Bonus Jangow

Relazione sulla Scansione di Rete e Identificazione dell'Indirizzo IP della Macchina Target

Nel contesto della nostra indagine, l'obiettivo era identificare l'indirizzo IP della macchina target all'interno di una rete locale, dato che eravamo consapevoli di trovarci nella stessa rete ma non conoscevamo l'indirizzo IP esatto della macchina di interesse. Per ottenere questa informazione, abbiamo utilizzato uno strumento di scansione della rete, Nmap, che ci consente di scoprire tutti i dispositivi connessi alla rete e di raccogliere informazioni utili su di essi.

Fase 1: Preparazione della Scansione

Per avviare il processo di identificazione, abbiamo eseguito una scansione sulla rete locale utilizzando il seguente comando Nmap: nmap 192.168.1.0/24

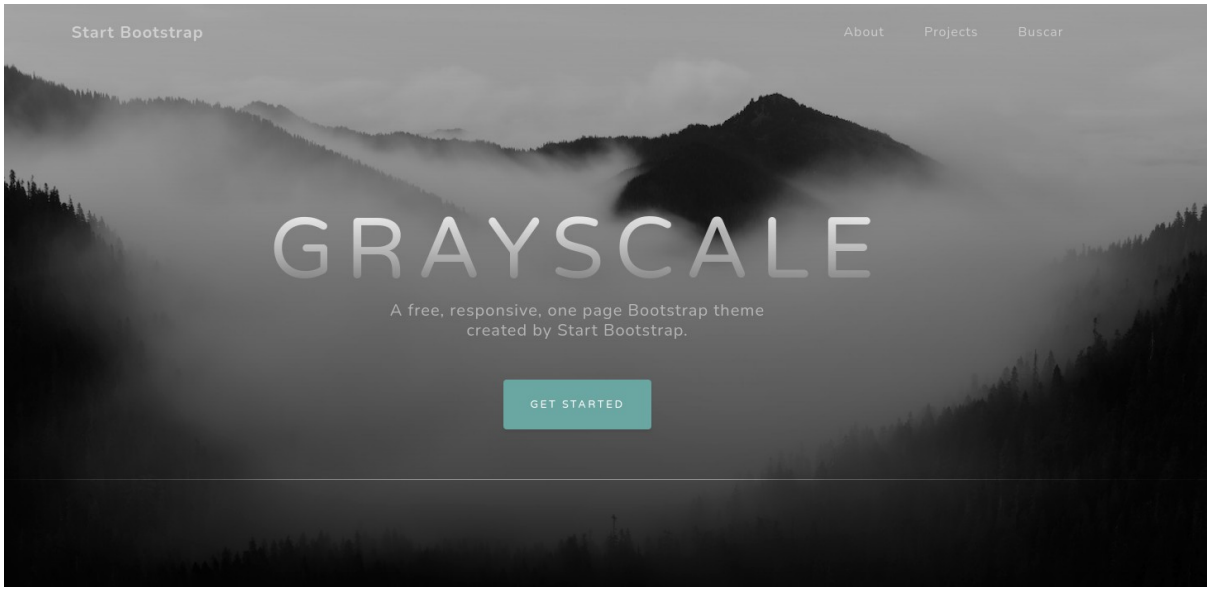
Il comando sopra specifica l'intervallo di indirizzi IP da esaminare, in questo caso l'intera sottorete **192.168.1.0/24**, che include tutti gli indirizzi IP da **192.168.1.1** a **192.168.1.254**. La scelta di questa subnet è stata motivata dalla conoscenza che la macchina target si trova all'interno di questa rete locale.

Dai risultati ottenuti dalla scansione, abbiamo potuto identificare l'indirizzo IP della macchina target. Il dispositivo di nostro interesse risultava avere l'indirizzo **192.168.1.185**

Successivamente, per ottenere maggiori dettagli sulla macchina target, utilizziamo un altro comando Nmap per verificare le versioni dei servizi in esecuzione e le porte aperte. Dai risultati della scansione, osserviamo che sono aperte la porta **21**, associata al servizio **FTP**, e la porta **80**, associata al servizio **HTTP**.

La prima azione che proviamo è quella di connetterci al servizio FTP sulla porta 21. Tuttavia, ci rendiamo conto che per accedere è necessario un nome utente e una password, quindi decidiamo di adottare un approccio alternativo.

Notando che la porta **80** è aperta e corrisponde al servizio HTTP, decidiamo di verificare se esiste una pagina web attiva sulla macchina target. A tal fine, inseriamo l'indirizzo IP della macchina, **192.168.1.185**, nella barra dell'URL del nostro browser per vedere se viene restituita una pagina web.



