# Описание топологии SEIRS-NIMFA на Kathara

Цель данного эксперимента - смоделировать распространение вредоносного трафика и исследовать динамику заражения в сети с несколькими сегментами.

Сценарий реализован в среде Kathará v3.8.0. Лаборатория демонстрирует поведение по аналогии с эпидемиологической моделью **SEIRS (Susceptible–Exposed–Infectious–Recovered–Susceptible)** в контексте сетевой безопасности.

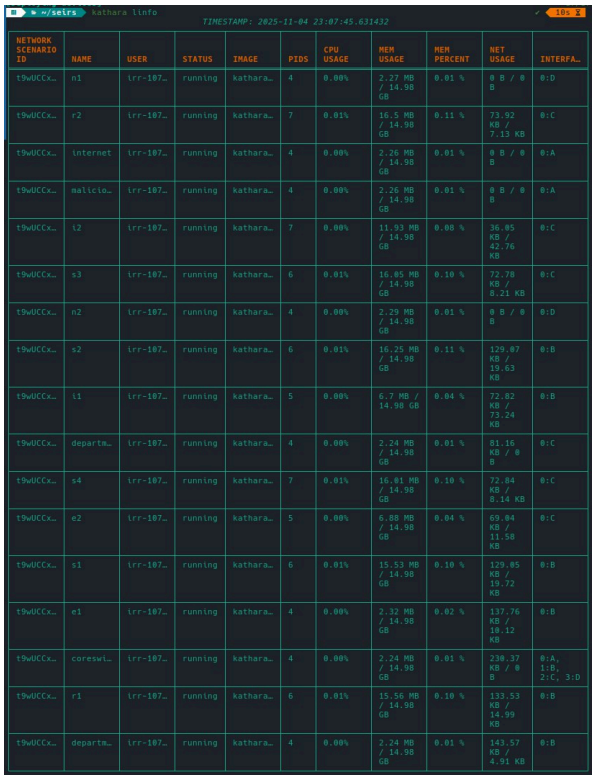
## Топология

Разберем составные части топологии сети. Топология лабораторной установки SEIRS-NIMFA представляет собой сегментированную сеть, состоящую из внешнего контура, ядра инфраструктуры, двух внутренних подразделений и зоны мониторинга.
Во внешнюю сеть (сегмент A) входят два узла: `internet` с адресом 203.0.113.1, который имитирует внешний интернет-канал, и `maliciousserver` — узел с адресом 198.51.100.50, выступающий в роли источника заражения и инициатора атак.

Центральным элементом сети является узел `coreswitch` (10.0.0.1/24), выполняющий функции коммутатора и маршрутизатора. Он соединяет четыре сегмента сети: внешний (A), первый отдел (B), второй отдел (C) и сеть мониторинга (D). Через него осуществляется весь межсегментный обмен и маршрутизация трафика, включая распространение вредоносного кода, моделируемого в эксперименте.

Первый отдел (сегмент B) представлен шлюзом `department1` (192.168.1.1) и пятью узлами, соответствующими различным состояниям модели SEIRS. Узлы `s1` и `s2` представляют восприимчивые хосты (Susceptible), узел `e1` — экспонированный (Exposed), `i1` — заражённый (Infected), а `r1` — восстановленный (Recovered). Второй отдел (сегмент C) имеет аналогичную структуру: шлюз `department2` (192.168.2.1) и набор узлов `s3`, `s4`, `e2`, `i2`, `r2`, которые моделируют те же состояния в отдельной подсети 192.168.2.0/24.

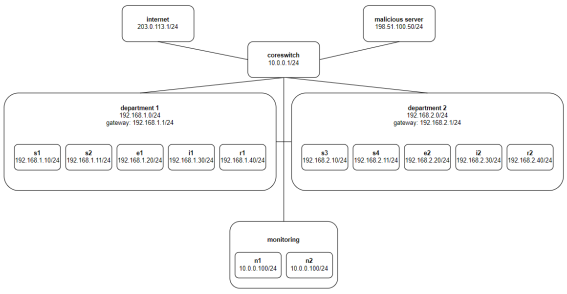
Отдельную подсеть D образует сеть Nymph, включающая узлы `n1` и `n2`. Эти узлы выполняют функции пассивных наблюдателей: собирают логи, отслеживают сетевую активность и позволяют анализировать распространение заражений без вмешательства в процесс. Такое деление на изолированные сегменты отражает структуру типичной корпоративной сети и обеспечивает возможность наблюдать, как заражение распространяется между подразделениями через ядро.



