Основы построения защищенных компьютерных сетей

Лекция 12
Системы обнаружения и предотвращения вторжений

Семён Новосёлов

2025

БФУ
ИМЕНИ И. КАНТА

Система обнаружения вторжений (СОВ, IDS) — устройство или программа для обнаружения вредоносной активности и нарушений политики безопасности в сетях и компьютерных системах.

Система предотвращения вторжений (IPS) **=** СОВ **+** механизм блокировки вторжений

Типы СОВ

сетевые (NIDS) — отслеживание сетевого трафика

хостовые (HIDS) — контроль событий на хосте:

- соблюдение политики безопасности
- действия программ
- целостность файлов

AppArmor

AIDE

Схема расположения сетевой СОВ

Основные возможности СОВ

- регистрация попыток доступа и сетевой разведки
- уведомление о подозрительной активности
- детектирование применения эксплойтов, бэкдоров
- детектирование DoS-атак

Способы выявления атак

По сигнатурам:

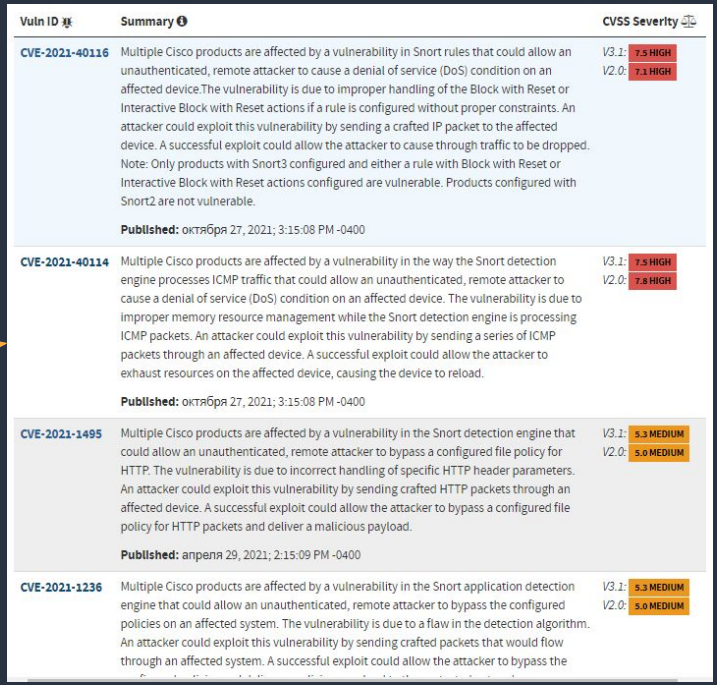
- детектирование известных атак по шаблону
- требует регулярно обновляемые списки правил детектирования

По аномалиям:

- подходит для неизвестных атак
- детектирование по статистическим характеристикам, отклонению от протоколов, используя нейронные сети
- много ложных срабатываний

Недостатки и ограничения СОВ

- шифрованный трафик не анализируется
- снижение пропускной способности сети и время отклика, так как анализ происходит не мгновенно
- СОВы выполняют полный разбор протоколов и они сами могут быть источником уязвимостей

