Network Pentesting

1. **FTP (21)**

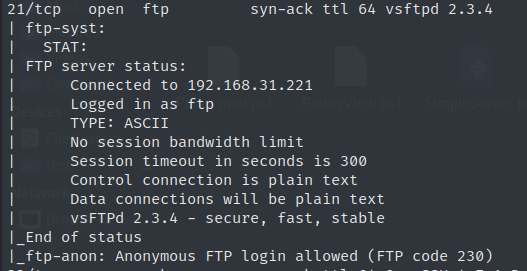
**Description:**

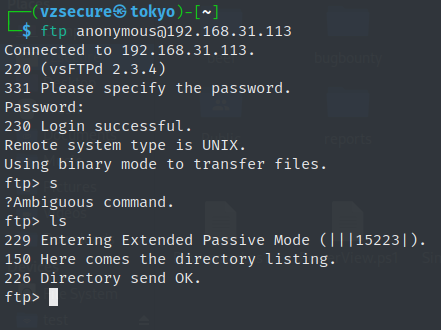
Anonymous File Transfer Protocol (FTP) enables remote users to use the FTP server without an assigned user ID and password. Anonymous FTP enables unprotected access (no password required) to selected information about a remote system. The remote site determines what information is made available for general access. Such information is considered to be publicly accessible and can be read by anyone. It is the responsibility of the person who owns the information and the system to assure that only appropriate information is made available.

**CVE-ID**: CVE-1999-0497

**CVE SCORE:** MEDIUM

**SCREENSHOTS:**





**REFERENCE:**

https://exchange.xforce.ibmcloud.com/vulnerabilities/543

**SOLUTION:**

In order to secure from anonymous login for FTP perform the following steps:

1. Open the FTP config file.
2. Set anonymous\_enable=NO
3. Restart the FTP service.
4. **SSH (22)**

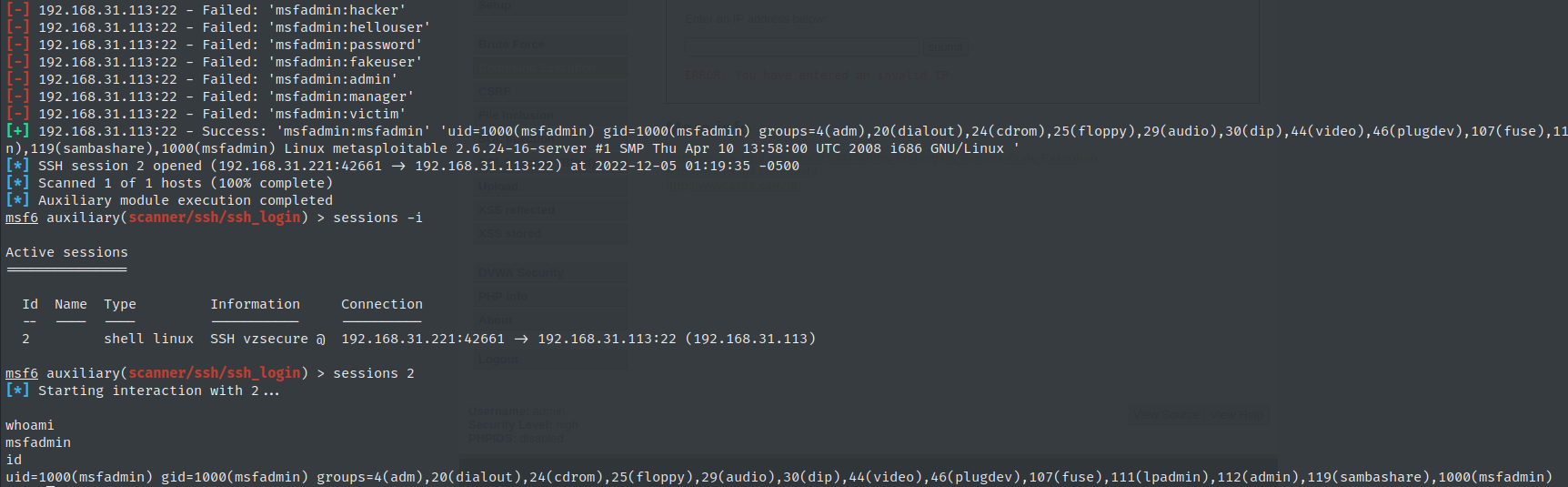
**Description:**

The weak password on the web user interface can be exploited via HTTP or HTTPS. Once such access has been obtained, the other passwords can be changed. The weak password on Linux accounts can be accessed via SSH or Telnet, the former of which is by default enabled on trusted interfaces. While the SSH service does not support root login, a user logging in using either of the other Linux accounts may elevate to root access using the su command if they have access to the associated password.

