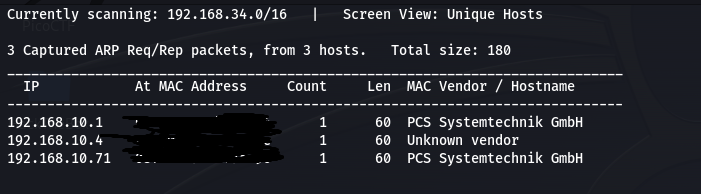
Név: Jangow: 1.0.1

Megjelenés dátuma: 2021.11.04

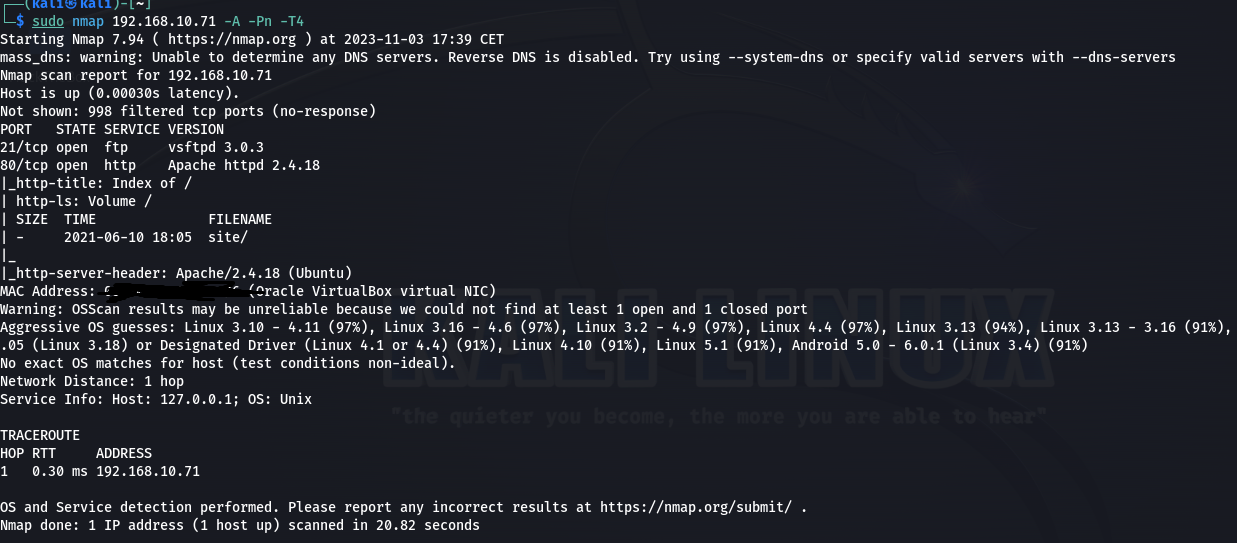
Szerző: Jangow

Leírás: A gép a vulnhubról származó VM, aminek szintén több megoldása is létezik és a nehézségét is a könnyű szintre sorolnám. Több jól ismert eszközt is fogunk használni. A célunk a gépen a root jogosultság megszerzése.

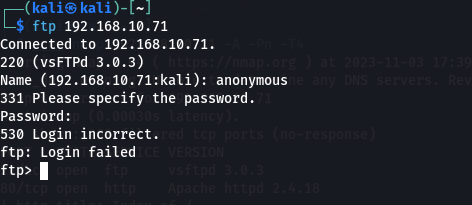
Kezdésnek a netdiscover parancsot fogom használni, amivel beazonosítom a célgépet.



