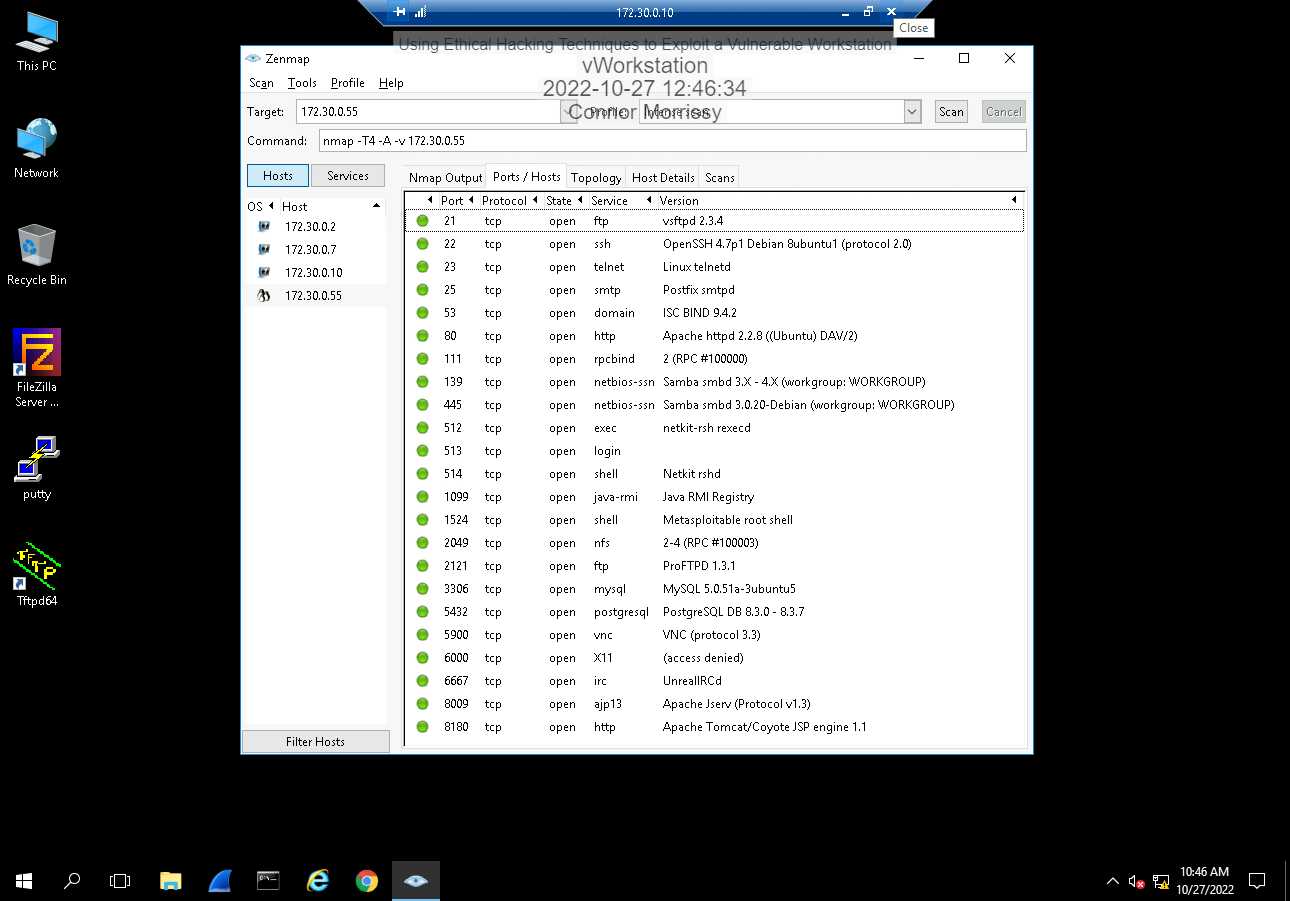