**CVE-ID**: CWE-521

**CVE SCORE:** CRITICAL

**SCREENSHOTS:**

****

**REFERENCE:**

https://cwe.mitre.org/data/definitions/521.html

**SOLUTION:**

Below are some solutions to prevent to get remote access of SSH:

1. Set Custom SSH port.
2. Using TCP wrappers
3. Filter the SSH port on your firewall
4. Disable Root Login
5. Strong passwords/passphrase for SSH users and keys

**3. TELNET (23)**

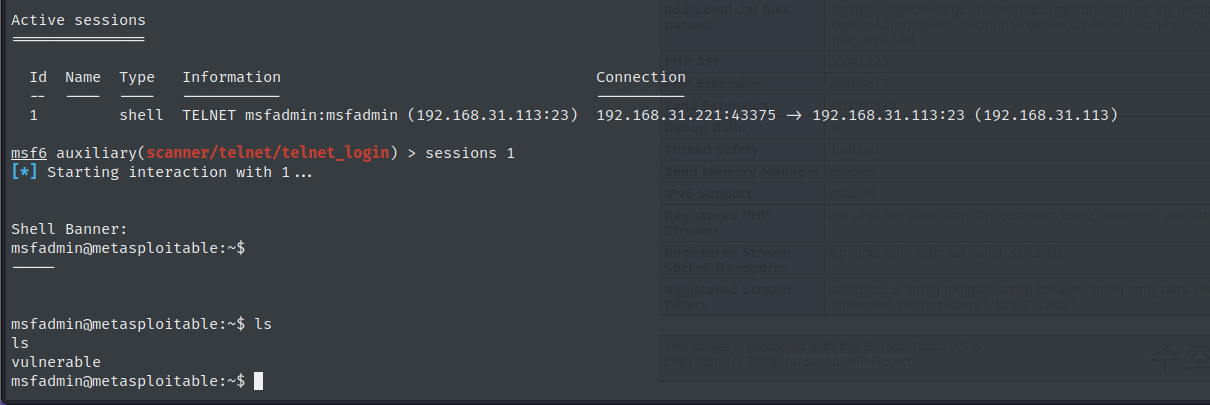
**Description:**

The weak password on the web user interface can be exploited via HTTP or HTTPS. Once such access has been obtained, the other passwords can be changed. The weak password on Linux accounts can be accessed via SSH or Telnet, the former of which is by default enabled on trusted interfaces. While the SSH service does not support root login, a user logging in using either of the other Linux accounts may elevate to root access using the su command if they have access to the associated password.

**CVE-ID**: CWE-521

**CVE SCORE:** CRITICAL

**SCREENSHOTS:**



**REFERENCE:**

https://cwe.mitre.org/data/definitions/521.html

**SOLUTION:**

Below are some solutions for prevention of attack:

1. Disable Telnet login if not in use.
2. Filter Telnet port on Firewall.
3. Set strong password.

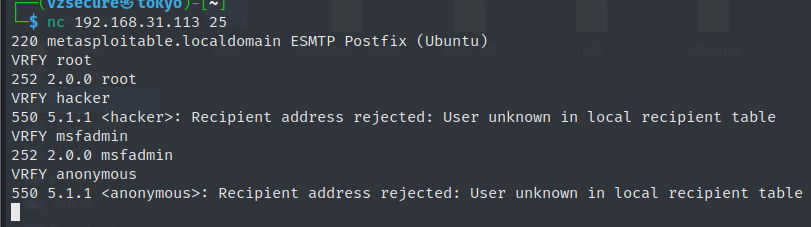
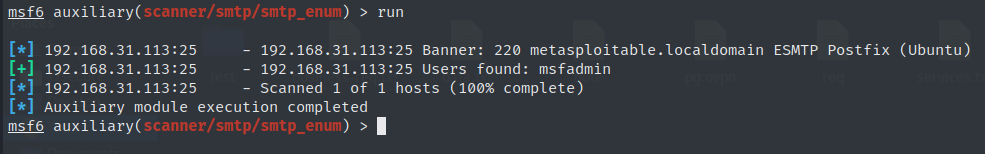
**4.SMTP (25)**

**Description:**

The SMTP service has two internal commands that allow the enumeration of users: VRFY (confirming the names of valid users) and EXPN (which reveals the actual address of user’s aliases and lists of e-mail (mailing lists)). Through the implementation of these SMTP commands can reveal a list of valid users.

**CVE-ID**: CVE-1999-0531

**CVE SCORE:** HIGH

**SCREENSHOTS:**

**REFERENCE:**

https://www.infosecmatter.com/metasploit-module-library/?mm=auxiliary/scanner/smtp/smtp\_enum

**SOLUTION:**

This functionality should be disabled, because these commands can be used for attack reconnaissance.

