

Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.056.5

САМАКЕ
Баче Александр

**МЕТОДИКА ТЕСТИРОВАНИЯ БЕЗОПАСНОСТИ
КОРПОРАТИВНЫХ СЕТЕЙ**

Автореферат
на соискание степени магистра
по специальности 1-98 80 01 Информационная безопасность

Научный руководитель
канд. техн. н., доцент
БЕЛОУСОВА Елена Сергеевна

Минск 2024

ВВЕДЕНИЕ

В современном мире, где информация является ценным ресурсом, а киберугрозы становятся все более изощренными, обеспечение безопасности корпоративной сети является первостепенной задачей для любой организации. Неэффективная система безопасности может привести к утечке конфиденциальных данных, финансовым потерям, нарушению деловой репутации и даже остановке работы компании.

Поэтому тестирование безопасности корпоративной сети является неотъемлемой частью ее защиты. Оно позволяет выявить уязвимости, которые могут быть использованы нарушителями, и разработать эффективные меры по их устранению.

Целью диссертационной работы является разработка методики тестирования безопасности корпоративной сети на основе анализа уязвимостей сетевых протоколов.

Для достижения поставленной цели в диссертации решены следующие задачи:

- 1 Изучение архитектуры построения корпоративных сетей, уязвимостей сетевых протоколов.

- 2 Обзор стандартов и методик тестирования безопасности.

- 3 Обоснование выбора инструментов для тестирования безопасности корпоративных сетей, построение модели корпоративной сети с целью анализа уязвимостей сетевых протоколов.

- 4 Разработка методики тестирования безопасности корпоративной сети и ее апробация для построенной модели корпоративной сети.

- 5 Составление рекомендации по совершенствованию информационной безопасности.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с крупными научными программами

Тема диссертационной работы соответствует пункту 6 приоритетных направлений научной, научно-технической и инновационной деятельности Республики Беларусь на 2021–2025 гг., утвержденных Указом Президента Республики Беларусь №156 от 7 мая 2020 г. «Обеспечение безопасности человека, общества, государства». Работа выполнялась в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники».

Цель и задачи исследования

Целью диссертационной работы является разработка методики тестирования безопасности корпоративной сети на основе анализа уязвимостей сетевых протоколов.

Для достижения поставленной цели в диссертации решены следующие задачи:

- 1 Изучение архитектуры построения корпоративных сетей, уязвимостей сетевых протоколов.
- 2 Обзор стандартов и методик тестирования безопасности.
- 3 Обоснование выбора инструментов для тестирования безопасности корпоративных сетей, построение модели корпоративной сети с целью анализа уязвимостей сетевых протоколов.
- 4 Разработка методики тестирования безопасности корпоративной сети и ее апробация для построенной модели корпоративной сети.
- 5 Составление рекомендации по совершенствованию информационной безопасности.

Личный вклад соискателя ученой степени

Содержание диссертации отображает личный вклад автора. Он заключается в построение корпоративной сети с помощью программного симулятора сетевого оборудования для проведения кибератак, определение уязвимостей, составления методики тестирования безопасности корпоративной сети, проведение ее апробации, составление рекомендаций для использования разработанной методики.

Определение целей и задач исследований, интерпретация и обобщение полученных результатов проводились совместно с научным руководителем, кандидатом технических наук, доцентом Е.С. Белоусовой.

Апробация диссертации и информация об использовании ее результатов

Основные положения и результаты диссертационной работы докладывались и обсуждались на: 59-ой научно-технической конференции аспирантов, магистрантов и студентов БГУИР и на 60-ой научно-технической конференции аспирантов, магистрантов и студентов БГУИР.

Опубликование результатов диссертации

По результатам исследований, представленных в диссертации, опубликованы 2 печатные работы, в том числе 2 статьи в сборниках и материалах конференций.

Структура и объем диссертации

Диссертационная работа состоит из введения, общей характеристики работы, трех глав с выводами по каждой главе, заключения, библиографического списка.

