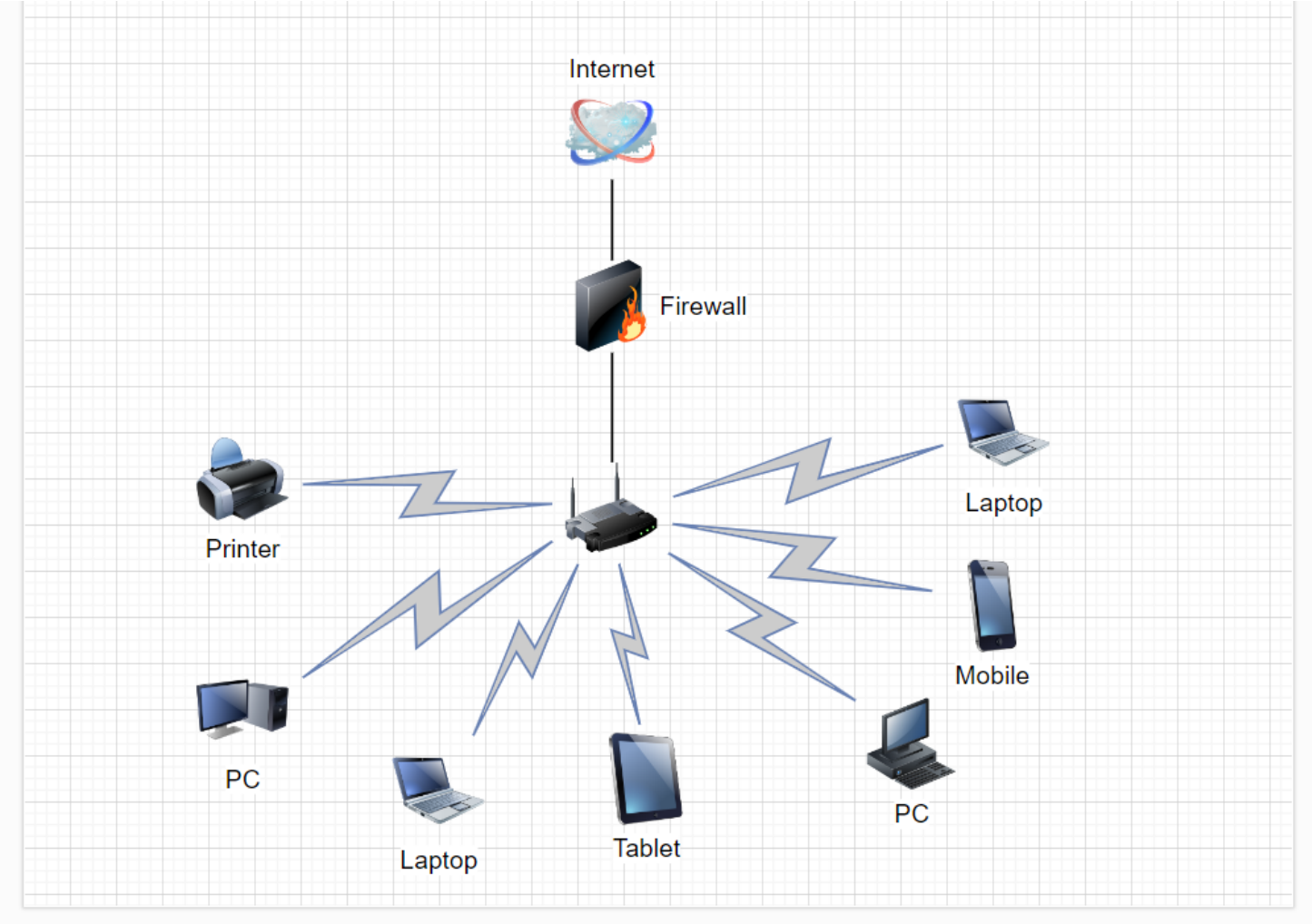
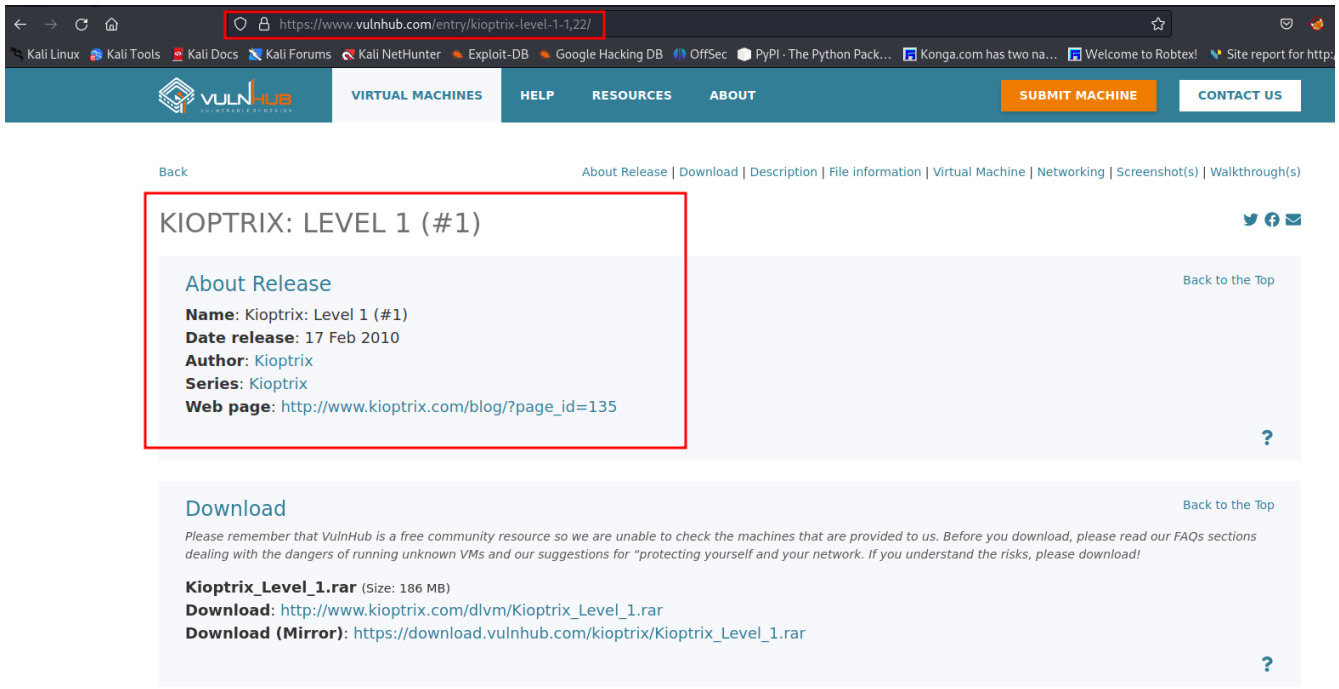
SAMPLE NETWORK INFRASTRUCTURE