**5.HTTP (82)**

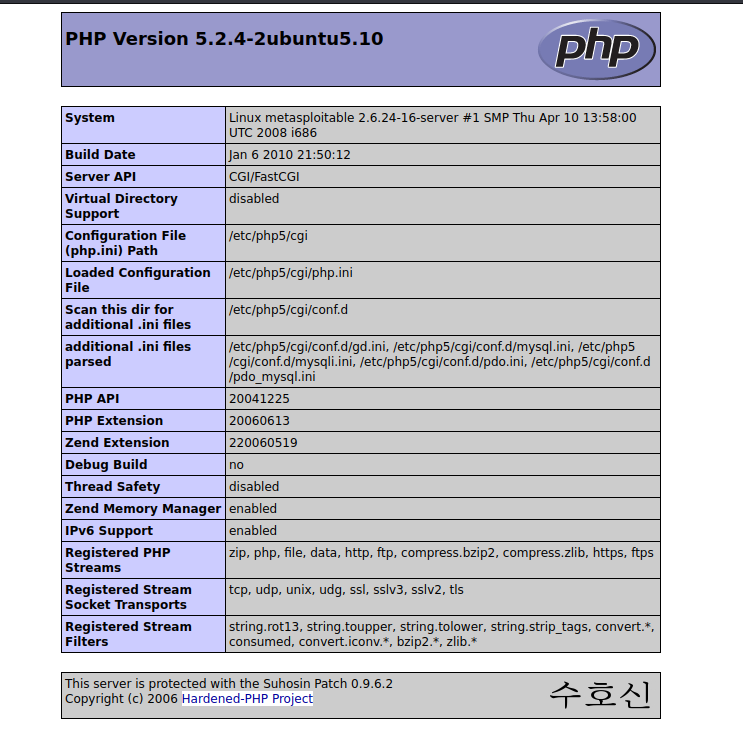
**Description:**

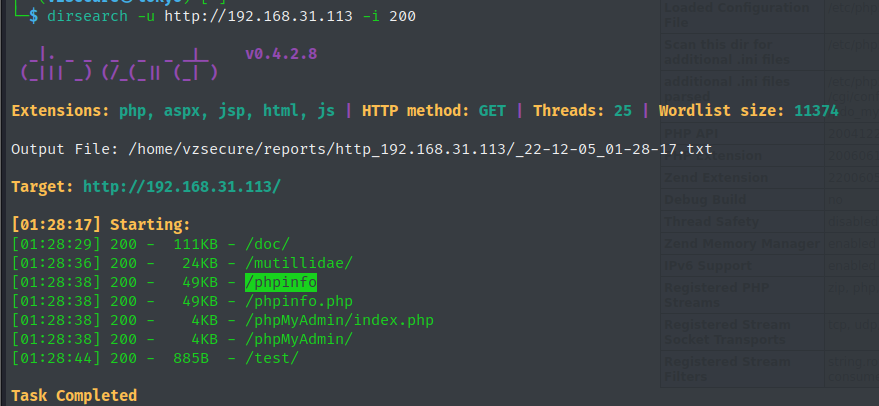
sapi/cgi/cgi\_main.c in PHP before 5.3.12 and 5.4.x before 5.4.2, when configured as a CGI script (aka php-cgi), does not properly handle query strings that lack an = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of skipping a certain php\_getopt for the 'd' case.

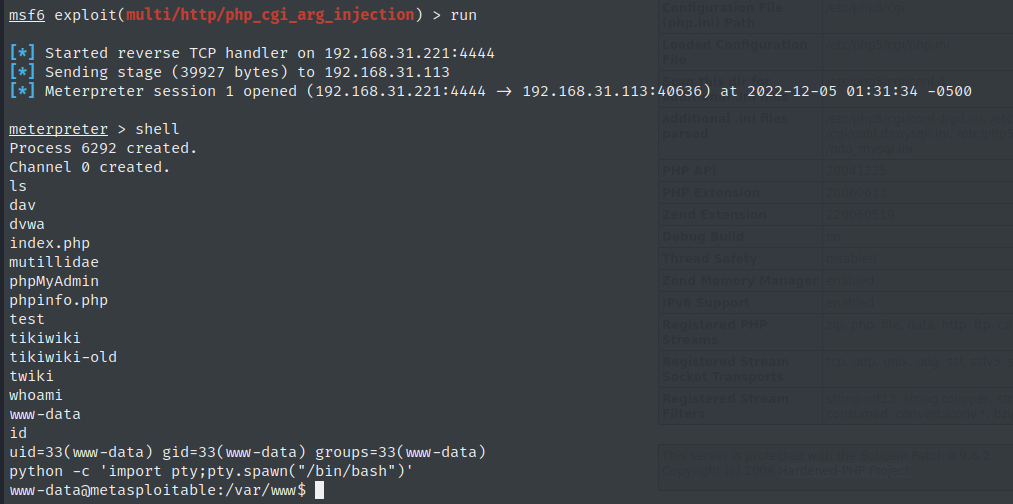
**CVE-ID**: CVE-2012-1823

**CVE SCORE:** HIGH

**SCREENSHOTS:**







**REFERENCE:**

<http://www.kb.cert.org/vuls/id/520827>

**SOLUTION:**

PHP is recommending that users upgrade to the latest version of PHP. PHP has stated, PHP 5.3.12/5.4.2 do not fix all variations of the CGI issues described in CVE-2012-1823. It has also come to our attention that some sites use an insecure cgiwrapper script to run PHP.