Общий объем диссертационной работы составляет 73 страниц, из них 65 страниц текста, 35 рисунков на 19 страницах, 2 таблицы на 1 страницу, список использованных библиографических источников (20 наименований на 2 страницы), список публикаций автора по теме диссертации (2 наименование на 1 страницу), графический материал на 7 страницах.

Проверка на уникальность

Проведена экспертиза диссертации Самаке Баче Александр «Методика тестирование безопасности корпоративной сети» на корректность использования заимствованных материалов с применением сетевого ресурса «Антиплагиат» (адрес доступа: <https://antiplagiat.ru>) в on-line режиме 11.06.2024 г. В результате проверки установлена корректность использования заимствованных материалов (оригинальность диссертационной работы составляет 72 %). Отчет о результатах проверки представлен в Приложении А.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении рассмотрена актуальность проведения тестирования безопасности корпоративной сети, которая является неотъемлемой частью ее защиты от утечки конфиденциальных данных, финансовых потерь, нарушения деловой репутации и остановке работы компании.

В общей характеристике работы показана связь работы с приоритетными направлениями научных исследований, цель и задачи исследования, личный вклад соискателя ученой степени, апробация результатов диссертации.

В первой главе рассмотрены архитектуры защищенных локальных сетей, такие как распределенная архитектура, централизованная архитектура и централизованно-распределенная архитектура. Проведен анализ уязвимостей сетевых протоколов такие как: протокол разрешения адресов (ARP), система доменных имен (DNS), протокол передачи файлов, протокол передачи гипертекста, почтовый протокол и другие.

Выполнен обзор стандартов и методик тестирования безопасности, среди которых методика OSSTMM, методика OWASP, Методика ISSAF. Были изучены такие стандарты как стандарт проведения тестирования на проникновение PTES и стандарт NIST SP 800–115.

Во второй главе был обоснован выбор инструментов для тестирования безопасности корпоративных сетей, среди них отметили Nmap (Network Mapper) для сканирования сети, предоставляющий информацию об устройствах в сети, открытых портах, операционных системах, службах и многом другом, Wireshark, который позволяет анализировать активность в компьютерных сетях и Nping, которая позволяет проверить доступность и проанализировать качество соединения с удаленным устройством. Она может использоваться для проверки статуса устройства в сети, определения времени отклика и оценки качества соединения. Была реализована модель сети для реализации тестирования (рисунок 1).

