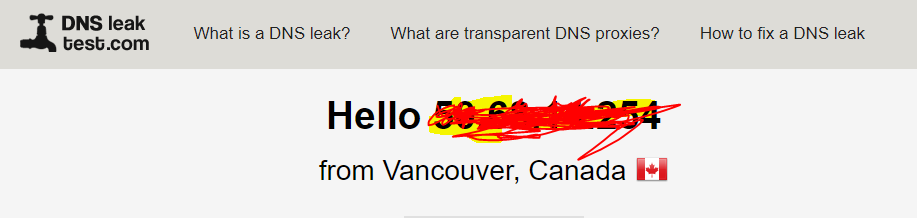
**Gaining access to a Web Server and being anonymous**

***Abstract --*** **In this project, an attempt is made by an ethical hacker to gain a root privilege access to a web server without revealing his/her identity. To achieve anonymity; proxychains and tor services are used. Initially, after enabling proxychains and tor, the information of the target server is secretly gathered by using port scanning with Nmap. Based upon the open ports and their versions of the services hosted by the target server, the malicious activities are planned. After anonymous scanning of a target server, we observed there is an open 21 port where ftp service of version vsftpd v2.3.4 is hosted. Finally, using the Metasploit tool the vulnerability of the above version is exploited, and the backdoor is planted on a target server, and root privileges are achieved successfully.**

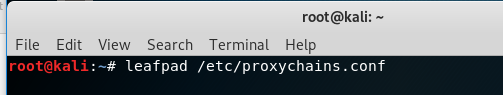
***Keywords: proxychains, tor, Nmap, and Metasploit***

**User Manual:**

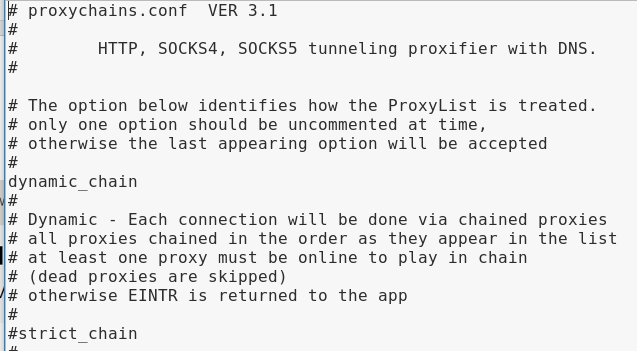
1. Before enabling proxychains, need to check the current IP address of the machine by visiting DNSleaktest.com



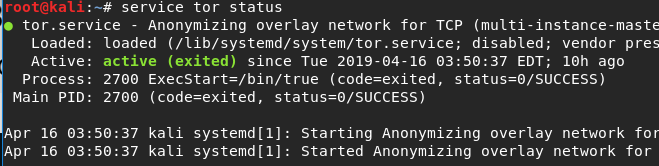
1. Since proxychains are already installed in Kali linux, we can directly edit the config in below path. If proxychains is not installed please type apt-get install proxychains



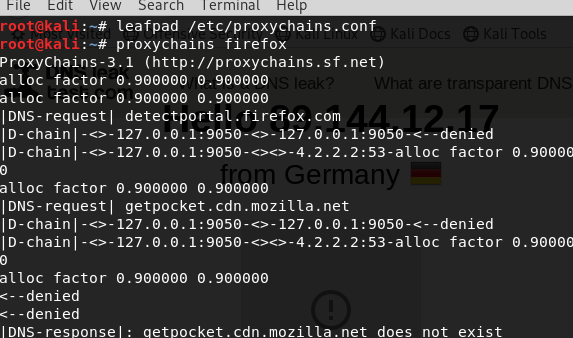
1. Uncomment the dynamic\_chain keyword to enable change in proxies for every search

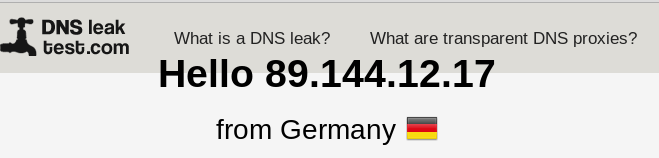


1. After editing the config file, we need to enable tor service as well to increase more anonymity

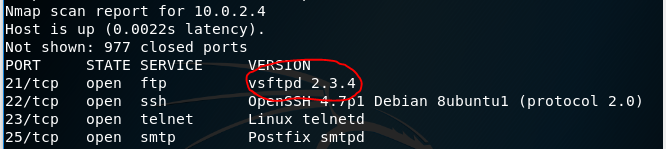


1. Then visit the browser again to check whether the IP address of the machine is changed or not

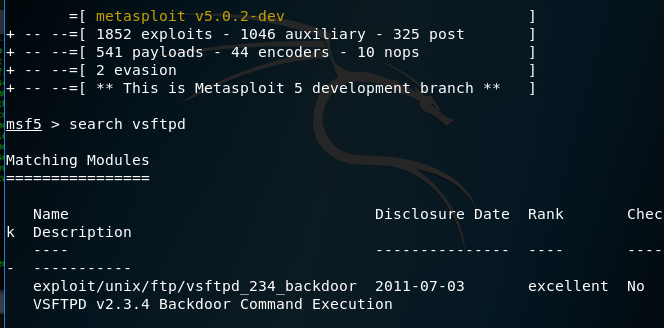




1. Using proxychains nmap -sV -v 10.0.2.4 command check the services and version details of the target server



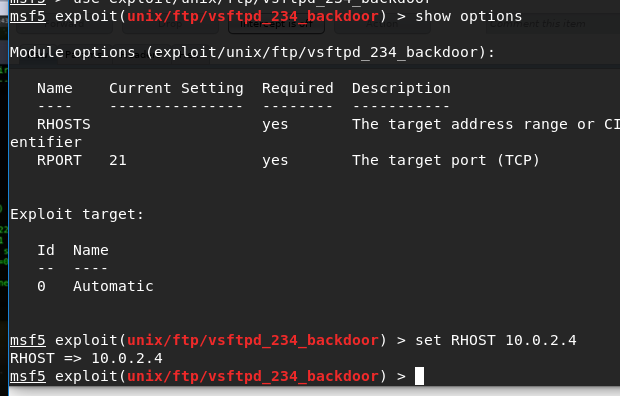
1. Next, using proxychains msfconsole command open the Metaspoilt tool and search for ftp service version vsftpd v2.3.4 for the existing exploit



1. Once the exploit is identified give use command for enabling the exploit



1. Set RHOST as 10.0.2.4 and check the options again whether the right values are set or not



1. Finally, give exploit command for executing the exploit that we had enabled. We can see that a shell session is opened from the target server using a backboor. To check that give whoami command to find username of the session

