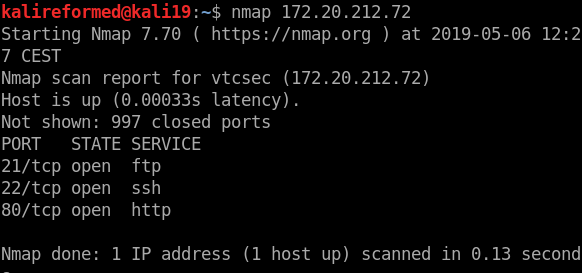


Prima di tutto vediamo l’indirizzo IP della macchina da attaccare (MA)

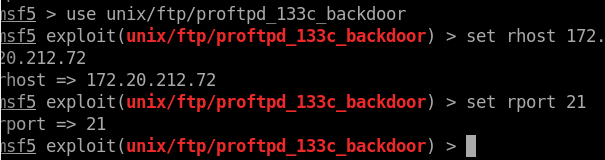


Successivamente facciamo il nmap con indirizzo della macchina da attaccare (MA)

Poi adesso che sappiamo le porte e i servizi 21 ftp, 22 ssh e 80 http

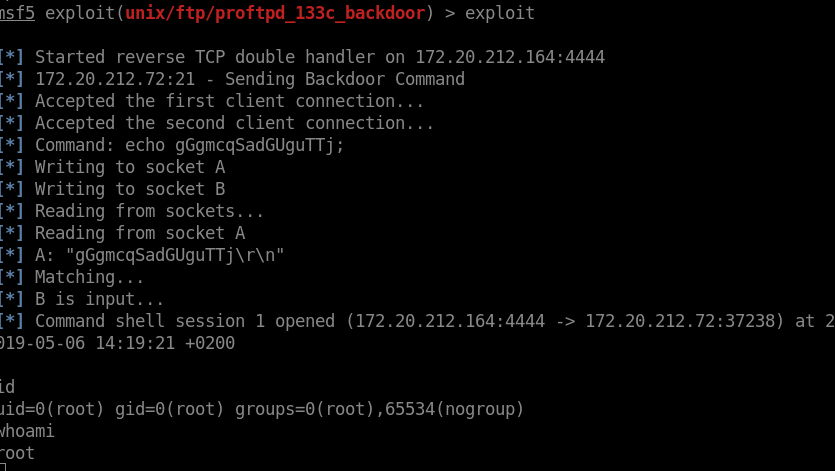
Entriamo nella msfconfole

Successivamente configuriamo il proftp assegnando un host remoto e con la sua suddetta porta

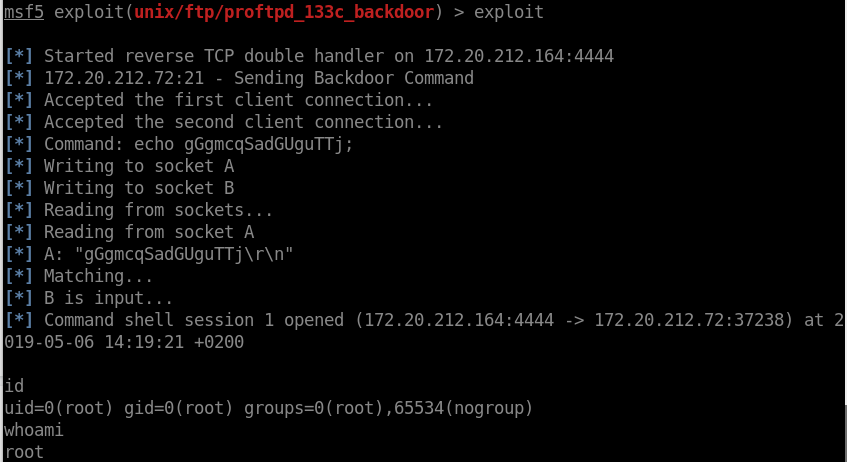


Dopo aver assegnato il rhost e il rport accediamo la parte di exploit

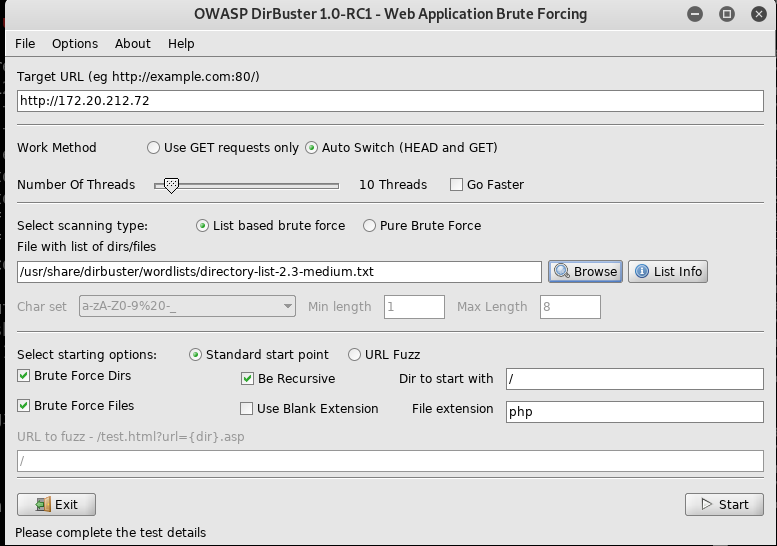
Nella parte di exploit attraverso il comando id e il comando whoami scopriamo che abbiamo fatto l’accesso da root