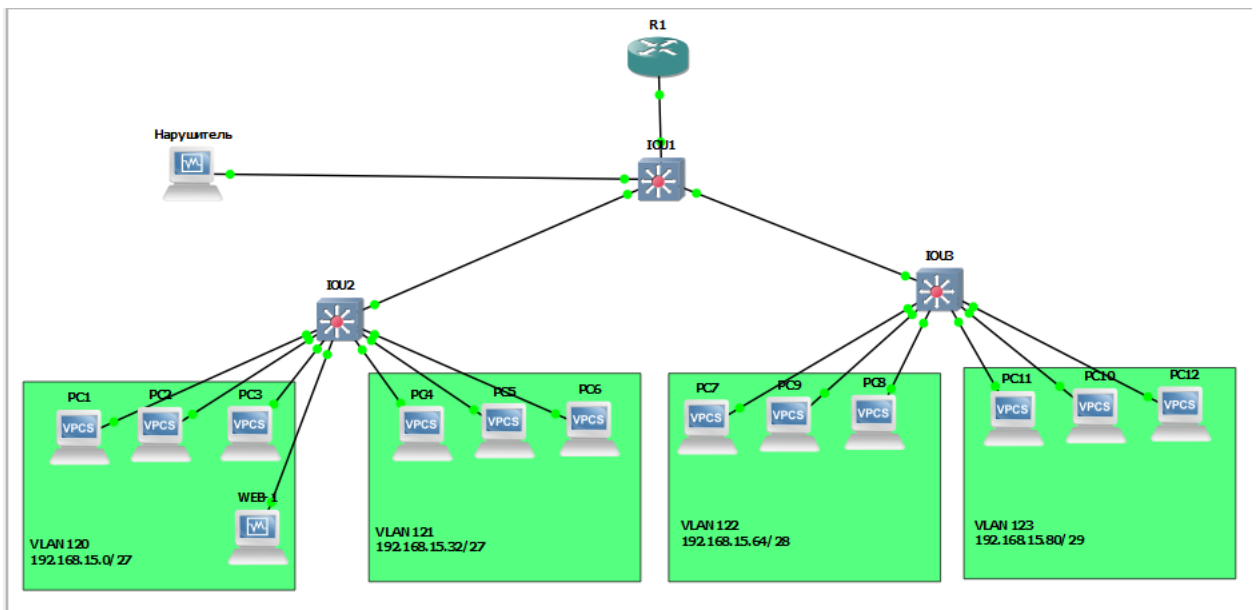


Рисунок 1 – Модель корпоративной сети

В результате анализа уязвимостей корпоративной сети и векторов атак для их эксплуатации был выбран один из наиболее эффективных приемов моделирование сценариев реализации угроз с помощью модели Cyber Kill Chain. Посредством техник модели Cyber Kill Chain была исследована уязвимость, связанная с ARP протоколом, который используется для идентификации MAC-адреса устройства по его известному IP-адресу, а также для формирования таблиц MAC-адресов на коммутаторах и ARP-таблиц на устройствах в сети. Уязвимость данного протокола заключается в попытке перехвата широковещательной рассылки ARP-пакетов, в которых есть IP и MAC-адреса устройств в сети. Таким образом, нарушитель может получить данные об устройствах в сети и реализовать атаку ARP spoofing. Было установлено, что нарушитель с помощью уязвимости, связанной с рассылкой ARP пакетов, получил информацию о IP-адресе легитимного пользователя, как предоставлено на рисунке 2. Таким образом, нарушитель способен перехватывать пакеты, которые будут адресованы доверенному пользователю и изменить таблицу ARP на маршрутизаторе как видно на рисунке 3. после чего выполнить DDoS-атаку на веб-сервере.

Destination	Protocol	Length	Info
Spanning-tree-(for-... STP	60	RST. Root = 32768/121/aa:bb:cc:00:01:00	Cost = 0
Spanning-tree-(for-... STP	60	RST. Root = 32768/121/aa:bb:cc:00:01:00	Cost = 0
Spanning-tree-(for-... STP	60	RST. Root = 32768/121/aa:bb:cc:00:01:00	Cost = 0
Spanning-tree-(for-... STP	60	RST. Root = 32768/121/aa:bb:cc:00:01:00	Cost = 0
Spanning-tree-(for-... STP	60	RST. Root = 32768/121/aa:bb:cc:00:01:00	Cost = 0
Spanning-tree-(for-... STP	60	RST. Root = 32768/121/aa:bb:cc:00:01:00	Cost = 0
Spanning-tree-(for-... STP	60	RST. Root = 32768/121/aa:bb:cc:00:01:00	Cost = 0
Spanning-tree-(for-... STP	60	RST. Root = 32768/121/aa:bb:cc:00:01:00	Cost = 0
Spanning-tree-(for-... STP	60	RST. Root = 32768/121/aa:bb:cc:00:01:00	Cost = 0
Broadcast	ARP	64	Who has 192.168.15.33? Tell 192.168.15.34
Spanning-tree-(for-... STP	60	RST. Root = 32768/121/aa:bb:cc:00:01:00	Cost = 0
Spanning-tree-(for-... STP	60	RST. Root = 32768/121/aa:bb:cc:00:01:00	Cost = 0
Spanning-tree-(for-... STP	60	RST. Root = 32768/121/aa:bb:cc:00:01:00	Cost = 0
Spanning-tree-(for-... STP	60	RST. Root = 32768/121/aa:bb:cc:00:01:00	Cost = 0

bytes captured (512 bits) on interface enp0s3, id 0	0000	ff ff ff ff
:79:66:68:04), Dst: Broadcast (ff:ff:ff:ff:ff:ff)	0010	08 00 06 04
ff)	0020	ff ff ff ff
8:04)	0030	00 00 00 06