Machine to scan against



SCANNING NETWORK WITH NMAP

```
┌──(venuskali㉿kali)-[~]
└─$ nmap -T4 -p- -A 192.168.220.133
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-06 03:22 EDT
Nmap scan report for 192.168.220.133
Host is up (0.0025s latency).
Not shown: 65529 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 2.9p2 (protocol 1.99)
|_sshv1: Server supports SSHv1
| ssh-hostkey:
|   1024 b8746cdbfd8be666e92a2bdf5e6f6486 (RSA1)
|   1024 8f8e5b81ed21abc180e157a33c85c471 (DSA)
|_  1024 ed4ea94a0614ff1514ceda3a80dbe281 (RSA)
80/tcp   open  http        Apache httpd 1.3.20 ((Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
|_http-server-header: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_http-title: Test Page for the Apache Web Server on Red Hat Linux
| http-methods:
|_  Potentially risky methods: TRACE
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100024  1          32768/tcp   status
|_  100024  1          32770/udp   status
139/tcp  open  netbios-ssn Samba smbd (workgroup: MYGROUP)
443/tcp  open  ssl/https   Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_http-server-header: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_ssl-date: 2023-08-06T12:23:31+00:00; +5h00m05s from scanner time.
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvince
Name=SomeState/countryName=--
| Not valid before: 2009-09-26T09:32:06
|_Not valid after:  2010-09-26T09:32:06
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_64_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|_    SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_http-title: 400 Bad Request
32768/tcp open  status      1 (RPC #100024)

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: 5h00m04s
```

