CFCS2R

Basic Network Analysis

CENTER FOR CYBER SECURITY STUDIES & RESEARCH

Introduction

This report covers a network security assessment performed on a local network to identify potential vulnerabilities and improve its security. The assessment involved scanning the network to find active devices, checking open ports and running services, and identifying any weaknesses that could be exploited. Tools like Nmap, Nikto, Zenmap, Wireshark, Netcat and OpenVAS were used to carry out these tasks. The report also includes a visual map of the network's layout and provides recommendations to improve the network's security.

Abstract

This report contains the findings of a structured network security assessment performed on a local network environment. The assignment associated with a multiple of tasks designed to identify active devices, detect open ports and running services, perform OS detection, and conduct vulnerability assessments involving manual testing and Automated scanning using various cybersecurity tools. The analysis also includes banner grabbing and service version detection, a vulnerability scan using Nikto, and a comprehensive vulnerability assessment with OpenVAS. The results are integrated into a detailed network topology map, providing a visual representation of the network's structure. Key vulnerabilities identified are documented along with their possible impacts, and preferable recommendations are provided to mitigate the risks identified during the assignment.

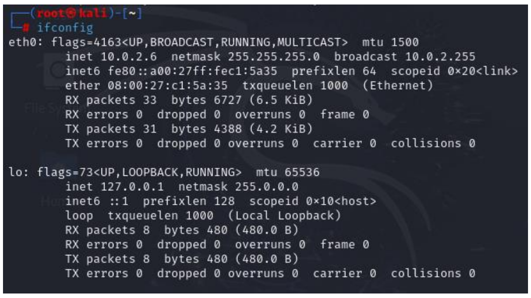
Basic Network Scanning with Nmap

Nmap: Nmap, also known as the "network mapper," is a popular and useful security tool with a long history and plenty of helpful guides. It's an open-source tool that helps users quickly explore and scan networks, making it easier to understand what's happening on their network.

Requirements:

Virtual box, Kalilinux, Nmap, Nikto, Open VAS, Netcat, Wireshark, Zenmap

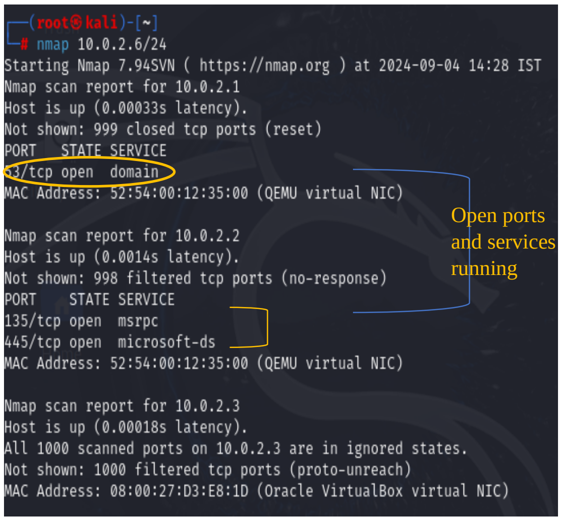
Get IP of network using command >ifconfig



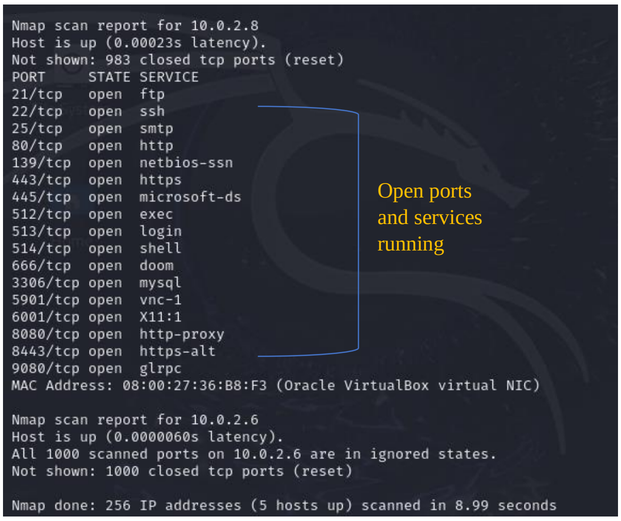
```
┌──(root㉿kali)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.6  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fec1:5a35  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:c1:5a:35  txqueuelen 1000  (Ethernet)
        RX packets 33  bytes 6727 (6.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 31  bytes 4388 (4.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

✸ Finding all hosts in Network and list the open ports and running services for each host

Command- >nmap 10.0.2.6/24



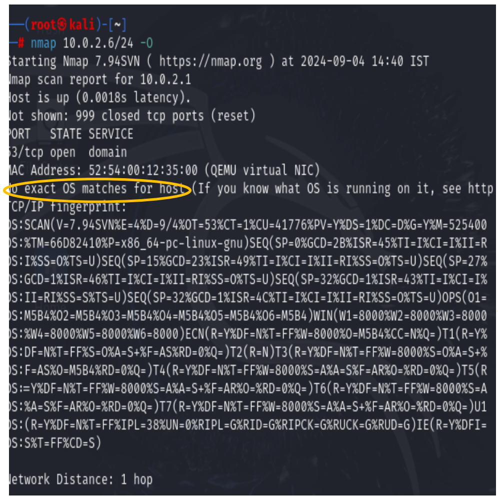
```
┌──(root㉿kali)-[~]
└─# nmap 10.0.2.6/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-04 14:28 IST
Nmap scan report for 10.0.2.1
Host is up (0.00033s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 10.0.2.2
Host is up (0.0014s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
445/tcp open  microsoft-ds
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 10.0.2.3
Host is up (0.00018s latency).
All 1000 scanned ports on 10.0.2.3 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:D3:E8:1D (Oracle VirtualBox virtual NIC)
```



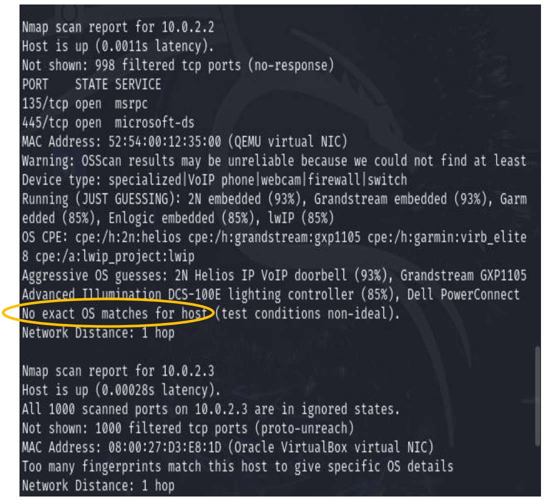
```
Nmap scan report for 10.0.2.8
Host is up (0.00023s latency).
Not shown: 983 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
25/tcp   open  smtp
80/tcp   open  http
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
666/tcp  open  doom
3306/tcp open  mysql
5901/tcp open  vnc-1
6001/tcp open  X11:1
8080/tcp open  http-proxy
8443/tcp open  https-alt
9080/tcp open  glrpc
MAC Address: 08:00:27:36:B8:F3 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.6
Host is up (0.0000060s latency).
All 1000 scanned ports on 10.0.2.6 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (5 hosts up) scanned in 8.99 seconds
```

✸ Find OS of hosts

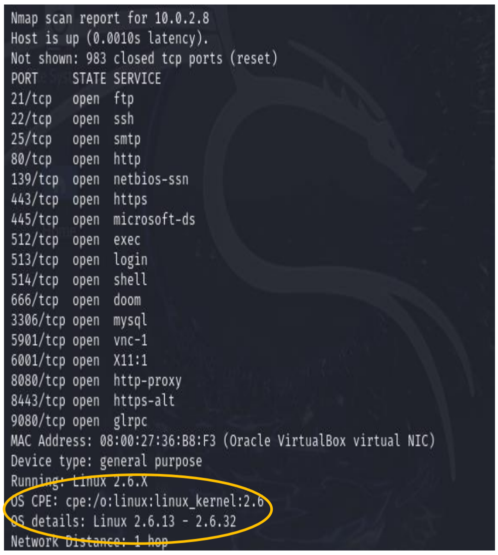
Command - >nmap 10.0.2.6/24 –O



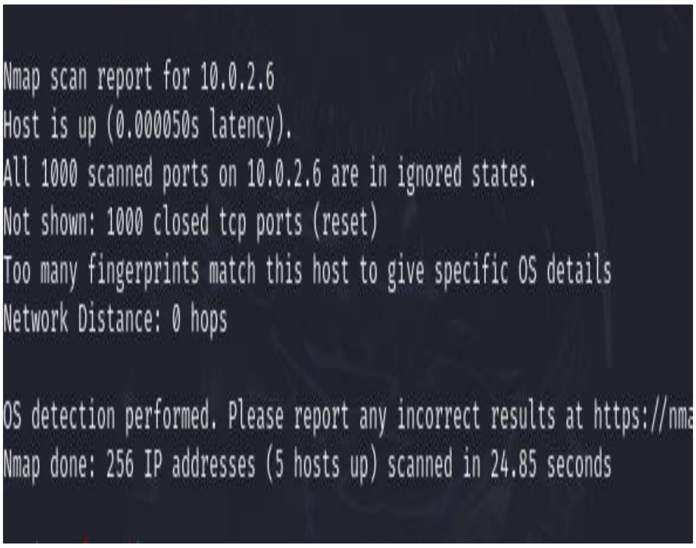
```
──(root㉿kali)-[~]
─# nmap 10.0.2.6/24 -O
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-04 14:40 IST
Nmap scan report for 10.0.2.1
Host is up (0.0018s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
No exact OS matches for host (If you know what OS is running on it, see http
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=9/4%OT=53%CT=1%CU=41776%PV=Y%DS=1%DC=D%G=Y%M=525400
OS:%TM=66D82410%P=x86_64-pc-linux-gnu)SEQ(SP=0%GCD=2B%ISR=45%TI=I%CI=I%II=R
OS:I%SS=O%TS=U)SEQ(SP=15%GCD=23%ISR=49%TI=I%CI=I%II=RI%SS=O%TS=U)SEQ(SP=27%
OS:GCD=1%ISR=46%TI=I%CI=I%II=RI%SS=O%TS=U)SEQ(SP=32%GCD=1%ISR=43%TI=I%CI=I%
OS:II=RI%SS=S%TS=U)SEQ(SP=32%GCD=1%ISR=4C%TI=I%CI=I%II=RI%SS=O%TS=U)OPS(O1=
OS:M5B4%O2=M5B4%O3=M5B4%O4=M5B4%O5=M5B4%O6=M5B4)WIN(W1=8000%W2=8000%W3=8000
OS:%W4=8000%W5=8000%W6=8000)ECN(R=Y%DF=N%T=FF%W=8000%O=M5B4%CC=N%Q=)T1(R=Y%
OS:DF=N%T=FF%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=Y%DF=N%T=FF%W=8000%S=O%A=S+%
OS:F=AS%O=M5B4%RD=0%Q=)T4(R=Y%DF=N%T=FF%W=8000%S=A%A=S%F=AR%O=%RD=0%Q=)T5(R
OS:=Y%DF=N%T=FF%W=8000%S=A%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=N%T=FF%W=8000%S=A
OS:%A=S%F=AR%O=%RD=0%Q=)T7(R=Y%DF=N%T=FF%W=8000%S=A%A=S+%F=AR%O=%RD=0%Q=)U1
OS:(R=Y%DF=N%T=FF%IPL=38%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=
OS:S%T=FF%CD=S)

Network Distance: 1 hop
```



```
Nmap scan report for 10.0.2.2
Host is up (0.0011s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
445/tcp open  microsoft-ds
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least
Device type: specialized|VoIP phone|webcam|firewall|switch
Running (JUST GUESSING): 2N embedded (93%), Grandstream embedded (93%), Garm
edded (85%), Enlogic embedded (85%), lwIP (85%)
OS CPE: cpe:/h:2n:helios cpe:/h:grandstream:gxp1105 cpe:/h:garmin:virb_elite
8 cpe:/a:lwip_project:lwip
Aggressive OS guesses: 2N Helios IP VoIP doorbell (93%), Grandstream GXP1105
Advanced Illumination DCS-100E lighting controller (85%), Dell PowerConnect
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Nmap scan report for 10.0.2.3
Host is up (0.00028s latency).
All 1000 scanned ports on 10.0.2.3 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:D3:E8:1D (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```



```
Nmap scan report for 10.0.2.8
Host is up (0.0010s latency).
Not shown: 983 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
25/tcp   open  smtp
80/tcp   open  http
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
666/tcp  open  doom
3306/tcp open  mysql
5901/tcp open  vnc-1
6001/tcp open  X11:1
8080/tcp open  http-proxy
8443/tcp open  https-alt
9080/tcp open  glrpc
MAC Address: 08:00:27:36:B8:F3 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.13 - 2.6.32
Network Distance: 1 hop
```



```
Nmap scan report for 10.0.2.6
Host is up (0.000050s latency).
All 1000 scanned ports on 10.0.2.6 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nma
Nmap done: 256 IP addresses (5 hosts up) scanned in 24.85 seconds
```

Finding: OS of 10.0.2.8 was linux 2.6.13 – 2.6.32

Vulnerable Services Using Nmap

Vulnerability: Vulnerabilities are weaknesses in a system that can let threats access and damage valuable assets.