Рисунок 2. – Результат перехвата ARP-протокола

```
R1#sh arp
Protocol Address Age (min) Hardware Addr Type Interface
Internet 192.168.15.65 - c001.5c58.0000 ARPA FastEthernet0/0.3
Internet 192.168.15.82 0 0050.7966.680a ARPA FastEthernet0/0.4
Internet 192.168.15.81 - c001.5c58.0000 ARPA FastEthernet0/0.4
Internet 192.168.15.34 0 0050.7966.6803 ARPA FastEthernet0/0.2
Internet 192.168.15.33 - c001.5c58.0000 ARPA FastEthernet0/0.2
Internet 192.168.15.3 0 0800.2778.7b50 ARPA FastEthernet0/0.1
Internet 192.168.15.1 - c001.5c58.0000 ARPA FastEthernet0/0.1
R1#
```

**MAC адрес
доверенного
пользователя**

```
R1#show arp
Protocol Address Age (min) Hardware Addr Type Interface
Internet 192.168.15.66 0 0050.7966.6808 ARPA FastEthernet0/0.3
Internet 192.168.15.65 - c001.5c58.0000 ARPA FastEthernet0/0.3
Internet 192.168.15.83 41 0050.7966.680b ARPA FastEthernet0/0.4
Internet 192.168.15.82 47 0050.7966.6809 ARPA FastEthernet0/0.4
Internet 192.168.15.81 - c001.5c58.0000 ARPA FastEthernet0/0.4
Internet 192.168.15.35 5 0800.2747.891a ARPA FastEthernet0/0.2
Internet 192.168.15.34 0 0800.2747.891a ARPA FastEthernet0/0.2
Internet 192.168.15.33 - c001.5c58.0000 ARPA FastEthernet0/0.2
Internet 192.168.15.2 58 0050.7966.6800 ARPA FastEthernet0/0.2
Internet 192.168.15.1 - c001.5c58.0000 ARPA FastEthernet0/0.1
```

**MAC адрес
нарушителя**

```
glpi@Glpi:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:47:89:1a brd ff:ff:ff:ff:ff:ff
    inet 192.168.15.34/27 brd 192.168.15.63 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe47:891a/64 scope link
        valid_lft forever preferred_lft forever
```

Рисунок 3 – Результат подмены записи в ARP-таблицы на устройстве

R1

Далее была реализована DDoS-атака с помощью hping с целью проверки работы сервера, результат представлен на рисунке 5.