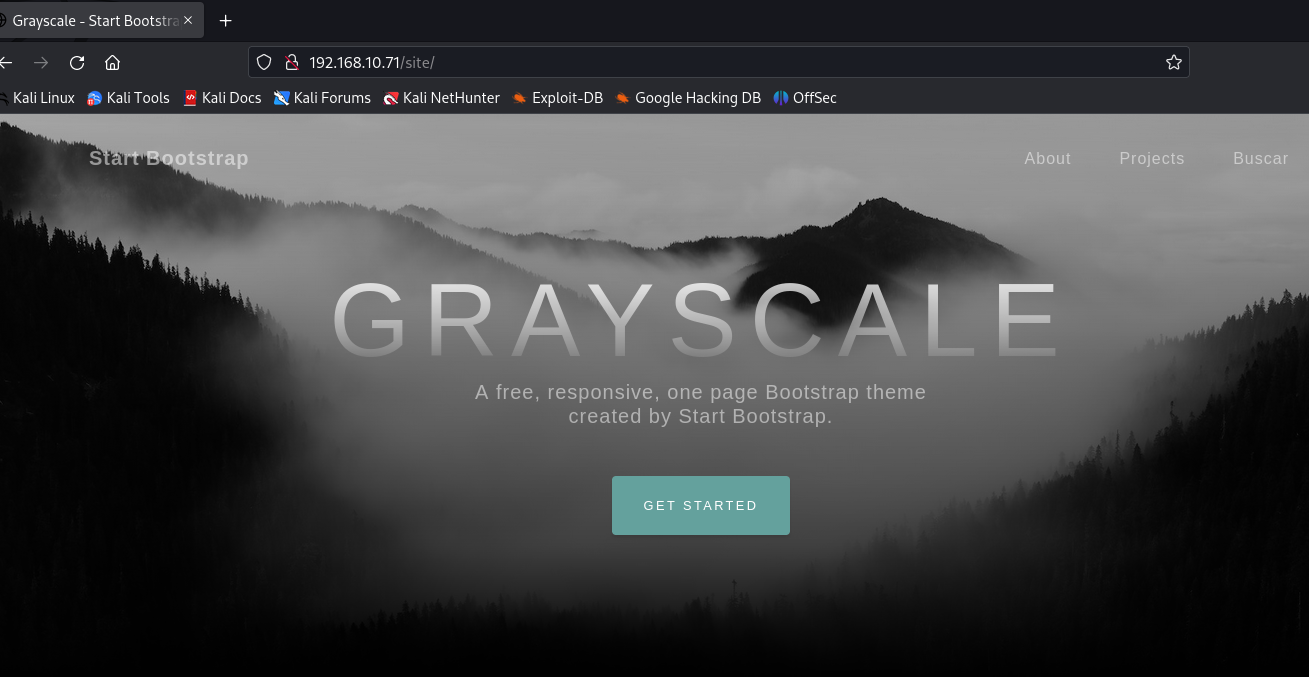
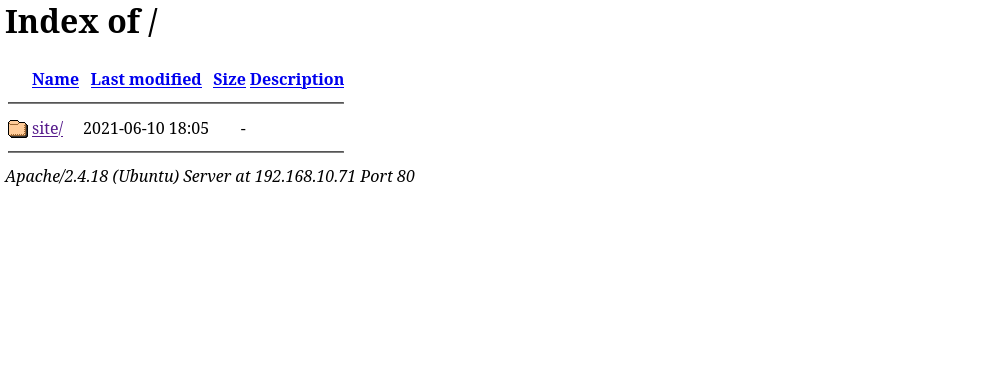
Miután ez megvan elvégezzük az alapvető scannelést az nmap-el amire a következő eredményt kapjuk.