Types of vulnerability scan:

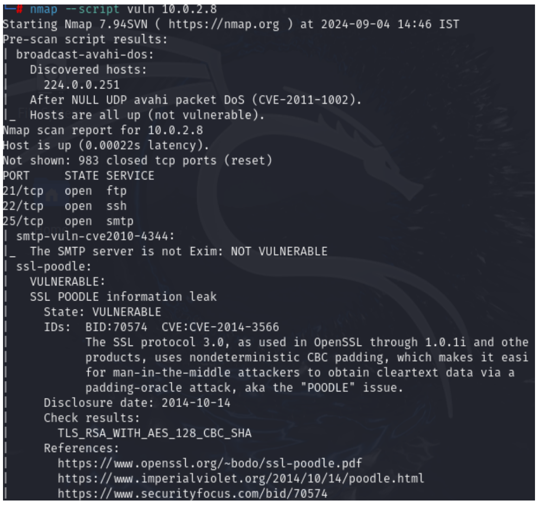
- **Network-based scan:** Looks for weak spots in an organization’s wired and wireless networks that could be targeted for attacks.
- **Host-based scan:** Checks individual computers and servers connected to the network for vulnerabilities and reviews their configuration and update history.
- **Wireless scan:** Examines Wi-Fi connections to find unauthorized access points and ensure the network is set up securely.
- **Application scan:** Tests websites to find known software issues and weaknesses in web applications.
- **Database scan:** Looks for problems in databases and data systems, like incorrect settings or insecure setups, to protect against potential attacks.

Performing Host vulnerability Scan using Nmap

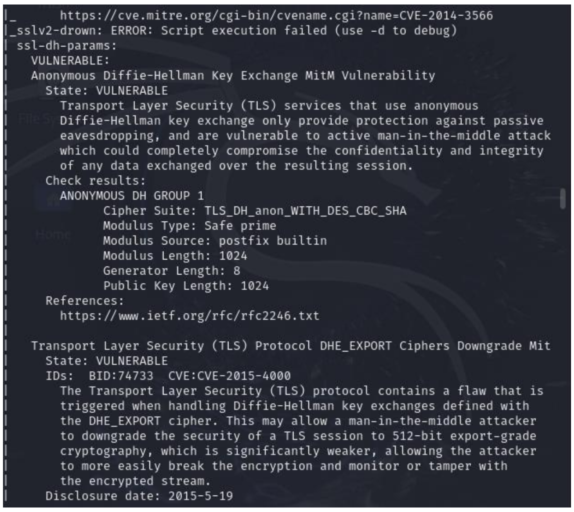
Target Host is Bee-Box IP-10.0.2.8

My target Host -10.0.2.8

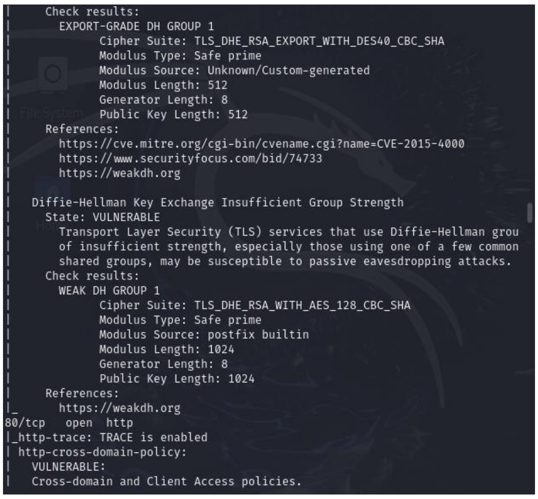
Command- >nmap --script vuln 10.0.2.8



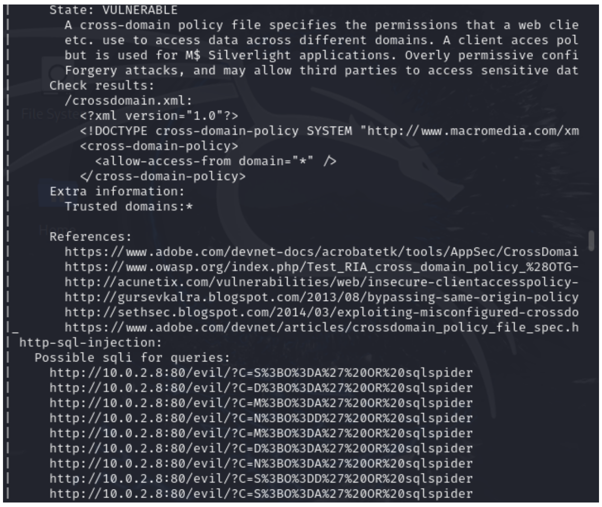
```
└─# nmap --script vuln 10.0.2.8
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-04 14:46 IST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 10.0.2.8
Host is up (0.00022s latency).
Not shown: 983 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
25/tcp   open  smtp
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  BID:70574  CVE:CVE-2014-3566
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and othe
|           products, uses nondeterministic CBC padding, which makes it easi
|           for man-in-the-middle attackers to obtain cleartext data via a
|           padding-oracle attack, aka the "POODLE" issue.
|     Disclosure date: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_AES_128_CBC_SHA
|     References:
|       https://www.openssl.org/~bodo/ssl-poodle.pdf
|       https://www.imperialviolet.org/2014/10/14/poodle.html
|       https://www.securityfocus.com/bid/70574
```



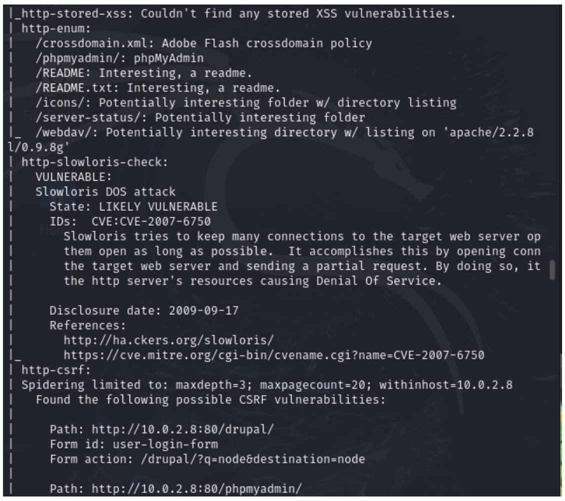
```
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|_sslv2-drown: ERROR: Script execution failed (use -d to debug)
| ssl-dh-params:
|   VULNERABLE:
|   Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use anonymous
|       Diffie-Hellman key exchange only provide protection against passive
|       eavesdropping, and are vulnerable to active man-in-the-middle attack
|       which could completely compromise the confidentiality and integrity
|       of any data exchanged over the resulting session.
|     Check results:
|       ANONYMOUS DH GROUP 1
|             Cipher Suite: TLS_DH_anon_WITH_DES_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: postfix builtin
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1024
|     References:
|       https://www.ietf.org/rfc/rfc2246.txt
|
|   Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade Mit
|     State: VULNERABLE
|     IDs:  BID:74733  CVE:CVE-2015-4000
|       The Transport Layer Security (TLS) protocol contains a flaw that is
|       triggered when handling Diffie-Hellman key exchanges defined with
|       the DHE_EXPORT cipher. This may allow a man-in-the-middle attacker
|       to downgrade the security of a TLS session to 512-bit export-grade
|       cryptography, which is significantly weaker, allowing the attacker
|       to more easily break the encryption and monitor or tamper with
|       the encrypted stream.
|     Disclosure date: 2015-5-19
```



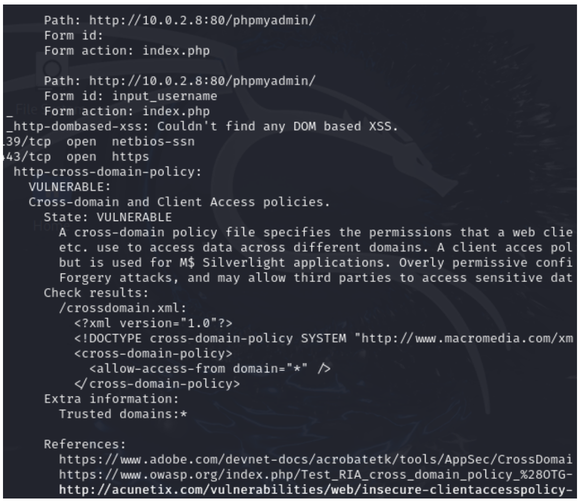
```
|     Check results:
|       EXPORT-GRADE DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: Unknown/Custom-generated
|             Modulus Length: 512
|             Generator Length: 8
|             Public Key Length: 512
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000
|       https://www.securityfocus.com/bid/74733
|       https://weakdh.org
|
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use Diffie-Hellman grou
|       of insufficient strength, especially those using one of a few common
|       shared groups, may be susceptible to passive eavesdropping attacks.
|     Check results:
|       WEAK DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: postfix builtin
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1024
|     References:
|_      https://weakdh.org
80/tcp   open  http
|_http-trace: TRACE is enabled
| http-cross-domain-policy:
|   VULNERABLE:
|   Cross-domain and Client Access policies.
```



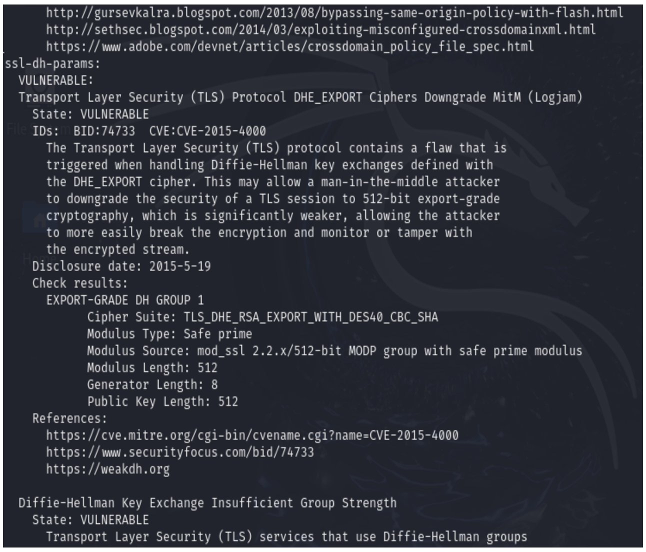
```
|     State: VULNERABLE
|       A cross-domain policy file specifies the permissions that a web clie
|       etc. use to access data across different domains. A client acces pol
|       but is used for M$ Silverlight applications. Overly permissive confi
|       Forgery attacks, and may allow third parties to access sensitive dat
|     Check results:
|       /crossdomain.xml:
|         <?xml version="1.0"?>
|         <!DOCTYPE cross-domain-policy SYSTEM "http://www.macromedia.com/xm
|         <cross-domain-policy>
|           <allow-access-from domain="*" />
|         </cross-domain-policy>
|     Extra information:
|       Trusted domains:*
|
|     References:
|       https://www.adobe.com/devnet-docs/acrobatetk/tools/AppSec/CrossDomai
|       https://www.owasp.org/index.php/Test_RIA_cross_domain_policy_%28OTG-
|       http://acunetix.com/vulnerabilities/web/insecure-clientaccesspolicy-
|       http://gursevkalra.blogspot.com/2013/08/bypassing-same-origin-policy
|       http://sethsec.blogspot.com/2014/03/exploiting-misconfigured-crossdo
|_      https://www.adobe.com/devnet/articles/crossdomain_policy_file_spec.h
| http-sql-injection:
|   Possible sqli for queries:
|     http://10.0.2.8:80/evil/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://10.0.2.8:80/evil/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://10.0.2.8:80/evil/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://10.0.2.8:80/evil/?C=N%3BO%3DD%27%20OR%20sqlspider
|     http://10.0.2.8:80/evil/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://10.0.2.8:80/evil/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://10.0.2.8:80/evil/?C=N%3BO%3DA%27%20OR%20sqlspider
|     http://10.0.2.8:80/evil/?C=S%3BO%3DD%27%20OR%20sqlspider
|     http://10.0.2.8:80/evil/?C=S%3BO%3DA%27%20OR%20sqlspider
```



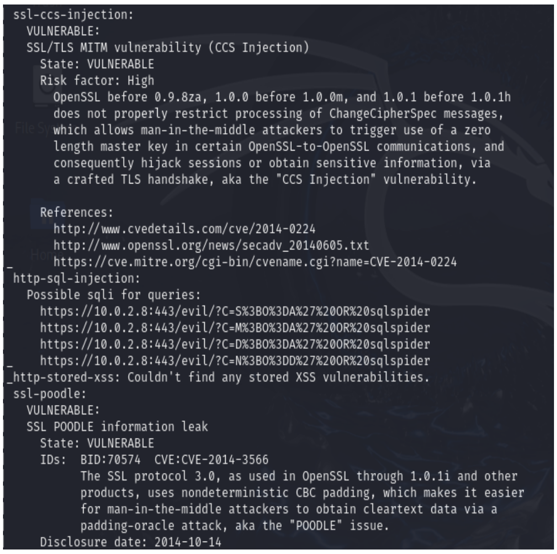
```
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-enum:
|   /crossdomain.xml: Adobe Flash crossdomain policy
|   /phpmyadmin/: phpMyAdmin
|   /README: Interesting, a readme.
|   /README.txt: Interesting, a readme.
|   /icons/: Potentially interesting folder w/ directory listing
|   /server-status/: Potentially interesting folder
|_  /webdav/: Potentially interesting directory w/ listing on 'apache/2.2.8
l/0.9.8g'
| 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 op
|       them open as long as possible.  It accomplishes this by opening conn
|       the target web server and sending a partial request. By doing so, it
|       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-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=10.0.2.8
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://10.0.2.8:80/drupal/
|     Form id: user-login-form
|     Form action: /drupal/?q=node&destination=node
|
|     Path: http://10.0.2.8:80/phpmyadmin/
```



