Выполнил Мешечкин Д. Инфобез-2837 (Ранее 2345)

Задание 1: Ознакомиться с темой Footprint. Изучить содержимое файла footprint.txt и попробовать запросы.

Footprint, дословный перевод с англ. языка - след. Является методом используемым для сбора как можно большего количества данных о конкретной целевой компьютерной системе, инфраструктуре и сетях для выявления возможностей проникновения в них. Это один из лучших методов поиска уязвимостей.

Процесс отслеживания кибербезопасности включает в себя профилирование организаций и сбор данных о сети, хосте, сотрудниках и сторонних партнерах. Эта информация включает в себя операционную систему , используемую организацией, брандмауэры , карты сети, IP-адреса , информацию о системе доменных имен , конфигурации безопасности целевой машины, URL-адреса , виртуальные частные сети , идентификаторы сотрудников, адреса электронной почты и номера телефонов.

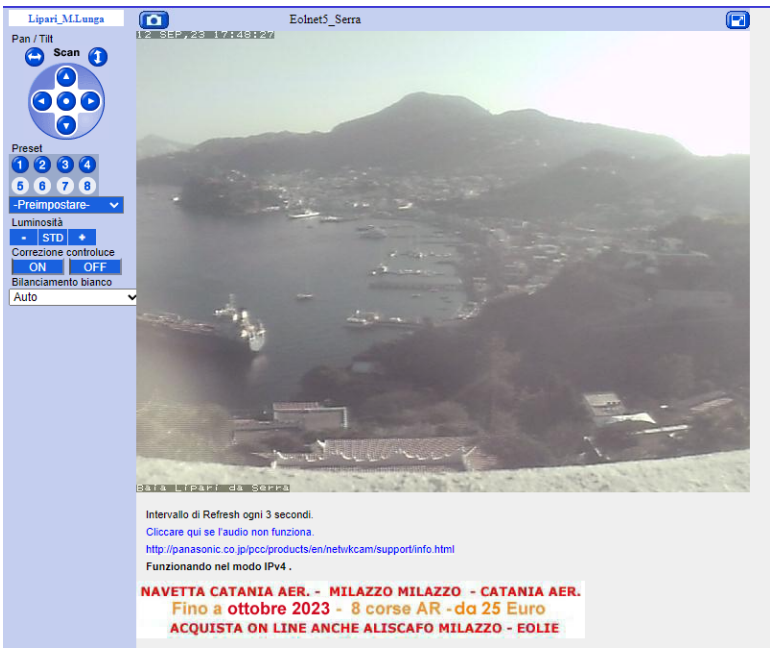
В этическом хакинге есть два типа слежения:

- активное
- пассивное

Активное отслеживание описывает процесс использования инструментов и методов, таких как использование команд трассировки или ping-сканирования (проверка протокола управляющих сообщений Интернета) для сбора данных о конкретной цели. Это часто приводит к срабатыванию системы обнаружения вторжений цели (IDS). Чтобы успешно избежать обнаружения, требуется определенный уровень скрытности и креативности.