**6.BINDSHELL (1524)**

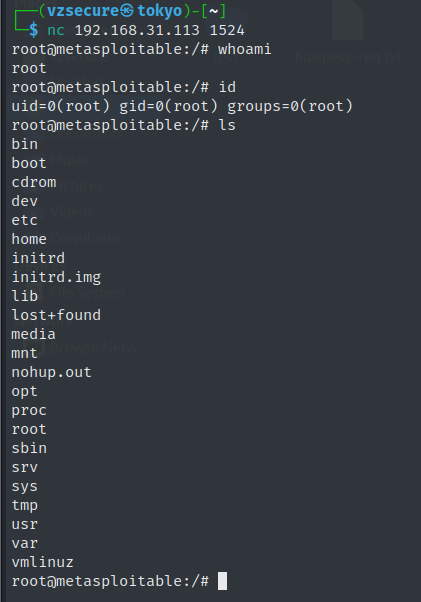
**Description:**

A bind shell is a type of shell, which, upon execution, actively listens for connections on a particular port. The attacker can then connect to this port in order to get shell access.

**CVE-ID**: NONE

**CVE SCORE:** HIGH

**SCREENSHOTS:**

****

**REFERENCE:** N/A

**SOLUTION:**

Verify if the remote host has been compromised, and reinstall the system if necessary.

**7.JAVA-RMI (1099)**

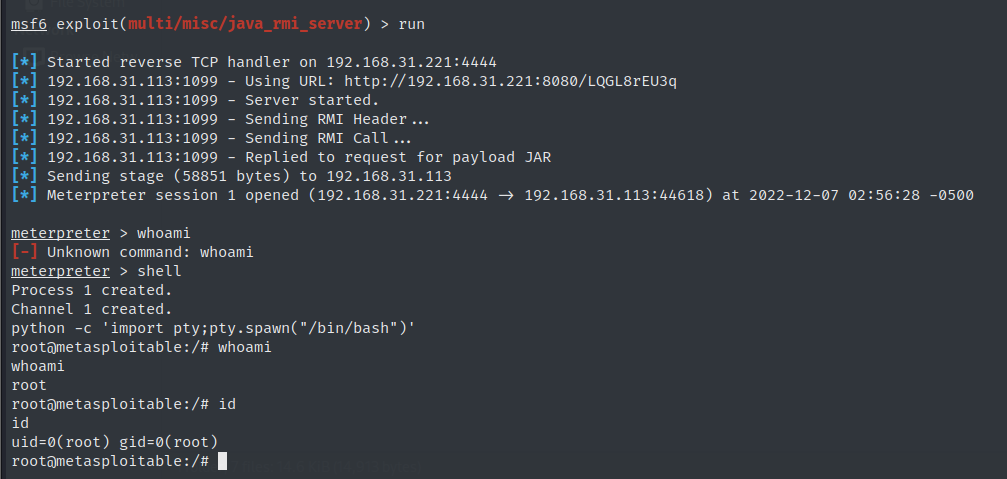
**Description:**

The Java Remote Method Invocation, or Java RMI, is a mechanism that allows an object that exists in one Java virtual machine to access and call methods that are contained in another Java virtual machine; This is basically the same thing as a RPC, but in an object-oriented paradigm instead of a procedural one, which allows for communication between Java programs that are not in the same address space. The Vulnerability is due to the default configuration of the RMI Registry and RMI Activation Services allowing the loading of classes from a remote URL.

**CVE-ID**: CVE-2020-5327

**CVE SCORE:** CRITICAL

**SCREENSHOTS:**



**REFERENCE:** https://www.dell.com/support/article/SLN320536

**SOLUTION:**

The Java RMI class loader exploit is resolved in Java 7.21, where the RMI property java.rmi.server.useCodebaseOnly defaults to true by default. Upgrade the current Java version used by Open Edge to the later supported version update.

**8.MY-SQL (3306)**

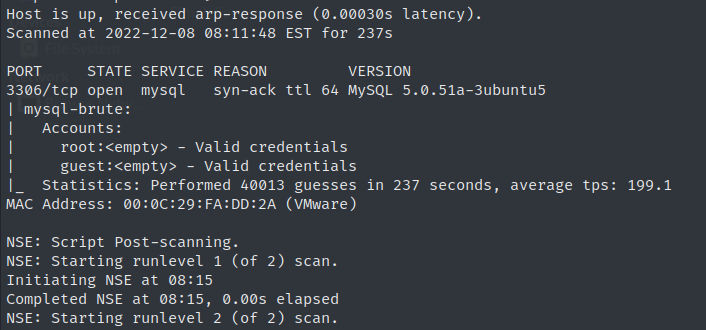
**Description:**

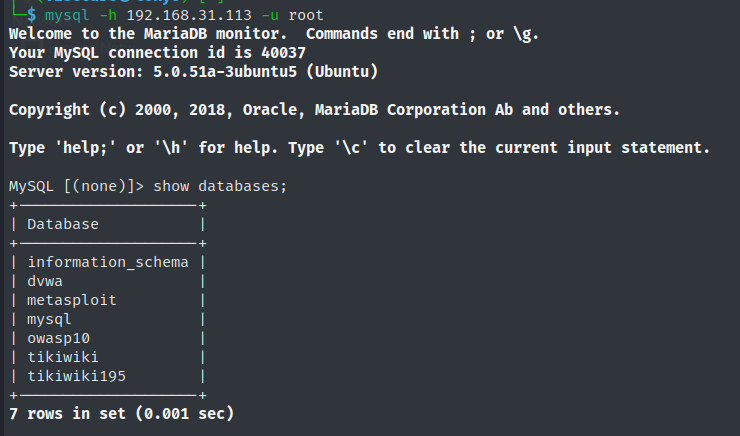
The default configuration of the Windows binary release of MySQL 3.23.2 through 3.23.52 has a NULL root password, which could allow remote attackers to gain unauthorized root access to the MySQL database.