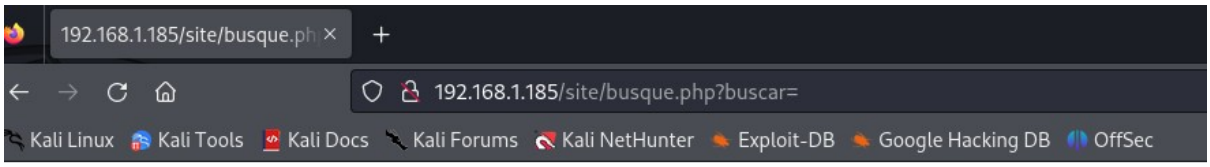
Accedendo all'indirizzo IP della macchina target, veniamo indirizzati a una pagina web denominata **Grayscale**. A questo punto, decidiamo di ispezionare la pagina per cercare eventuali vulnerabilità. Per farlo, utilizziamo due strumenti di sicurezza: **Gobuster** e **Nikto**.

Gobuster è uno strumento di brute forcing che ci permette di scoprire directory, file nascosti, sottodomini, bucket S3 e altre risorse non visibili direttamente su un server web. Utilizzando questo strumento, siamo in grado di identificare alcune directory a cui possiamo accedere, rivelando risorse che altrimenti sarebbero rimaste nascoste.

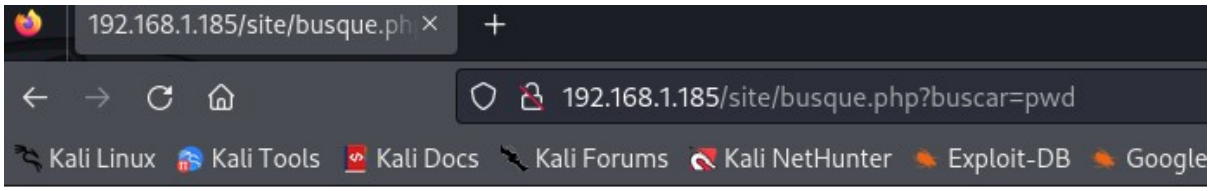
Nikto, invece, è uno scanner di vulnerabilità per applicazioni web. Analizza un server web per rilevare configurazioni deboli, software obsoleti e vulnerabilità note. Grazie a Nikto, veniamo a conoscenza di una vulnerabilità nel sito web.

In sintesi, grazie a questi due strumenti, siamo riusciti a scoprire delle directory accessibili e a identificare una vulnerabilità nel sito web.

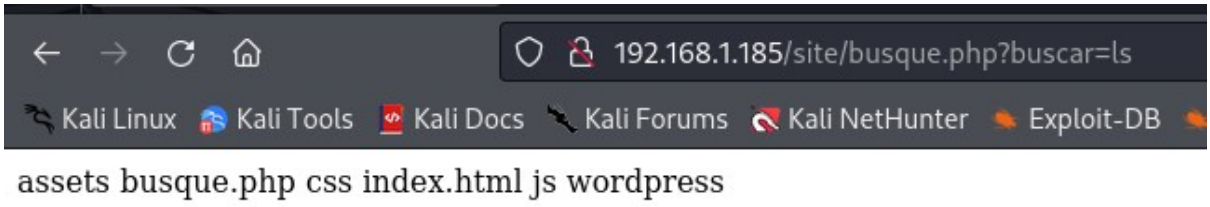
Scopriamo che il parametro buscar è vulnerabile, quindi partiamo da li:



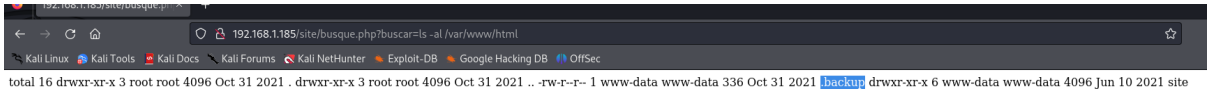
Attraverso l'URL, iniziamo a esplorare le diverse directory del sito web. Per farlo, una volta aperta la pagina nella nostra console, utilizziamo il comando **pwd** (print working directory) per visualizzare la directory corrente in cui ci troviamo. Successivamente, eseguiamo il comando **ls** per elencare i file presenti nella directory, e utilizziamo **ls -al** per visualizzare anche i file nascosti, che potrebbero contenere informazioni o risorse utili per ulteriori indagini.



