Информационная безопасность

Антон Карпов для студентов КИТ, 30 октября 2012 г.

Яндекс

Свойства информации

Конфиденциальность

Целостность

Доступность

Угроза

Уязвимость

Атака

Классификация уязвимостей

CVE — Common Vulnerabilities and Exposures (1999)

- Уязвимости проектирования
- Уязвимости реализации
- Уязвимости эксплуатации

Классификация атак

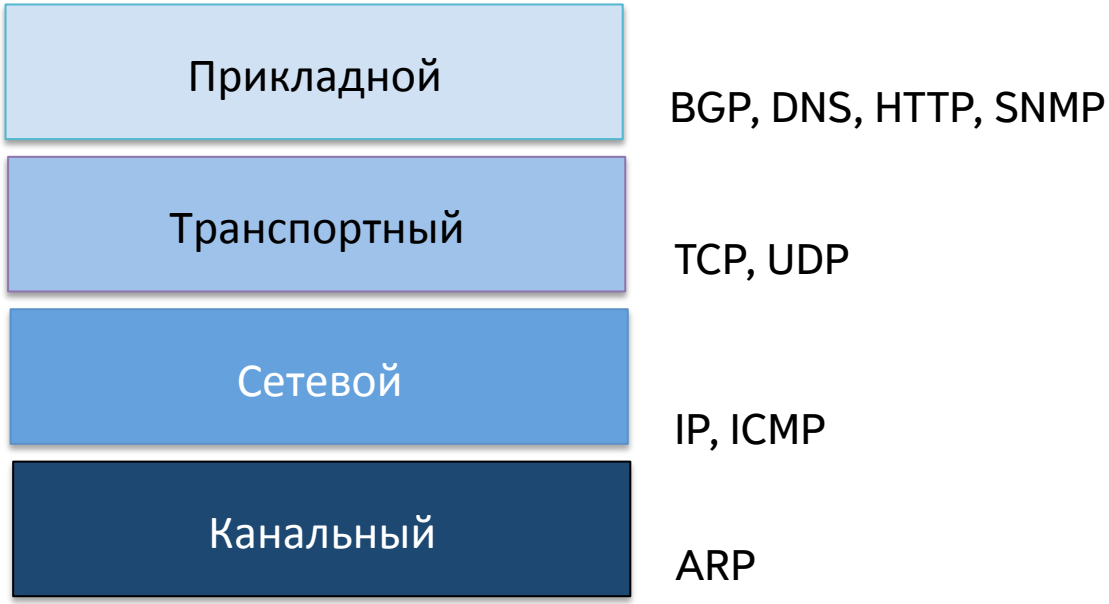
- ✓ Локальные
- ✓ Удаленные

- ✓ Злонамеренные
- ✓ Случайные

- ✓ Атаки на пользователей (СИ)
- ✓ Атаки на клиентское ПО
- ✓ Атаки на серверные приложения
- ✓ Атаки на системные сервисы
- ✓ Атаки на стек протоколов TCP/IP

- ✓ Получение доступа к системе
- ✓ Повышение привилегий в системе
- ✓ Раскрытие конфиденциальной информации
- ✓ Нарушение целостности информации (вирусы, черви, MITM-атаки)
- ✓ Снижение доступности информации (DoS/DDoS)