Enumerating http and https

80/tcp open http Apache httpd 1.3.20 ((Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)

|_http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b

scanning with nikto vulnerabilities scanner

```
venuskali@kali: ~ ×   venuskali@kali: ~ ×   venuskali@kali: ~ ×
┌──(venuskali㉿kali)-[~]
└─$ nikto -h http://192.168.220.133
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.220.133
+ Target Hostname:    192.168.220.133
+ Target Port:        80
+ Start Time:         2023-08-06 03:50:39 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
+ /: Server may leak inodes via ETags, header found with file /, inode: 34821, size: 28
p  5 23:12:46 2001. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://develope
US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to r
+ of the site in a different fashion to the MIME type. See: https://www.netsparker.com/
-scanner/vulnerabilities/missing-content-type-header/
+ Apache/1.3.20 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2
+ the 2.x branch.
+ OpenSSL/0.9.6b appears to be outdated (current is at least 3.0.7). OpenSSL 1.1.1s is
.x branch and will be supported until Nov 11 2023.
+ mod_ssl/2.8.4 appears to be outdated (current is at least 2.9.6) (may depend on serve
+ /: Apache is vulnerable to XSS via the Expect header. See: http://cve.mitre.org/cgi-b
me=CVE-2006-3918
+ Apache/1.3.20 - Apache 1.x up 1.2.34 are vulnerable to a remote DoS and possible code
+ Apache/1.3.20 - Apache 1.3 below 1.3.27 are vulnerable to a local buffer overflow whi
rs to kill any process on the system.
+ Apache/1.3.20 - Apache 1.3 below 1.3.29 are vulnerable to overflows in mod_rewrite an
+ mod_ssl/2.8.4 - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow wh
emote shell.
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, OPTIONS, TRACE .
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: htt
w-community/attacks/Cross_Site_Tracing
+ ///etc/hosts: The server install allows reading of any system file by adding an extra
+ /usage/: Webalizer may be installed. Versions lower than 2.01-09 vulnerable to Cross
SS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0835
+ /manual/: Directory indexing found.
+ /manual/: Web server manual found.
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restri
consreadme/
```

