Penetration reconnaissance testing in metasploitable - 4geeks

Carlos Duclaud

Objective:
To conduct a comprehensive security assessment of the Metasploit virtual machine, including enumeration of target services, collection of system information, identification of open ports, and execution of a vulnerability scan to identify potential security weaknesses.

Scope:
The scope of this engagement includes the reconnaissance and scanning of the target system to identify potential vulnerabilities, gather system information, enumerate active services, and assess security weaknesses.

Tools Used for Analysis:
The tools utilized for this assessment include Kali Linux for its comprehensive suite of penetration testing tools, and Nmap for network discovery, port scanning, and service enumeration.

ANALYSIS 3 most dangerous vulnerabilities:

1. vsFTPd 2.3.4 Backdoor (CVE-2011-2523):
   - Port: 21 (FTP)
   - Impact: Critical. Full system compromise due to remote command execution.
   - Reference: CVE-2011-2523
   - Description: This vulnerability exists in vsFTPd version 2.3.4, where a backdoor was introduced that allows remote attackers to gain root access to the server. It enables attackers to execute arbitrary commands with root privileges.

2. RMI Registry Remote Code Execution (CVE-2010-4476)
   - Port: 1099 (RMI Registry)
   - Impact: Critical. Remote code execution on the affected system, which could lead to full compromise.
   - Reference: Metasploit Module for RMI Registry
   - Description: The default configuration of the RMI registry allows classes to be loaded from remote URLs. An attacker can exploit this flaw to load arbitrary classes, potentially leading to remote code execution.

3. SSL/TLS Vulnerabilities (Weak DH Group & POODLE)
   - Port: 443 (SSL/TLS)
   - Impact: Both of these SSL/TLS vulnerabilities put encrypted traffic at risk, allowing attackers to potentially intercept sensitive information, decrypt it, or conduct man-in-the-middle (MITM) attacks.
   - References: Weak DH Group, POODLE CVE-2014-3566
   - Description: Weak DH Group (CVE-2016-0800): The Diffie-Hellman key exchange uses weak parameters (Group 1), making the connection vulnerable to passive eavesdropping attacks. POODLE (CVE-2014-3566): SSL 3.0 is vulnerable to padding oracle attacks, allowing an attacker to decrypt parts of the encrypted communication.

Mitigation strategy based on the vulnerabilities and open ports encountered in the scans

Patch OS and Services
- Update the system to a supported version of Linux.
- Enable automatic updates for security patches.

Close Unnecessary Ports
- Block unused ports (FTP, Telnet, NFS, etc.) using a firewall.
- Restrict access to critical ports (SSH, MySQL, PostgreSQL).

Use Strong Authentication and Encryption
- Replace Telnet with SSH.
- Use SSL/TLS for SMTP, HTTP, and MySQL.
- Use SFTP instead of FTP for secure file transfers.

Harden SMB and Network Shares
- Disable SMB if not needed.
- Enable SMB message signing.
- Limit SMB access to trusted networks only.

Limit User Privileges
- Use the principle of least privilege for user access.
- Disable unnecessary services (exec, login, shell).

Secure Database Services
- Restrict MySQL/PostgreSQL to local-only access.
- Use strong passwords and encryption for database connections.

Disable Unnecessary or Unknown Services
- Investigate and disable unknown services.
- Audit services regularly to ensure only necessary ones are running.

Improve Time Synchronization and Logging
- Sync system time using NTP.
- Enable logging and secure log storage.

Conduct Regular Security Audits
- Regularly scan for vulnerabilities using tools like Nessus or OpenVAS.
- Perform internal and external penetration testing.

Implement IDS/IPS
- Deploy an Intrusion Detection/Prevention System (e.g., Snort, Suricata).
- Consider using honeypots to detect malicious activity.

Summary of the system info:

Host: 192.168.1.12 (reachable with 0.0016s latency)
Device Type: General-purpose device
Operating System: Linux 2.6.X (specifically, Linux kernel versions 2.6.9 to 2.6.33)
MAC Address: 08:00:27:D5:A7:85 (Oracle VirtualBox NIC)
NetBIOS Name: METASPLOITABLE
SMB Info:
Protocol: SMB2 (with some issues during negotiation)
Message Signing: Disabled (which is risky)
SMB OS: Samba 3.0.20-Debian
Host Name: metasploitable.localdomain
Account: No account used; authentication set to “user” level
System Time: 2025-04-12, 00:23:15 (timezone: EDT)
Traceroute: 1 hop to 192.168.1.12 (RTT: 1.57 ms)