No.	Time	Source	Destination	Protocol	Length	Info
2849...	4964.2002869...	192.168.15.34	192.168.15.3	TCP	174	[TCP Port numbers reused] 22345 - 80 [SYN] Seq=0 Win=64 Len=120...
2849...	4964.2002927...	192.168.15.34	192.168.15.3	TCP	174	[TCP Port numbers reused] 22346 - 80 [SYN] Seq=0 Win=64 Len=120...
2849...	4964.2003558...	192.168.15.34	192.168.15.3	TCP	174	[TCP Port numbers reused] 22347 - 80 [SYN] Seq=0 Win=64 Len=120...
2849...	4964.2003660...	192.168.15.34	192.168.15.3	TCP	174	[TCP Port numbers reused] 22348 - 80 [SYN] Seq=0 Win=64 Len=120...
2849...	4964.2003721...	192.168.15.34	192.168.15.3	TCP	174	[TCP Port numbers reused] 22349 - 80 [SYN] Seq=0 Win=64 Len=120...
2849...	4964.2003815...	192.168.15.34	192.168.15.3	TCP	174	[TCP Port numbers reused] 22350 - 80 [SYN] Seq=0 Win=64 Len=120...
2849...	4964.2004164...	192.168.15.34	192.168.15.3	TCP	174	[TCP Port numbers reused] 22351 - 80 [SYN] Seq=0 Win=64 Len=120...
2850...	4964.2004629...	192.168.15.34	192.168.15.3	TCP	174	[TCP Port numbers reused] 22352 - 80 [SYN] Seq=0 Win=64 Len=120...
2850...	4964.2004736...	192.168.15.34	192.168.15.3	TCP	174	[TCP Port numbers reused] 22353 - 80 [SYN] Seq=0 Win=64 Len=120...
2850...	4964.2005232...	192.168.15.34	192.168.15.3	TCP	174	[TCP Port numbers reused] 22354 - 80 [SYN] Seq=0 Win=64 Len=120...
2850...	4964.2005364...	192.168.15.34	192.168.15.3	TCP	174	[TCP Port numbers reused] 22355 - 80 [SYN] Seq=0 Win=64 Len=120...
2850...	4964.2005444...	192.168.15.34	192.168.15.3	TCP	174	[TCP Port numbers reused] 22356 - 80 [SYN] Seq=0 Win=64 Len=120...
2850...	4964.2005515...	192.168.15.34	192.168.15.3	TCP	174	[TCP Port numbers reused] 22357 - 80 [SYN] Seq=0 Win=64 Len=120...
2850...	4964.2005600...	192.168.15.34	192.168.15.3	TCP	174	[TCP Port numbers reused] 22358 - 80 [SYN] Seq=0 Win=64 Len=120...
2850...	4964.2005700...	192.168.15.34	192.168.15.3	TCP	174	[TCP Port numbers reused] 22359 - 80 [SYN] Seq=0 Win=64 Len=120...
2850...	4964.2006019...	192.168.15.34	192.168.15.3	TCP	174	[TCP Port numbers reused] 22360 - 80 [SYN] Seq=0 Win=64 Len=120...
2850...	4964.2006538...	192.168.15.34	192.168.15.3	TCP	174	[TCP Port numbers reused] 22361 - 80 [SYN] Seq=0 Win=64 Len=120...
2850...	4964.2007011...	192.168.15.34	192.168.15.3	TCP	174	[TCP Port numbers reused] 22362 - 80 [SYN] Seq=0 Win=64 Len=120...
2850...	4964.2007133...	192.168.15.34	192.168.15.3	TCP	174	[TCP Port numbers reused] 22363 - 80 [SYN] Seq=0 Win=64 Len=120...
2850...	4964.2007211...	192.168.15.34	192.168.15.3	TCP	174	[TCP Port numbers reused] 22364 - 80 [SYN] Seq=0 Win=64 Len=120...
2850...	4964.2008034...	192.168.15.34	192.168.15.3	TCP	174	[TCP Port numbers reused] 22365 - 80 [SYN] Seq=0 Win=64 Len=120...
2850...	4964.2008143...	192.168.15.34	192.168.15.3	TCP	174	[TCP Port numbers reused] 22366 - 80 [SYN] Seq=0 Win=64 Len=120...
2850...	4964.2008216...	192.168.15.34	192.168.15.3	TCP	174	[TCP Port numbers reused] 22367 - 80 [SYN] Seq=0 Win=64 Len=120...
2850...	4964.2008289...	192.168.15.34	192.168.15.3	TCP	174	[TCP Port numbers reused] 22368 - 80 [SYN] Seq=0 Win=64 Len=120...
2850...	4964.2008365...	192.168.15.34	192.168.15.3	TCP	174	[TCP Port numbers reused] 22369 - 80 [SYN] Seq=0 Win=64 Len=120...
2850...	4964.2008444...	192.168.15.34	192.168.15.3	TCP	174	[TCP Port numbers reused] 22370 - 80 [SYN] Seq=0 Win=64 Len=120...