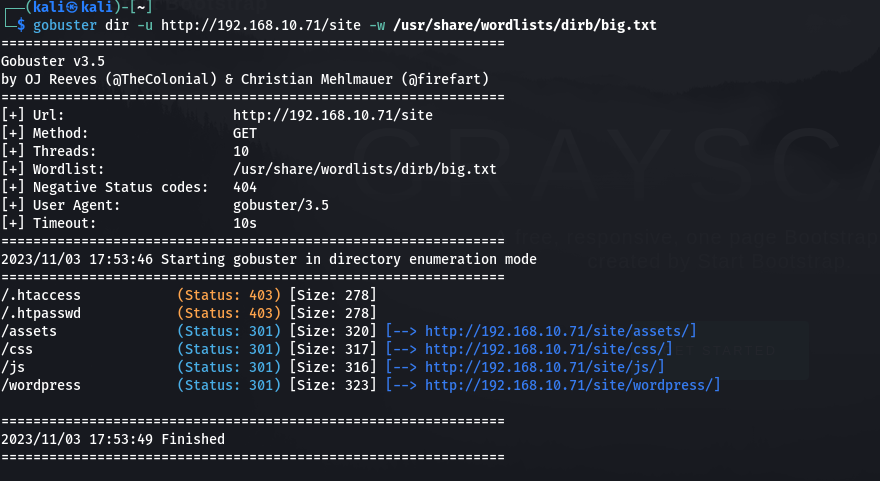
A nyitott portok között megtaláljuk a jól ismert 21 és 80-as portot. Az nmap általában jelzi, ha az ftp porton engedélyezett a vendég belépés, de próbáljuk meg, hátha. Ezt az ftp ip-cím paranccsal tudjuk megtenni és utána a bejelentkező névnek és a jelszónak is a következőt kell megadni: **anonymous**



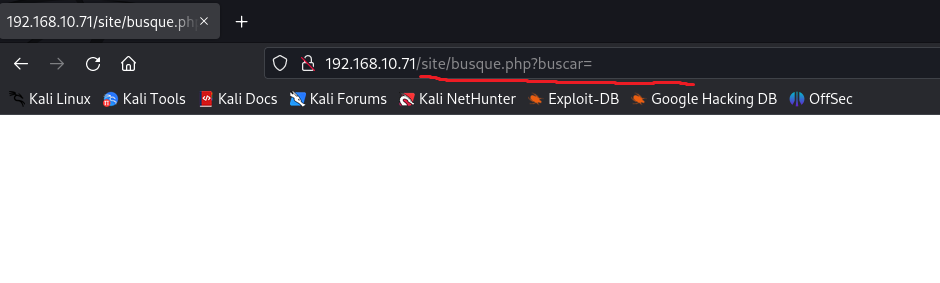
Ezután nézzük meg a 80-as portot a böngészőnkben. A következő fogad minket:



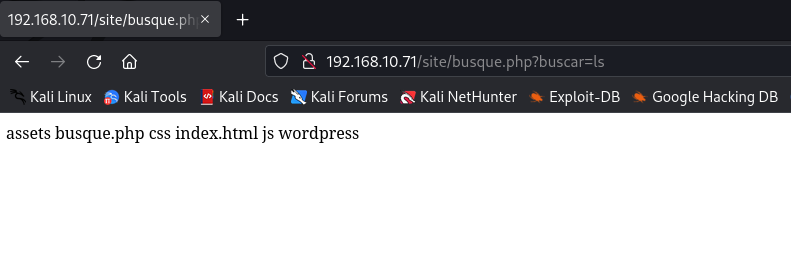
Ezt követően szétnézhetünk a honlapon is és én még szét fogok nézni a gobusterrel is, hogy találok-e valami érdekes directoryt. Két kiindulópontot is észrevehetünk, az egyik, hogy az oldalon egy Wordpress oldalt fut.



A másik érdekesség, hogy ha a weboldalon megnézzük az egyes linkeket találhatunk egy furcsaságot, ami nagy sérülékenységre utalhat.

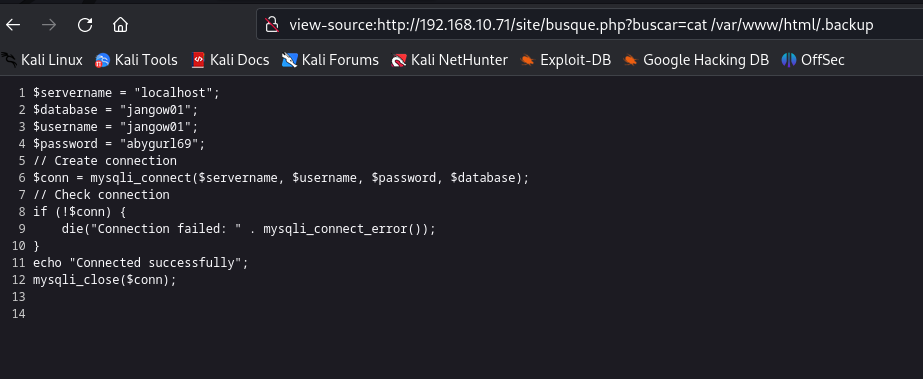


Ezen a gépen a példát láthatunk a command execution vulnerabilityre, ahol a saját kódunkat tudjuk lefuttatni, a helytelenül konfigurált weboldal miatt. Ezt az egyszerű ls paranccsal le is tudjuk tesztelni.