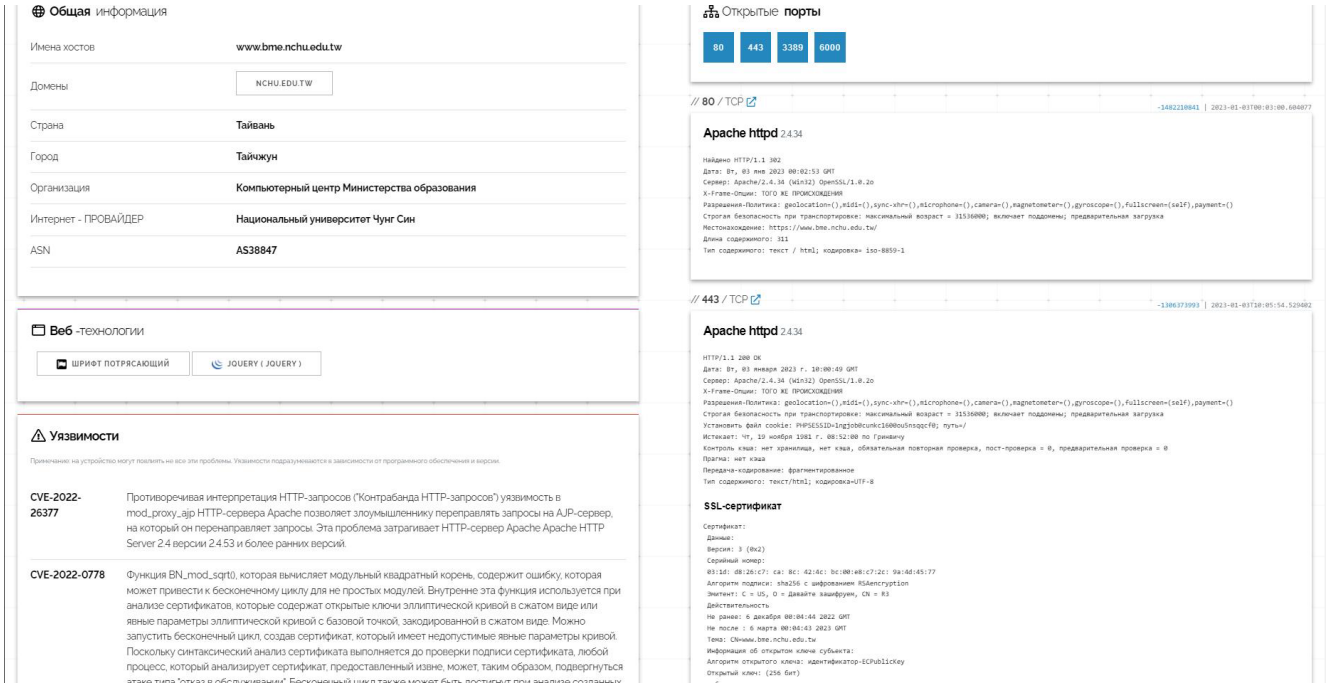
Пассивное отслеживание включает сбор данных о конкретной цели с использованием безобидных методов, таких как поиск в Google, просмотр Archive.org, использование NeoTrace, просмотр профилей сотрудников в социальных сетях, просмотр сайтов вакансий и использование Whois . Веб-сайт, предоставляющий доменные имена и связанные сети для конкретной организации. Это более скрытый подход к отслеживанию, поскольку он не активирует IDS цели.

При ознакомлении с содержимым файла footprint google.txt "ознакамливает" с некоторыми возможностями поиска различных ip-камер, смотрящих в глобальную сеть. В большинстве своём - это камеры офисов, уличного наблюдения, и большинство из этих камер находятся где-то в стране восходящего солнца. Во время выполнения домашнего задания - там около часа ночи, большинство камер имеет доступ с разрешением 480p. Смотреть не очень интересно. Где-то в глубине запроса можно было нарваться на камеры порта. Но впрочем снова ни чего "сверхестественного".



Задание 2: Изучить возможности Shodan, Censys. В отчете указать что для себя интересного выяснили о данных системах.

По большому счёту - Shodan и Censys являются альтернативными поисковыми системами, которые ищут информацию об устройствах, подключенных к глобальной сети. Весьма полезны при разведке и поиске уязвимостей на ресурсе. Шодан при удачно настроеных фильтрах может выдать очень много полезной, интересной информации, включая уже известные уязвимости на ресурсе с возможностью их эксплуатации.



Задание 3: Провести различные виды сканирования NMap на вашем собственном стенде или же ресурсах, которые разрешают себя сканировать (например, scanme.nmap.org). Сканировать в Глобальной сети Интернет не рекомендуется, особенно в адресном пространстве РФ.) Выбрать подсеть с маской 16 и просканировать ее по tcp по всем портам с детектированием версий сервисов и ОС. Желательно использовать скрипты NSE. Результаты могут быть и не впечатляющими. Не надо искать самую «интересную» сеть. Задача — попрактиковаться и сдать отчет.