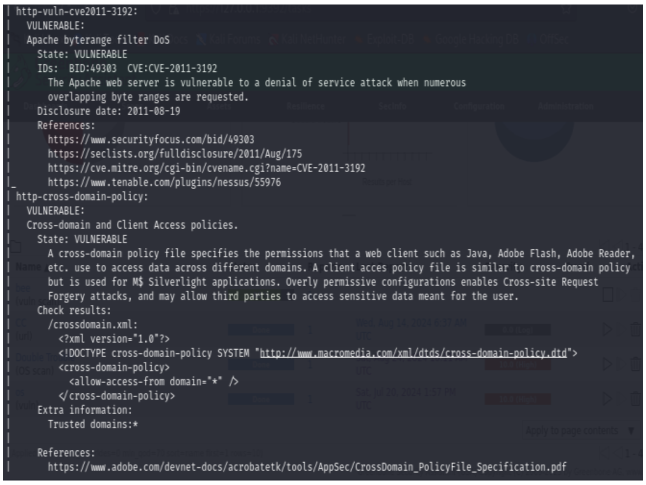
```
     Path: http://10.0.2.8:80/phpmyadmin/
     Form id:
     Form action: index.php

     Path: http://10.0.2.8:80/phpmyadmin/
     Form id: input_username
_    Form action: index.php
_http-dombased-xss: Couldn't find any DOM based XSS.
39/tcp  open  netbios-ssn
43/tcp  open  https
 http-cross-domain-policy:
   VULNERABLE:
   Cross-domain and Client Access policies.
     State: VULNERABLE
       A cross-domain policy file specifies the permissions that a web clie
       etc. use to access data across different domains. A client acces pol
       but is used for M$ Silverlight applications. Overly permissive confi
       Forgery attacks, and may allow third parties to access sensitive dat
     Check results:
       /crossdomain.xml:
         <?xml version="1.0"?>
         <!DOCTYPE cross-domain-policy SYSTEM "http://www.macromedia.com/xm
         <cross-domain-policy>
           <allow-access-from domain="*" />
         </cross-domain-policy>
     Extra information:
       Trusted domains:*

     References:
       https://www.adobe.com/devnet-docs/acrobatetk/tools/AppSec/CrossDomai
       https://www.owasp.org/index.php/Test_RIA_cross_domain_policy_%28OTG-
       http://acunetix.com/vulnerabilities/web/insecure-clientaccesspolicy-
```



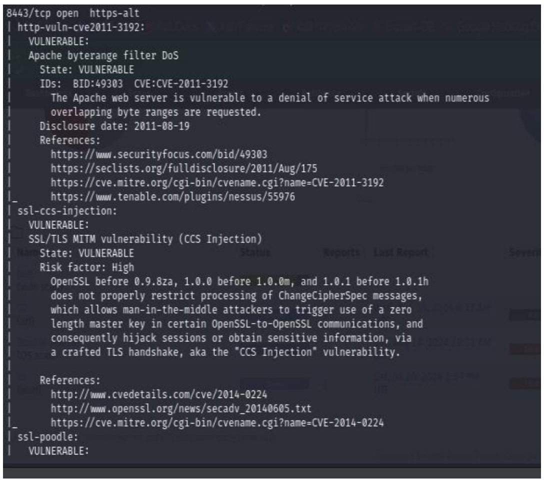
```
      http://gursevkalra.blogspot.com/2013/08/bypassing-same-origin-policy-with-flash.html
      http://sethsec.blogspot.com/2014/03/exploiting-misconfigured-crossdomainxml.html
      https://www.adobe.com/devnet/articles/crossdomain_policy_file_spec.html
ssl-dh-params:
  VULNERABLE:
  Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MitM (Logjam)
    State: VULNERABLE
    IDs:  BID:74733  CVE:CVE-2015-4000
      The Transport Layer Security (TLS) protocol contains a flaw that is
      triggered when handling Diffie-Hellman key exchanges defined with
      the DHE_EXPORT cipher. This may allow a man-in-the-middle attacker
      to downgrade the security of a TLS session to 512-bit export-grade
      cryptography, which is significantly weaker, allowing the attacker
      to more easily break the encryption and monitor or tamper with
      the encrypted stream.
    Disclosure date: 2015-5-19
    Check results:
      EXPORT-GRADE DH GROUP 1
            Cipher Suite: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
            Modulus Type: Safe prime
            Modulus Source: mod_ssl 2.2.x/512-bit MODP group with safe prime modulus
            Modulus Length: 512
            Generator Length: 8
            Public Key Length: 512
    References:
      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000
      https://www.securityfocus.com/bid/74733
      https://weakdh.org

  Diffie-Hellman Key Exchange Insufficient Group Strength
    State: VULNERABLE
      Transport Layer Security (TLS) services that use Diffie-Hellman groups
```



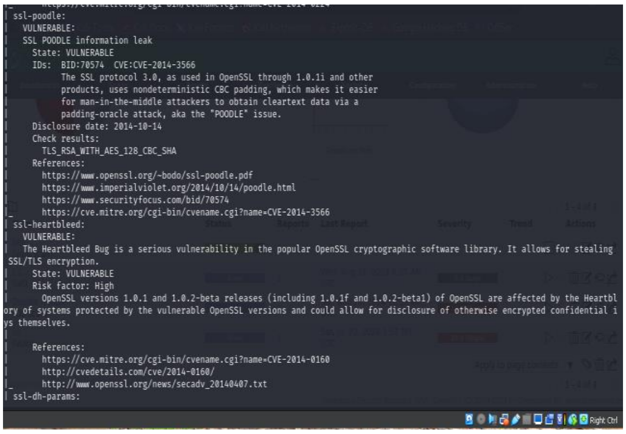
```
ssl-ccs-injection:
  VULNERABLE:
  SSL/TLS MITM vulnerability (CCS Injection)
    State: VULNERABLE
    Risk factor: High
      OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
      does not properly restrict processing of ChangeCipherSpec messages,
      which allows man-in-the-middle attackers to trigger use of a zero
      length master key in certain OpenSSL-to-OpenSSL communications, and
      consequently hijack sessions or obtain sensitive information, via
      a crafted TLS handshake, aka the "CCS Injection" vulnerability.

    References:
      http://www.cvedetails.com/cve/2014-0224
      http://www.openssl.org/news/secadv_20140605.txt
_     https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
http-sql-injection:
  Possible sqli for queries:
    https://10.0.2.8:443/evil/?C=S%3BO%3DA%27%20OR%20sqlspider
    https://10.0.2.8:443/evil/?C=M%3BO%3DA%27%20OR%20sqlspider
    https://10.0.2.8:443/evil/?C=D%3BO%3DA%27%20OR%20sqlspider
_   https://10.0.2.8:443/evil/?C=N%3BO%3DD%27%20OR%20sqlspider
_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
ssl-poodle:
  VULNERABLE:
  SSL POODLE information leak
    State: VULNERABLE
    IDs:  BID:70574  CVE:CVE-2014-3566
          The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
          products, uses nondeterministic CBC padding, which makes it easier
          for man-in-the-middle attackers to obtain cleartext data via a
          padding-oracle attack, aka the "POODLE" issue.
    Disclosure date: 2014-10-14
```



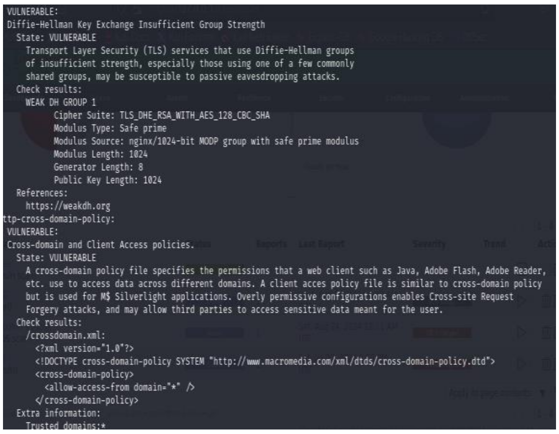
```
| http-vuln-cve2011-3192:
|   VULNERABLE:
|   Apache byterange filter DoS
|     State: VULNERABLE
|     IDs:  BID:49303  CVE:CVE-2011-3192
|       The Apache web server is vulnerable to a denial of service attack when numerous
|       overlapping byte ranges are requested.
|     Disclosure date: 2011-08-19
|     References:
|       https://www.securityfocus.com/bid/49303
|       https://seclists.org/fulldisclosure/2011/Aug/175
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192
|_      https://www.tenable.com/plugins/nessus/55976
| http-cross-domain-policy:
|   VULNERABLE:
|   Cross-domain and Client Access policies.
|     State: VULNERABLE
|       A cross-domain policy file specifies the permissions that a web client such as Java, Adobe Flash, Adobe Reader,
|       etc. use to access data across different domains. A client acces policy file is similar to cross-domain policy
|       but is used for M$ Silverlight applications. Overly permissive configurations enables Cross-site Request
|       Forgery attacks, and may allow third parties to access sensitive data meant for the user.
|     Check results:
|       /crossdomain.xml:
|         <?xml version="1.0"?>
|         <!DOCTYPE cross-domain-policy SYSTEM "http://www.macromedia.com/xml/dtds/cross-domain-policy.dtd">
|         <cross-domain-policy>
|           <allow-access-from domain="*" />
|         </cross-domain-policy>
|     Extra information:
|       Trusted domains:*
|
|     References:
|       https://www.adobe.com/devnet-docs/acrobatetk/tools/AppSec/CrossDomain_PolicyFile_Specification.pdf
```



```
8443/tcp open  https-alt
| http-vuln-cve2011-3192:
|   VULNERABLE:
|   Apache byterange filter DoS
|     State: VULNERABLE
|     IDs:  BID:49303  CVE:CVE-2011-3192
|       The Apache web server is vulnerable to a denial of service attack when numerous
|       overlapping byte ranges are requested.
|     Disclosure date: 2011-08-19
|     References:
|       https://www.securityfocus.com/bid/49303
|       https://seclists.org/fulldisclosure/2011/Aug/175
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192
|_      https://www.tenable.com/plugins/nessus/55976
| ssl-ccs-injection:
|   VULNERABLE:
|   SSL/TLS MITM vulnerability (CCS Injection)
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
|       does not properly restrict processing of ChangeCipherSpec messages,
|       which allows man-in-the-middle attackers to trigger use of a zero
|       length master key in certain OpenSSL-to-OpenSSL communications, and
|       consequently hijack sessions or obtain sensitive information, via
|       a crafted TLS handshake, aka the "CCS Injection" vulnerability.
|
|     References:
|       http://www.cvedetails.com/cve/2014-0224
|       http://www.openssl.org/news/secadv_20140605.txt
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
| ssl-poodle:
|   VULNERABLE:
```



```
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  BID:70574  CVE:CVE-2014-3566
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|           products, uses nondeterministic CBC padding, which makes it easier
|           for man-in-the-middle attackers to obtain cleartext data via a
|           padding-oracle attack, aka the "POODLE" issue.
|     Disclosure date: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_AES_128_CBC_SHA
|     References:
|       https://www.openssl.org/~bodo/ssl-poodle.pdf
|       https://www.imperialviolet.org/2014/10/14/poodle.html
|       https://www.securityfocus.com/bid/70574
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
| ssl-heartbleed:
|   VULNERABLE:
|   The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. It allows for stealing
 SSL/TLS encryption.
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and 1.0.2-beta1) of OpenSSL are affected by the Heartbl
ory of systems protected by the vulnerable OpenSSL versions and could allow for disclosure of otherwise encrypted confidential i
ys themselves.
|
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
|       http://cvedetails.com/cve/2014-0160/
|_      http://www.openssl.org/news/secadv_20140407.txt
| ssl-dh-params:
```



```
VULNERABLE:
Diffie-Hellman Key Exchange Insufficient Group Strength
  State: VULNERABLE
    Transport Layer Security (TLS) services that use Diffie-Hellman groups
    of insufficient strength, especially those using one of a few commonly
    shared groups, may be susceptible to passive eavesdropping attacks.
  Check results:
    WEAK DH GROUP 1
          Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA
          Modulus Type: Safe prime
          Modulus Source: nginx/1024-bit MODP group with safe prime modulus
          Modulus Length: 1024
          Generator Length: 8
          Public Key Length: 1024
  References:
    https://weakdh.org
ttp-cross-domain-policy:
VULNERABLE:
Cross-domain and Client Access policies.
  State: VULNERABLE
    A cross-domain policy file specifies the permissions that a web client such as Java, Adobe Flash, Adobe Reader,
    etc. use to access data across different domains. A client acces policy file is similar to cross-domain policy
    but is used for M$ Silverlight applications. Overly permissive configurations enables Cross-site Request
    Forgery attacks, and may allow third parties to access sensitive data meant for the user.
  Check results:
    /crossdomain.xml:
      <?xml version="1.0"?>
      <!DOCTYPE cross-domain-policy SYSTEM "http://www.macromedia.com/xml/dtds/cross-domain-policy.dtd">
      <cross-domain-policy>
        <allow-access-from domain="*" />
      </cross-domain-policy>
  Extra information:
    Trusted domains:*
```

Key vulnerabilities that I found through Nmap scan:

- SSL POODLE Information Leak

- CVE ID: CVE-2014-3566
- Risk Level: VULNERABLE
- Description: A man-in-the-middle attacker can exploit weaknesses in SSL 3.0, allowing cleartext data extraction through a padding oracle attack.

