**Задача 1**

В процессе прослушивания сети в неразборчивом режиме, вы зафиксировали использование протоколов: ARP, CDP, RPC, DHCP, DTP, HSRP, DNS, SMB, STP, HTTP. Какие действия вы можете предпринять для развития атаки, основываясь на полученных данных?

Ответ

### Spuffing ARP, подмена MAC адреса для CDP выдать себя за главный маршрутизатор, STP выдать себя за коммутатор с низкой стоимостью, DHCP для получения адреса в сети, DNS подмена, HTTP перехват данных, если SMB v1 - [CVE-2017-0144](https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0144)

**Задача 2**

В сети используется Microsoft Active Directory на базе Windows Server 2016. На рабочие станции сотрудников установлена Windows 10. Какие шаги необходимо предпринять, чтобы недопустить или уменьшить вероятность заражения сети вирусом использующим сходные с [NonPetya](https://ru.wikipedia.org/wiki/Petya" \l ".D0.9C.D0.B0.D1.81.D1.81.D0.BE.D0.B2.D0.BE.D0.B5_.D0.B7.D0.B0.D1.80.D0.B0.D0.B6.D0.B5.D0.BD.D0.B8.D0.B5_.D0.B2_2017" \t "_blank) вектора распространения.

1. В разрезе сети заблокировать порты 135, 139, 445;
2. Поставить обновление MS17-010, обновить версию протокола до SMB2, поставить контроль целостности папки **C:\Windows\perfс;**
3. При наличие ids/ips включить в правила при запуске сессии PSExe уведомить администратора.

**Задача 3**

Чем опасна запись в /etc/sudoers:  
  
non\_root\_user ALL=(ALL) NOPASSWD: /usr/sbin/less

Пользователь non\_root\_user с флагом (ALL) возможно может мимикрировать под других пользователей, считаю правильным запись:

non\_root\_user ALL=(root) NOPASSWD: /usr/sbin/less

Предложите безопасный вариант записи.

**Задача 4**

Дан пример конфигурационного файла для ssh-сервера. Как бы вы изменили данную конфигурацию и почему?  
Конфигурационный файл:

Port 22

Protocol 2

# HostKeys for protocol version 2

HostKey /etc/ssh/ssh\_host\_rsa\_key

HostKey /etc/ssh/ssh\_host\_dsa\_key

HostKey /etc/ssh/ssh\_host\_ecdsa\_key

HostKey /etc/ssh/ssh\_host\_ed25519\_key

#Privilege Separation is turned on for security

UsePrivilegeSeparation yes

# Lifetime and size of ephemeral version 1 server key

KeyRegenerationInterval 3600

ServerKeyBits 1024

# Logging

SyslogFacility AUTH

LogLevel VERBOSE

LoginGraceTime 120

PermitRootLogin yes

StrictModes yes

RSAAuthentication yes

PubkeyAuthentication yes

IgnoreRhosts yes

RhostsRSAAuthentication no

HostbasedAuthentication no

PermitEmptyPasswords no

ChallengeResponseAuthentication yes

PasswordAuthentication yes

X11Forwarding yes

X11DisplayOffset 10

PrintMotd no

PrintLastLog yes

TCPKeepAlive yes

#UseLogin no

AcceptEnv LANG LC\_\*

Subsystem sftp /usr/lib/openssh/sftp-server

UsePAM yes

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Задача 5**  Напишите программу, обрабатывающую приложенный [журнал](https://yadi.sk/d/GPLjKA_f3Rykid) и выполняющую следующие функции (можно реализовать не полный набор функций. оценка за задание будет равна сумме баллов корректно работающих функций):   |  |  |  | | --- | --- | --- | | № п\п | балл | суть задания | | 1 | 1 | Поиск 5ти пользователей, сгенерировавших наибольшее количество запросов | | 2 | 1 | Поиск 5ти пользователей, отправивших наибольшее количество данных | | 3 | 3 | Поиск регулярных запросов (запросов выполняющихся периодически) по полю src\_user | | 4 | 3 | Поиск регулярных запросов (запросов выполняющихся периодически) по полю src\_ip | | 5 | 5 | Рассматривая события сетевого трафика как символы неизвестного языка, найти 5 наиболее устойчивых N-грамм журнала событий (текста на неизвестном языке), ([https://ru.wikipedia.org/wiki/N-грамм](https://ru.wikipedia.org/wiki/N-%D0%B3%D1%80%D0%B0%D0%BC%D0%BC)), где N=3-5. Тип символа задается квартетом user+src\_port+dest\_ip+dest\_port. |   Отчет должен быть сгенерирован в текстовом файле (result.txt), в кодировке UTF-8, в формате:  # Поиск 5ти пользователей, сгенерировавших наибольшее количество запросов  Решение1  ...  # Рассматривая события сетевого трафика как символы неизвестного языка,  # найти 5 наиболее устойчивых N-грамм журнала событий  # (текста на неизвестном языке)  Решение2  Необходимо прислать исходный код программы (либо ссылку на репозиторий с кодом) и файл с результатами. Программа должна выполняться на Ubuntu Xenial (16.04 LTS) |
| ЗагрузитьЗагрузитьМаксимум 20 файлов общим размером до 20 МБ |

**Задача 6**

Изучите JavaScript-код ниже:  
  
**var** npage;  
fetch('https://news.yandex.ru/yandsearch?rpt=nnews2&grhow=clutop&text=security')  
    .then(**function**(response) {  
         **return** response.text();  
    }).then(**function**(content) {  
        npage = content;  
    });  
  
Допустим, что этот код размещен на произвольном веб-ресурсе (например, на https://testsite.com/). Какие данные будут в переменной npage ? А что будет в переменной npage , если выполнить этот код на https://news.yandex.ru ? Из-за чего возникла разница?

**Задача 7**

Уязвим ли следующий код:  
  
mysql\_query("SELECT \* FROM news WHERE \  
id = ".mysql\_real\_escape\_string($\_GET['id']));  
  
mysql\_real\_escape\_string добавляет обратные слэши к следующим символам: \x00, \n, \r, \, ', " и \x1a.

?id=-1 SELECT \* FROM USERMANE

**Задача 8**

Максимально подробно расскажите, что иллюстрируют данные ниже. В своем рассказе обязательно укажите, что по этим данным вы можете сказать о действиях пользователя и о его ПО, а также опишите, зачем нужны все эти строки.  
  
POST /passport?mode=auth&retpath=https://mail.yandex.ru HTTP/1.1  
Host: passport.yandex.ru  
Connection: close  
Content-Length: 27  
Cache-Control: max-age=0  
Origin: https://www.yandex.ru  
Upgrade-Insecure-Requests: 1  
Content-Type: application/x-www-form-urlencoded  
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_13\_2) \  
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.99 Safari/537.36  
Accept:<text/html,application/xhtml+xml,application/xml;q=0.9, \  
image/webp,image/apng,\*/\*;q=0.8  
Referer: https://www.yandex.ru/  
Accept-Encoding: gzip, deflate  
Accept-Language: ru-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7  
Cookie: userid=3133731337; x\_val=029349fssjkjsdf.asdjuioqiwe; axr=0;  
login=login&passwd=password

**Задача 9**

Изучите код ниже:   
  
#include <stdio.h>  
**int** main(**int** argc, **char** \* argv[]) {  
    **char** user\_input[64];  
    fgets(user\_input, 64, stdin);  
    printf(user\_input);  
    **return** 0;  
}  
  
Есть ли в нем какая-либо уязвимость?

**Задача 10**

Чем друг от друга отличаются алгоритмы Диффи-Хеллмана и RSA?

В алгоритме Диффи-Хеллмана используеться общий секретный ключ, который передается всем участникам обмена, а в RSA передаются открытые части ключей участникам обмена, при этом секретная и открытая часть у каждого индивидуальная.