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-12 00:20 EDT
Nmap scan report for 192.168.1.12
Host is up (0.0016s latency).
Not shown: 977 closed tcp ports (reset)

MAC Address: 08:00:27:D5:A7:85 (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 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE:
cpe:/o:linux:linux_kernel

Host script results:
| _clock-skew: mean: 1h19m59s, deviation: 2h18m34s, median: 0s
| _nbstat: NetBIOS name: METASPLOITABLE
| _smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2025-04-12T00:23:15-04:00

TRACEROUTE
HOP RTT     ADDRESS
1   1.57 ms 192.168.1.12
```

Summary of the full port scan:

Host: 192.168.1.12 (up with 0.00093s latency)
Open Ports: 22 open ports in total:
Common Services:
FTP (21), SSH (22), Telnet (23), SMTP (25), HTTP (80), RPCBind (111)
NetBIOS (139), Microsoft DS (445), MySQL (3306), PostgreSQL (5432), VNC (5900)
IRC (6667), AJP13 (8009), X11 (6000), and others (like NFS, distccd, msgsrvr)
Uncommon Services: Several unknown services on ports 8180, 38728, 48772, 58693, and 59207
MAC Address: 08:00:27:D5:A7:85 (Oracle VirtualBox NIC)

The system has a large number of open ports, including services like FTP, SSH, MySQL, PostgreSQL, and VNC, which could be potential entry points. Some ports also run obscure or unknown services.

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-12 00:49 EDT
Nmap scan report for 192.168.1.12
Host is up (0.00093s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
38728/tcp open  unknown
48772/tcp open  unknown
58693/tcp open  unknown
59207/tcp open  unknown
MAC Address: 08:00:27:D5:A7:85 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 70.39 seconds
```

Based on Nmap results, here's a brief analysis of the vulnerabilities found across the system:

1. vsFTPd 2.3.4 Backdoor (CVE-2011-2523)

Port: 21 (FTP)
Risk: High. The vsFTPd version 2.3.4 contains a backdoor allowing remote command execution with root privileges.
Exploit: Remote code execution via FTP service (testable with commands like id).
Fix: Upgrade vsFTPd to a patched version.

2. RMI Registry Remote Code Execution (CVE-XXXX-XXXX)

Port: 1099 (RMI)
Risk: High. The RMI registry's default configuration allows remote code execution by loading malicious classes from remote URLs.
Exploit: Potential for a remote attacker to execute arbitrary code.
Fix: Disable class loading from remote URLs or configure RMI registry securely.

3. SSL/TLS Vulnerabilities

Port: Multiple (443, 3306, 5432, etc.)
Weak DH Group (CVE-XXXX-XXXX): Uses weak Diffie-Hellman groups susceptible to passive eavesdropping.
CCS Injection (CVE-2014-0224): MITM vulnerability that allows attackers to hijack sessions.
POODLE (CVE-2014-3566): Vulnerable to a padding oracle attack allowing cleartext data leakage.
Risk: Medium to High. These vulnerabilities could allow attackers to intercept sensitive information or hijack secure sessions.
Fix: Update OpenSSL to a version patched for these issues and disable SSL 3.0.

4. XSS and CSRF Vulnerabilities

Port: 80 (HTTP)
Cross-Site Request Forgery (CSRF): Forms on various paths like /dvwa/login.php, /twiki/TWikiDocumentation.html, and /mutillidae/index.php are susceptible to CSRF, allowing an attacker to perform actions on behalf of a user.
XSS: No stored XSS found, but other potential XSS issues were identified.
Risk: Medium. CSRF could allow unauthorized actions without user consent, while XSS may expose users to malicious scripts.
Fix: Implement CSRF tokens in forms and sanitize user input to prevent XSS.

5. UnrealIRCd Backdoor

Port: 6667 (IRC)
Risk: High. The UnrealIRCd service is likely compromised, exposing the system to a backdoor.
Exploit: Remote attackers may gain unauthorized access via this backdoor.
Fix: Replace the trojaned UnrealIRCd with a clean, patched version.

6. Missing HttpOnly Flag in Cookies

Port: 80 (HTTP)
Risk: Low. The absence of the HttpOnly flag in cookies makes them vulnerable to theft via client-side scripts.
Fix: Add the HttpOnly flag to cookies to mitigate this risk.

7. Weak Authentication and Exposed Admin Folders

Port: 80 (HTTP)
Admin Folders: Potentially exposed admin pages, like /admin/ and /admin/login.html, may allow unauthorized access to sensitive functions.
Fix: Secure these pages with proper authentication and restrict access.