Модель TCP/IP



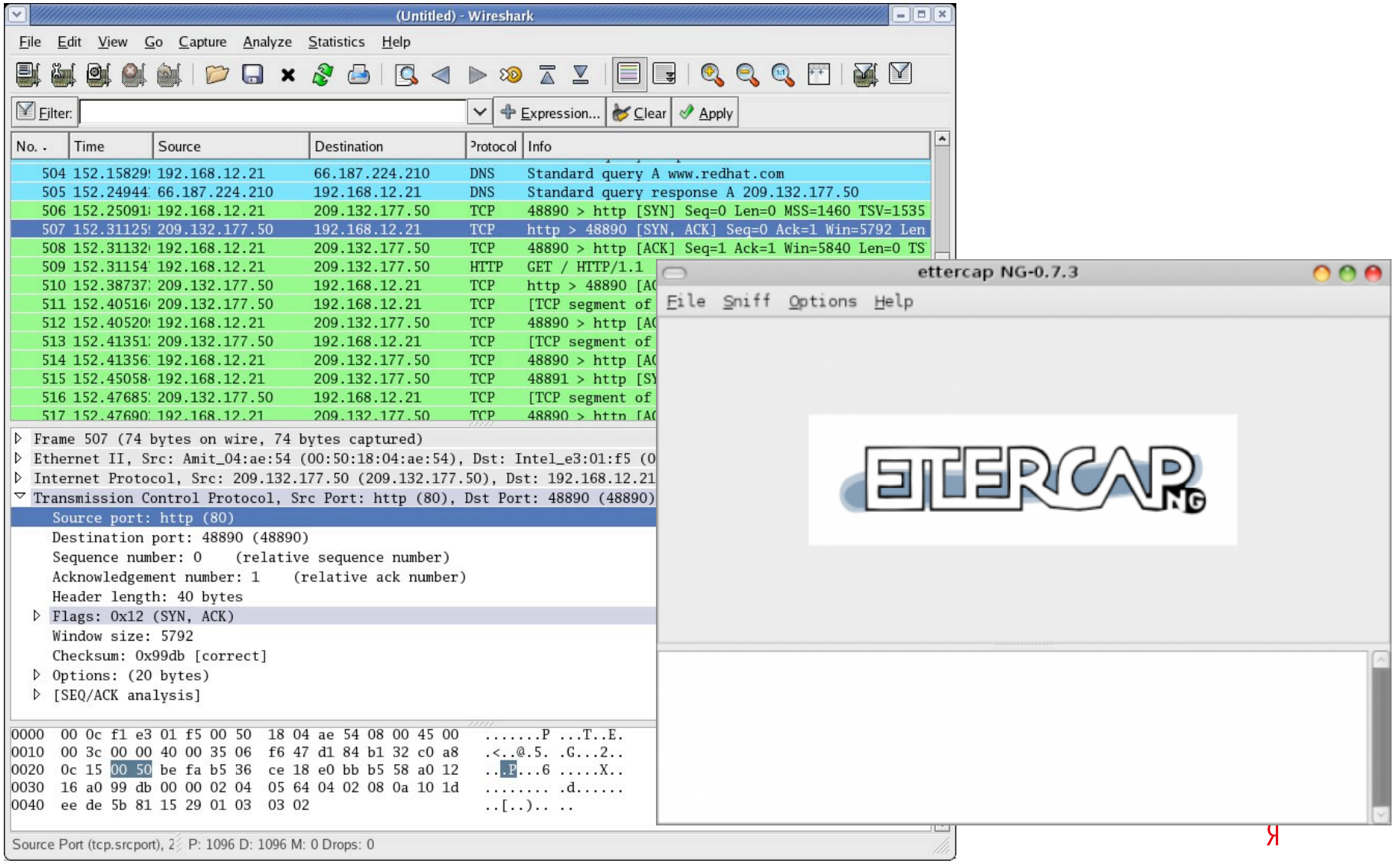
BGP, DNS, HTTP, SNMP

TCP, UDP

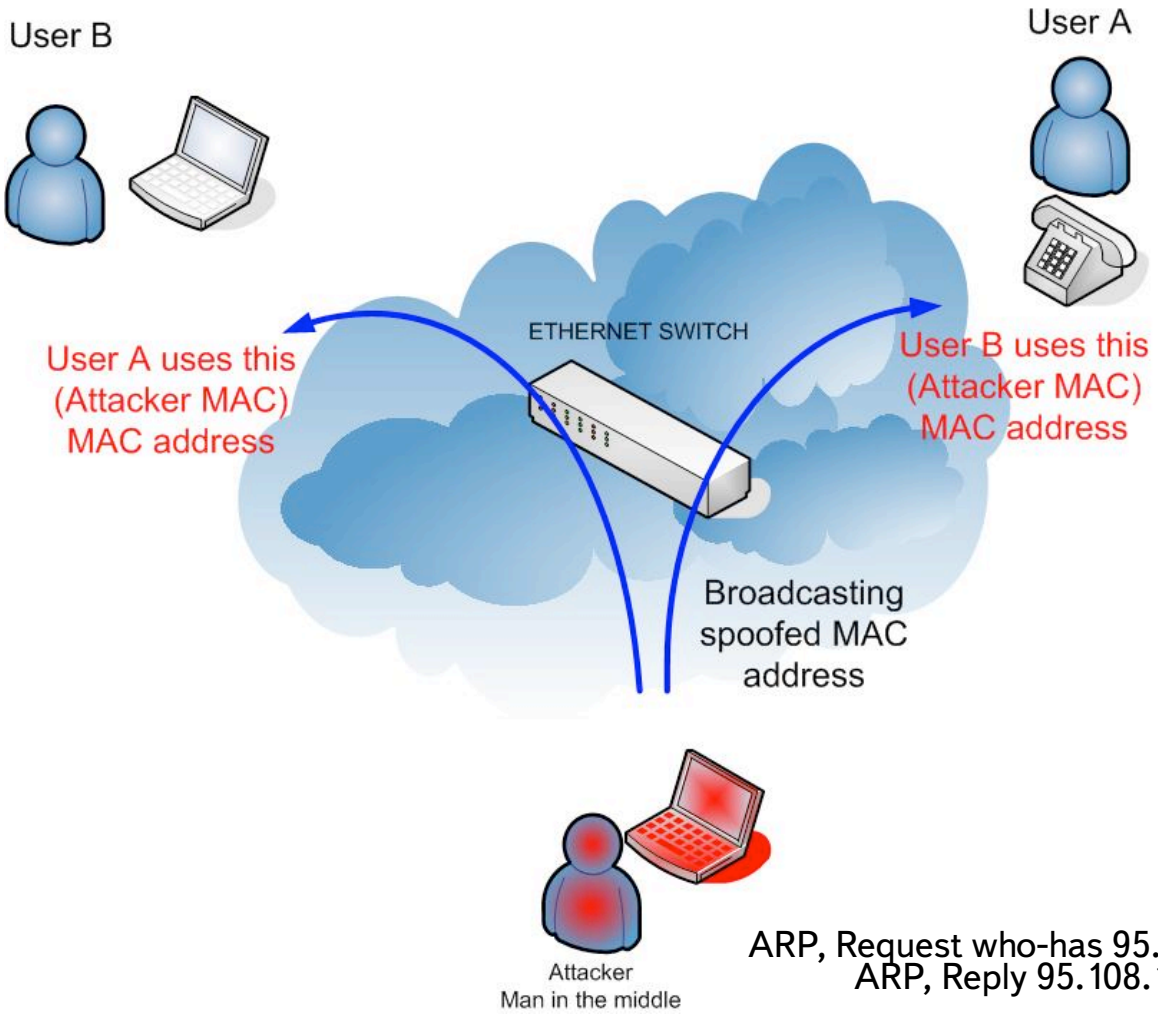
IP, ICMP

ARP

Перехват пакетов



Уязвимости канального уровня



ARP-спуфинг

ARP, Request who-has 95.108.170.39 tell 95.108.170.37, length 28
ARP, Reply 95.108.170.39 is-at 00:23:14:82:f2:68, length 46