TIMESTAMP: 2025-11-04 23:07:45.631432

| NETWORK SCENARIO ID | NAME | USER | STATUS | IMAGE | PIDS | CPU USAGE | MEM USAGE | MEM PERCENT | NET USAGE | INTERFA… |
|---|---|---|---|---|---|---|---|---|---|---|
| t9wUCCx… | n1 | irr-107… | running | kathara… | 4 | 0.00% | 2.27 MB / 14.98 GB | 0.01 % | 0 B / 0 B | 0:D |
| t9wUCCx… | r2 | irr-107… | running | kathara… | 7 | 0.01% | 16.5 MB / 14.98 GB | 0.11 % | 73.92 KB / 7.13 KB | 0:C |
| t9wUCCx… | internet | irr-107… | running | kathara… | 4 | 0.00% | 2.26 MB / 14.98 GB | 0.01 % | 0 B / 0 B | 0:A |
| t9wUCCx… | malicio… | irr-107… | running | kathara… | 4 | 0.00% | 2.26 MB / 14.98 GB | 0.01 % | 0 B / 0 B | 0:A |
| t9wUCCx… | i2 | irr-107… | running | kathara… | 7 | 0.00% | 11.93 MB / 14.98 GB | 0.08 % | 36.05 KB / 42.76 KB | 0:C |
| t9wUCCx… | s3 | irr-107… | running | kathara… | 6 | 0.01% | 16.05 MB / 14.98 GB | 0.10 % | 72.78 KB / 8.21 KB | 0:C |
| t9wUCCx… | n2 | irr-107… | running | kathara… | 4 | 0.00% | 2.29 MB / 14.98 GB | 0.01 % | 0 B / 0 B | 0:D |
| t9wUCCx… | s2 | irr-107… | running | kathara… | 6 | 0.01% | 16.25 MB / 14.98 GB | 0.11 % | 129.07 KB / 19.63 KB | 0:B |
| t9wUCCx… | i1 | irr-107… | running | kathara… | 5 | 0.00% | 6.7 MB / 14.98 GB | 0.04 % | 72.82 KB / 73.24 KB | 0:B |
| t9wUCCx… | departm… | irr-107… | running | kathara… | 4 | 0.00% | 2.24 MB / 14.98 GB | 0.01 % | 81.16 KB / 0 B | 0:C |
| t9wUCCx… | s4 | irr-107… | running | kathara… | 7 | 0.01% | 16.01 MB / 14.98 GB | 0.10 % | 72.84 KB / 8.14 KB | 0:C |
| t9wUCCx… | e2 | irr-107… | running | kathara… | 5 | 0.00% | 6.88 MB / 14.98 GB | 0.04 % | 69.84 KB / 11.58 KB | 0:C |
| t9wUCCx… | s1 | irr-107… | running | kathara… | 6 | 0.01% | 15.53 MB / 14.98 GB | 0.10 % | 129.05 KB / 19.72 KB | 0:B |
| t9wUCCx… | e1 | irr-107… | running | kathara… | 4 | 0.00% | 2.32 MB / 14.98 GB | 0.02 % | 137.76 KB / 10.12 KB | 0:B |
| t9wUCCx… | coreswi… | irr-107… | running | kathara… | 4 | 0.00% | 2.24 MB / 14.98 GB | 0.01 % | 230.37 KB / 0 B | 0:A, 1:B, 2:C, 3:D |
| t9wUCCx… | r1 | irr-107… | running | kathara… | 6 | 0.01% | 15.56 MB / 14.98 GB | 0.10 % | 133.53 KB / 14.99 KB | 0:B |
| t9wUCCx… | departm… | irr-107… | running | kathara… | 4 | 0.00% | 2.24 MB / 14.98 GB | 0.01 % | 143.57 KB / 4.91 KB | 0:B |

Информация об устройствах в Kathara




Визуальное представление сети

# Структура файлов

Разберем структуру файлов в лабораторном стенде. Основной файл `lab.conf` описывает сетевую топологию, интерфейсы и адресацию. При запуске эксперимента эмулятор обращается сначала к этому файлу. Узлы инициализируются с помощью скриптов вида `*.startup`, где описывается настройка IP и запуск служб. Основная симуляция распространения червя находится в `worm_simulation.py`. В каталоге `shared/` хранятся скрипты для общего доступа `vulnerable_*.py`, имитирующие уязвимые FTP/HTTP сервисов, веб-страницы и логи, фиксирующие активность узлов, атак и заражений.

Для примера, скрипт `coreswitch.startup` назначает IP-адрес 10.0.0.1/24, активирует пересылку пакетов и запускает бесконечный цикл для поддержания соединений между сегментами. Узел `maliciousserver` в своём скрипте получает адрес 198.51.100.50/24 и

периодически записывает информацию об активности в `malicious_activity.log`, моделируя работу внешнего вредоносного источника, ведущего сетевое сканирование.

## Скрипт симуляции заражения

Остдельно рассмотрим логику распространения вредоносного кода по сценарию `worm_simulation.py`. Он реализует сетевую аналогию эпидемиологической модели SEIRS, последовательно перебирая узлы и проверяя доступность характерных уязвимых портов 21 (FTP) и 80 (HTTP). При обнаружении открытого порта происходит попытка эксплуатации (`try_exploit`); в случае успеха узел помечается как INFECTED, что соответствует переходу в состояние I. Все действия подробно фиксируются в файле `/shared/logs/seirs_worm.log`, после чего цикл повторяется с интервалом в 60 секунд.

Такой сценарий моделирует непрерывное движение состояний S → E → I → R → S. Узлы s1–s4 представляют восприимчивую часть системы (S), e1 и e2 — экспонированные хосты, i1 и i2 — активно заражённые источники, а r1 и r2 — восстановленные после атаки, временно невосприимчивые. В дальнейшем восстановленные узлы могут снова стать восприимчивыми, что имитирует утрату «иммунитета» после обновлений.

## Логирование

Вся активность в сети детально фиксируется в каталоге `/shared/logs`. Здесь хранятся отдельные журналы узлов (`r1.log`, `s4.log`), фоновые процессы (`maliciousserver_bg.log`, `coreswitch.log`) и основной лог симуляции `seirs_worm.log`, где записываются события заражений. Дополнительные файлы (`ftp_server.log`, `internet.log`, `n2_activity.log`) содержат сетевые взаимодействия и наблюдения мониторинговых узлов.