Для первого "ознакомления" использую nmap на допустимом для этого ресурсе:

```
└─$ sudo nmap -A -Pn -sC -O -sV scanme.nmap.org --min-rate 1000 -p0-65535
[redacted]
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-12 19:26 MSK
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.22s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 65530 closed tcp ports (reset)
PORT      STATE    SERVICE       VERSION
0/tcp     filtered unknown
22/tcp    open     ssh           OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ac00a01a82ffcc5599dc672b34976b75 (DSA)
|   2048 203d2d44622ab05a9db5b30514c2a6b2 (RSA)
|   256 9602bb5e57541c4e452f564c4a24b257 (ECDSA)
|_  256 33fa910fe0e17b1f6d05a2b0f1544156 (ED25519)
80/tcp    open     http          Apache httpd 2.4.7 ((Ubuntu))
|_http-title: Go ahead and ScanMe!
|_http-favicon: Nmap Project
|_http-server-header: Apache/2.4.7 (Ubuntu)
4786/tcp  filtered smart-install
9929/tcp  open     nping-echo    Nping echo
31337/tcp open     tcpwrapped
Aggressive OS guesses: Linux 5.0 (91%), Linux 5.4 (91%), Linux 5.0 - 5.4 (91%), HP P2000 G3 NAS device (89%), Linux 4.15 - 5.6
x NanoStation WAP (Linux 2.6.32) (89%), Linux 3.7 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 23 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 993/tcp)
HOP RTT       ADDRESS
1   0.77 ms   RT-AC66U-C1B0 (192.168.1.1)
2   1.67 ms   asr7.kmv.ru (217.13.214.10)
3   1.48 ms   bdr68105-fgbe.kmv.ru (217.13.213.81)
4   5.90 ms   178.35.225.117
5   20.19 ms  188.128.126.238
6   67.19 ms  frkt-cr7.intl.ip.rostelecom.ru (188.128.104.173)
7   71.32 ms  217.161.68.33
8   70.21 ms  telia-gw.fnt.cw.net (195.2.22.238)
9   ...
10  79.38 ms  prs-bb1-link.ip.twelve99.net (62.115.123.13)
11  150.97 ms rest-bb1-link.ip.twelve99.net (62.115.122.159)
12  151.68 ms ash-b2-link.ip.twelve99.net (62.115.123.125)
13  146.42 ms akamai-ic-352275.ip.twelve99-cust.net (62.115.184.199)
14  ...
15  165.59 ms ae5.r01.ord01.icn.netarch.akamai.com (23.32.63.20)
16  165.55 ms ae0.r02.ord01.icn.netarch.akamai.com (23.32.63.81)
17  217.21 ms ae4.r02.sjc01.icn.netarch.akamai.com (23.32.63.27)
18  216.68 ms ae2.r12.sjc01.ien.netarch.akamai.com (23.207.232.41)
19  214.65 ms a23-203-158-53.deploy.static.akamaitechnologies.com (23.203.158.53)
20  ... 22
23  218.69 ms scanme.nmap.org (45.33.32.156)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 91.13 seconds
```

Сканирование scanme.nmap.org позволяет "посмотреть" доступность различных портов. За счёт дополнительных флагов соответственно открывается дополнительная информация, где:
-A - возможность определения ОС, версии ОС, сканирование скриптов и трасеровки
-Pn - обозначать все хосты как "онлайн"
-sC - сканирование скриптом --script=default
-O - включение возможности определения ОС
-sV - проверка открытых портов на определение сервиса/версии.

Ни чего сверхестественного в данном отчёте нет, обычный ресурс со своими сервисами.