8. NFS and SMB Vulnerabilities

Port: 2049 (NFS), 445 (Microsoft-DS)
Risk: Medium. Exposed NFS and SMB services can be exploited for unauthorized access to shared files or resources.
Fix: Restrict access to these services through firewalls or VPNs.

9. SQL Injection

Port: 80 (HTTP)
Risk: Medium. Several URLs were identified as potentially vulnerable to SQL Injection, particularly in /dav/?C=S%3BO%3DA%27 OR sqlspider.
Fix: Implement prepared statements and proper input validation to prevent SQL injection.

10. HTTP TRACE Method

Port: 80 (HTTP)
Risk: Low. The TRACE HTTP method can be exploited to gather information about HTTP headers, potentially revealing sensitive data like cookies.

Complete nmap vulnerability scan results

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-12 00:25 EDT
Nmap scan report for 192.168.1.12
Host is up (0.0011s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  BID:48539  CVE:CVE-2011-2523
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.
html
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/
ftp/vsftpd_234_backdoor.rb
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|_      https://www.securityfocus.com/bid/48539
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
|_http-trace: TRACE is enabled
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.1.12
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://192.168.1.12:80/dvwa/
|     Form id:
|     Form action: login.php
|
|     Path: http://192.168.1.12:80/twiki/TWikiDocumentation.html
|     Form id:
|     Form action: http://TWiki.org/cgi-bin/passwd/TWiki/WebHome
|
|     Path: http://192.168.1.12:80/twiki/TWikiDocumentation.html
|     Form id:
|     Form action: http://TWiki.org/cgi-bin/passwd/Main/WebHome
|
|     Path: http://192.168.1.12:80/twiki/TWikiDocumentation.html
|     Form id:
|     Form action: http://TWiki.org/cgi-bin/edit/TWiki/
|
|     Path: http://192.168.1.12:80/twiki/TWikiDocumentation.html
|     Form id:
|     Form action: http://TWiki.org/cgi-bin/view/TWiki/TWikiSkins
|
|     Path: http://192.168.1.12:80/twiki/TWikiDocumentation.html
|     Form id:
|     Form action: http://TWiki.org/cgi-bin/manage/TWiki/ManagingWebs
|
|     Path: http://192.168.1.12:80/dvwa/login.php
|     Form id:
|_    Form action: login.php
| http-fileupload-exploiter:
|
|_    Couldn't find a file-type field.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-sql-injection:
|   Possible sqli for queries:
|     http://192.168.1.12:80/dav/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.1.12:80/dav/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.1.12:80/dav/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.1.12:80/dav/?C=N%3BO%3DD%27%20OR%20sqlspider
|     http://192.168.1.12:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.
php%27%20OR%20sqlspider
|     http://192.168.1.12:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspi-
der
```

| http://192.168.1.12:80/mutillidae/index.php?do=toggle-security%27%20OR%20sqlspider&page=home.php
| http://192.168.1.12:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
| http://192.168.1.12:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
| http://192.168.1.12:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
| http://192.168.1.12:80/mutillidae/?page=login.php%27%20OR%20sqlspider
| http://192.168.1.12:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
| http://192.168.1.12:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
| http://192.168.1.12:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
| http://192.168.1.12:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
| http://192.168.1.12:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
| http://192.168.1.12:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
| http://192.168.1.12:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
| http://192.168.1.12:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
| http://192.168.1.12:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
| http://192.168.1.12:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
| http://192.168.1.12:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
| http://192.168.1.12:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
| http://192.168.1.12:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
| http://192.168.1.12:80/mutillidae/index.php?page=php-errors.php%27%20OR%20sqlspider
| http://192.168.1.12:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
| http://192.168.1.12:80/mutillidae/index.php?page=usage-instructions.php%27%20OR%20sqlspider
| http://192.168.1.12:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider
| http://192.168.1.12:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
| http://192.168.1.12:80/mutillidae/index.php?page=notes.php%27%20OR%20sqlspider
| http://192.168.1.12:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
| http://192.168.1.12:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
| http://192.168.1.12:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
| http://192.168.1.12:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
| http://192.168.1.12:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
| http://192.168.1.12:80/mutillidae/index.php?username=anonymous&page=password-generator.php%27%20OR%20sqlspider
| http://192.168.1.12:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
| http://192.168.1.12:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
| http://192.168.1.12:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
| http://192.168.1.12:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
| http://192.168.1.12:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
| http://192.168.1.12:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
| http://192.168.1.12:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
| http://192.168.1.12:80/mutillidae/index.php?do=toggle-hints%27%20OR%20sqlspider&page=home.php
| http://192.168.1.12:80/rdiff/TWiki/TWikiHistory?rev2=1.7%27%20OR%20sqlspider&rev1=1.8
| http://192.168.1.12:80/rdiff/TWiki/TWikiHistory?rev2=1.7&rev1=1.8%27%20OR%20sqlspider
| http://192.168.1.12:80/view/TWiki/TWikiHistory?rev=1.7%27%20OR%20sqlspider
| http://192.168.1.12:80/rdiff/TWiki/TWikiHistory?rev2=1.9%27%20OR%20sqlspider&rev1=1.10
| http://192.168.1.12:80/rdiff/TWiki/TWikiHistory?rev2=1.9&rev1=1.10%27%20OR%20sqlspider
| http://192.168.1.12:80/view/TWiki/TWikiHistory?rev=1.9%27%20OR%20sqlspider
| http://192.168.1.12:80/oops/TWiki/TWikiHistory?param1=1.10%27%20OR%20sqlspider&template=oopsrev
| http://192.168.1.12:80/oops/TWiki/TWikiHistory?param1=1.10&template=oopsrev%27%20OR%20sqlspider
| http://192.168.1.12:80/rdiff/TWiki/TWikiHistory?rev2=1.8%27%20OR%20sqlspider&rev1=1.9
| http://192.168.1.12:80/rdiff/TWiki/TWikiHistory?rev2=1.8&rev1=1.9%27%20OR%20sqlspider
| http://192.168.1.12:80/view/TWiki/TWikiHistory?rev=1.8%27%20OR%20sqlspider
| http://192.168.1.12:80/rdiff/TWiki/TWikiHistory?rev2=1.8%27%20OR%20sqlspider&rev1=1.9
| http://192.168.1.12:80/rdiff/TWiki/TWikiHistory?rev2=1.8&rev1=1.9%27%20OR%20sqlspider
| http://192.168.1.12:80/view/TWiki/TWikiHistory?rev=1.9%27%20OR%20sqlspider