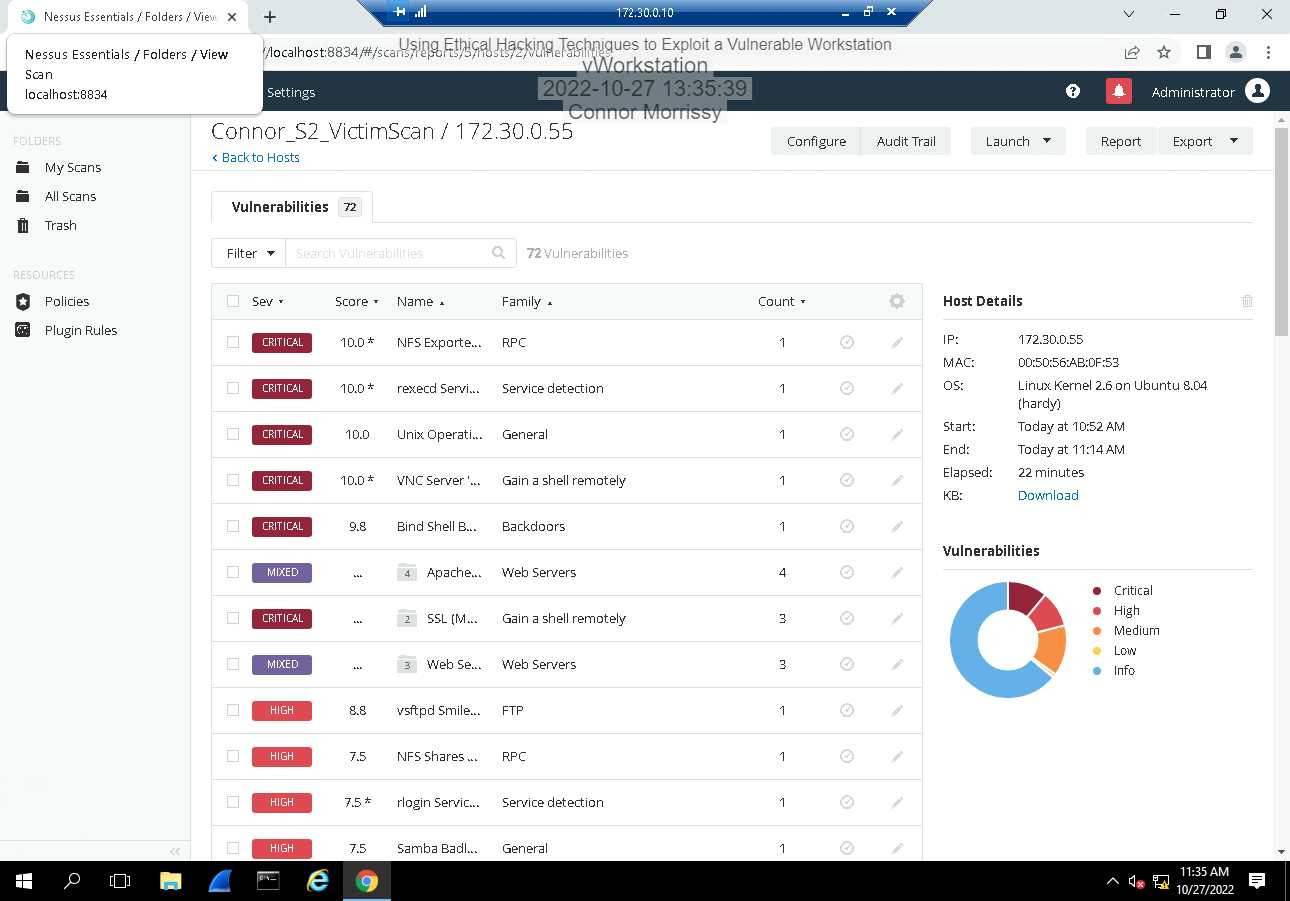