- Anonymous Diffie-Hellman Key Exchange MitM Vulnerability

- Risk Level: VULNERABLE
- Description: Vulnerable to active man-in-the-middle attacks, compromising the confidentiality and integrity of data exchanged in a session using anonymous Diffie-Hellman key exchange.

- Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade (Logjam)

- CVE ID: CVE-2015-4000
- Risk Level: VULNERABLE
- Description: A man-in-the-middle attacker can downgrade a TLS session to weaker 512-bit export-grade cryptography, allowing them to monitor or tamper with encrypted streams.

- Slowloris DOS Attack

- CVE ID: CVE-2007-6750
- Risk Level: LIKELY VULNERABLE
- Description: This DoS attack keeps connections to the target server open as long as possible, starving the server's resources and leading to denial of service.

- SSL/TLS MITM Vulnerability (CCS Injection)

- CVE ID: CVE-2014-0224
- Risk Level: HIGH
- Description: A man-in-the-middle attacker can trigger the use of a zero-length master key in OpenSSL-to-OpenSSL communication, hijacking sessions or obtaining sensitive information.

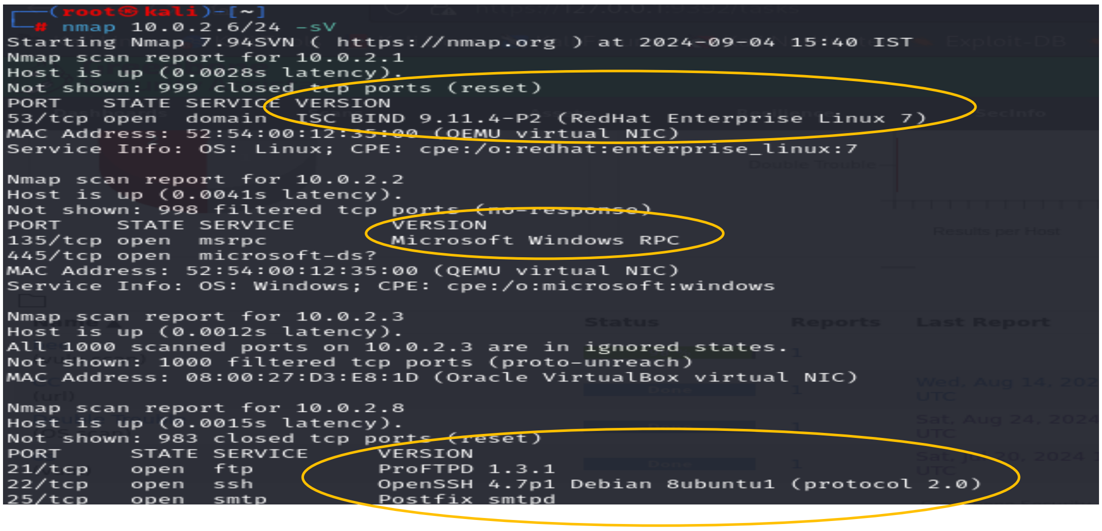
➢ Cross-domain and Client Access Policies Vulnerability

- Risk Level: VULNERABLE
- Description: Overly permissive cross-domain policy configurations can enable cross-site request forgery (CSRF) attacks, allowing third-party access to sensitive data.

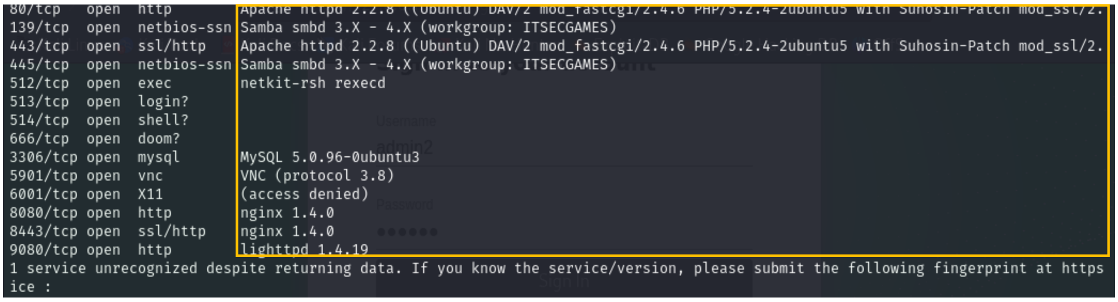
Banner Grabbing and Service version Detection using Nmap

Banner Grabbing: Banner grabbing is a technique used by attackers and security experts to gather information about a network and the services running on open ports. A banner is a text message shown by a system that reveals details like the type and version of the software it’s using. This information can help attackers understand the system better and find weaknesses to exploit. Banner grabbing involves collecting this software information, including its name and version.

Command- >nmap 10.0.2.6/24 –sV



```
┌──(root㉿kali)-[~]
└─# nmap 10.0.2.6/24 -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-04 15:40 IST
Nmap scan report for 10.0.2.1
Host is up (0.0028s latency).
Not shown: 999 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
53/tcp open   domain   ISC BIND 9.11.4-P2 (RedHat Enterprise Linux 7)
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:redhat:enterprise_linux:7

Nmap scan report for 10.0.2.2
Host is up (0.0041s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE        VERSION
135/tcp open   msrpc           Microsoft Windows RPC
445/tcp open   microsoft-ds?
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 10.0.2.3
Host is up (0.0012s latency).
All 1000 scanned ports on 10.0.2.3 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:D3:E8:1D (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.8
Host is up (0.0015s latency).
Not shown: 983 closed tcp ports (reset)
PORT      STATE  SERVICE         VERSION
21/tcp    open   ftp             ProFTPD 1.3.1
22/tcp    open   ssh             OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
25/tcp    open   smtp            Postfix smtpd
```



```
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: ITSECGAMES)
443/tcp  open  ssl/http    Apache httpd 2.2.8 ((Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: ITSECGAMES)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell?
666/tcp  open  doom?
3306/tcp open  mysql       MySQL 5.0.96-0ubuntu3
5901/tcp open  vnc         VNC (protocol 3.8)
6001/tcp open  X11         (access denied)
8080/tcp open  http        nginx 1.4.0
8443/tcp open  ssl/http    nginx 1.4.0
9080/tcp open  http        lighttpd 1.4.19
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https
ice :
```

Vulnerabilities associated with these versions in detail

1. ISC BIND 9.11.4-P2 (RedHat Enterprise Linux 7) - Port 53 (DNS)

- Description: ISC BIND (Berkeley Internet Name Domain) is a popular DNS server.
- Known Vulnerabilities:
  - CVE-2018-5740: A memory leak in DNSSEC verification.
  - CVE-2019-6477: An attacker could exploit BIND via crafted TCP messages, leading to DoS attacks.

2. Microsoft Windows RPC (msrpc) - Port 135

- Description: Windows Remote Procedure Call is used for interprocess communication.
- Known Vulnerabilities:
  - CVE-2020-0601: Vulnerability in RPC service that could allow remote code execution.

3. ProFTPD 1.3.1 - Port 21 (FTP)

- Description: ProFTPD is an FTP server. Version 1.3.1 is outdated.
- Known Vulnerabilities:
  - CVE-2010-4221: SQL injection vulnerability.
  - CVE-2009-3639: A buffer overflow issue could lead to remote code execution.

4. OpenSSH 4.7p1 (Debian 8ubuntu1) - Port 22 (SSH)

- Description: OpenSSH is a secure shell service.
- Known Vulnerabilities:
  - CVE-2008-5161: Vulnerability related to insufficient key exchange validation, allowing man-in-the-middle attacks.

5. Postfix smtpd - Port 25 (SMTP)

- Description: Postfix is a mail transfer agent (MTA) used for sending and receiving email.
- Known Vulnerabilities:
  - CVE-2020-1710: Memory exhaustion in Postfix leading to a DoS.

6. Apache httpd 2.2.8 ((Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5) - Port 80 (HTTP)

- Description: Apache HTTP server with DAV, FastCGI, and PHP modules.
- Known Vulnerabilities:
  - CVE-2011-3368: HTTP request smuggling.
  - CVE-2010-1452: Denial of service via mod_dav.
  - CVE-2012-0053: Integer overflow in mod_ssl.

7. Samba smbd 3.X - 4.X - Port 139/445 (NetBIOS)

- Description: Samba is used for file and print services for SMB/CIFS clients.
- Known Vulnerabilities:
  - CVE-2017-7494: Remote code execution in Samba when handling certain SMB requests.

8. Apache httpd 2.2.8 ((Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5) - Port 443 (HTTPS)

- Description: Same as on Port 80 but secured with SSL.
- Known Vulnerabilities:
  - CVE-2013-5704: Denial of service vulnerability due to SSL renegotiation.

9. netkit-rsh rexecd - Port 512 (exec)

- Description: Remote shell service used for remote command execution.
- Known Vulnerabilities:
  - Generally considered insecure due to lack of encryption, susceptible to man-in-the-middle attacks.

10. login service (Unknown) - Port 513

- Description: Used for remote logins, like rlogin.
- Known Vulnerabilities:
  - Generally insecure due to plaintext transmissions and vulnerable to replay attacks.

11. shell service (Unknown) - Port 514

- Description: Remote shell service, similar to rsh.
- Known Vulnerabilities:
  - Similar issues to rexecd with lack of encryption.

12. doom service - Port 666

- Description: Originally used for the Doom multiplayer game, may indicate an unusual service.
- Known Vulnerabilities:
  - Potential for exploitation if running an old or improperly secured version.

13. MySQL 5.0.96-0ubuntu3 - Port 3306 (MySQL)

- Description: MySQL database service.
- Known Vulnerabilities:
  - CVE-2012-2122: Authentication bypass vulnerability.
  - CVE-2016-6662: Privilege escalation due to a remote code execution vulnerability.

14. VNC (protocol 3.8) - Port 5901

- Description: VNC service used for remote desktop.
- Known Vulnerabilities:
  - CVE-2016-9942: VNC authentication bypass.
  - CVE-2019-15681: Buffer overflow in certain VNC implementations.

15. X11 (access denied) - Port 6001

- Description: X11 window system, generally associated with graphical display in Unix-like systems.
- Known Vulnerabilities:
  - CVE-2018-14665: Potential for privilege escalation in X.Org Server.

16. nginx 1.4.0 - Port 8080/8443

- Description: Nginx web server.
- Known Vulnerabilities:
    - CVE-2013-4547: Denial of service vulnerability due to improper handling of certain requests.
    - CVE-2014-3556: Potential buffer overflow leading to remote code execution.

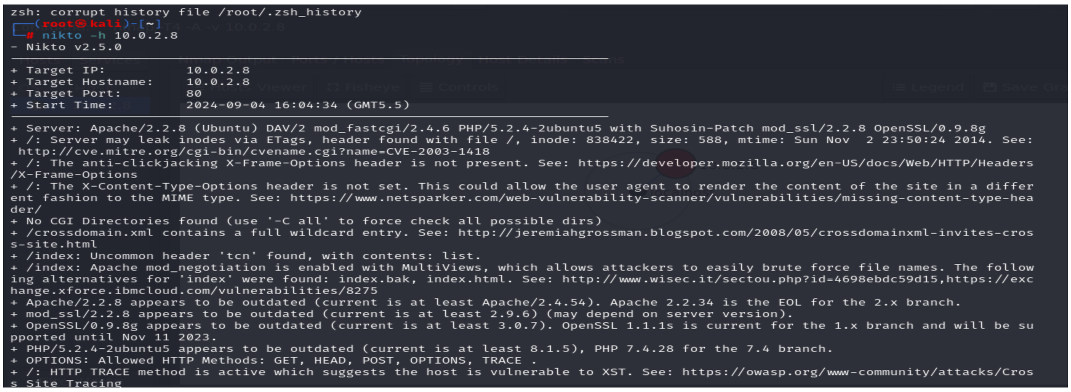
17. lighttpd 1.4.19 - Port 9080 (HTTP)

- Description: Lightweight web server.
- Known Vulnerabilities:
    - CVE-2011-4362: Denial of service vulnerability due to improper handling of headers.