```
|      http://192.168.1.12:80/view/TWiki/TWikiHistory?rev=1.7%27%20OR%20sqlspider
|      http://192.168.1.12:80/rdiff/TWiki/TWikiHistory?rev2=1.7%27%20OR%20sqlspi-
der&rev1=1.8
|      http://192.168.1.12:80/rdiff/TWiki/TWikiHistory?rev2=1.7&rev1=1.8%27%20OR%20sqlspi-
der
|      http://192.168.1.12:80/view/TWiki/TWikiHistory?rev=1.8%27%20OR%20sqlspider
|      http://192.168.1.12:80/oops/TWiki/TWikiHistory?param1=1.10%27%20OR%20sqlspider&tem-
plate=oopsrev
|      http://192.168.1.12:80/oops/TWiki/TWikiHistory?param1=1.10&template=oopsrev%27%20
OR%20sqlspider
|      http://192.168.1.12:80/rdiff/TWiki/TWikiHistory?rev2=1.9%27%20OR%20sqlspi-
der&rev1=1.10
|      http://192.168.1.12:80/rdiff/TWiki/TWikiHistory?rev2=1.9&rev1=1.10%27%20OR%20sqlspi-
der
|      http://192.168.1.12:80/dav/?C=M%3BO%3DA%27%20OR%20sqlspider
|      http://192.168.1.12:80/dav/?C=D%3BO%3DA%27%20OR%20sqlspider
|      http://192.168.1.12:80/dav/?C=S%3BO%3DD%27%20OR%20sqlspider
|      http://192.168.1.12:80/dav/?C=N%3BO%3DA%27%20OR%20sqlspider
|      http://192.168.1.12:80/dav/?C=M%3BO%3DD%27%20OR%20sqlspider
|      http://192.168.1.12:80/dav/?C=D%3BO%3DA%27%20OR%20sqlspider
|      http://192.168.1.12:80/dav/?C=N%3BO%3DA%27%20OR%20sqlspider
|      http://192.168.1.12:80/dav/?C=S%3BO%3DA%27%20OR%20sqlspider
|      http://192.168.1.12:80/dav/?C=S%3BO%3DA%27%20OR%20sqlspider
|      http://192.168.1.12:80/dav/?C=M%3BO%3DA%27%20OR%20sqlspider
|      http://192.168.1.12:80/dav/?C=D%3BO%3DD%27%20OR%20sqlspider
|      http://192.168.1.12:80/dav/?C=N%3BO%3DA%27%20OR%20sqlspider
|      http://192.168.1.12:80/dav/?C=S%3BO%3DA%27%20OR%20sqlspider
|      http://192.168.1.12:80/dav/?C=M%3BO%3DA%27%20OR%20sqlspider
|      http://192.168.1.12:80/dav/?C=D%3BO%3DA%27%20OR%20sqlspider
|_     http://192.168.1.12:80/dav/?C=N%3BO%3DA%27%20OR%20sqlspider
| http-enum:
|   /tikiwiki/: Tikiwiki
|   /test/: Test page
|   /phpinfo.php: Possible information file
|   /phpMyAdmin/: phpMyAdmin
|   /doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) dav/2'
|   /icons/: Potentially interesting folder w/ directory listing
|_  /index/: Potentially interesting folder
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
| rmi-vuln-classloader:
|   VULNERABLE:
|   RMI registry default configuration remote code execution vulnerability
|     State: VULNERABLE
|       Default configuration of RMI registry allows loading classes from remote URLs
which can lead to remote code execution.
|
|     References:
|_      https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/
misc/java_rmi_server.rb
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
| 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: Unknown/Custom-generated
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1024
|     References:
|_      https://weakdh.org
| 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.openssl.org/news/secadv_20140605.txt
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
|_      http://www.cvedetails.com/cve/2014-0224
| 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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|       https://www.openssl.org/~bodo/ssl-poodle.pdf
|       https://www.securityfocus.com/bid/70574
|_      https://www.imperialviolet.org/2014/10/14/poodle.html
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
|_irc-unrealircd-backdoor: Looks like trojaned version of unrealircd. See http://seclists.
org/fulldisclosure/2010/Jun/277
8009/tcp open  ajp13
8180/tcp open  unknown
| http-cookie-flags:
|   /admin/:
|     JSESSIONID:
|       httponly flag not set
|   /admin/index.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/login.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/admin.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/account.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/admin_login.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/home.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/admin-login.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/adminLogin.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/controlpanel.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/cp.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/index.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/login.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/admin.jsp:
|     JSESSIONID:
|       httponly flag not set
```