**CVE-ID**: CVE-2002-1809

**CVE SCORE:** HIGH

**SCREENSHOTS:**





**REFERENCE:** https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1809

**SOLUTION:**

To prevent this attack, set the strong user password to MY\_SQL server. So that those who want to login they should use right password.

**9.NFS (2049)**

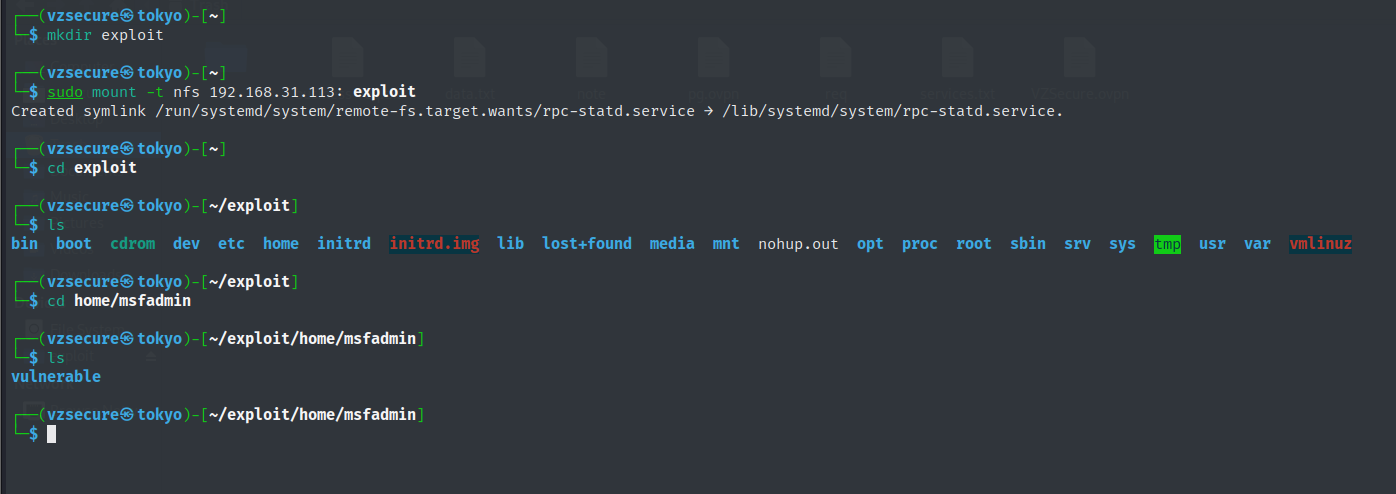
**Description:**

An out of memory bounds write flaw (1 or 2 bytes of memory) in the Linux kernel NFS subsystem was found in the way users use mirroring (replication of files with NFS). A user, having access to the NFS mount, could potentially use this flaw to crash the system or escalate privileges on the system.

**CVE-ID**: CVE-2021-4157

**CVE SCORE:** HIGH

**SCREENSHOTS:**



**REFERENCE:** <https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc753731(v=ws.11)>

**SOLUTION:**

NFS shares can be commonly found open on the internal Linux-based servers or workstations. It is important not to use the service with default settings. This may lead to complete system compromise! The attacker with root privilege on the compromised machine may use the machine as a pivot point to attack further into the network leading to big compromise.