Обнаружение снифферов

ICMP-запросами

Отслеживанием DNS-запросов

ARP- запросами

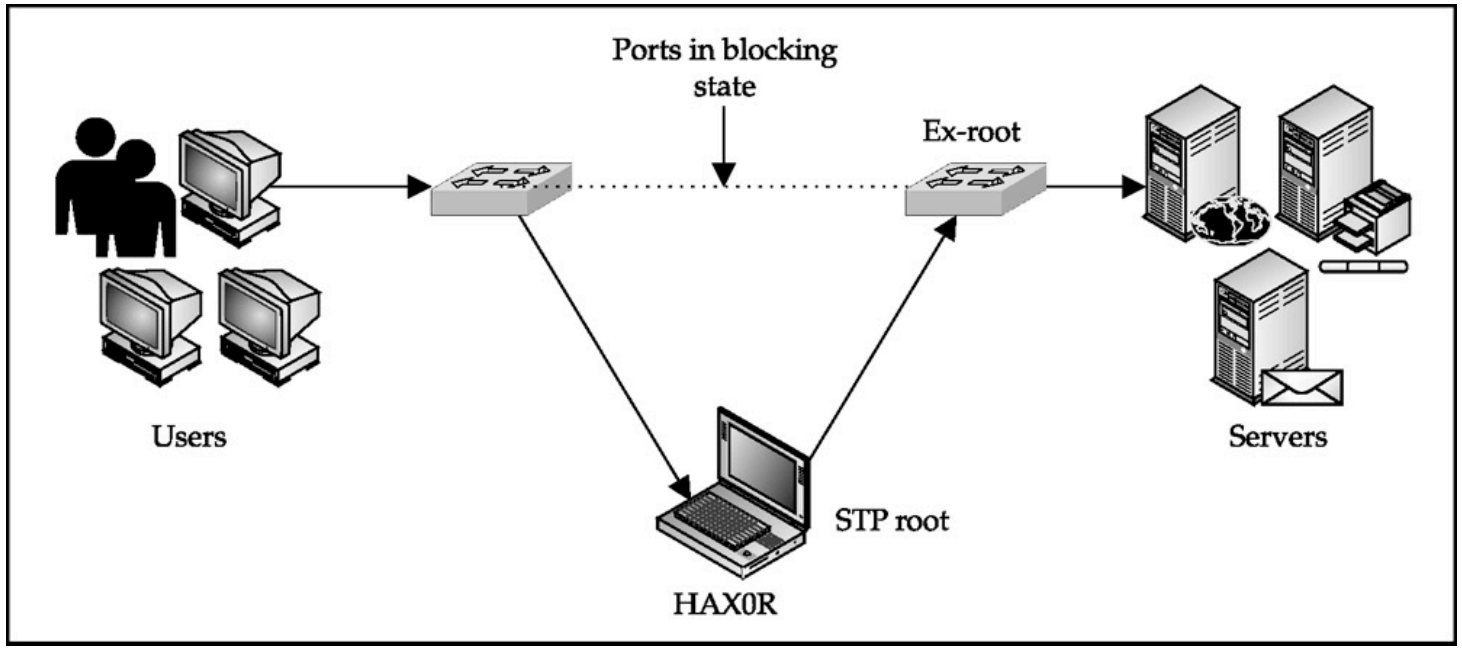
Аутентификация в сети (802.1x)

Шифрование трафика

Уязвимости канального уровня

Атаки на STP

- Configuration BPDU (CBPDU), used for Spanning Tree computation
- Topology Change Notification (TCN) BPDU
- Topology Change Notification Acknowledgment (TCA)



Уязвимости сетевого уровня

Атаки на ICMP (2005 год)

- Destination unreachable
- Protocol unreachable
- Fragmentation needed but DF is set

Проблемы с IP

- IP source routing
- IP fragmentation

IPv6

- IPv4-to-IPv6 миграция
- Type 0 routing header
- Сниффинг и MITM (без IPSec)

Уязвимости транспортного уровня

TCP Sockstress (2009)