/var/www/html/site

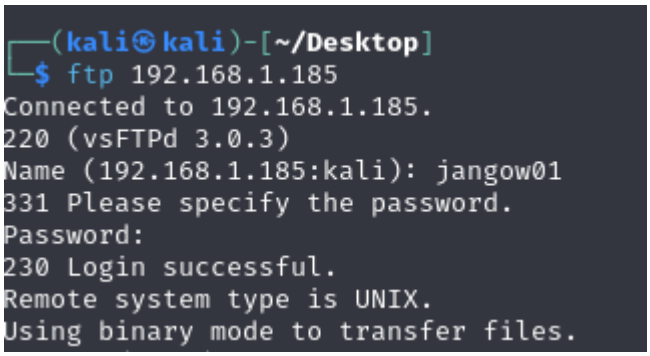


Vediamo che c'è una directory chiamata .backup



Successivamente, utilizziamo il comando **cat** per aprire il contenuto della cartella **.backup**. All'interno di questa cartella, troviamo diversi file che contengono informazioni utili, tra cui **username** e **password**, che stavamo cercando. Questi dettagli potrebbero essere fondamentali per proseguire nelle fasi successive.

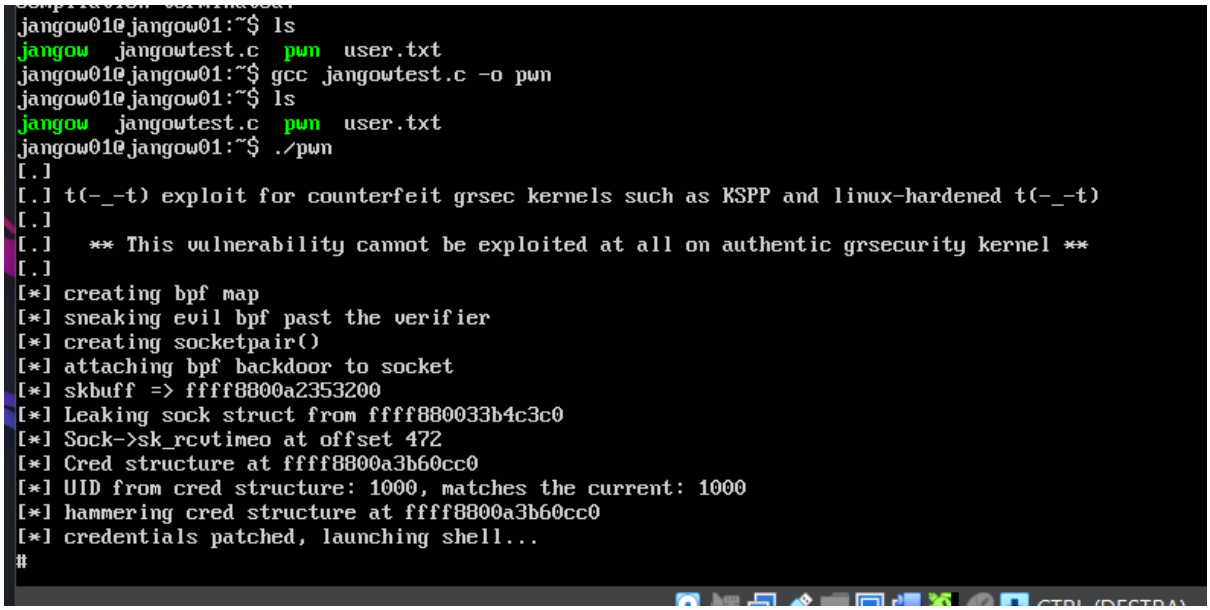
Dopo aver trovato le credenziali, proviamo ad accedere alla porta **21** (associata al servizio **FTP**) utilizzando le informazioni ottenute. Il login ha successo, permettendoci di entrare nel sistema con le credenziali scoperte precedentemente



Per completare l'esercizio e ottenere i permessi di **root**, decidiamo di caricare un **exploit** tramite la connessione **FTP**. Dopo aver ottenuto l'accesso alla macchina, eseguiamo il comando **uname -a** sulla macchina target per raccogliere informazioni sul sistema operativo e la versione del kernel. Grazie ai dati ottenuti, cerchiamo un exploit adatto su **Exploit Database**.

Una volta trovato l'exploit compatibile, lo scarichiamo sulla nostra macchina **Kali** e lo carichiamo sulla macchina target tramite la connessione FTP. Dopo aver caricato correttamente il file, accediamo alla macchina target e completiamo l'exploit utilizzando il comando **gcc** per compilare il codice.

Successivamente, eseguiamo il comando **whoami** per verificare i privilegi correnti. Infine, eseguiamo il comando **root** per ottenere i permessi di **root**. Con questo, siamo riusciti a ottenere i privilegi di amministratore sulla macchina target.



Successivamente, una volta ottenuti i permessi di **root**, esploriamo i file all'interno del sistema utilizzando il comando **ls**, notiamo la presenza del file **proof.txt**. Decidiamo di aprirlo e, una volta visualizzato il suo contenuto, troviamo la **flag finale**, che segna il completamento dell'esercizio con successo.


whoami
root
ls /root
proof.txt
cat /root/proof.txt
JANGOW
da39a3ee5e6b4b0d3255bfef95601890afd80709
_