Рисунок 4 – Признак DDoS атаки представлена через Wireshark



Рисунок 5 –Неуспешное выполнение DDoS-атак

В третьей главе разработан методика тестирования безопасности корпоративной сети, которая состоит из следующих этапов:

- получения разрешения на проведение тестирования безопасности сети;
- определение целей тестирования;
- планирование тестирования;
- проведение тестирования;
- анализ результатов;
- рекомендации по обеспечению безопасности.

После проведения апробации методики тестирования на сервера в

разработанной модели корпоративной сети, были выявлены уязвимости. Первая уязвимость, которая была рассмотрена, эта уязвимость, которая может возникнуть в том случае, когда у нарушителя не получается подключиться к локальной сети организации, и этот метод является самая распространенная, и это социальная инженерия. Этот метод заключается в несанкционированном доступе к информации или системам хранения информации без использования технических средств.

Данная уязвимость, связана с человеческим фактором может привести к таким серьезным кибератакам как:

- фишинг, отправка электронных писем с инфицированными файлами или ссылками на зараженные сайты;
- спам, массовая реклам;
- fraud, электронные письма с подмененными адресами отправителей, чтобы убедить получателя выполнить определенные действия.

Цель этих кибератак заключаются в инфицирование компьютеров, сборе определенной информации. Были сформированы рекомендации для снижения риска, так как эти атаки в основном зависят от человеческого фактора, для его снижения необходима проводить мероприятия, в котором будет объясняться риски таких атак, научить сотрудников не взаимодействовать с такими письмами и не сохранять рабочие адреса в разных сервисах для снижения полученных писем.

Вторая уязвимость связана с DDoS-атаками, которые были рассмотрены во втором разделе. Для защиты использовались модули apache. На рисунке 5 представлена настройка от DDoS-атаки с помощью mod-evasive.

```
GNU nano 7.2                               evasive.conf *
<IfModule mod_evasive20.c>
  DOSHashTableSize 3097

  # Pas plus de 2 pages par seconde.
  DOSPageCount 2
  DOSPageInterval 1

  # Pas plus de 100 requetes par seconde (Images, CSS, ...)
  DOSSiteCount 100
  DOSSiteInterval 1

  # Période en seconde durant laquelle on bloque le client.
  DOSBlockingPeriod 500

  # Ajouter une ou plusieurs adresse IP en liste blanche.
  # L'adresse IP locale peut être mise en liste blanche.
  # DOSWhitelist 127.0.0.1
  # L'adresse IP du serveur peut être mise en liste blanche.
  # DOSWhitelist xxx.xx.xxx.xxx
  # Les 3 adresses IP sont celles du Bot de Google.
  # DOSWhitelist 66.249.65.*
  # DOSWhitelist 66.249.66.*
  # DOSWhitelist 66.249.71.*

  # Notifier l'alerte avec un mail.
  DOSEmailNotify admin@example.org
  DOSSystemCommand "/bin/echo %s >> /var/log/apache2/mod_evasive/dos_evasive.log && /bin/date >> /var/
</IfModule>
```