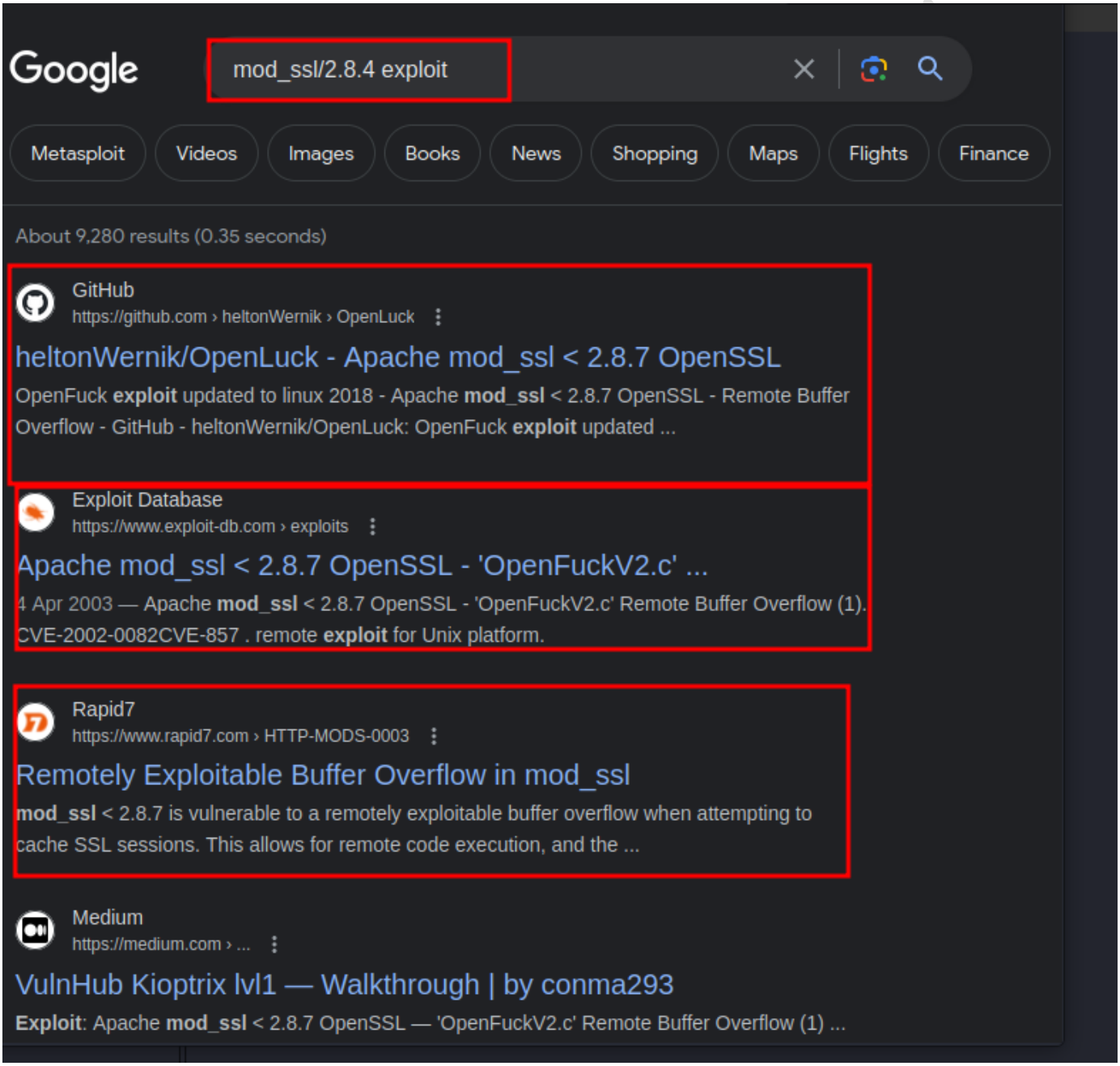
-h for your host, either an ip or url

Researching potential vulnerabilities

use google to search for the exploit of any analysis you saw in your enumeration

Example:

vulnerability for mod_ssl



EXPLOIT DATABASE

Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1)