- FIN_WAIT2

TCP SYN flood

UDP flood

Уязвимости прикладного уровня

SMTP

- Promisc relay
- Подделка заголовков

SNMP

- Community strings

Протоколы аутентификации

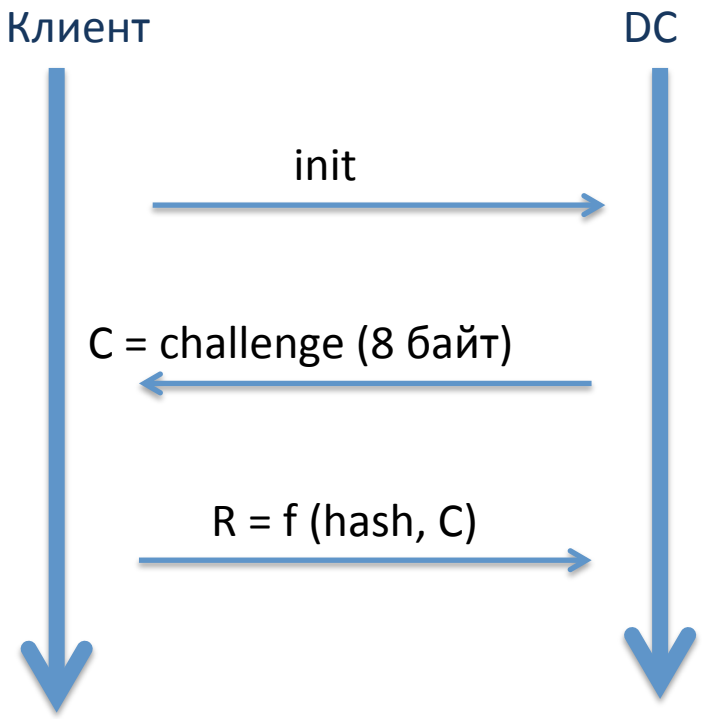
- NTLM (smbrelay, pass the hash)

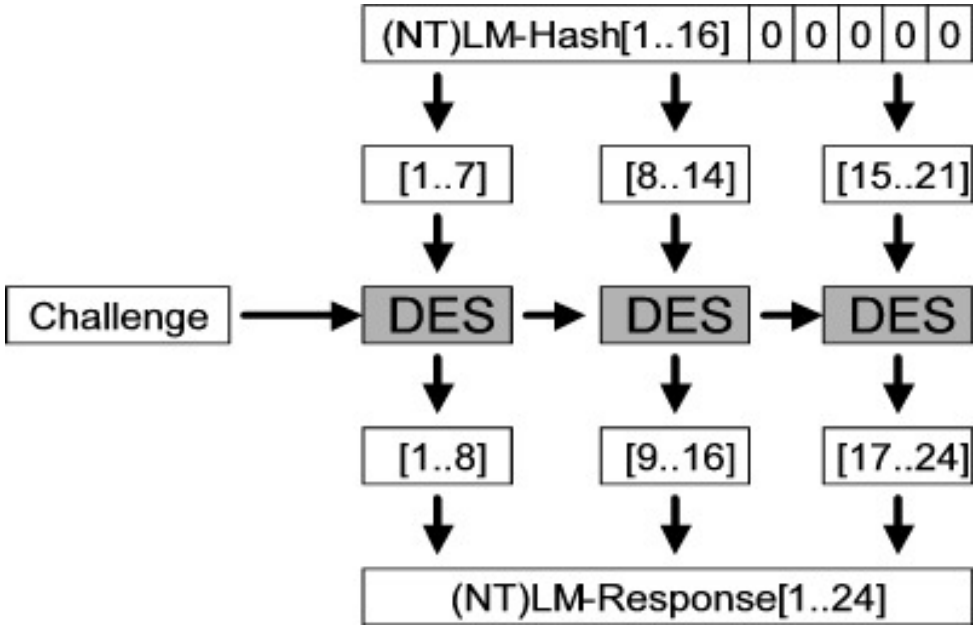
Application level DDoS

- HTTP Slow GET/POST

Уязвимости прикладного уровня

LM/NTLM challenge-response





R’ = f (SAM[hash], C)
R’ == R -> access granted

Pass the Hash

- Если в challenge-response участвует только LM/ NTLM хэш, то пароль знать не обязательно. Можно использовать хэш для аутентификации.

Почему это все актуально. LMCompatibilityLevel

HKLM\System\CurrentControlSet\Control\LSA

0: Клиент: LM/NTLMv1. Контроллер: LM/NTLMv1/NTLMv2
1: Клиент: LM/NTLMv1/NTLMv2. Контроллер: LM/NTLMv1/ NTLMv2
2: Клиент: NTLMv1/NTLMv2. Контроллер: LM/NTLMv1/NTLMv2
3: Клиент: NTLMv2. Контроллер: LM/NTLMv1/NTLMv2
4: Клиент: NTLMv2. Контроллер: NTLMv1/NTLMv2
5: Клиент: NTLMv2. Контроллер: NTLMv2