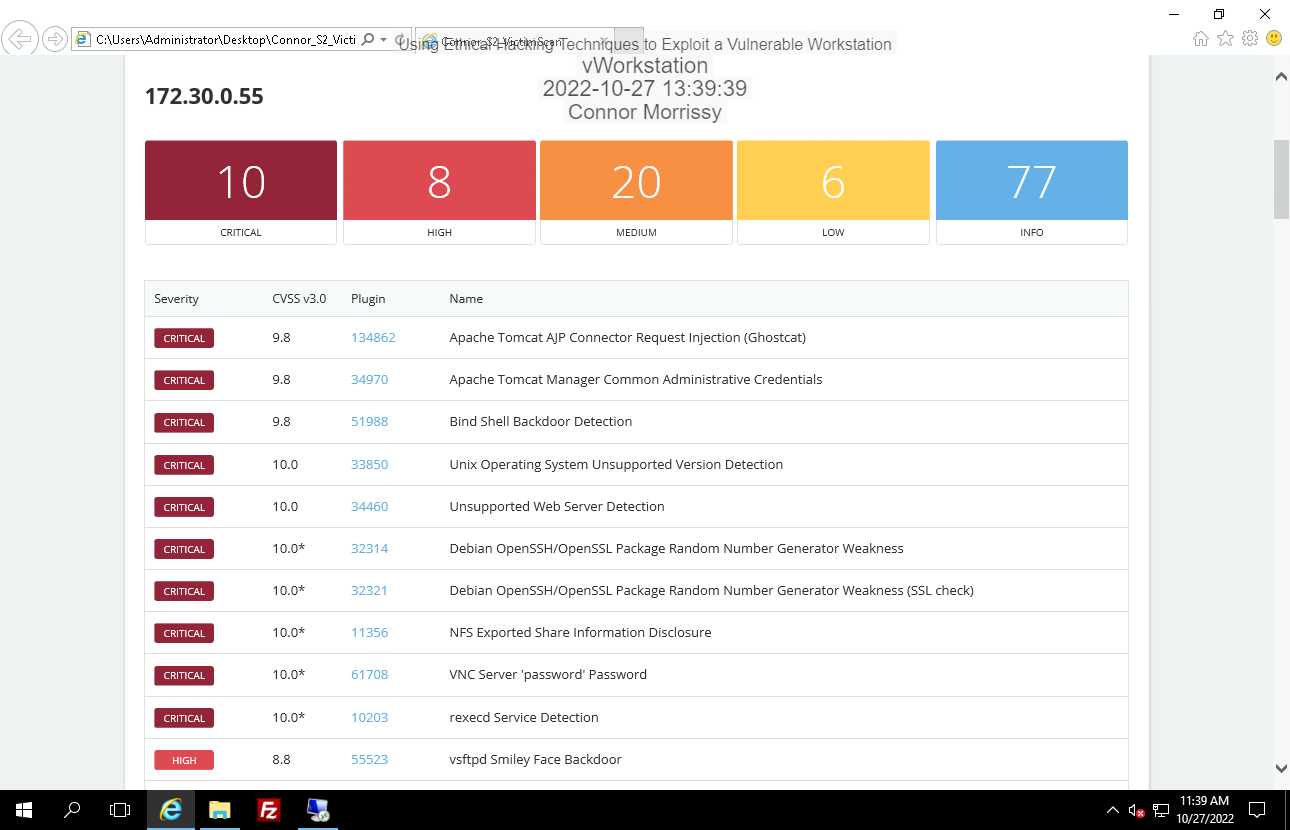