Рисунок 6 – Настройка модуля от DDoS атаки с помощью apache

Для обеспечения безопасности рекомендуется настраивать таблицы правил фильтрации пакетов, используя программу iptable. Результат этой настройки представлена на рисунке 7.

```
IpTables.txt – Блокнот
Файл Правка Формат Вид Справка
#Effacer toutes les règles et les chaînes existantes
iptables -F
iptables -X

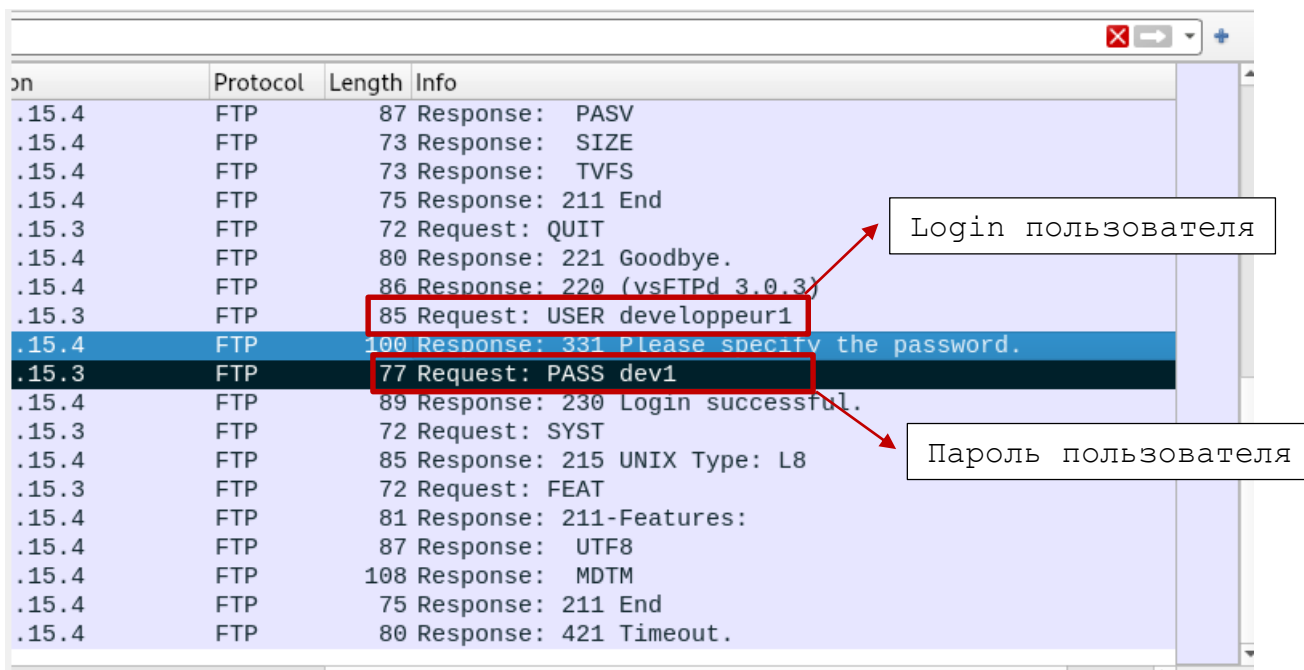
#Par défaut, on bloque tout le trafic entrant et sortant
iptables -P INPUT DROP
iptables -P OUTPUT DROP

#Autoriser le trafic la patte interne
iptables -A INPUT -i enp0s8 -p tcp -m multiport --dport 80,443,20,21,22 -j ACCEPT
iptables -A OUTPUT -p tcp -m multiport --sport 80,443,20,21,22 -j ACCEPT

#Autoriser le trafic la patte externe
iptables -A INPUT -i enp0s3 -p tcp -m multiport --dport 80,443 -j ACCEPT
iptables -A OUTPUT -p tcp -m multiport --sport 80,443 -j ACCEPT
```

Рисунок 7 – Настройка фильтрации пакета с помощью iptable

После тестирования веб-сервера, было проведено тестирование на VSFTPД сервер, цель данного тестирования заключалась в перехвате пакетов при подключении к серверу VSFTPД. На рисунке 8 видно, что при попытке авторизации пользователя на сервере его login и пароль передается без шифрования, что может привести к утечке данных пользователя, если нарушитель имеет доступ к сети организации.