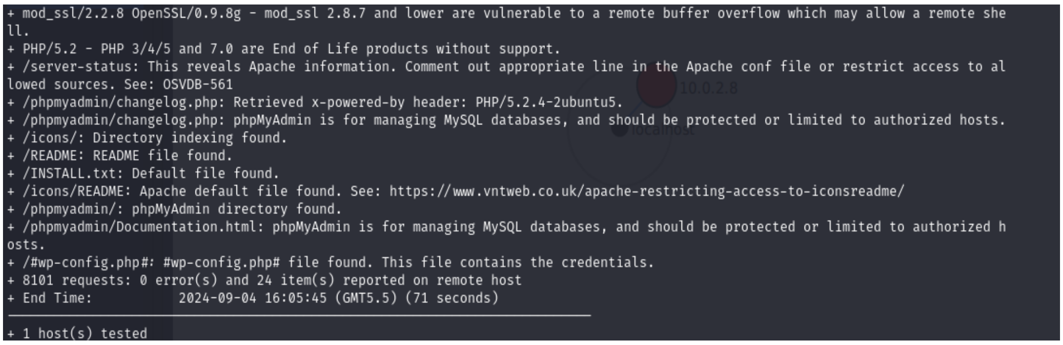
Vulnerability Scanning with Nikto

Nikto: Nikto is a command-line tool written in Perl that performs comprehensive security scans. It scans for common vulnerabilities and misconfigurations, including outdated software versions, server misconfigurations, vulnerable server components, and more.