**10.UNREAL (6667)**

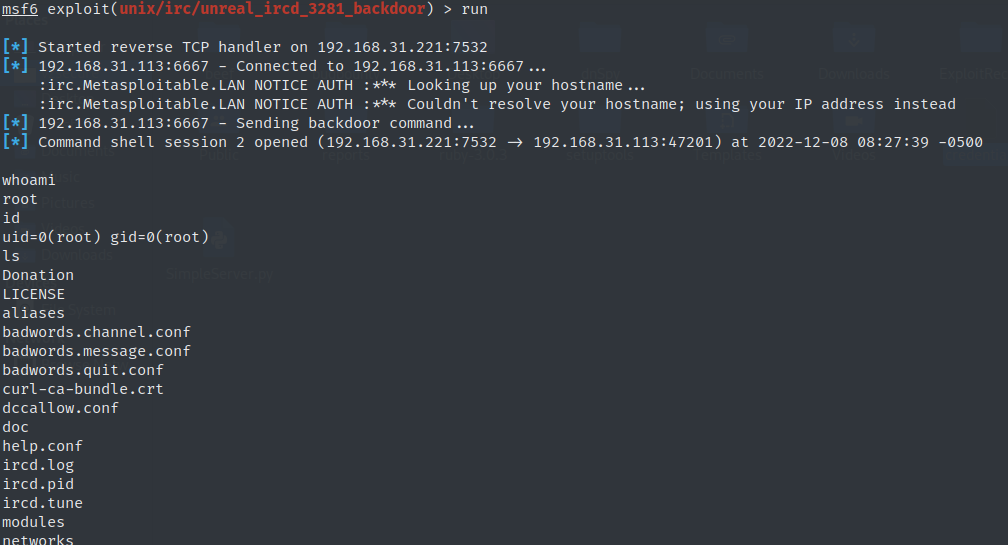
**Description:**

UnrealIRCd 3.2.8.1, as distributed on certain mirror sites from November 2009 through June 2010, contains an externally introduced modification (Trojan Horse) in the DEBUG3\_DOLOG\_SYSTEM macro, which allows remote attackers to execute arbitrary commands.

**CVE-ID**: CVE-2010-2075

**CVE SCORE:** HIGH

**SCREENSHOTS:**



**REFERENCE:** https://security.gentoo.org/glsa/201006-21

**SOLUTION:**

1. Re download the latest version.
2. Verify MD5 (or SHA1) checksums
3. Recompile and restart UnrealIRCd

**11.** **DISTCCD (3632)**

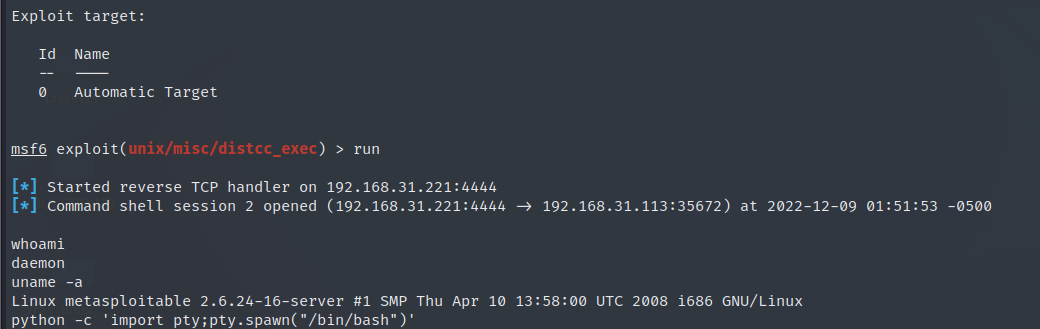
**Description:**

distcc is designed to speed up compilation by taking advantage of unused processing power on other computers. A machine with distcc installed can send code to be compiled across the network to a computer which has the distccd daemon and a compatible compiler installed. distcc 2.x, as used in XCode 1.5 and others, when not configured to restrict access to the server port, allows remote attackers to execute arbitrary commands via compilation jobs, which are executed by the server without authorization checks.

**CVE-ID**: CVE-2004-2687

**CVE SCORE:** HIGH

**SCREENSHOTS:**



**REFERENCE:** https://www.distcc.org/security.html

**SOLUTION:**

Vendor updates are available. Please see the references for more information. For more information about DistCC's security see the references.