Time	Source	Destination	Protocol	Length	Info
.15.4	.15.4	.15.4	FTP	87	Response: PASV
.15.4	.15.4	.15.4	FTP	73	Response: SIZE
.15.4	.15.4	.15.4	FTP	73	Response: TVFS
.15.4	.15.4	.15.4	FTP	75	Response: 211 End
.15.3	.15.3	.15.4	FTP	72	Request: QUIT
.15.4	.15.4	.15.4	FTP	80	Response: 221 Goodbye.
.15.4	.15.4	.15.4	FTP	86	Response: 220 (vsFTPD 3.0.3)
.15.3	.15.3	.15.4	FTP	85	Request: USER developpeur1
.15.4	.15.4	.15.4	FTP	100	Response: 331 Please specify the password.
.15.3	.15.3	.15.4	FTP	77	Request: PASS dev1
.15.4	.15.4	.15.4	FTP	89	Response: 230 Login successful.
.15.3	.15.3	.15.4	FTP	72	Request: SYST
.15.4	.15.4	.15.4	FTP	85	Response: 215 UNIX Type: L8
.15.3	.15.3	.15.4	FTP	72	Request: FEAT
.15.4	.15.4	.15.4	FTP	81	Response: 211-Features:
.15.4	.15.4	.15.4	FTP	87	Response: UTF8
.15.4	.15.4	.15.4	FTP	108	Response: MDTM
.15.4	.15.4	.15.4	FTP	75	Response: 211 End
.15.4	.15.4	.15.4	FTP	80	Response: 421 Timeout.

Рисунок 8 – Результат перехвата пакеты FTP при подключений

```
pam_service_name=vsftpd
#
# This option specifies the location of the RSA certificate to use for SSL
# encrypted connections.
#rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
#rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
#ssl_enable=NO
rsa_cert_file=/etc/ssl/private/vsftpd.pem
rsa_private_key_file=/etc/ssl/private/vsftpd.pem
ssl_enable=YES
```

Рисунок 9 – Рекомендация для устранения уязвимости связана с FTP протоколом

Таким образом, посредством методики тестирования были составлены рекомендации по совершенствованию информационной безопасности корпоративной сети, которые включают следующие действия: стратегия и политика, технические меры, использование процессов и процедур, инфраструктура, которая должна состоят из облачных сервисов и виртуализации, для упрощения управления и обеспечения безопасности серверов и других сетевых устройств.

ЗАКЛЮЧЕНИЕ

В ходе работы над диссертацией были изучены основные архитектуры защищенных локальных сетей, такие как распределенная, централизованная и централизованно-распределенная архитектура. Были также изучены разные методики такие как OSSTMM, OWASP. Проведен анализ стандартов проведения тестирования на проникновение PTES и стандарт NIST SP 800–115.

Была также смоделирована корпоративная сеть с помощью GNS3 для создания серверов, на которых проводилась апробация методики тестирования. После моделирования, осуществлены кибератаки на данную сеть такие как ARP-spoofing и DDoS. Таким образом показано, что разработанная модель сети, является уязвимой к различным кибератакам.

В разработанной методике тестирования безопасности корпоративной сети описана последовательность действий, имитирующих действия нарушителя. В результате апробации методики на сервера корпоративной сети были выявлены уязвимости, связанные с социальной инженерии, DDoS-атаки и уязвимость VSFTPD, которая передавала login и пароли пользователей по сети в открытом виде. В разработанной методике для каждой из выявленных уязвимостей был предложен способ их устранения.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

Тезисы конференций

1–А. Самаке, Б. А. Модель эксплуатации уязвимости ARP-протокола / Самаке Б. А. // Информационная безопасность : сборник материалов 59-й научной конференции аспирантов, магистрантов и студентов БГУИР, Минск, 17–21 апреля 2023 г. / Белорусский государственный университет информатики и радиоэлектроники. – Минск, 2023. – С. 52–54.

2–А. Самаке, Б. А. Анализ и защита от DDoS-атак в сетях на базе GNS3 / Самаке Б. А. // Информационная безопасность : сборник материалов 60-й научной конференции аспирантов, магистрантов и студентов БГУИР, Минск, 22–26 апреля 2024 г. / Белорусский государственный университет информатики и радиоэлектроники. – Минск, 2024.