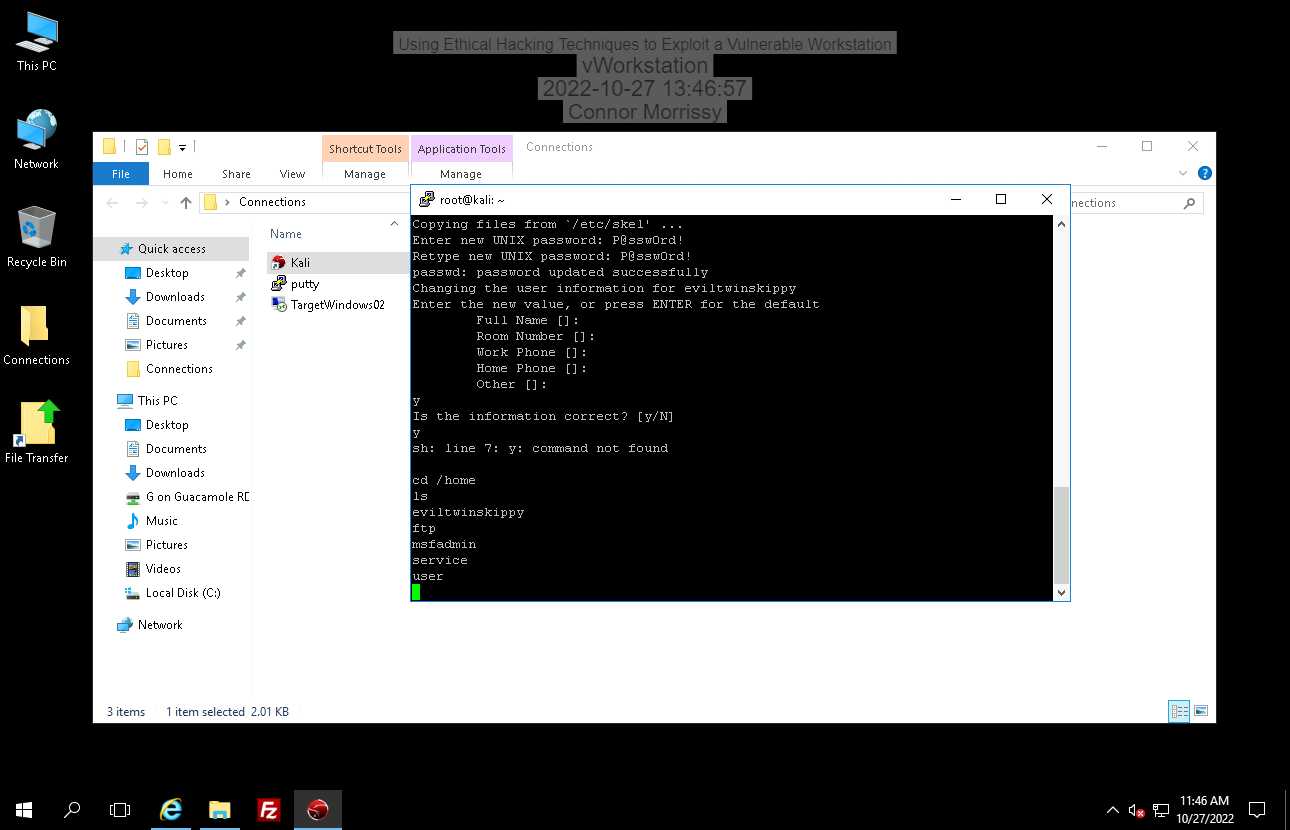