**12.APACHE JSERV (8009)**

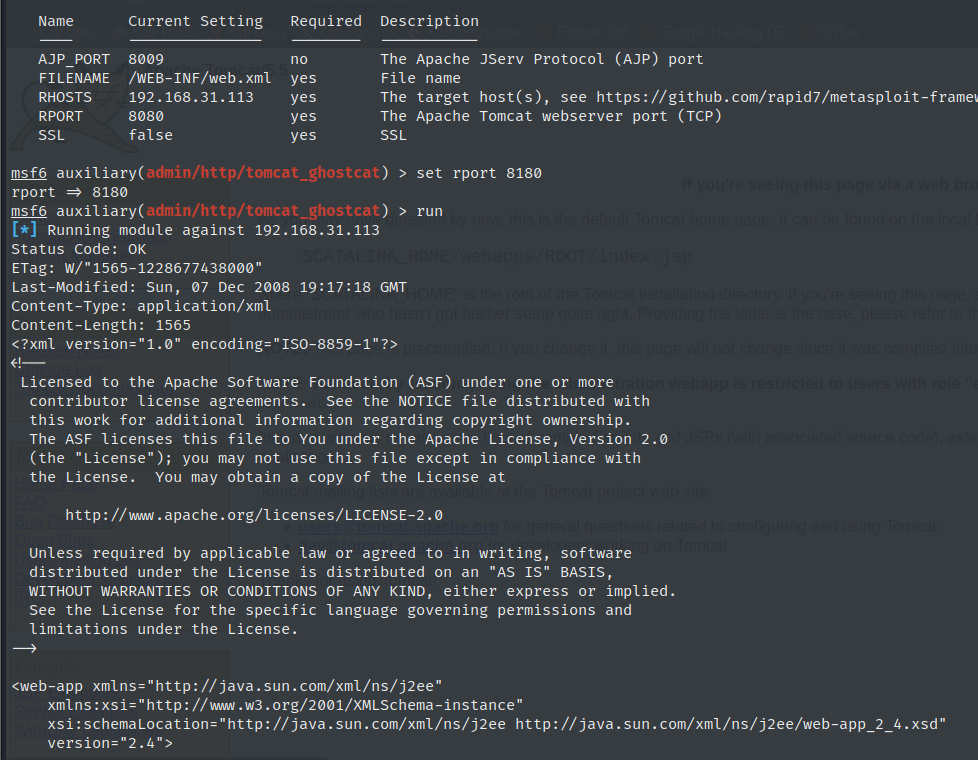
**Description:**

When using the Apache JServ Protocol (AJP), care must be taken when trusting incoming connections to Apache Tomcat. Tomcat treats AJP connections as having higher trust than, for example, a similar HTTP connection. If such connections are available to an attacker, they can be exploited in ways that may be surprising. In Apache Tomcat 9.0.0.M1 to 9.0.0.30, 8.5.0 to 8.5.50 and 7.0.0 to 7.0.99, Tomcat shipped with an AJP Connector enabled by default that listened on all configured IP addresses.

**CVE-ID**: CVE-2020-1938

**CVE SCORE:** CRITICAL

**SCREENSHOTS:**



**REFERENCE:** https://snyk.io/blog/ghostcat-breach-affects-all-tomcat-versions/

**SOLUTION:**

Apache Tomcat has officially released versions 9.0.31, 8.5.51, and 7.0.100 to fix this vulnerability. To fix this vulnerability correctly, you first need to determine if the Tomcat AJP Connector service is used in your server environment:

1. If no cluster or reverse proxy is used, you can basically determine that AJP is not used.
2. Otherwise, you need to figure out if the cluster or reverse server is communicating with the Tomcat AJP Connector service.

**13. SAMBA (139)**

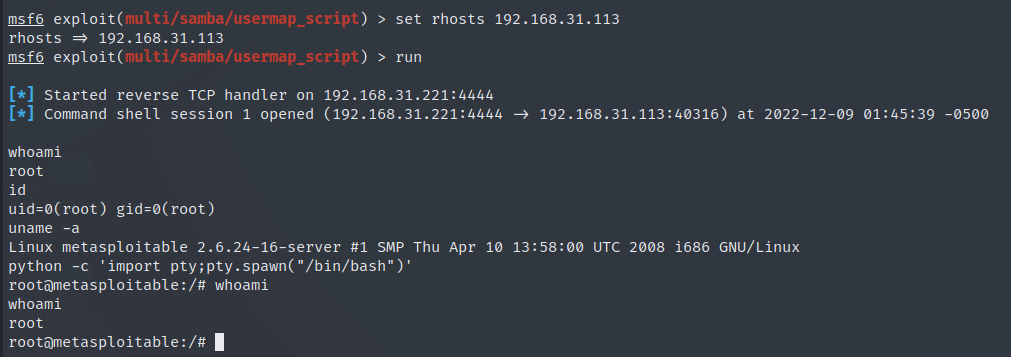
**Description:**

The MS-RPC functionality in smbd in Samba 3.0.0 through 3.0.25rc3 allows remote attackers to execute arbitrary commands via shell metacharacters involving the (1) SamrChangePassword function, when the "username map script" smb.conf option is enabled, and allows remote authenticated users to execute commands via shell metacharacters involving other MS-RPC functions in the (2) remote printer and (3) file share management.

**CVE-ID**: CVE-2007-2447

**CVE SCORE:** CRITICAL

**SCREENSHOTS:**



**REFERENCE:** https://www.kb.cert.org/vuls/id/268336

**SOLUTION:**

Follow the below mentioned step to prevent the attack:

1. Apply a patch or upgrade
2. Do not load external shell scripts
3. Restrict access

**14. POSTGRES-SQL (5432)**

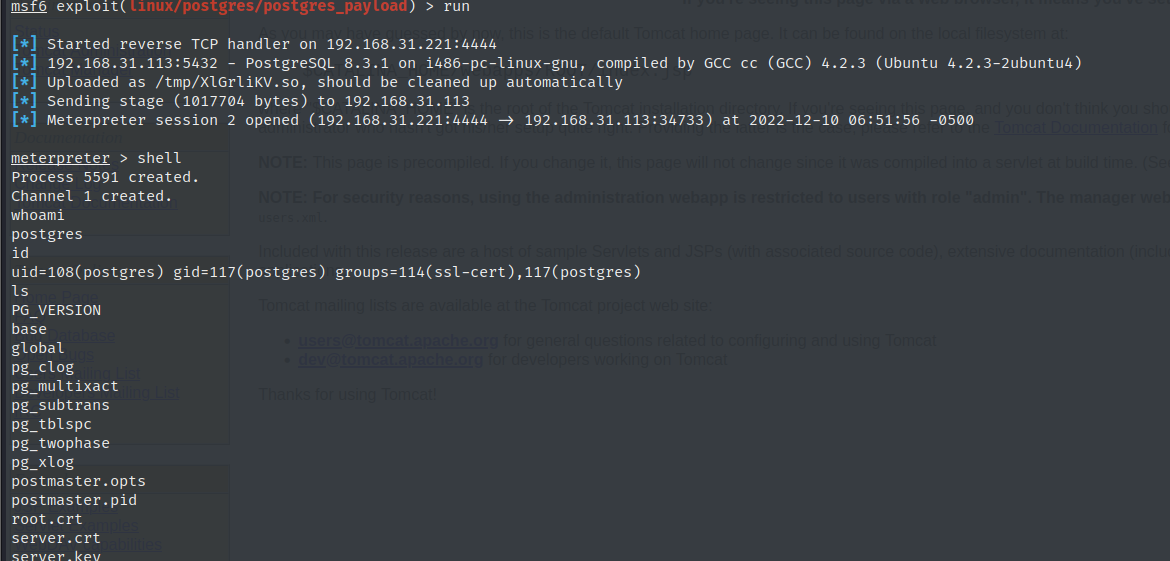
**Description:**

On some default Linux installations of PostgreSQL, the postgres service account may write to the /tmp directory, and may source UDF Shared Libraries from there as well, allowing execution of arbitrary code. This module compiles a Linux shared object file, uploads it to the target host via the UPDATE pg\_largeobject method of binary injection, and creates a UDF (user defined function) from that shared object. Because the payload is run as the shared object's constructor, it does not need to conform to specific Postgres API versions.

**CVE-ID**: CVE-2007-3280

**CVE SCORE:** HIGH

**SCREENSHOTS:**



**REFERENCE:** https://exchange.xforce.ibmcloud.com/vulnerabilities/35145

**SOLUTION:**

The first thing one should do to prevent the attacks outlined here is to disable the local trust authentication. This forces identification of any user connecting to the database from the local host or a remote host. Privilege escalation via dblink is then no longer possible. To disable function mapping with arbitrary libraries it's probably best to upgrade to the latest PostgreSQL version.

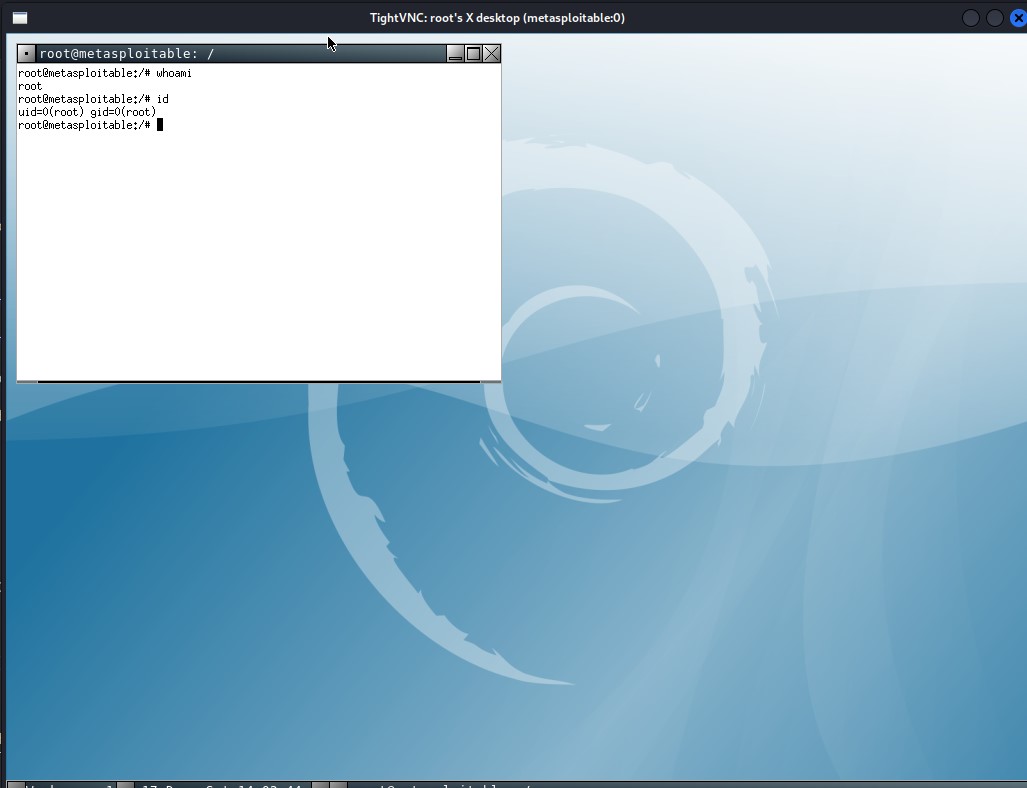
**15. VNC (5432)**

**Description:**

The VNC server is using the password "password". This would allow anyone to log into the machine via VNC and take complete control.

**CVE-ID**: CVE-1999-0506

**CVE SCORE:** CRITICAL

**SCREENSHOTS:**

**REFERENCE:** https://www.cve.org/CVERecord?id=CVE-1999-0506

**SOLUTION:**

Using the following methods to prevent this attack:

1. Use strong Authentication.
2. Isolate using Virtual Machine.
3. Stay up-to-date, install updates as they are release.
4. Setup VPN over the network