EDB-ID:	CVE:	Author:	Type:
764	2002-0082	SPABAM	REMOTE

EDB Verified: ✓

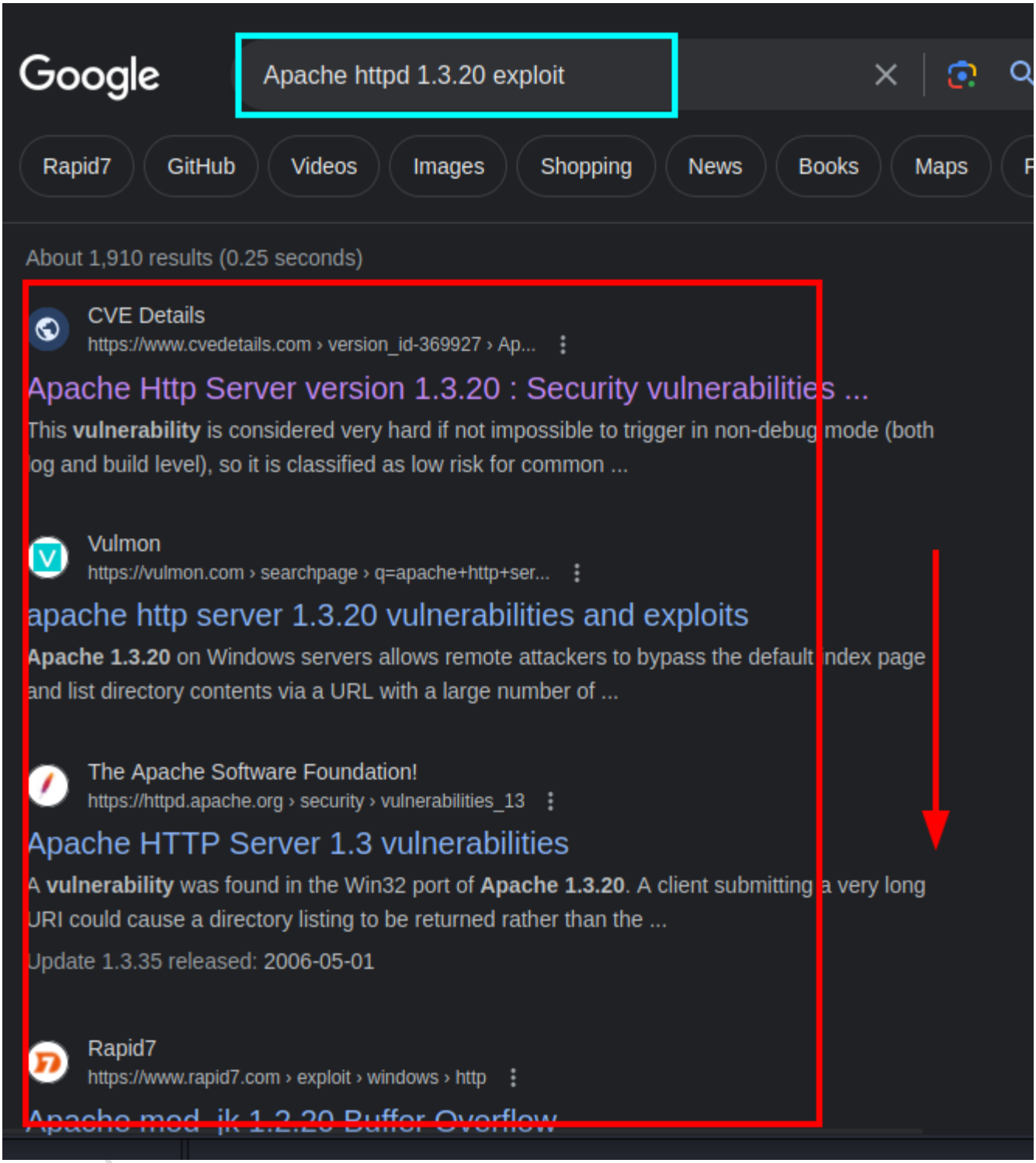
Exploit: / {}

Platform:	Date:
UNIX	2003-04-04

Vulnerable App:

80 / 443 - pontentially vulnerable to OPENLOCK (https://www.exploit-db.com/exploits/764), https://github.com/heltonWernik/OpenLuck

80/ 443 pontentially vulnerabiltiy to openlock (https://www.rapid7.com/db/modules/exploit/windows/http/apache_modjk_overflow/)



139 - pontentially vulnerabilty to
https://www.rapid7.com/db/modules/exploit/linux/samba/trans2open/()

Google

Samba 2.2.1a exploit

Github | Videos | Shopping | Images | News | Books | Maps | Flights | Finan

About 79,600 results (0.27 seconds)

Rapid7
https://www.rapid7.com › modules › exploit › samba

Samba trans2open Overflow (Linux x86)

30 May 2018 — This **exploits** the buffer overflow found in **Samba** versions **2.2**.0 to **2.2**.8. This particular module is capable of **exploiting** the flaw on x86 ...

CVE Details
https://www.cvedetails.com › version_id-373318 › Sa...

Samba Samba version 2.2.1a : Security vulnerabilities, CVEs

A flaw was found in **Samba**. The security **vulnerability** occurs when KDC and the kpasswd service share a single account and set of keys, allowing them to ...