Command- >nikto –h 10.0.2.8



```
zsh: corrupt history file /root/.zsh_history
┌──(root㉿kali)-[~]
└─# nikto -h 10.0.2.8
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.0.2.8
+ Target Hostname:    10.0.2.8
+ Target Port:        80
+ Start Time:         2024-09-04 16:04:34 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
+ /: Server may leak inodes via ETags, header found with file /, inode: 838422, size: 588, mtime: Sun Nov  2 23:50:24 2014. 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://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 differ
ent fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-hea
der/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /crossdomain.xml contains a full wildcard entry. See: http://jeremiahgrossman.blogspot.com/2008/05/crossdomainxml-invites-cros
s-site.html
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The follow
ing alternatives for 'index' were found: index.bak, index.html. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exc
hange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ mod_ssl/2.2.8 appears to be outdated (current is at least 2.9.6) (may depend on server version).
+ OpenSSL/0.9.8g appears to be outdated (current is at least 3.0.7). OpenSSL 1.1.1s is current for the 1.x branch and will be su
pported until Nov 11 2023.
+ PHP/5.2.4-2ubuntu5 appears to be outdated (current is at least 8.1.5), PHP 7.4.28 for the 7.4 branch.
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE .
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cros
s Site Tracing
```



```
+ mod_ssl/2.2.8 OpenSSL/0.9.8g - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow a remote she
ll.
+ PHP/5.2 - PHP 3/4/5 and 7.0 are End of Life products without support.
+ /server-status: This reveals Apache information. Comment out appropriate line in the Apache conf file or restrict access to al
lowed sources. See: OSVDB-561
+ /phpmyadmin/changelog.php: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.
+ /phpmyadmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /icons/: Directory indexing found.
+ /README: README file found.
+ /INSTALL.txt: Default file found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpmyadmin/: phpMyAdmin directory found.
+ /phpmyadmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized h
osts.
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8101 requests: 0 error(s) and 24 item(s) reported on remote host
+ End Time:           2024-09-04 16:05:45 (GMT5.5) (71 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

My findings regarding outdated software, configuration issues, or potential vulnerabilities through Nikto scan report

Outdated Software:

1. Apache/2.2.8 (Ubuntu):

   - Outdated Version: The current stable version is at least Apache 2.4.54.
   - Impact: Apache 2.2.x branch is end-of-life (EOL). Upgrading is crucial to avoid unpatched vulnerabilities.

2. PHP/5.2.4-2ubuntu5:

   - Outdated Version: PHP 5.x is no longer supported. The latest version is PHP 8.1.5.
   - Impact: PHP 5.2 is vulnerable to various security issues, including CVE-2007-2872 (remote code execution).

3. mod_ssl/2.2.8:

   - Outdated Version: Current is mod_ssl 2.9.6.
   - Impact: Vulnerable to remote buffer overflow (mod_ssl 2.8.7 and lower), which can allow remote shell access.

4. OpenSSL/0.9.8g:

   - Outdated Version: Latest stable is OpenSSL 3.0.7, with OpenSSL 1.1.1s as a stable branch.
   - Impact: OpenSSL 0.9.8g is vulnerable to several critical issues, including CVE-2014-0160 (Heartbleed).

Configuration Issues:

1. ETags Information Leak (CVE-2003-1418):

   - Issue: The server leaks inodes via ETags, allowing attackers to infer internal file system details.
   - Fix: Disable ETags or configure them to only use "hashes" rather than inode metadata.

2. Missing X-Frame-Options Header:

    - Issue: Lack of the X-Frame-Options header makes the site vulnerable to clickjacking attacks.
    - Fix: Add the X-Frame-Options header to deny framing or allow framing only from trusted sources.

3. Missing X-Content-Type-Options Header:

    - Issue: Absence of X-Content-Type-Options allows MIME-sniffing by user agents, potentially leading to security risks.
    - Fix: Set X-Content-Type-Options: nosniff to prevent browsers from interpreting files as different MIME types.

4. Wildcard Entry in crossdomain.xml:

    - Issue: A full wildcard entry in crossdomain.xml can open the server to cross-domain attacks.
    - Fix: Restrict access to trusted domains.

5. mod_negotiation Enabled with MultiViews:

    - Issue: MultiViews allows attackers to brute-force file names (e.g., index.bak and index.html were found).
    - Fix: Disable MultiViews in Apache configuration or restrict access.

6. HTTP TRACE Method Enabled (Cross-Site Tracing):

    - Issue: The TRACE method is enabled, which can be used in Cross-Site Tracing (XST) attacks.
    - Fix: Disable the TRACE method by updating the Apache configuration.

7. Directory Indexing Found (/icons/):

    - Issue: Directory indexing is enabled, revealing directory contents to attackers.
    - Fix: Disable directory indexing in the server's configuration.

8. Exposed Sensitive Files:

    - Files such as README, INSTALL.txt, /icons/README, and #wp-config.php# are accessible.
    - Fix: Restrict access to sensitive files, or remove them from the public directory.

9. Exposed phpMyAdmin Directory:

   - ❖ Issue: phpMyAdmin is exposed, which could allow unauthorized access to the MySQL database.
   - ❖ Fix: Restrict access to phpMyAdmin by using authentication mechanisms, or block access from external sources.

10. Server Information Disclosure (/server-status):

   - ❖ Issue: The server-status page is exposed, revealing Apache server information.
   - ❖ Fix: Restrict or disable access to the server-status page.

Potential Vulnerabilities:

1. Cross-Site Tracing (XST):

   - ➢ Vulnerability: HTTP TRACE method enabled allows cross-site tracing.

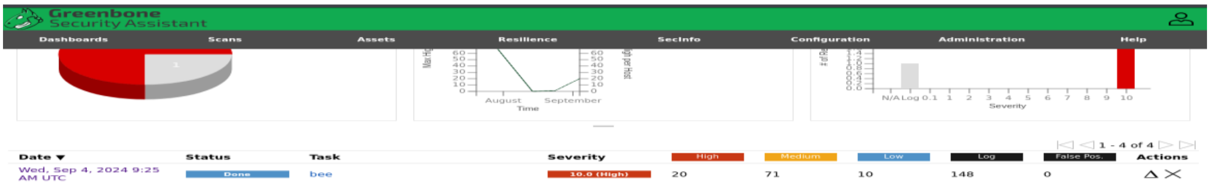
2. mod_ssl Remote Buffer Overflow:

   - ➢ Vulnerability: Old version of mod_ssl (2.8.7 and lower) is vulnerable to buffer overflow, which may allow attackers to execute a remote shell.

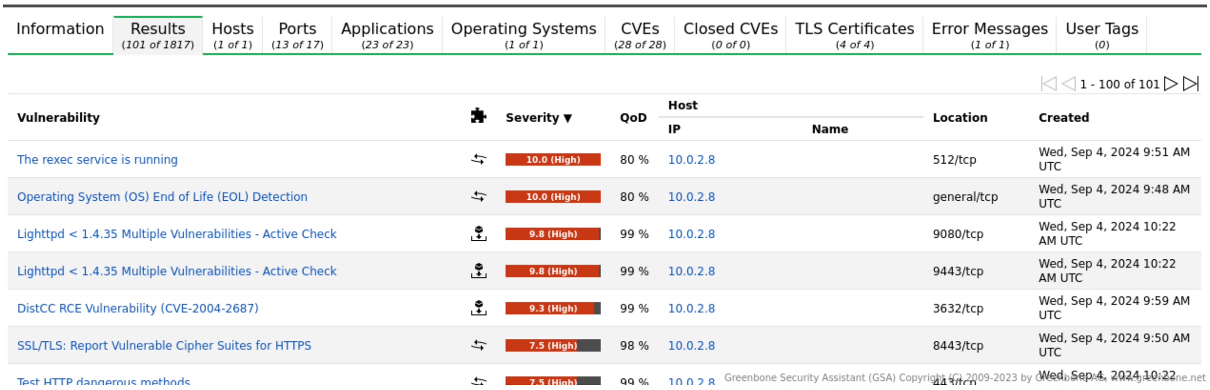
Comprehensive Vulnerability Assessment with OpenVAS

Open VAS: OpenVAS (Vulnerability Assessment Scanner) is a free tool source vulnerability scanning and management tool that scans for security problems, such as misconfigured settings, old software, and weak passwords that attackers could exploit.

Vulnerability Assessment: A vulnerability assessment helps organizations check their systems for these weaknesses. It finds out if there are known risks, rates how serious these risks are, and advises on how to fix or reduce them.



Date ▾	Status	Task	Severity	High	Medium	Low	Log	False Pos.	Actions
Wed, Sep 4, 2024 9:25 AM UTC	Done	bee	10.0 (High)	20	71	10	148	0	△ ✕

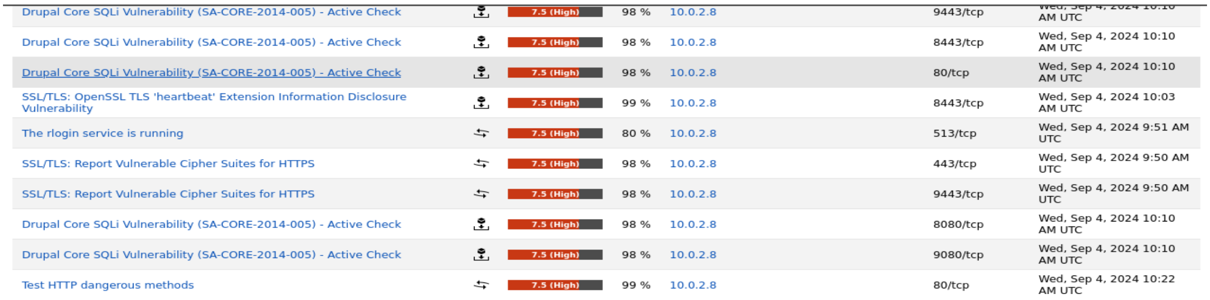


Information | Results (101 of 1817) | Hosts (1 of 1) | Ports (13 of 17) | Applications (23 of 23) | Operating Systems (1 of 1) | CVEs (28 of 28) | Closed CVEs (0 of 0) | TLS Certificates (4 of 4) | Error Messages (1 of 1) | User Tags (0)

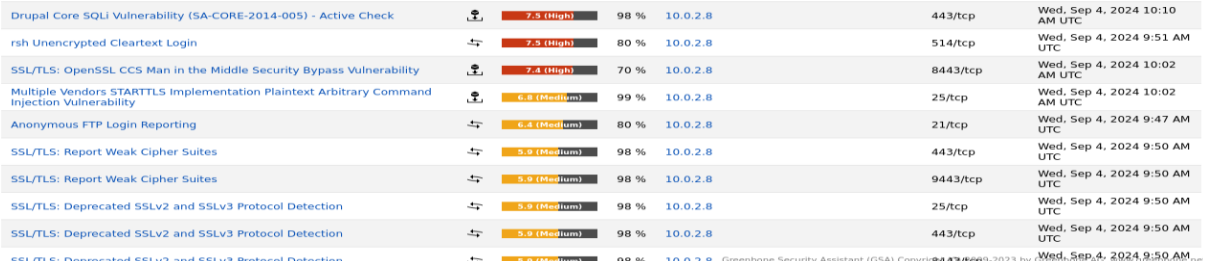
1 - 100 of 101

Vulnerability		Severity ▼	QoD	Host IP	Host Name	Location	Created
The rexec service is running		10.0 (High)	80 %	10.0.2.8		512/tcp	Wed, Sep 4, 2024 9:51 AM UTC
Operating System (OS) End of Life (EOL) Detection		10.0 (High)	80 %	10.0.2.8		general/tcp	Wed, Sep 4, 2024 9:48 AM UTC
Lighttpd < 1.4.35 Multiple Vulnerabilities - Active Check		9.8 (High)	99 %	10.0.2.8		9080/tcp	Wed, Sep 4, 2024 10:22 AM UTC
Lighttpd < 1.4.35 Multiple Vulnerabilities - Active Check		9.8 (High)	99 %	10.0.2.8		9443/tcp	Wed, Sep 4, 2024 10:22 AM UTC
DistCC RCE Vulnerability (CVE-2004-2687)		9.3 (High)	99 %	10.0.2.8		3632/tcp	Wed, Sep 4, 2024 9:59 AM UTC
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS		7.5 (High)	98 %	10.0.2.8		8443/tcp	Wed, Sep 4, 2024 9:50 AM UTC
Test HTTP dangerous methods		7.5 (High)	99 %	10.0.2.8		443/tcp	Wed, Sep 4, 2024 10:22

Greenbone Security Assistant (GSA) Copyright (C) 2009-2023 by Greenbone AG, www.greenbone.net

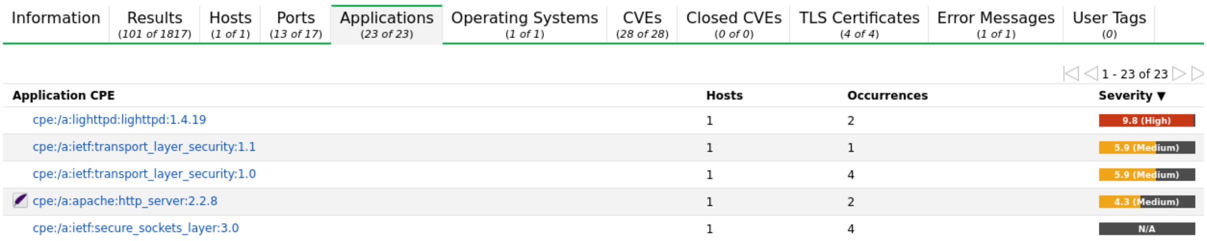


Drupal Core SQLi Vulnerability (SA-CORE-2014-005) - Active Check		7.5 (High)	98 %	10.0.2.8	9443/tcp	Wed, Sep 4, 2024 10:10 AM UTC
Drupal Core SQLi Vulnerability (SA-CORE-2014-005) - Active Check		7.5 (High)	98 %	10.0.2.8	8443/tcp	Wed, Sep 4, 2024 10:10 AM UTC
Drupal Core SQLi Vulnerability (SA-CORE-2014-005) - Active Check		7.5 (High)	98 %	10.0.2.8	80/tcp	Wed, Sep 4, 2024 10:10 AM UTC
SSL/TLS: OpenSSL TLS 'heartbeat' Extension Information Disclosure Vulnerability		7.5 (High)	99 %	10.0.2.8	8443/tcp	Wed, Sep 4, 2024 10:03 AM UTC
The rlogin service is running		7.5 (High)	80 %	10.0.2.8	513/tcp	Wed, Sep 4, 2024 9:51 AM UTC
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS		7.5 (High)	98 %	10.0.2.8	443/tcp	Wed, Sep 4, 2024 9:50 AM UTC
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS		7.5 (High)	98 %	10.0.2.8	9443/tcp	Wed, Sep 4, 2024 9:50 AM UTC
Drupal Core SQLi Vulnerability (SA-CORE-2014-005) - Active Check		7.5 (High)	98 %	10.0.2.8	8080/tcp	Wed, Sep 4, 2024 10:10 AM UTC
Drupal Core SQLi Vulnerability (SA-CORE-2014-005) - Active Check		7.5 (High)	98 %	10.0.2.8	9080/tcp	Wed, Sep 4, 2024 10:10 AM UTC
Test HTTP dangerous methods		7.5 (High)	99 %	10.0.2.8	80/tcp	Wed, Sep 4, 2024 10:22 AM UTC



Drupal Core SQLi Vulnerability (SA-CORE-2014-005) - Active Check		7.5 (High)	98 %	10.0.2.8	443/tcp	Wed, Sep 4, 2024 10:10 AM UTC
rsh Unencrypted Cleartext Login		7.5 (High)	80 %	10.0.2.8	514/tcp	Wed, Sep 4, 2024 9:51 AM UTC
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability		7.4 (High)	70 %	10.0.2.8	8443/tcp	Wed, Sep 4, 2024 10:02 AM UTC
Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection Vulnerability		6.8 (Medium)	99 %	10.0.2.8	25/tcp	Wed, Sep 4, 2024 10:02 AM UTC
Anonymous FTP Login Reporting		6.4 (Medium)	80 %	10.0.2.8	21/tcp	Wed, Sep 4, 2024 9:47 AM UTC
SSL/TLS: Report Weak Cipher Suites		5.9 (Medium)	98 %	10.0.2.8	443/tcp	Wed, Sep 4, 2024 9:50 AM UTC
SSL/TLS: Report Weak Cipher Suites		5.9 (Medium)	98 %	10.0.2.8	9443/tcp	Wed, Sep 4, 2024 9:50 AM UTC
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection		5.9 (Medium)	98 %	10.0.2.8	25/tcp	Wed, Sep 4, 2024 9:50 AM UTC
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection		5.9 (Medium)	98 %	10.0.2.8	443/tcp	Wed, Sep 4, 2024 9:50 AM UTC
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection		5.9 (Medium)	98 %	10.0.2.8	8443/tcp	Wed, Sep 4, 2024 9:50 AM

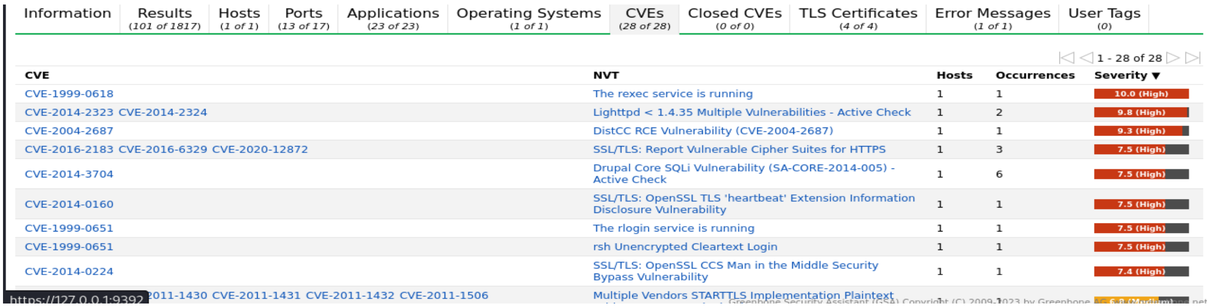
Greenbone Security Assistant (GSA) Copyright (C) 2009-2023 by Greenbone AG, www.greenbone.net



Information | Results (101 of 1817) | Hosts (1 of 1) | Ports (13 of 17) | Applications (23 of 23) | Operating Systems (1 of 1) | CVEs (28 of 28) | Closed CVEs (0 of 0) | TLS Certificates (4 of 4) | Error Messages (1 of 1) | User Tags (0)

1 - 23 of 23

Application CPE	Hosts	Occurrences	Severity ▼
cpe:/a:lighttpd:lighttpd:1.4.19	1	2	9.8 (High)
cpe:/a:ietf:transport_layer_security:1.1	1	1	5.9 (Medium)
cpe:/a:ietf:transport_layer_security:1.0	1	4	5.9 (Medium)
cpe:/a:apache:http_server:2.2.8	1	2	4.3 (Medium)
cpe:/a:ietf:secure_sockets_layer:3.0	1	4	N/A



Information | Results (101 of 1817) | Hosts (1 of 1) | Ports (13 of 17) | Applications (23 of 23) | Operating Systems (1 of 1) | CVEs (28 of 28) | Closed CVEs (0 of 0) | TLS Certificates (4 of 4) | Error Messages (1 of 1) | User Tags (0)

1 - 28 of 28

CVE	NVT	Hosts	Occurrences	Severity ▼
CVE-1999-0618	The rexec service is running	1	1	10.0 (High)
CVE-2014-2323 CVE-2014-2324	Lighttpd < 1.4.35 Multiple Vulnerabilities - Active Check	1	2	9.8 (High)
CVE-2004-2687	DistCC RCE Vulnerability (CVE-2004-2687)	1	1	9.3 (High)
CVE-2016-2183 CVE-2016-6329 CVE-2020-12872	SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	1	3	7.5 (High)
CVE-2014-3704	Drupal Core SQLi Vulnerability (SA-CORE-2014-005) - Active Check	1	6	7.5 (High)
CVE-2014-0160	SSL/TLS: OpenSSL TLS 'heartbeat' Extension Information Disclosure Vulnerability	1	1	7.5 (High)
CVE-1999-0651	The rlogin service is running	1	1	7.5 (High)
CVE-1999-0651	rsh Unencrypted Cleartext Login	1	1	7.5 (High)
CVE-2014-0224	SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	1	1	7.4 (High)
2011-1430 CVE-2011-1431 CVE-2011-1432 CVE-2011-1506	Multiple Vendors STARTTLS Implementation Plaintext	1	1	6.8 (Medium)

https://127.0.0.1:9392

Greenbone Security Assistant (GSA) Copyright (C) 2009-2023 by Greenbone AG, www.greenbone.net

Here detailing the vulnerabilities at high severity

1. rexec service is running

The rexec service is enabled, which can lead to potential remote code execution if exploited. This service sends passwords in cleartext, making it vulnerable to interception and misuse.

2. Operating System (OS) End of Life (EOL) Detection

The operating system in use has reached end-of-life, meaning it no longer receives security updates, making it vulnerable to known and unknown vulnerabilities.

3. Lighttpd < 1.4.35 Multiple Vulnerabilities

The Lighttpd server version is outdated and vulnerable to multiple exploits, including potential remote code execution (RCE) and denial-of-service (DoS) attacks.

4. DistCC RCE Vulnerability (CVE-2004-2687)

The DistCC service has a remote code execution vulnerability that allows attackers to execute arbitrary code on the server remotely.

5. SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

The SSL/TLS service is configured with vulnerable cipher suites that can lead to cryptographic weaknesses, making the connection susceptible to man-in-the-middle (MITM) attacks.

6. Test HTTP Dangerous Methods

Dangerous HTTP methods (e.g., PUT, DELETE, TRACE) are enabled, which could allow attackers to exploit vulnerabilities such as file uploads, deletion, or cross-site tracing (XST).

7. Drupal Core SQL Injection Vulnerability (SA-CORE-2014-005)

This is a SQL injection vulnerability in Drupal core that allows attackers to execute arbitrary SQL queries, potentially gaining full access to the application database.

8. SSL/TLS: OpenSSL 'heartbeat' Extension Information Disclosure (CVE-2014-0160)

This is the well-known Heartbleed vulnerability in OpenSSL, which allows attackers to retrieve sensitive data from the server's memory, such as private keys, usernames, and passwords.

9. rlogin service is running

The rlogin service allows unencrypted login access, making it vulnerable to eavesdropping and credential theft

10. rsh Unencrypted Cleartext Login

The rsh service allows cleartext login, making it vulnerable to interception and credential theft.

11. SSL/TLS: OpenSSL CCS Man-in-the-Middle Security Bypass Vulnerability

This vulnerability allows a man-in-the-middle (MITM) attacker to exploit a flaw in the ChangeCipherSpec (CCS) handling in OpenSSL, potentially bypassing security mechanisms

Mitigation Techniques:

- Disable the rexec service unless absolutely required.
- Replace rexec with more secure alternatives like SSH for remote execution.
- Upgrade the operating system to a supported version that receives security updates.
- Ensure the latest patches are applied regularly to all critical systems.
- Upgrade Lighttpd to the latest stable version (at least 1.4.35 or above).
- Disable the DistCC service unless explicitly required.
- Consider upgrading or replacing DistCC with a secure alternative
- Disable vulnerable and weak cipher suites (e.g., RC4, DES).
- Implement strong encryption standards (TLS 1.2 or TLS 1.3).
- Regularly audit the SSL/TLS configuration using tools like SSL Labs or Nessus to ensure secure configurations.
- Disable dangerous HTTP methods such as TRACE, PUT, and DELETE in the web server configuration.
- Limit HTTP methods to only those that are required (typically GET, POST, HEAD).
- Update Drupal to the latest version where this vulnerability is patched.

- ➢ Regularly monitor Drupal's security advisories and apply patches promptly.
- ➢ Use web application firewalls (WAFs) to mitigate SQL injection attempts.
- ➢ Upgrade OpenSSL to a version where the Heartbleed vulnerability is patched (OpenSSL 1.0.1g or later).
- ➢ Disable rlogin service as it transmits data in cleartext.
- ➢ Use encrypted alternatives like SSH for remote login.
- ➢ Disable the rsh service and replace it with SSH, which encrypts communication.
- ➢ Upgrade OpenSSL to a version where this vulnerability is patched (OpenSSL 1.0.1m or later).

Recommendations:

Service Hardening: Disable or restrict access to legacy services (rexec, rlogin, rsh), and use more secure alternatives like SSH.

Regular Vulnerability Scans: Schedule periodic scans to identify and remediate emerging vulnerabilities.

Patch Management: Regularly apply security patches to the operating system, applications, and services.

Using Netcat and Wireshark tools

Netcat: Netcat is a Unix utility which reads and writes data across network connections using TCP or UDP protocol.

Following tasks can be done easily with Netcat:

- ✓ Connect to a port of a target host.
- ✓ Listen to a certain port for any inbound connections.
- ✓ Send data across client and server once the connection is established.
- ✓ Transfer files across the network once the connection is established.
- ✓ Can execute programs and scripts of the client on the server and vice versa.
- ✓ Can Provide remote shell access of server to a client where shell commands can be executed.

Manual port scan using Netcat utility and comparing with Nmap port scan result

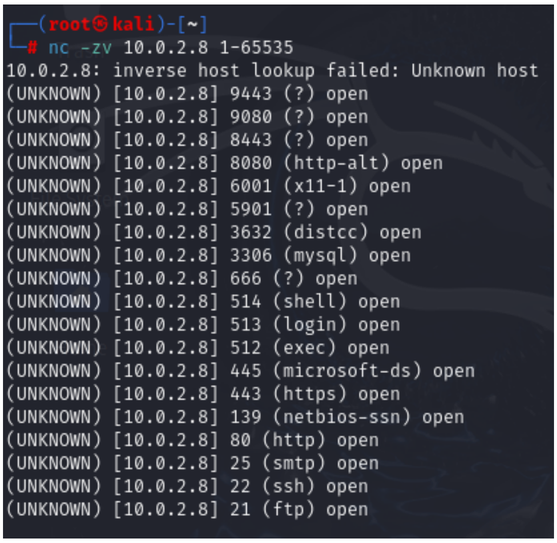
Command- >nc –zv <target ip> <port range>

nc- netcat

-z - Tells Netcat to perform a scan without sending data (just checks for open ports)

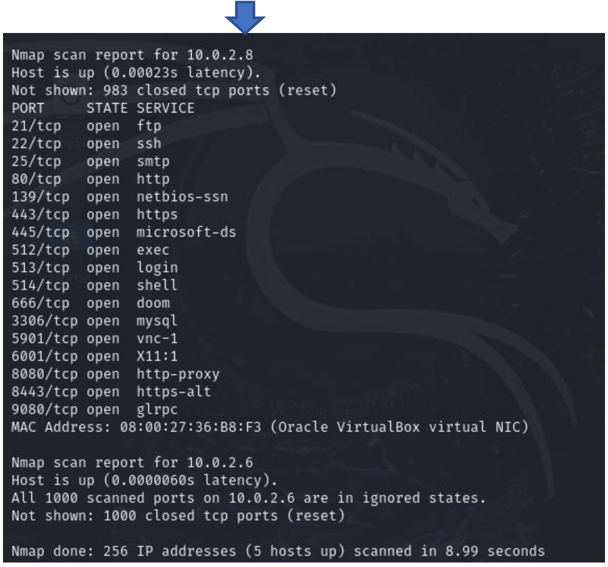
-v - Enables verbose output to show which ports are open.

>nc –zv 10.0.2.8 1-65535