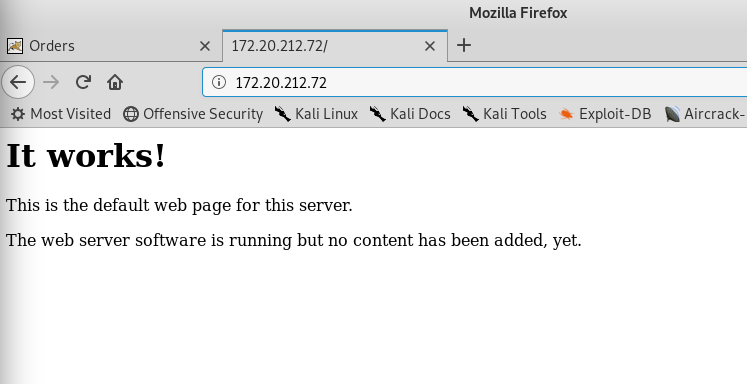
Subito dopo abbiamo fatto un analisi attraverso dirbuster



Nel mentre che fa l’analisi abbiamo inserito nell’url l’indirizzo della macchina da attaccare con la porta 80



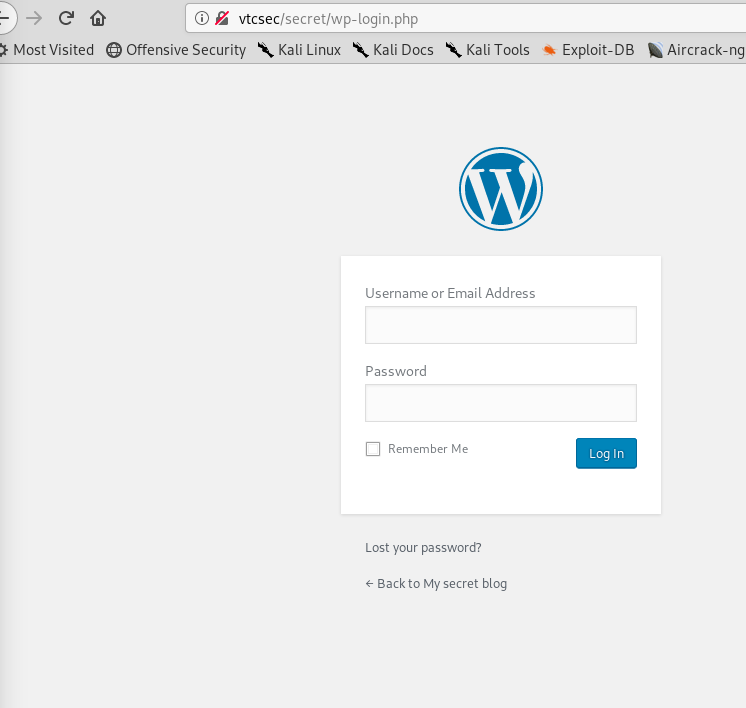
Attraverso dirbuster abbiamo trovato una sottocartella secret dove possiamo accedere a Wordpress



-nota bene:

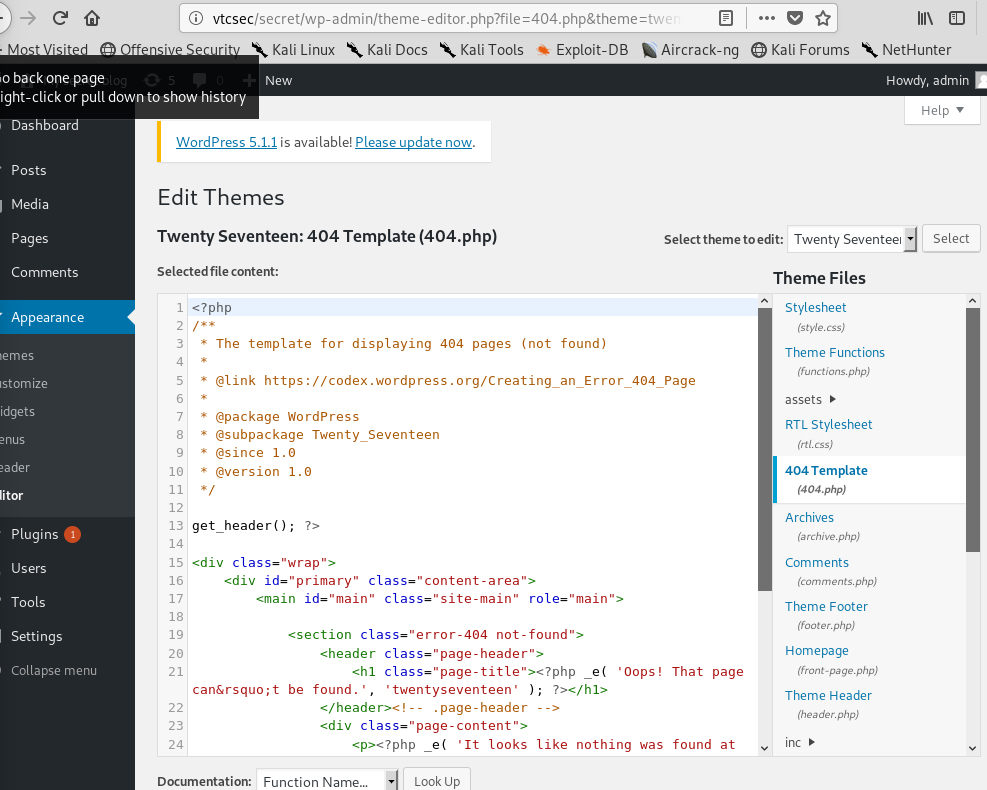
è possibile non accedere alla sezione login di W3C se non abbiamo inserito l’indirizzo ip della macchina host da attaccare nell file /hosts della nostra macchina

Abbiamo provato con le credenziali base admin e admin ad entrare nella sezione Login

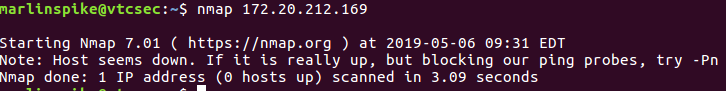


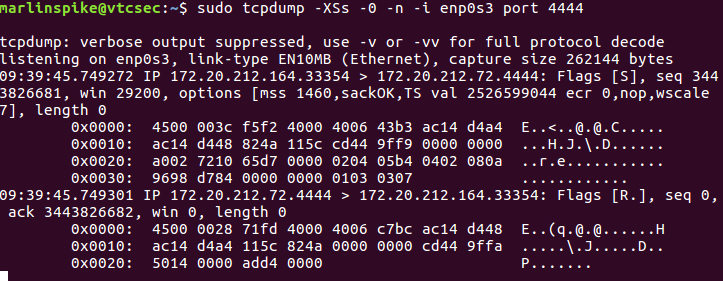
Poi nella sezione Appearance/404 template

possiamo modificare la pagina in caso di errore

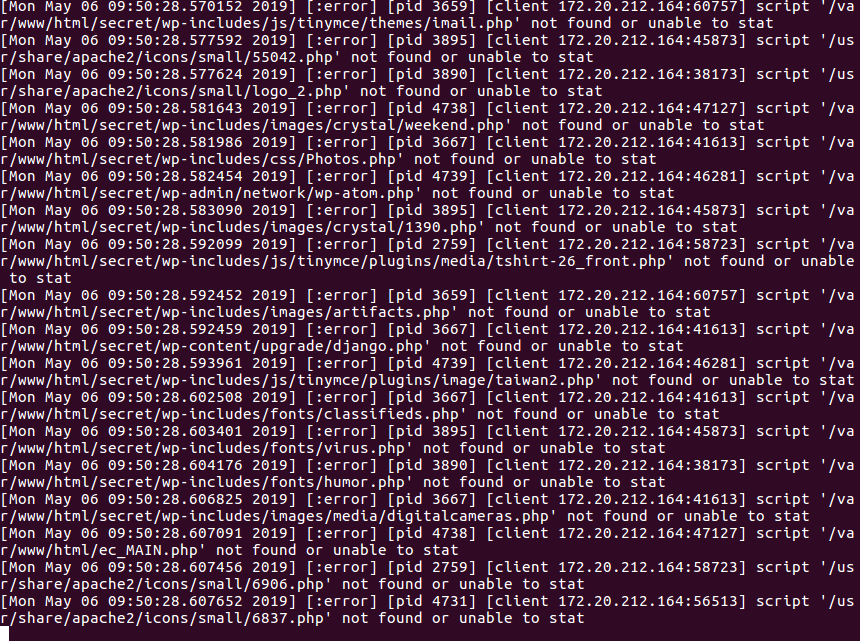


poi abbiamo messo usato il tcpdump dalla macchina ubuntu per vedere le connessioni stabilite e nell’ altra macchina abbiamo fatto nmap dalla macchina attaccante





questi sono i syslog della macchina che si presentano sulla macchina attaccante



-Riccardo Bruzzese