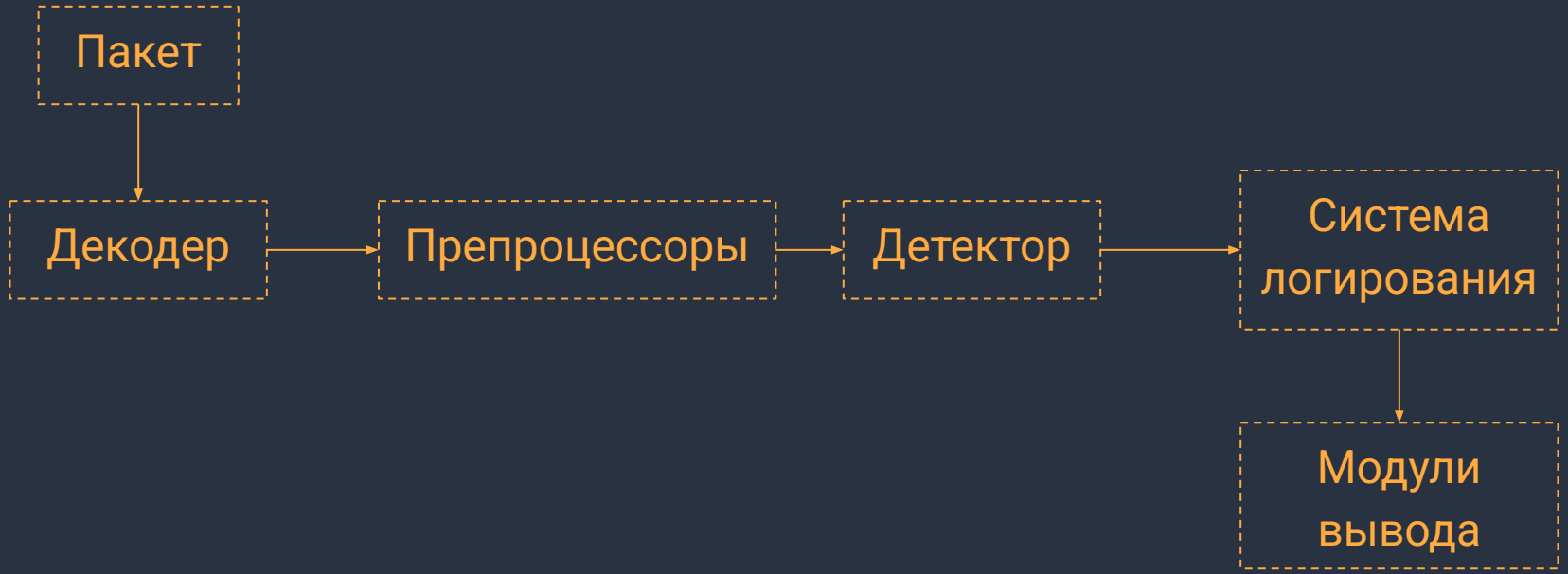


Vuln ID	Summary	CVSS Severity
CVE-2021-40116	Multiple Cisco products are affected by a vulnerability in Snort rules that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device.The vulnerability is due to improper handling of the Block with Reset or Interactive Block with Reset actions if a rule is configured without proper constraints. An attacker could exploit this vulnerability by sending a crafted IP packet to the affected device. A successful exploit could allow the attacker to cause through traffic to be dropped. Note: Only products with Snort3 configured and either a rule with Block with Reset or Interactive Block with Reset actions configured are vulnerable. Products configured with Snort2 are not vulnerable. **Published:** октября 27, 2021; 3:15:08 PM -0400	*V3.1:* 7.5 HIGH *V2.0:* 7.1 HIGH
CVE-2021-40114	Multiple Cisco products are affected by a vulnerability in the way the Snort detection engine processes ICMP traffic that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper memory resource management while the Snort detection engine is processing ICMP packets. An attacker could exploit this vulnerability by sending a series of ICMP packets through an affected device. A successful exploit could allow the attacker to exhaust resources on the affected device, causing the device to reload. **Published:** октября 27, 2021; 3:15:08 PM -0400	*V3.1:* 7.5 HIGH *V2.0:* 7.8 HIGH
CVE-2021-1495	Multiple Cisco products are affected by a vulnerability in the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect handling of specific HTTP header parameters. An attacker could exploit this vulnerability by sending crafted HTTP packets through an affected device. A successful exploit could allow the attacker to bypass a configured file policy for HTTP packets and deliver a malicious payload. **Published:** апреля 29, 2021; 2:15:09 PM -0400	*V3.1:* 5.3 MEDIUM *V2.0:* 5.0 MEDIUM
CVE-2021-1236	Multiple Cisco products are affected by a vulnerability in the Snort application detection engine that could allow an unauthenticated, remote attacker to bypass the configured policies on an affected system. The vulnerability is due to a flaw in the detection algorithm. An attacker could exploit this vulnerability by sending crafted packets that would flow through an affected system. A successful exploit could allow the attacker to bypass the	*V3.1:* 5.3 MEDIUM *V2.0:* 5.0 MEDIUM