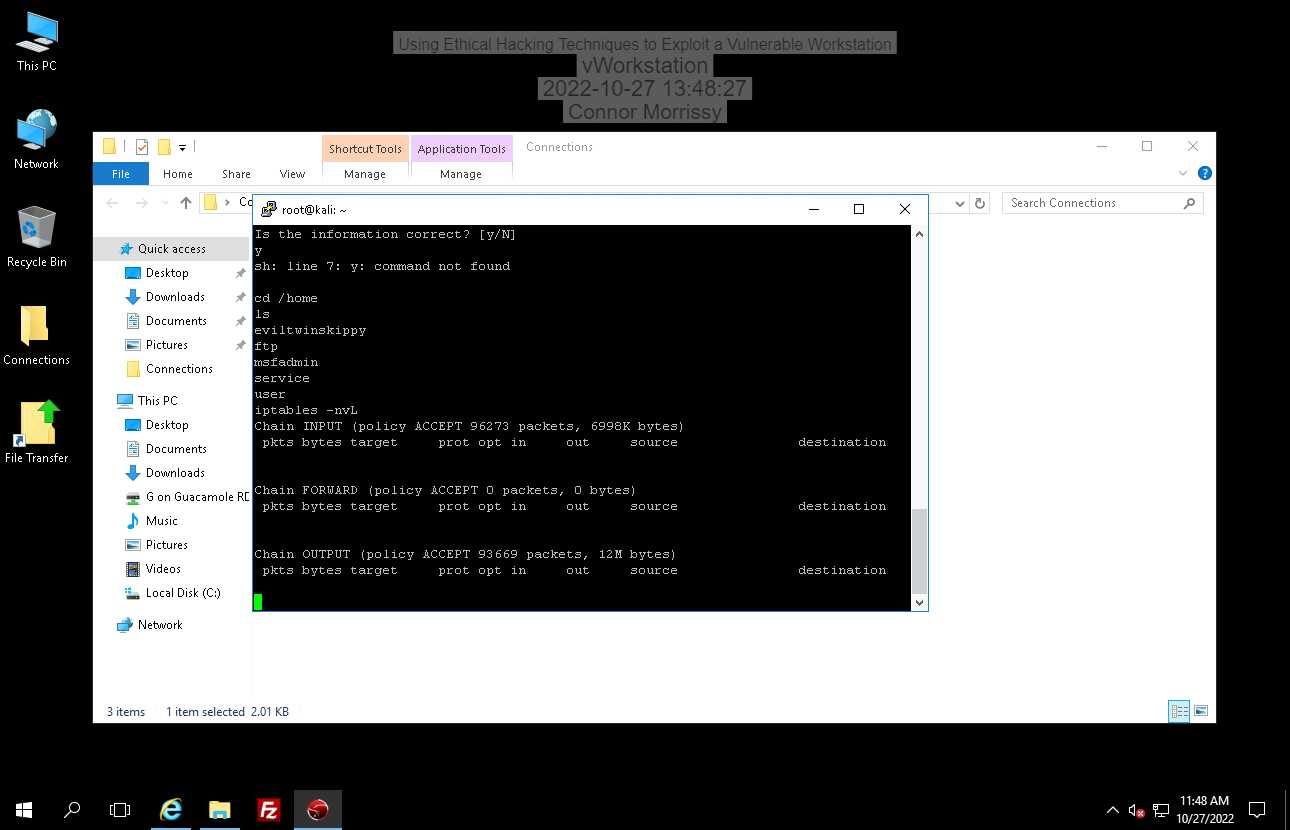
**Solution on nessus:** Validate and recompile a legitimate copy of the source code.