Windows XP: **0**
Windows 2003: **2**
Windows Vista/2008: **3**
Windows 7/2008 R2: **3**

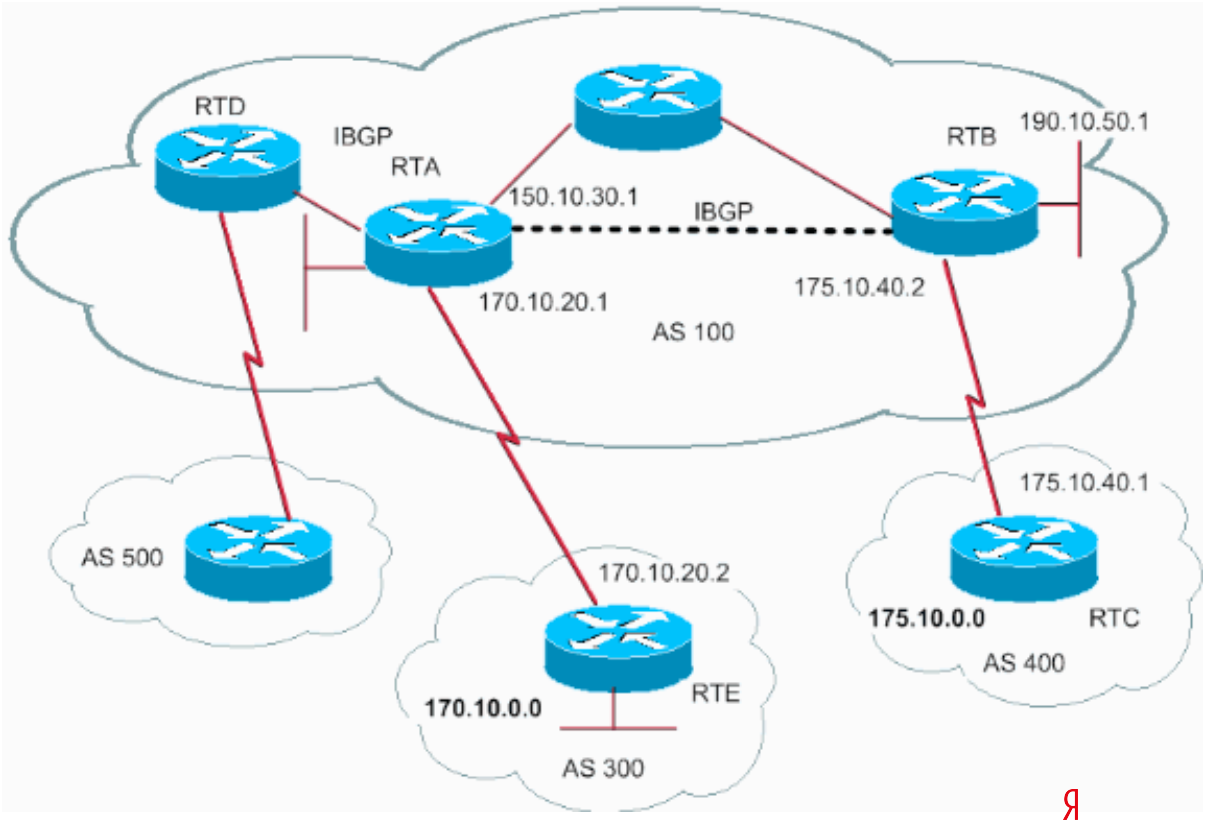
Уязвимости прикладного уровня

DNS

- Трансфер зоны
- Рекурсивные запросы (DNS amplification)
- Kaminsky DNS vulnerability

BGP

- DDoS



Уязвимости прикладного уровня: HTTP

Cookies

Same **O**rigin **P**olicy

- Инъекции (SQL, LDAP и т.д.)
- Cross Site Scripting (XSS)
- Cross Site Request Forgery (CSRF)
- Небезопасное управление сессией
- ...

Антон Карпов
Служба информационной безопасности

tokza@yandex-team.ru
+7 495 739-70-00

ул. Льва Толстого, 16
Москва, Россия, 119021
Яндекс Москва

Яндекс