

Презентация по 4 этапу индивидуального проекта

Использование nikto

Танрибергенов Э.

2024 г.

Российский университет дружбы народов, Москва, Россия

Информация

- Танрибергенов Эльдар
- студент 4 курса из группы НПИбд-02-21
- ФМиЕН, кафедра прикладной информатики и теории вероятностей
- Российский университет дружбы народов

Цели и задачи

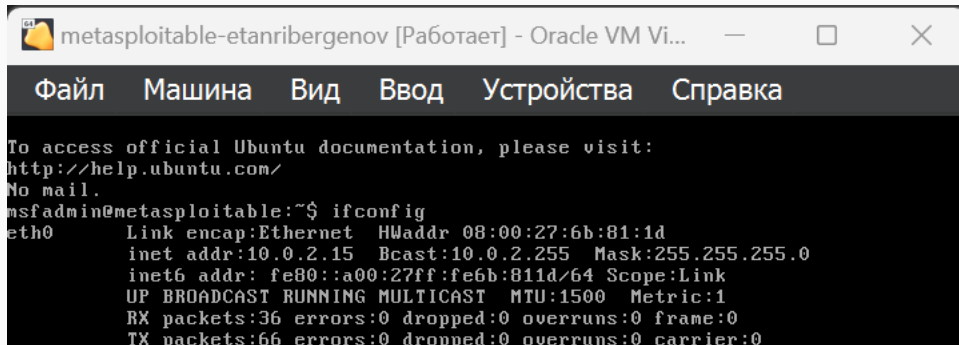
Ознакомиться с утилитой `nikto` в Kali Linux и испытать.

- Ознакомиться с утилитой `nikto` в Kali Linux и испытать.

Результаты

Включение испытательной VM

- *Metasploitable* - специальная нарочно очень уязвимая для всякого рода атак виртуальная машина



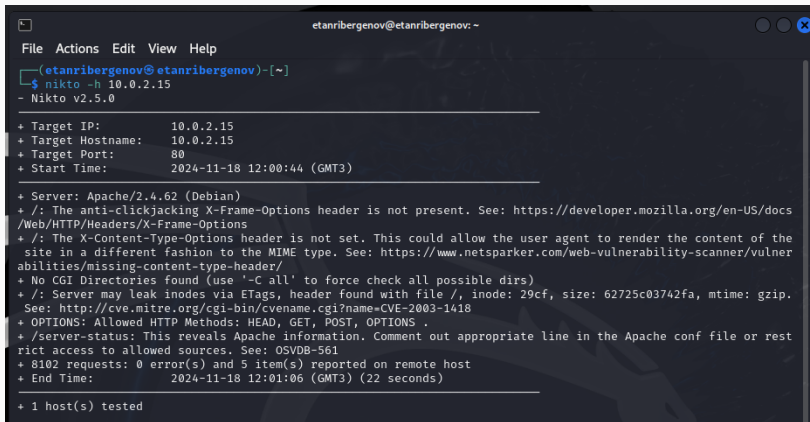
```
metasploitable-etanribergenov [Работает] - Oracle VM Vi...
Файл  Машина  Вид  Ввод  Устройства  Справка

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:6b:81:1d
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe6b:811d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:36 errors:0 dropped:0 overruns:0 frame:0
          TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
```

Рис. 1: Запуск VM и просмотр интерфейсов для получения ip-адреса

- ***nikto*** — базовый сканер безопасности веб-сервера. Он сканирует и обнаруживает уязвимости в веб-приложениях, обычно вызванные неправильной конфигурацией на самом сервере, файлами, установленными по умолчанию, и небезопасными файлами, а также устаревшими серверными приложениями.

Испытание nikto



```
etanribergenov@etanribergenov: ~  
File Actions Edit View Help  
(etanribergenov@etanribergenov)~  
$ nikto -h 10.0.2.15  
- Nikto v2.5.0  
  
+ Target IP: 10.0.2.15  
+ Target Hostname: 10.0.2.15  
+ Target Port: 80  
+ Start Time: 2024-11-18 12:00:44 (GMT3)  
  
+ Server: Apache/2.4.62 (Debian)  
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options  
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/  
+ No CGI Directories found (use '-C all' to force check all possible dirs)  
+ /: Server may leak inodes via ETags, header found with file /, inode: 29cf, size: 62725c03742fa, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418  
+ OPTIONS: Allowed HTTP Methods: HEAD, GET, POST, OPTIONS .  
+ /server-status: This reveals Apache information. Comment out appropriate line in the Apache conf file or restrict access to allowed sources. See: OSVDB-561  
+ 8102 requests: 0 error(s) and 5 item(s) reported on remote host  
+ End Time: 2024-11-18 12:01:06 (GMT3) (22 seconds)  
  
+ 1 host(s) tested
```

Рис. 2: Результат

Вывод

В результате выполнения работы я познакомился с инструментом поиска уязвимостей - nikto.