Далее, чтобы не придумывать какие-то октеты адреса через шодан был выбран адрес из последних просканированных комьюнити и был запущен nmap на сканирование по маске /18 (была выбрана именно эта маска, во избежании излишне долгого сканирования, смысл не потерялся).

```
└─$ sudo nmap -A -Pn -sC -O -sV 142.132.139.0/18 --min-rate 5000
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-12 19:33 MSK
Nmap scan report for static.0.128.132.142.clients.your-server.de (142.132.128.0)
Host is up.
All 1000 scanned ports on static.0.128.132.142.clients.your-server.de (142.132.128.0) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Too many fingerprints match this host to give specific OS details

TRACEROUTE (using proto 1/icmp)
HOP RTT      ADDRESS
-   Hops 1-6 are the same as for 142.132.128.41
7   67.70 ms core23.fsn1.hetzner.com (213.239.224.65)
8   ... 30

Nmap scan report for static.1.128.132.142.clients.your-server.de (142.132.128.1)
Host is up.
All 1000 scanned ports on static.1.128.132.142.clients.your-server.de (142.132.128.1) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Too many fingerprints match this host to give specific OS details

TRACEROUTE (using proto 1/icmp)
HOP RTT    ADDRESS
-   Hops 1-8 are the same as for 142.132.128.12
9   ... 30

Nmap scan report for static.2.128.132.142.clients.your-server.de (142.132.128.2)
Host is up.
All 1000 scanned ports on static.2.128.132.142.clients.your-server.de (142.132.128.2) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Too many fingerprints match this host to give specific OS details

TRACEROUTE (using proto 1/icmp)
HOP RTT    ADDRESS
-   Hops 1-8 are the same as for 142.132.128.4
9   ... 30

Nmap scan report for static.3.128.132.142.clients.your-server.de (142.132.128.3)
Host is up.
All 1000 scanned ports on static.3.128.132.142.clients.your-server.de (142.132.128.3) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Too many fingerprints match this host to give specific OS details

TRACEROUTE (using proto 1/icmp)
HOP RTT    ADDRESS
-   Hops 1-8 are the same as for 142.132.128.29
9   ... 30
```

```
Nmap scan report for jasmin.rs (142.132.128.12)
Host is up (0.076s latency).
Not shown: 993 closed tcp ports (reset)
PORT     STATE    SERVICE         VERSION
21/tcp   open     ftp             Pure-FTPd
22/tcp   filtered ssh
80/tcp   open     http            nginx 1.20.1
|_http-server-header: nginx/1.20.1
|_http-title: Did not follow redirect to https://www.jasmin.rs/
443/tcp  open     ssl/http        nginx 1.20.1
|_ssl-date: TLS randomness does not represent time
|_http-title: Did not follow redirect to https://www.jasmin.rs/
|_http-server-header: nginx/1.20.1
| ssl-cert: Subject: commonName=jasmin.rs
| Subject Alternative Name: DNS:jasmin.rs, DNS:www.jasmin.rs
| Not valid before: 2023-08-26T00:06:14
|_Not valid after:  2023-11-24T00:06:13
3306/tcp open     mysql           MySQL (unauthorized)
8081/tcp filtered blackice-icecap
48080/tcp filtered unknown
Aggressive OS guesses: Linux 3.10 - 4.11 (95%), Linux 5.1 (94%), Linux 3.18 (93
P (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 9 hops
```

```
Nmap scan report for static.40.128.132.142.clients.your-server.de (142.132.128.40)
Host is up (0.074s latency).
Not shown: 986 closed tcp ports (reset)
PORT     STATE SERVICE  VERSION
21/tcp   open  ftp      Pure-FTPd
| ssl-cert: Subject: commonName=142-132-128-40.cprapid.com
| Subject Alternative Name: DNS:142-132-128-40.cprapid.com, DNS:mail.142-132-128-40.cprapid.com, DNS:www.142-132-128-40.cprapid.com
| Not valid before: 2023-08-10T00:00:00
|_Not valid after:  2023-11-08T23:59:59
|_ssl-date: TLS randomness does not represent time
22/tcp   open  ssh      OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 ea6c9ebb7c9ee04a07d6cb342326c28e (RSA)
|   256 054ffda92d22ddf9b1eb9292a8e769a0 (ECDSA)
|_  256 13775bbe39c9620960d7c7d215b4a38e (ED25519)
25/tcp   open  smtp?
