. Для затруднения обнаружения сервис был перемещен на нестандартный порт 2323, однако полное сканирование командой `nmap -sV -p- 192.168.10.5` выявило его незамедлительно.

Следующим шагом стало позиционирование атакующего между жертвой и маршрутизатором посредством ARP-спуфинга. Инструмент `arp spoof` рассылал поддельные ARP-ответы, убеждая узлы сети в соответствии с IP-адресом шлюза MAC-адресу атакующего хоста. После активации IP-форвардинга весь трафик жертвы начал транзитно проходить через атакующую машину (рисунок 2).



Рисунок 2 – Схема атаки ARP-спуфинг: перехват трафика между жертвой и шлюзом

Параллельно запущенный tcpdump захватил первые пакеты Telnet-сессии. В перехваченном трафике обнаружена строка аутентификации в открытом виде

login: admin Password: P@ssw0rd!123

Получение учетных данных не потребовало подбора или расшифровки: пароль был передан открытым текстом вследствие использования незащищенного протокола. Данный случай демонстрирует, что угроза определяется не сложностью атаки, а отсутствием базовых механизмов защиты [1].

По итогам полного цикла тестирования составлена таблица обнаруженных уязвимостей с оценкой критичности по методологии CVSS (таблица 1). Привлекает внимание, что наиболее критические уязвимости связаны не с использованием сложных эксплойтов, а с применением заведомо небезопасных протоколов.

Таблица 1 – Уязвимости, выявленные в ходе тестирования

Критичность	Уязвимость	Порт/сервис
Критический	Telnet/FTP без шифрования на нестандартных портах	23, 21, 2323/tcp
Высокий	Активные SSLv3 / TLS 1.0	443, 8443/tcp
Высокий	Отсутствие Dynamic ARP Inspection (DAI)	L2-сеть
Средний	VLAN hopping через DTP	Trunk-порты
Средний	SNMP public community string	161/udp
Низкий	Поддержка SSH v1	22/tcp

Разработанные рекомендации сгруппированы по четырем направлениям:

1 *Замена устаревших протоколов.* Telnet и FTP подлежат замене на SSH и SFTP. Поддержка SSLv3 и TLS 1.0/1.1 отключается на всех сервисах, допустимы только TLS 1.2 и TLS 1.3 [5].

2 *Защита канального уровня.* Включение Dynamic ARP Inspection (DAI) блокирует поддельные ARP-ответы. IP Source Guard ограничивает трафик с неизвестных IP. Команда switchport nonegotiate исключает VLAN hopping через DTP [1].

3 *Разграничение доступа.* Правила Access Control List закрывают все порты, не требующиеся явно. Принцип минимальных привилегий распространяется как на учетные записи, так и на сетевые соединения.

4 *Мониторинг и обнаружение аномалий.* Развертывание IDS/IPS (Snort, Suricata) совместно с SIEM-системой (ELK Stack, Splunk) обеспечивает обнаружение аномального трафика в реальном времени [6]. NetFlow-анализ эффективен для выявления нетипичных потоков данных.

Реализация принципа многоуровневой защиты показана на рисунке 3.

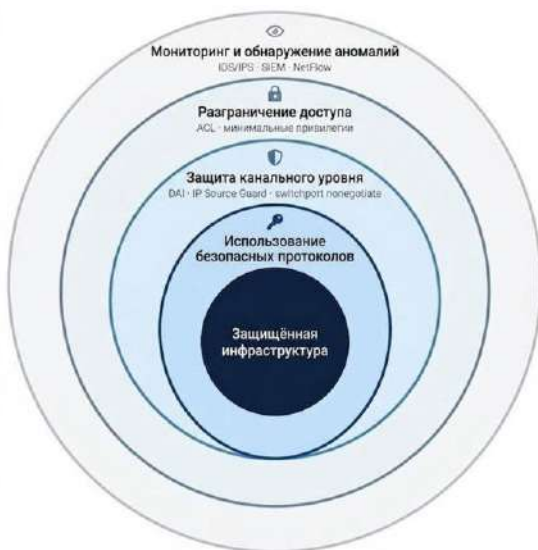


Рисунок 3 – Принцип Defense in Depth: многоуровневая защита сетевой инфраструктуры