Система Snort

- система обнаружения и предотвращения вторжений разработанная Мартином Рёшем (Sourcefire/Cisco)
- имеет открытый исходный код
- поддерживает как детектирование по сигнатурам, так и анализ аномалий протоколов

Архитектура Snort



Декодер пакетов

- определяет протокол пакета и проверяет соответствие данных этому протоколу
- генерирует сигналы в случае:
  - неправильно сформированных пакетов
  - наличия необычных или неправильных опций TCP в заголовке
  - и т.д.

Препроцессоры

- подключаемые модули, которые позволяют различными способами анализировать входные данные
- собирают пакеты в соединения, потоки, из фрагментов
- Snort содержит широкий выбор препроцессоров, которые можно использовать в различных режимах работы

Препроцессор frag3

- модуль дефрагментации IP-пакетов
- собирает пакеты вместе и сортирует их по порядку для последующего анализа

Препроцессор sfPortscan

- модуль, позволяющий детектировать сканирование портов
- работает не слишком надёжно

```
preprocessor sfportscan: proto <protocols> \
scan_type <portscan|portsweep|decoy_portscan|distributed_portscan|all> \
sense_level <low|medium|high> \
watch_ip <IP or IP/CIDR> \
ignore_scanners <IP list> \
ignore_scanned <IP list> \
logfile <path and filename> \
disabled
```

Правила Snort

- сигнатуры атак
- Snort имеет несколько наборов правил для разных типов атак и сервисов
- это позволяет настроить систему под конкретную сеть, отключив ненужные наборы

Пример правила

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (
  msg:"WEB-MISC /etc/passwd";
  flow:to_server,established;
  content:"/etc/passwd";
  nocase;
  classtype:attempted-recon;
  sid:1122;
  rev:5;
)
```

Разворачивание Snort на Ubuntu

Установка:

```
sudo apt install snort snort-rules-default
```

Настройка:

- Добавить в /etc/snort/snort.conf строку:
  `output alert_fast: alert.fast`
  для отображения записи событий в /var/log/snort/alert.fast
- Перезагрузка после изменения файла конфигурации:

```
sudo service snort restart
```

Пример вывода

```
root@novsem1:/home/n7v# sudo tail -f /var/log/snort/alert.fast
11/03-03:14:22.301014  [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 128.71.54.192 -> 79.174.13.91
11/03-03:14:22.301014  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 128.71.54.192 -> 79.174.13.91
11/03-03:14:48.514545  [**] [1:469:3] ICMP PING NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 128.71.54.192 -> 79.174.13.91
11/03-03:14:48.514545  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 128.71.54.192 -> 79.174.13.91
11/03-03:14:48.519590  [**] [1:453:5] ICMP Timestamp Request [**] [Classification: Misc activity] [Priority: 3] {ICMP} 128.71.54.192 -> 79.174.13.91
11/03-03:14:50.618320  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 128.71.54.192:47621 -> 79.174.13.91:70
5
11/03-03:14:50.868214  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 128.71.54.192:47621 -> 79.174.13.91:161
11/03-03:18:35.864735  [**] [1:469:3] ICMP PING NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 185.146.159.234 -> 79.174.13.91
11/03-03:18:35.864735  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 185.146.159.234 -> 79.174.13.91
11/03-03:21:15.162606  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 194.110.115.99 -> 79.174.13.91
11/03-03:24:26.697974  [**] [1:469:3] ICMP PING NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 185.146.159.234 -> 79.174.13.91
11/03-03:24:26.697974  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 185.146.159.234 -> 79.174.13.91
```

Детектирование применения команд:

- `ping 79.174.13.91`
- `nmap -sV 79.174.13.91`

Литература и ссылки

- Snort Users Manual
  https://www.snort.org/documents/snort-users-manual
- Snort Rule Infographic
  https://www.snort.org/documents/snort-rule-infographic