|_smtp-commands: Couldn't establish connection on port 25
53/tcp   open  domain   PowerDNS Authoritative Server 4.7.3
| dns-nsid:
|   NSID: 142-132-128-40.cprapid.com (3134322d3133322d3132382d34302e637072617069642e636f6d)
|   id.server: 142-132-128-40.cprapid.com
|_  bind.version: PowerDNS Authoritative Server 4.7.3 (built Apr 25 2023 12:34:07 by root@bh-centos-7.dev.cpanel.net)
80/tcp   open  http     Apache httpd
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache
110/tcp  open  pop3     Dovecot pop3d
| ssl-cert: Subject: commonName=142-132-128-40.cprapid.com
| Subject Alternative Name: DNS:142-132-128-40.cprapid.com, DNS:mail.142-132-128-40.cprapid.com, DNS:www.142-132-128-40.cprapid.com
| Not valid before: 2023-08-10T00:00:00
|_Not valid after:  2023-11-08T23:59:59
|_pop3-capabilities: SASL(PLAIN LOGIN) RESP-CODES UIDL CAPA PIPELINING TOP STLS USER AUTH-RESP-CODE
111/tcp  open  rpcbind  2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|_  100000  3,4          111/udp6  rpcbind
```

```
143/tcp  open  imap     Dovecot imapd
| ssl-cert: Subject: commonName=142-132-128-40.cprapid.com
| Subject Alternative Name: DNS:142-132-128-40.cprapid.com, DNS:mail.142-132-128-40.cprapid.com, DNS:www.142-132-128-40.cprapid.com
| Not valid before: 2023-08-10T00:00:00
|_Not valid after:  2023-11-08T23:59:59
|_imap-capabilities: STARTTLS listed Pre-login AUTH=LOGINA0001 LITERAL+ IMAP4rev1 ID ENABLE LOGIN-REFERRALS have NAMESPACE more OK IDLE capabilities post-login SASL-IR AUTH=PLAIN
443/tcp  open  ssl/http Apache httpd
|_http-generator: WPML ver:2.9.2 stt:1,4,2,44;0
|_http-title: \xD8\xAC\xD8\xB1\xD8\xA7\xD9\x86\xD8\xAF \xD8\xA3\xD9\x81\xD8\xB6\xD9\x84 \xD8\xB4\xD8\xB1\xD9\x83\xD8\xA9 \xD8\xA8\xD8\xB1\xD9\x85\xD8\xAC\xD8\xA9 \xD9\x88\xD8\xAA\xD8\xB5\xD
AA\xD8\xB7\xD8\xA8\xD9\x8A\xD9 ...
| ssl-cert: Subject: commonName=2grand.net
| Subject Alternative Name: DNS:2grand.net
| Not valid before: 2023-03-05T17:37:21
|_Not valid after:  2024-04-05T17:37:20
|_http-favicon: CakePHP 1.2.x-1.3.x Application
|_http-server-header: Apache
|_ssl-date: TLS randomness does not represent time
465/tcp  open  ssl/smtp Exim smtpd 4.96
| smtp-commands: 142-132-128-40.cprapid.com Hello static.40.128.132.142.clients.your-server.de [178.159.89.141], SIZE 52428800, 8BITMIME, PIPELINING, PIPECONNECT, AUTH PLAIN LOGIN, HELP
|_ Commands supported: AUTH HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
| ssl-cert: Subject: commonName=142-132-128-40.cprapid.com
| Subject Alternative Name: DNS:142-132-128-40.cprapid.com, DNS:mail.142-132-128-40.cprapid.com, DNS:www.142-132-128-40.cprapid.com
| Not valid before: 2023-08-10T00:00:00
|_Not valid after:  2023-11-08T23:59:59
587/tcp  open  smtp     Exim smtpd 4.96
|_smtp-ntlm-info: ERROR: Script execution failed (use -d to debug)
| smtp-commands: 142-132-128-40.cprapid.com Hello static.40.128.132.142.clients.your-server.de [178.159.89.141], SIZE 52428800, 8BITMIME, PIPELINING, PIPECONNECT, STARTTLS, HELP
|_ Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
| ssl-cert: Subject: commonName=142-132-128-40.cprapid.com
| Subject Alternative Name: DNS:142-132-128-40.cprapid.com, DNS:mail.142-132-128-40.cprapid.com, DNS:www.142-132-128-40.cprapid.com
| Not valid before: 2023-08-10T00:00:00
|_Not valid after:  2023-11-08T23:59:59
993/tcp  open  imaps?
| ssl-cert: Subject: commonName=142-132-128-40.cprapid.com
| Subject Alternative Name: DNS:142-132-128-40.cprapid.com, DNS:mail.142-132-128-40.cprapid.com, DNS:www.142-132-128-40.cprapid.com
| Not valid before: 2023-08-10T00:00:00
|_Not valid after:  2023-11-08T23:59:59
995/tcp  open  pop3s?
| ssl-cert: Subject: commonName=142-132-128-40.cprapid.com
| Subject Alternative Name: DNS:142-132-128-40.cprapid.com, DNS:mail.142-132-128-40.cprapid.com, DNS:www.142-132-128-40.cprapid.com
| Not valid before: 2023-08-10T00:00:00
|_Not valid after:  2023-11-08T23:59:59
3306/tcp open  mysql    MySQL (unauthorized)
```