```
┌──(root㉿kali)-[~]
└─# nc -zv 10.0.2.8 1-65535
10.0.2.8: inverse host lookup failed: Unknown host
(UNKNOWN) [10.0.2.8] 9443 (?) open
(UNKNOWN) [10.0.2.8] 9080 (?) open
(UNKNOWN) [10.0.2.8] 8443 (?) open
(UNKNOWN) [10.0.2.8] 8080 (http-alt) open
(UNKNOWN) [10.0.2.8] 6001 (x11-1) open
(UNKNOWN) [10.0.2.8] 5901 (?) open
(UNKNOWN) [10.0.2.8] 3632 (distcc) open
(UNKNOWN) [10.0.2.8] 3306 (mysql) open
(UNKNOWN) [10.0.2.8] 666 (?) open
(UNKNOWN) [10.0.2.8] 514 (shell) open
(UNKNOWN) [10.0.2.8] 513 (login) open
(UNKNOWN) [10.0.2.8] 512 (exec) open
(UNKNOWN) [10.0.2.8] 445 (microsoft-ds) open
(UNKNOWN) [10.0.2.8] 443 (https) open
(UNKNOWN) [10.0.2.8] 139 (netbios-ssn) open
(UNKNOWN) [10.0.2.8] 80 (http) open
(UNKNOWN) [10.0.2.8] 25 (smtp) open
(UNKNOWN) [10.0.2.8] 22 (ssh) open
(UNKNOWN) [10.0.2.8] 21 (ftp) open
```

Nmap port scan result



```
Nmap scan report for 10.0.2.8
Host is up (0.00023s latency).
Not shown: 983 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
25/tcp   open  smtp
80/tcp   open  http
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
666/tcp  open  doom
3306/tcp open  mysql
5901/tcp open  vnc-1
6001/tcp open  X11:1
8080/tcp open  http-proxy
8443/tcp open  https-alt
9080/tcp open  glrpc
MAC Address: 08:00:27:36:B8:F3 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.6
Host is up (0.0000060s latency).
All 1000 scanned ports on 10.0.2.6 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (5 hosts up) scanned in 8.99 seconds
```

9443 is the port additionaly I found in ncat scanning result compared to nmap result.

Wireshark: Wireshark is a software tool used to monitor he network traffic through a network interface. It is the most widely used network monitoring tool today.

Steps:

Start capturing packets and stop capturing after 5min

Analyse the captured packets using filters

>tcp - for TCP traffic.

>ssh - for SSH traffic.

>http - to see HTTP traffic

>ftp - for FTP traffic.

>icmp - for ICMP traffic

>dns - to view DNS requests and responses

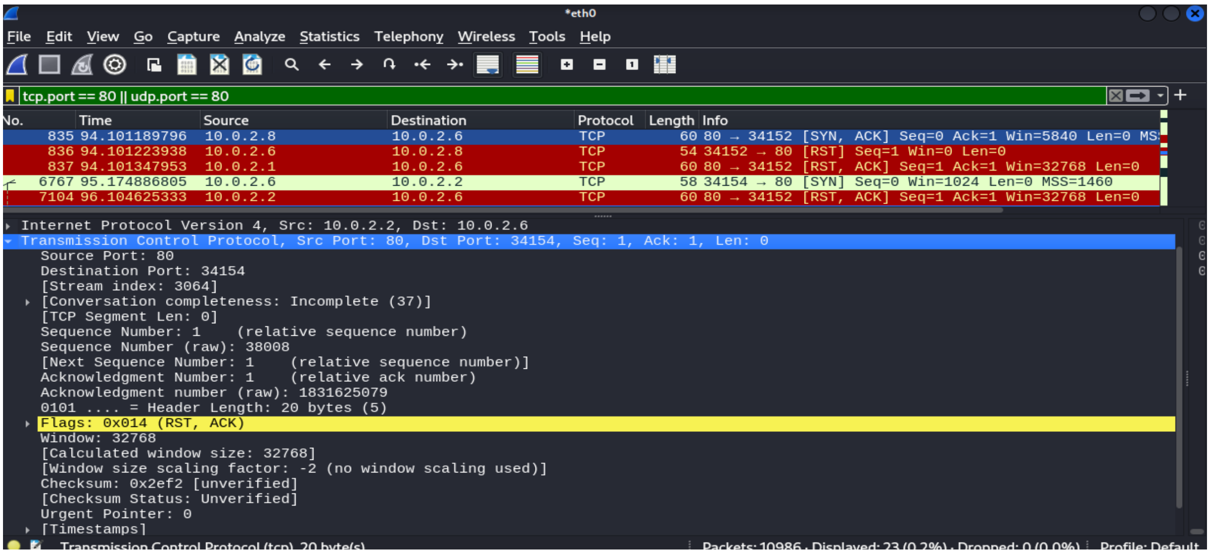
>tcp.port = = <port number> -to show traffic on specific port

>ip.addr = = <target ip> - to display traffic involving a specific IP address.

Use **"Statistics"** > **"Endpoints"** to identify IP addresses generating high amounts of traffic.

>http.request -to review HTTP requests for suspicious URLs

Look at **"Analyze"** > **"Expert Information"** to see alerts, which can include anomalies, errors, and warnings.



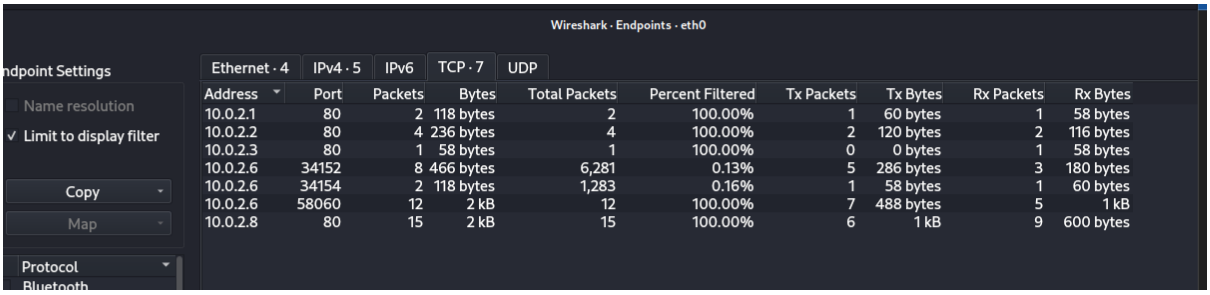
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 80 || udp.port == 80

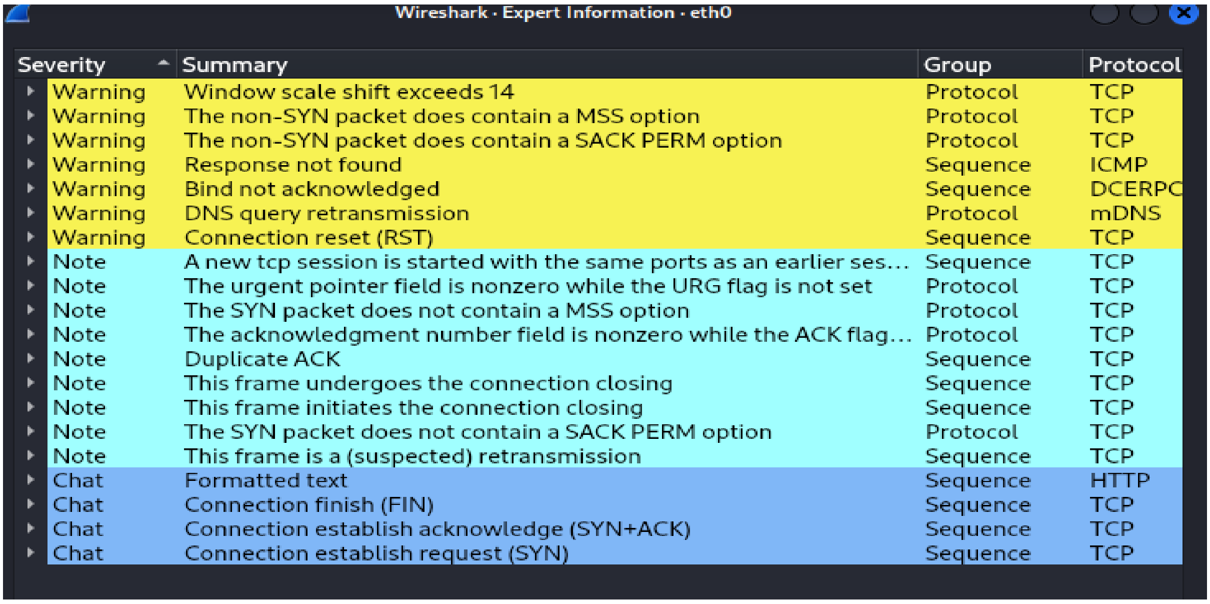
```
No.    Time          Source     Destination  Protocol  Length Info
  835 94.101189796  10.0.2.8   10.0.2.6     TCP         60 80 → 34152 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MS
  836 94.101223938  10.0.2.6   10.0.2.8     TCP         54 34152 → 80 [RST] Seq=1 Win=0 Len=0
  837 94.101347953  10.0.2.1   10.0.2.6     TCP         60 80 → 34152 [RST, ACK] Seq=1 Ack=1 Win=32768 Len=0
 6767 95.174886805  10.0.2.6   10.0.2.2     TCP         58 34154 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 7104 96.104625333  10.0.2.2   10.0.2.6     TCP         60 80 → 34152 [RST, ACK] Seq=1 Ack=1 Win=32768 Len=0
```

