**RAPPORTO ESTENSITO**

Questo è un rapporto esteso. Il suo inizio può essere trovato nelle ultime pagine del file denominato "raport" in github progetto S6 L5.

Ho usato il comando gobuster dir per scoprire directory URL nascoste. Sono state trovate alcune directory sospette come robots, robots.txt. Incluse backup\_wordpress. Ho usato anche questo nell'URL. E mi ha reindirizzato a un'altra pagina. Ho tenuto le analisi, ma non ci sono riuscito. Quindi ho deciso di cercare vulnerabilità tramite altre porte. L'ho fatto prima per il servizio FTP tramite la porta 21. Ho usato anonimo come credenziale di accesso, perché è stato menzionato nel terminale quando ho avviato il servizio:

A screen shot of a computer

Description automatically generated

Poi ho cercato le directory e ne ho trovata una: public. L'ho inserita e ho usato il comando ls per cercare un file qualsiasi. E ho trovato un file in formato txt:

A computer screen with green text

Description automatically generated

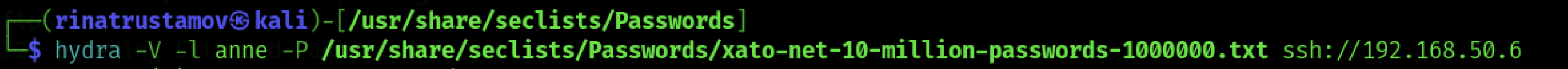
L'ho scaricato per un'analisi più approfondita. Quando ho aperto il file di testo, ho notato che ci sono diverse parole:

A screenshot of a computer screen

Description automatically generated

Ho pensato che potessero essere nomi utente o password. Poi mi sono ricordato che un'altra porta era aperta anche per questo host: la 22 per il servizio ssh. Quindi ho deciso di entrare per ogni utente per controllare manualmente se uno di questi è un nome utente. Per ogni nome utente ho ricevuto l'errore "permesso negato". Ma per anne:A computer screen with text and images

Description automatically generated

Ciò significa che anne è il login! Ora è il momento di crackare la password usando Hydra xD:

E ha trovato la password:A screen shot of a computer screen

Description automatically generated

Ora andrò alla VM di Vancouver 2018 per annotare le credenziali di accesso (login: anne, password: princess):

A black screen with white text

Description automatically generated

Ha effettuato l'accesso!

Quindi è ora di ottenere i privilegi di root. Per prima cosa ho controllato se l'utente anne ha privilegi di superutente. Ho visto che li ha. Quindi ho semplicemente usato il comando sudo su per ottenere i privilegi di root:

A screenshot of a computer

Description automatically generated