```
|     /admin/home.jsp:
|       JSESSIONID:
|         httponly flag not set
|     /admin/controlpanel.jsp:
|       JSESSIONID:
|         httponly flag not set
|     /admin/admin-login.jsp:
|       JSESSIONID:
|         httponly flag not set
|     /admin/cp.jsp:
|       JSESSIONID:
|         httponly flag not set
|     /admin/account.jsp:
|       JSESSIONID:
|         httponly flag not set
|     /admin/admin_login.jsp:
|       JSESSIONID:
|         httponly flag not set
|     /admin/adminLogin.jsp:
|       JSESSIONID:
|         httponly flag not set
|     /admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html:
|       JSESSIONID:
|         httponly flag not set
|     /admin/includes/FCKeditor/editor/filemanager/upload/test.html:
|       JSESSIONID:
|         httponly flag not set
|     /admin/jscript/upload.html:
|       JSESSIONID:
|_        httponly flag not set
| http-enum:
|   /admin/: Possible admin folder
|   /admin/index.html: Possible admin folder
|   /admin/login.html: Possible admin folder
|   /admin/admin.html: Possible admin folder
|   /admin/account.html: Possible admin folder
|   /admin/admin_login.html: Possible admin folder
|   /admin/home.html: Possible admin folder
|   /admin/admin-login.html: Possible admin folder
|   /admin/adminLogin.html: Possible admin folder
|   /admin/controlpanel.html: Possible admin folder
|   /admin/cp.html: Possible admin folder
|   /admin/index.jsp: Possible admin folder
|   /admin/login.jsp: Possible admin folder
|   /admin/admin.jsp: Possible admin folder
|   /admin/home.jsp: Possible admin folder
|   /admin/controlpanel.jsp: Possible admin folder
|   /admin/admin-login.jsp: Possible admin folder
|   /admin/cp.jsp: Possible admin folder
|   /admin/account.jsp: Possible admin folder
|   /admin/admin_login.jsp: Possible admin folder
|   /admin/adminLogin.jsp: Possible admin folder
|   /manager/html/upload: Apache Tomcat (401 Unauthorized)
|   /manager/html: Apache Tomcat (401 Unauthorized)
|   /admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html: OpenCart/
FCKeditor File upload
|   /admin/includes/FCKeditor/editor/filemanager/upload/test.html: ASP Simple Blog /
FCKeditor File Upload
|   /admin/jscript/upload.html: Lizard Cart/Remote File upload
|_  /webdav/: Potentially interesting folder
MAC Address: 08:00:27:D5:A7:85 (Oracle VirtualBox virtual NIC)

Host script results:
| _smb-vuln-ms10-061: false
| _smb-vuln-ms10-054: false
| _smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)

Nmap done: 1 IP address (1 host up) scanned in 337.80 seconds
```