Exploit Database
https://www.exploit-db.com › exploits

Samba < 2.2.8 (Linux/BSD) - Remote Code Execution

10 Apr 2003 — Remote root **exploit** for **Samba 2.2**.x and prior that works against Linux (all distributions), FreeBSD (4.x, 5.x), NetBSD (1.x) and OpenBSD ...

https://www.exploit-db.com › exploits

Samba 2.2.x - Remote Buffer Overflow

7 Apr 2003 — **Samba 2.2**.x - Remote Buffer Overflow. CVE-4469CVE-2003-0201 . remote **exploit** for Linux platform

https://www.rapid7.com/db/modules/exploit/li

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

RAPID7

TRY NOW

Rapid7 Vulnerability & Exploit Database

Samba trans2open Overflow (Linux x86)

Back to Search

Samba trans2open Overflow (Linux x86)

Disclosed: 04/07/2003

Created: 05/30/2018

Description

Using searchsploit to search for vulnerabilities

use - searchspolit

```
┌──(venuskali㉿kali)-[~]
└─$ searchsploit samba 2.2.1a
---------------------------------------------------------------------------
 Exploit Title                                           |  Path
---------------------------------------------------------------------------
Samba 2.2.0 < 2.2.8 (OSX) - tr                           | osx/remote/9924.rb
Samba < 2.2.8 (Linux/BSD) - Re                           | multiple/remote/10.c
Samba < 3.0.20 - Remote Heap O                           | linux/remote/7701.txt
Samba < 3.6.2 (x86) - Denial o                           | linux_x86/dos/36741.py
---------------------------------------------------------------------------
Shellcodes: No Results

┌──(venuskali㉿kali)-[~]
└─$
```

```
┌──(venuskali㉿kali)-[~]
└─$ searchsploit mod ssl 2
---------------------------------------------------------------------------
 Exploit Title                                           |  Path
---------------------------------------------------------------------------
Apache 2.0.58 mod_rewrite (Win                           | windows/remote/3996.c
Apache < 1.3.37/2.0.59/2.2.3 m                           | multiple/remote/2237.sh
Apache mod_rewrite (Windows x8                           | windows_x86/remote/3680.sh
Apache mod_rewrite - LDAP prot                           | windows/remote/16752.rb
Apache mod_ssl 2.0.x - Remote                            | linux/dos/24590.txt
Apache mod_ssl 2.8.x - Off-by-                           | multiple/dos/21575.txt
Apache mod_ssl < 2.8.7 OpenSSL                           | unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL                           | unix/remote/47080.c
Apache mod_ssl < 2.8.7 OpenSSL                           | unix/remote/764.c
Apache mod_ssl OpenSSL < 0.9.6                           | unix/remote/40347.txt
Apache Struts < 1.3.10 / < 2.3                           | multiple/remote/41690.rb
Cisco ASA 8.x - VPN SSL Module                           | hardware/remote/10510.txt
DomainMod 4.09.03 - 'sslpaid'                            | php/webapps/44783.txt
DomainMOD 4.11.01 - 'ssl-accou                           | php/webapps/46373.txt
DomainMOD 4.11.01 - 'ssl-provi                           | php/webapps/46372.txt
DomainMOD 4.11.01 - Custom SSL                           | php/webapps/45947.txt
Flash - Issues in DefineBitsLo                           | windows/dos/37846.txt
Fortinet FortiOS 6.0.4 - Unaut                           | hardware/webapps/49074.py
Microsoft Edge Chakra - 'Inter                           | windows/dos/42469.html
Microsoft Edge Chakra - 'Inter                           | windows/dos/42470.html
Modbus Slave 7.0.0 - Denial of                           | windows/dos/45732.txt
Modbus Slave 7.3.1 - Buffer Ov                           | windows/dos/50536.py
Modbus Slave PLC 7 - '.msw' Bu                           | windows_x86/local/45710.pl
Veritas/Symantec Backup Exec -                           | windows/remote/42282.rb
---------------------------------------------------------------------------
Shellcodes: No Results

┌──(venuskali㉿kali)-[~]
└─$
```

Vulnerability Rating Based On Severity, Mitigation and Recommendation

Vulnerability Description: **Samba 2.2.1a**
Outdated Software (High Severity):

1. **Outdated Software (High Severity):**

   - **Vulnerability:** Samba 2.2.1a is an outdated version likely to have multiple known vulnerabilities.
   - **Mitigation:** Upgrade to a supported version of Samba to receive security patches and fixes.
   - **Recommendation:** Upgrade to the latest stable version of Samba to ensure protection against known vulnerabilities.