```
▸ Internet Protocol Version 4, Src: 10.0.2.2, Dst: 10.0.2.6
▾ Transmission Control Protocol, Src Port: 80, Dst Port: 34154, Seq: 1, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 34154
    [Stream index: 3064]
  ▸ [Conversation completeness: Incomplete (37)]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 38008
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 1831625079
    0101 .... = Header Length: 20 bytes (5)
  ▸ Flags: 0x014 (RST, ACK)
    Window: 32768
    [Calculated window size: 32768]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x2ef2 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▸ [Timestamps]
```

Transmission Control Protocol (tcp), 20 byte(s) | Packets: 10986 · Displayed: 23 (0.2%) · Dropped: 0 (0.0%) | Profile: Default



Address	Port	Packets	Bytes	Total Packets	Percent Filtered	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
10.0.2.1	80	2	118 bytes	2	100.00%	1	60 bytes	1	58 bytes
10.0.2.2	80	4	236 bytes	4	100.00%	2	120 bytes	2	116 bytes
10.0.2.3	80	1	58 bytes	1	100.00%	0	0 bytes	1	58 bytes
10.0.2.6	34152	8	466 bytes	6,281	0.13%	5	286 bytes	3	180 bytes
10.0.2.6	34154	2	118 bytes	1,283	0.16%	1	58 bytes	1	60 bytes
10.0.2.6	58060	12	2 kB	12	100.00%	7	488 bytes	5	1 kB
10.0.2.8	80	15	2 kB	15	100.00%	6	1 kB	9	600 bytes



Severity	Summary	Group	Protocol
Warning	Window scale shift exceeds 14	Protocol	TCP
Warning	The non-SYN packet does contain a MSS option	Protocol	TCP
Warning	The non-SYN packet does contain a SACK PERM option	Protocol	TCP
Warning	Response not found	Sequence	ICMP
Warning	Bind not acknowledged	Sequence	DCERPC
Warning	DNS query retransmission	Protocol	mDNS
Warning	Connection reset (RST)	Sequence	TCP
Note	A new tcp session is started with the same ports as an earlier ses…	Sequence	TCP
Note	The urgent pointer field is nonzero while the URG flag is not set	Protocol	TCP
Note	The SYN packet does not contain a MSS option	Protocol	TCP
Note	The acknowledgment number field is nonzero while the ACK flag…	Protocol	TCP
Note	Duplicate ACK	Sequence	TCP
Note	This frame undergoes the connection closing	Sequence	TCP
Note	This frame initiates the connection closing	Sequence	TCP
Note	The SYN packet does not contain a SACK PERM option	Protocol	TCP
Note	This frame is a (suspected) retransmission	Sequence	TCP
Chat	Formatted text	Sequence	HTTP
Chat	Connection finish (FIN)	Sequence	TCP
Chat	Connection establish acknowledge (SYN+ACK)	Sequence	TCP
Chat	Connection establish request (SYN)	Sequence	TCP

1. Window scale shift exceeds 14
    - Meaning: This could indicate an unusually large TCP window size scaling option. It can be a result of large-scale traffic or misconfiguration.
2. The non-SYN packet does contain a MSS option
    - Meaning: The MSS (Maximum Segment Size) option should typically appear in the SYN packet during the connection establishment phase. Its presence in a non-SYN packet might indicate unusual behavior or misconfiguration.
3. The non-SYN packet does contain a SACK PERM option
    - Meaning: SACK (Selective Acknowledgment) options are typically expected during the SYN phase. If it appears in non-SYN packets, it might indicate protocol violation or packet corruption.
4. Response not found
    - Meaning: Wireshark expected a response to a request, but it didn’t find one. This could indicate packet loss, network issues, or potential security concerns like dropped packets.
5. Bind not acknowledged
    - Meaning: A bind request from a service (like DCE RPC) was not acknowledged by the target, which could indicate a problem with the protocol or network communication.
6. DNS query retransmission
    - Meaning: A DNS query was sent again because the first attempt didn't receive a response, which might indicate network delays or DNS server issues.
7. Connection reset (RST)
    - Meaning: The connection was forcefully closed by one side (via a TCP RST packet). This could be due to errors, protocol violations, or potentially malicious activity like port scanning.

Summary of Findings:

- Protocol Anomalies: Issues such as MSS and SACK appearing in non-SYN packets and window scaling exceeding typical limits may indicate unusual network behavior or misconfigurations.
- Potential Network Issues: Lack of responses to requests, connection resets, and DNS retransmissions suggest potential network reliability problems or even targeted disruption.

1. Traffic Type and Protocols:

   - ✓ TCP Protocol is the primary protocol used, with traffic focusing on port 80 (HTTP). This is a typical web communication port.
   - ✓ Notable flag combinations: SYN (connection initiation) and RST (connection reset). The presence of multiple RST packets indicates that some connections are being forcefully closed, which could point to potential issues like misconfigurations, scanning, or malicious activities.

2. Source and Destination IPs:

   - ✓ Source IPs: The primary source IPs involved are from the 10.0.2.x range, which appears to be an internal network.
   - ✓ Destination IPs: These are also within the 10.0.2.x range, suggesting the traffic is staying within the local network.

3. Suspicious Activities:

   - ✓ RST (Reset) Packets:

     - ▪ Several RST packets are seen in the capture. A TCP RST is typically used to abruptly terminate a connection. Multiple RSTs in a short time may indicate scanning or an attempt to probe open ports.
     - ▪ From the Wireshark Expert Information, it is highlighted that many RST packets are being sent, which might indicate aggressive connection termination or possible port scanning attempts.

   - ✓ SYN-ACK without Completion:

     - ▪ Some SYN-ACK packets are present, but the absence of follow-up ACK packets (to complete the TCP three-way handshake) points to incomplete connections. This is often a sign of SYN scanning, where a host is checking for open ports but not completing the connection.

4. Connection Resets & Packet Drops:

    - ✓ RST Packets:

      Multiple instances of RST packets between 10.0.2.6 and 10.0.2.8 were observed. In a normal scenario, an RST packet should be rare, but here it appears repeatedly, suggesting network instability or malicious activity like SYN flood attacks or port scanning.

    - ✓ Dropped/Incomplete Conversations:

      The expert information indicates that some conversations are incomplete, meaning the expected responses or further communications weren't detected. This could result from packet loss, filtering (e.g., firewalls), or intentional blocking.

5. Flags and Anomalies:

    - ✓ Window Scale Shift:

      A window scale shift exceeds typical limits, possibly indicating large amounts of traffic or misconfigurations in the TCP window size.

    - ✓ MSS and SACK Options in Non-SYN Packets:

      The MSS and SACK options appearing in non-SYN packets is unusual and could indicate protocol misuse or potential issues with network equipment.

Key Indicators of Suspicious Activity:

- ✷ RST Flooding: The excessive number of reset packets could indicate that a system or attacker is trying to close connections abruptly. This could be part of a DoS (Denial of Service) attack or an aggressive port scan.
- ✷ Unsuccessful Connection Attempts: The large number of SYN-ACK packets without finalizing the handshake is typical of SYN scanning, a technique used by attackers to identify open ports.
- ✷ Potential Misconfigurations: The unusual presence of MSS and SACK options and the high window scaling shift might indicate improper network settings, which could also open doors for network exploitation.

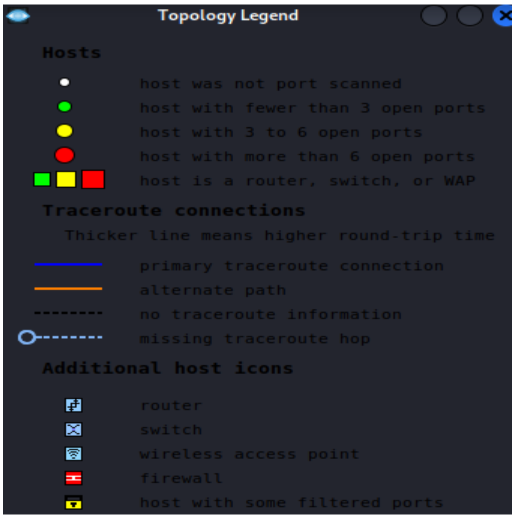
Recommendations:

- Monitor for SYN Scans: Given the behavior, it would be useful to enable logging or alerts for excessive SYN scans to identify the source of this suspicious activity.
- Examine RST Packets: Investigate why so many RST packets are being generated. This could be a sign of unwanted traffic or configuration issues.
- Review Network Configuration: Check the TCP/IP configuration of hosts involved to ensure that settings like window scaling, MSS, and SACK are correctly applied.
- Deploy Intrusion Detection System (IDS): Use IDS tools like Snort or Suricata to detect potential attacks like SYN floods, port scans, or abnormal connection resets.

Network Topology Map

Network topology is the physical and analytical arrangement of nodes and links in a network, often represented in the form of a diagram or a map.

Network topologies define the layout of networks and the relative placement of traffic flows. Using network topology diagrams, admins can efficiently place each node for successful data transmission.



Topology Legend

Hosts

●	host was not port scanned
●	host with fewer than 3 open ports
●	host with 3 to 6 open ports
●	host with more than 6 open ports
🟩 🟨 🟥	host is a router, switch, or WAP

Traceroute connections

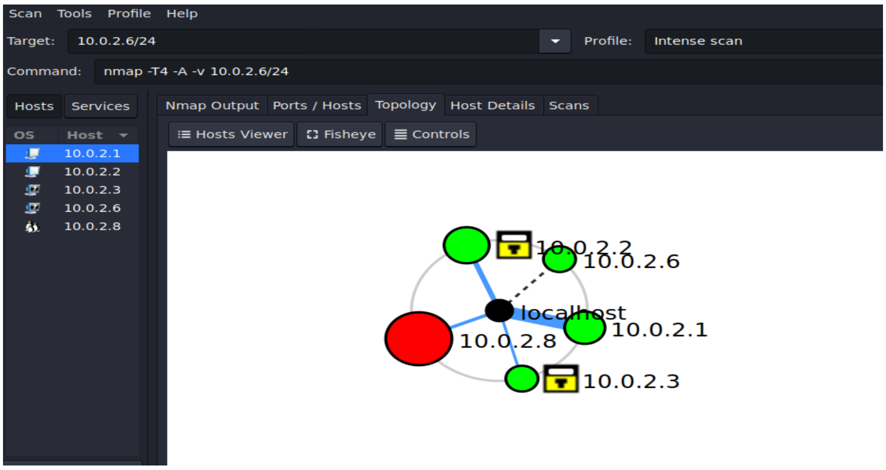
Thicker line means higher round-trip time

———	primary traceroute connection
———	alternate path
--------	no traceroute information
○--------	missing traceroute hop

Additional host icons

▣	router
☒	switch
▣	wireless access point
▣	firewall
▣	host with some filtered ports

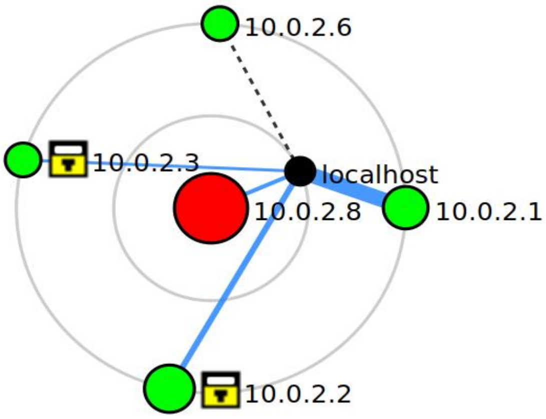
Topology Map symbol representation



Target: 10.0.2.6/24

Profile: Intense scan

Command: nmap -T4 -A -v 10.0.2.6/24



Safety Measures

- ✓ **Keep Systems and Software Updated**: Make sure all systems, applications, and security tools are always updated with the latest security patches to reduce the risk of vulnerabilities.
- ✓ **Network Segmentation**: Separate critical systems from less important parts of the network. This limits the chances of an attack spreading if a vulnerability is exploited.
- ✓ **Strong Authentication and Access Control**: Use strong authentication methods like multi-factor authentication (MFA) and control who can access systems. Regularly review and update user permissions to follow the "least privilege" principle, meaning users should only have access to what they need.
- ✓ **Regular Vulnerability Checks**: Regularly perform vulnerability scans to find and fix weaknesses in the network. Tools like Nmap, Nikto, and OpenVAS can help spot vulnerabilities.
- ✓ **Intrusion Detection and Prevention**: Set up systems (IDS/IPS) that can detect and stop suspicious network activity. Ensure these systems send alerts for quick response.

- ✓ **Data Encryption**: Protect sensitive data by encrypting it both when it's being transferred and when it's stored. This helps prevent unauthorized access.
- ✓ **Incident Response Plan**: Create and maintain a plan for how to respond if a security breach happens. Regularly practice the plan to make sure the team is ready.
- ✓ **Employee Training**: Train employees on basic cybersecurity practices and the risks of social engineering (tricking people to reveal information). Regular training helps reinforce safe behaviors.
- ✓ **Logging and Monitoring**: Keep detailed logs of network traffic and system activity. Regularly check these logs, especially after major updates or changes, to spot anything unusual.

Conclusion

The tasks performed during this network analysis and vulnerability assessment gave a clear picture of the network's security. Tools like Nmap, Nikto, OpenVAS, and Wireshark helped identify active devices, open services, and vulnerabilities that need attention. The assessment found several weaknesses, such as outdated software, misconfigurations, and weak access controls, which could be exploited by attackers.

Fixing these vulnerabilities by updating systems, separating networks, using strong authentication, and monitoring regularly will improve security standards. Adding regular vulnerability scans, training employees, and having a solid incident response plan will further reduce the chance of future attacks.

This analysis provided valuable insights and recommendations, helping to create a stronger and safer network.

THANK YOU

Report by:

SriRam Leburi

Contact: 8978715891

Linkedin: www.linkedin.com/in/sriram-leburi-840085215

Date: 05/09/2024