При сканировании данного массива адресов было множество "пустых" ответов, ответов которые "ограничивались" 2-3 или же "стандартным" набором открытых портов (21,22,80,443, иногда 3306). Но были и индивидуумы, которые торчали в сеть всем чем только можно, включая и древнии версии томкэта, различные шары дисков и много другое.

Для "проверки" возможностей nmap со скриптами был выбран один ресурс.

```
└─$ sudo nmap -sV --script vuln 142.132.128.57 -p T:22,80,443,902,5988,5989,8000,8300,9080
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-12 20:10 MSK
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for static.57.128.132.142.clients.your-server.de (142.132.128.57)
Host is up (0.083s latency).

PORT     STATE  SERVICE         VERSION
22/tcp   closed ssh
80/tcp   open   http            VMware ESXi Server httpd
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_http-litespeed-sourcecode-download: ERROR: Script execution failed (use -d to debug)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-vuln-cve2013-7091: ERROR: Script execution failed (use -d to debug)
|_http-passwd: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
443/tcp  open   ssl/https       VMware ESXi SOAP API 7.0.3
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200 OK
|     Date: Tue, 12 Sep 2023 15:09:21 GMT
|     Connection: close
|     Content-Security-Policy: upgrade-insecure-requests
|     Content-Type: text/html
|     Strict-Transport-Security: max-age=31536000
|     X-Content-Type-Options: nosniff
|     X-Frame-Options: DENY
|     X-XSS-Protection: 1
|     Content-Length: 258
|     <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
|     <html lang="en">
|     <head>
|     <meta http-equiv="content-type" content="text/html; charset=utf8">
|     <meta http-equiv="refresh" content="0;URL='/ui'"/>
|     </head>
|     </html>
|   HTTPOptions:
|     HTTP/1.1 501 Not Implemented
|     Date: Tue, 12 Sep 2023 15:09:21 GMT
|     Connection: close
|     Content-Security-Policy: upgrade-insecure-requests
|     Content-Type: text/plain; charset=utf-8
|     Strict-Transport-Security: max-age=31536000
|     X-Content-Type-Options: nosniff
|     X-Frame-Options: DENY
|     X-XSS-Protection: 1
|     Content-Length: 0
|   RTSPRequest:
|     HTTP/1.1 400 Bad Request
|     Date: Tue, 12 Sep 2023 15:09:32 GMT
|     Connection: close
|     Content-Type: text/html
|     Content-Length: 50
|_    <HTML><BODY><H1>400 Bad Request</H1></BODY></HTML>
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| http-enum:
|_  /cgi-bin/mj_wwwusr: Majordomo2 Mailing List (401 Unauthorized)
| vmware-version:
|   Server version: VMware ESXi 7.0.3
|   Build: 18905247
|   Locale version: INTL 000
|   OS type: vmnix-x86
|_  Product Line ID: embeddedEsx
902/tcp  open   ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
|_ssl-ccs-injection: No reply from server (TIMEOUT)
5988/tcp closed wbem-http
5989/tcp closed wbem-https
8000/tcp open   http-alt?
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
8300/tcp open   tmi?
9080/tcp closed glrpc
```

Использование --script vuln "выдало" несколько уязвимых мест на данном ресурсе. Не зависимо от "расположения" ресурса, а так же от геополитического состояния страны размещения ресурса - пусть развлекаются сами с исправлениями и ограничениями.