Látható is, hogy kilistázza a jelenlegi könyvtárban lévő mappákat. Innen több módszerrel is be lehet jutni a gépbe, ezek közül fogok bemutatni egyet.

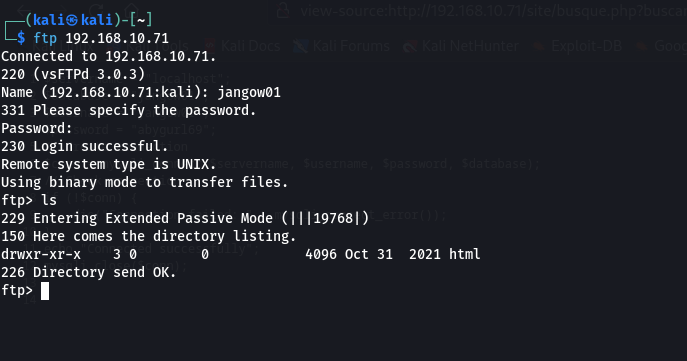
http://192.168.10.71/site/busque.php?buscar=cat /var/www/html/.backup sorral megnézhetünk egy backup filet, amiben találunk egy felhasználónév jelszó párost.



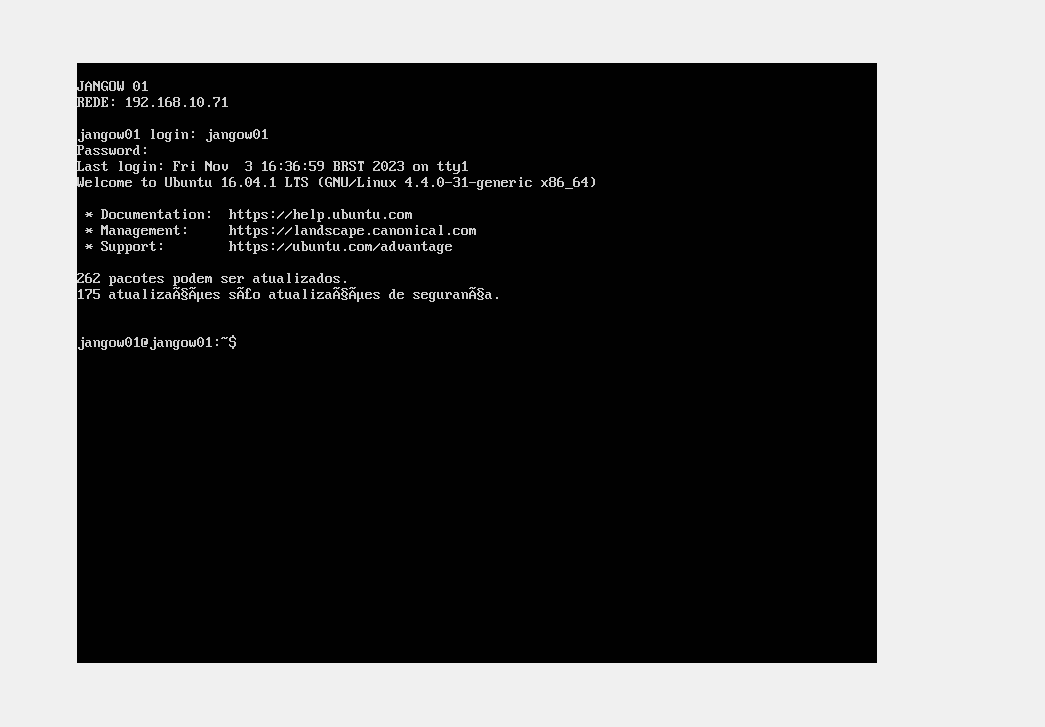
Ennek segítségével beléphetünk az ftp szerverre.