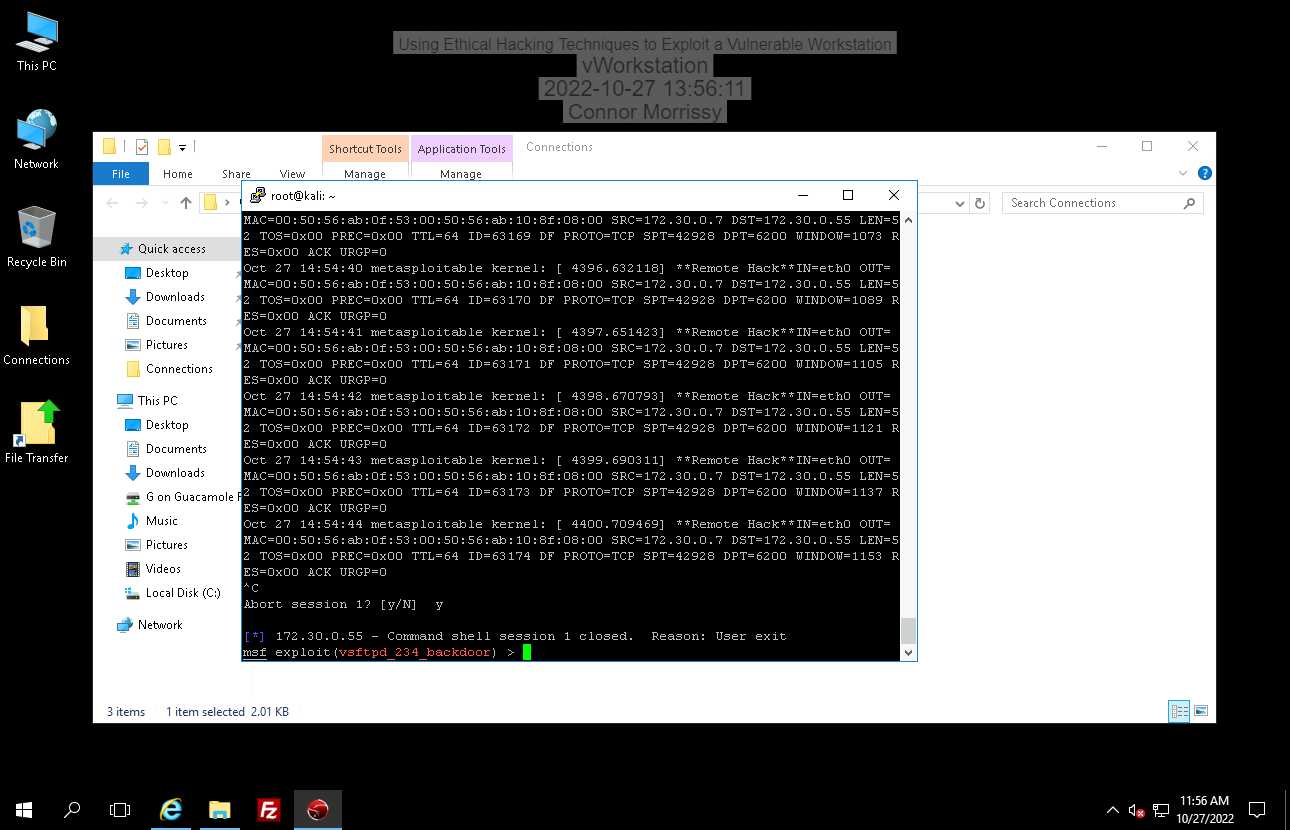












**Solution on nessus:** Validate and recompile a legitimate copy of the source code.

**3.1:**

134862 – Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.

34970 – Edit the associated 'tomcat-users.xml' file and change or remove the affected set of credentials.

51988 – Verify if the remote host has been compromised, and reinstall the system if necessary.

33850 – Upgrade to a version of the Unix operating system that is currently supported.

34460 – Remove the web server if it is no longer needed. Otherwise, upgrade to a supported version if possible or switch to another server.

32314 – Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

32321 – Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

11356 – Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

61708 – Secure the VNC service with a strong password.

10203 – Comment out the 'exec' line in /etc/inetd.conf and restart the inetd process.

**3.2:**

iptables -A INPUT -p tcp --dport 22 -j ACCEPT

For the second iptables command, it does not seem that you can drop and log a packet in one command. It appears you need to use multiple commands and create an additional chain for logging. There is no way to log AND drop a packet in a single command.

**3.3:**

The second vulnerability that can allow a hacker to open a remote shell is the 51988 Bind Shell Backdoor Detection  
The recommended solution is to verify if the remote host has been compromised, and reinstall the system if necessary.