2. **Weak Authentication (High Severity):**
   - **Vulnerability:** Samba 2.2.1a may use weak authentication methods, such as plaintext passwords.
   - **Mitigation:** Implement strong authentication mechanisms like Kerberos or LDAP.
   - **Recommendation:** Configure Samba to use strong authentication methods to prevent unauthorized access.

3. **Remote Code Execution (High Severity):**
   - **Vulnerability:** Vulnerabilities in Samba 2.2.1a may allow remote attackers to execute arbitrary code.
   - **Mitigation:** Apply security patches provided by the Samba project.
   - **Recommendation:** Regularly update Samba to the latest version and apply security patches promptly to prevent remote code execution vulnerabilities.

Vulnerability Description: **mod_ssl < 2.8.7**
Severity Rating: High severity

1. Outdated Software (High Severity):

- **Vulnerability:** Apache mod_ssl versions prior to 2.8.7 may contain multiple known vulnerabilities.
- **Mitigation:** Upgrade to a newer version of Apache mod_ssl that includes security patches and fixes.
- **Recommendation:** Upgrade to the latest version of Apache mod_ssl to address known vulnerabilities and improve security.

2. SSL/TLS Vulnerabilities (High Severity):

- **Vulnerability:** Older versions of mod_ssl may be susceptible to SSL/TLS vulnerabilities, such as protocol downgrade attacks or cipher suite vulnerabilities.
- **Mitigation:** Configure SSL/TLS settings securely, including using strong cipher suites and disabling deprecated protocols.
- **Recommendation:** Regularly update SSL/TLS configurations to adhere to best practices and industry standards. Monitor security advisories for any new SSL/TLS vulnerabilities and apply patches promptly.

3. Denial of Service (DoS) (Medium Severity):

- **Vulnerability:** Apache mod_ssl < 2.8.7 may be vulnerable to denial of service attacks.
- **Mitigation:** Implement rate limiting, request throttling, or IP blocking to mitigate DoS attacks.
- **Recommendation:** Configure web server settings to handle DoS attacks gracefully and deploy intrusion detection/prevention systems to detect and block malicious traffic.

4. Certificate Handling Vulnerabilities (Medium Severity):

- **Vulnerability:** Older versions of mod_ssl may have vulnerabilities related to certificate handling, such as improper validation or insecure storage.
- **Mitigation:** Ensure proper configuration of certificate authorities and certificate chains. Use secure storage mechanisms for private keys and certificates.
- **Recommendation:** Regularly review and update certificate configurations. Implement secure key management practices to protect private keys from unauthorized access.

Vulnerability Description: **Apache HTTP Server 1.3.20**
Severity Rating: High severity

1. **Outdated Software (High Severity):**
   - **Vulnerability:** Apache HTTP Server 1.3.20 is an outdated version likely to have multiple known vulnerabilities.
   - **Mitigation:** Upgrade to a supported version of Apache HTTP Server to receive security patches and fixes.
   - **Recommendation:** Upgrade to the latest stable version of Apache HTTP Server (2.4.x or later) to ensure protection against known vulnerabilities.

2. **Remote Code Execution (High Severity):**
   - **Vulnerability:** Vulnerabilities in Apache HTTP Server 1.3.20 may allow remote attackers to execute arbitrary code.
   - **Mitigation:** Apply security patches provided by the Apache Software Foundation.
   - **Recommendation:** Regularly update Apache HTTP Server to the latest version and apply security patches promptly to prevent remote code execution vulnerabilities.

3. **Denial of Service (DoS) (Medium Severity):**
   - **Vulnerability:** Apache HTTP Server 1.3.20 may be susceptible to denial of service attacks.
   - **Mitigation:** Implement network-level protections to mitigate DoS attacks.
   - **Recommendation:** Configure firewalls or intrusion prevention systems to detect and block DoS attacks targeting Apache HTTP Server.

4. **Information Disclosure (Medium Severity):**
   - **Vulnerability:** Apache HTTP Server 1.3.20 may leak sensitive information due to misconfigurations or vulnerabilities.
   - **Mitigation:** Review and adjust Apache HTTP Server configurations to restrict access to sensitive data.
   - **Recommendation:** Regularly audit Apache HTTP Server configurations and apply access controls to prevent unauthorized information disclosure.