Felh: jangow01

Jelszó: abygurl69



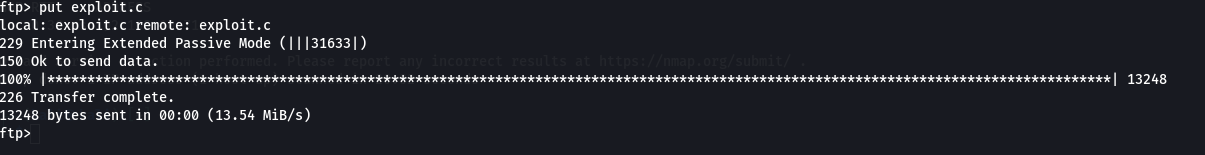
Ha elnavigálunk a /home/jangow01 mappába, akkor észrevehető, hogy hozhatunk létre filekot is ott. Ezt követően belépünk a jangow01 felhasználóba a másik VM-en és ott keresünk további sérülékenységeket.



A **uname –a** paranccsal meghatározhatjuk, hogy az operációsrendszer linux 4.4.0-31 generic. Nem is kellett sokat keresni, hogy megtaláljam az exploitot, ami pontosabban a **CVE:2017-16995**

link: <https://www.exploit-db.com/exploits/45010>

Ezután létrehozunk egy filet .c kiterjesztéssel és feltöltjük az ftp szerveren keresztül a jangow01 felhasználó mappájába.



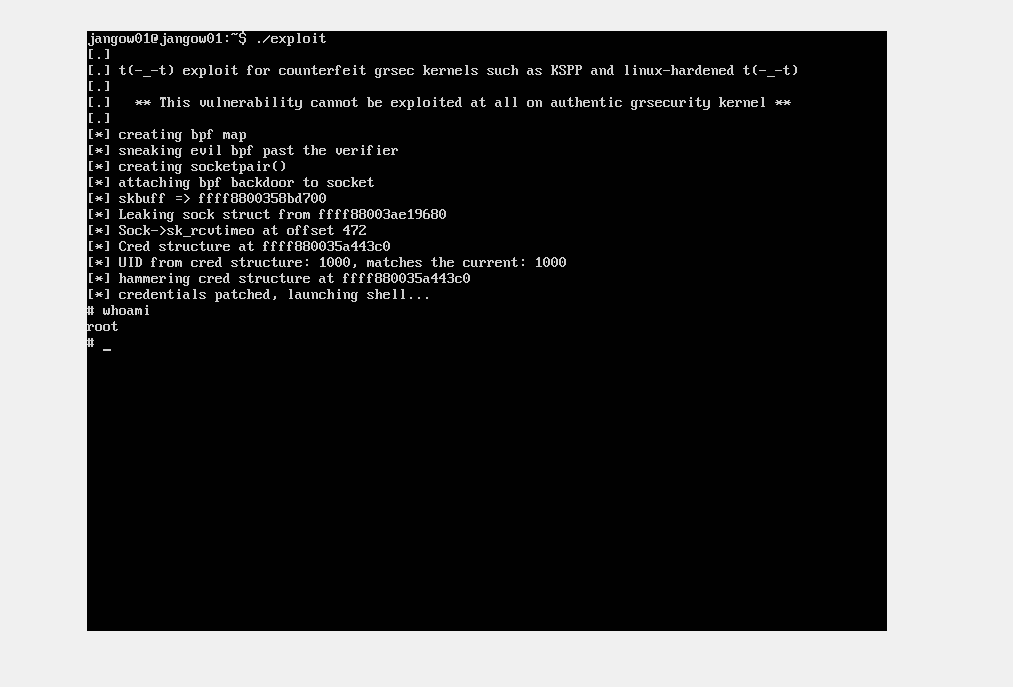
Miután ez megvolt a következőket hajtottam végre.

gcc exploit.c –o exploit

chmod +x exploit

./exploit

Végül lefutattjuk a scriptet, amit létrehoztunk és egy whoami kóddal ki is derült, hogy sikeres volt a privilege escalation és eljutottunk a root jogig.



A privilege escalation eléggé egyértelmű és jön magától viszont a gépbe való bejutásnak több megoldása is lett volna, tudtunk volna egy revshellt is indítani a weboldalról. A közeljövőben lehet, hogy azt a formát is le fogom dokumentálni.