Проведенное тестирование подтвердило, что наиболее распространенные уязвимости сетевой инфраструктуры определяются не изощренными атаками, а использованием устаревших конфигураций и отсутствием базовых защитных механизмов. ARP-спуфинг, перехват незашифрованного трафика, обход сегментации VLAN. Все рассмотренные угрозы воспроизводимы при минимальных технических ресурсах.

Регулярный пентест, анализ трафика и своевременное обновление конфигураций позволяют устранить большую часть рисков без существенных затрат. Принцип Defense in Depth (защита на каждом уровне без опоры на единственную меру) остается основополагающим при проектировании защищенной инфраструктуры.

СПИСОК ЛИТЕРАТУРЫ

- 1 Kali Linux Библия Пентестера / Raphaël Hertzog, Jim O'Gorman, Mati Aharoni, Joe O'Gorman. – 2nd ed. – Offsec Press, 2021. – 342 p.
- 2 **Plummer, D. C.** An Ethernet Address Resolution Protocol / D. C. Plummer // RFC 826. – IETF, 1982. – URL: <https://www.rfc-editor.org/rfc/rfc826> (date of access: 01.05.2025).
- 3 **Lyon, G. F.** Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning / G. F. Lyon. – Insecure.Com LLC, 2009. – 468 p.
- 4 Metasploit: The Penetration Tester's Guide / D. Kennedy, Jim O'Gorman, D. Kearns, M. Aharoni. – No Starch Press, 2011. – 336 p.

5 **Rescorla, E.** The Transport Layer Security (TLS) Protocol Version 1.3 / E. Rescorla // RFC 8446. – IETF, 2018. – URL: <https://www.rfc-editor.org/rfc/rfc8446> (date of access: 01.05.2025).

6 **Sanders, C.** Applied Network Security Monitoring: Collection, Detection, and Analysis / C. Sanders, J. Smith. – Syngress, 2014. – 496 p.

7 Wireshark User's Guide // Wireshark Foundation. – URL: https://www.wireshark.org/docs/wsug_html_chunked/ (date of access: 04.04.2026).

Получено 11.06.2026

ISSN 2227-1155. Сборник студенческих научных работ.

Вып. 31. Гомель, 2026

УДК 336.748.3

В. А. БОХАН, В. В. ДУБИНИНА (ГТ-31)

Научный руководитель – канд. экон. наук *Л. В. МИЩЕНКО*

ВАЛЮТНЫЕ РИСКИ И СПОСОБЫ ИХ СТРАХОВАНИЯ

Систематизированы теоретические подходы к определению валютного риска, раскрыты его сущность и источники возникновения. Охарактеризованы внутренние и внешние методы их страхования.

Углубление международного разделения труда и высокая волатильность валютных рынков делают проблему валютных рисков одной из центральных для субъектов внешнеэкономической деятельности. Роль валютного курса в условиях глобализации постоянно растет, оказывая прямое влияние на корпоративные и банковские прибыли, экспансию на новые рынки и иностранные инвестиции. По некоторым оценкам, до 30 % доходов или убытков от вложений в иностранные акции и до 60 % – от инвестиций в облигации обусловлены колебаниями валютных курсов, причём даже незначительные изменения способны привести к существенным финансовым потерям из-за крупных объёмов сделок [1]. Как отмечается в литературе, валютный риск – это вероятность возникновения финансовых потерь вследствие изменения курса иностранной валюты к национальной [2].

Анализ источников показывает, что единого определения термина «валютный риск» в науке не сложилось, однако большинство дефиниций акцентируют вероятность финансовых потерь из-за неблагоприятного изменения курса валют [2]. Обобщая существующие подходы, можно определить валютный риск как объективно существующую в условиях неопределённости потенциальную возможность денежных потерь (недополучения запла-