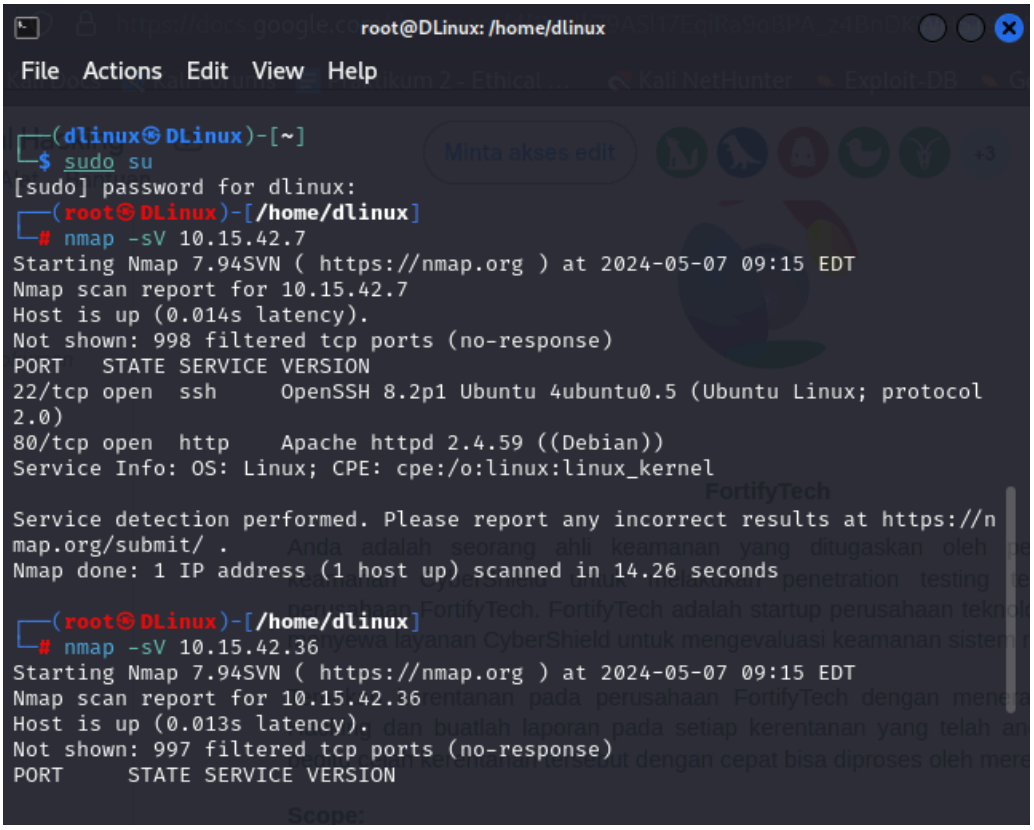
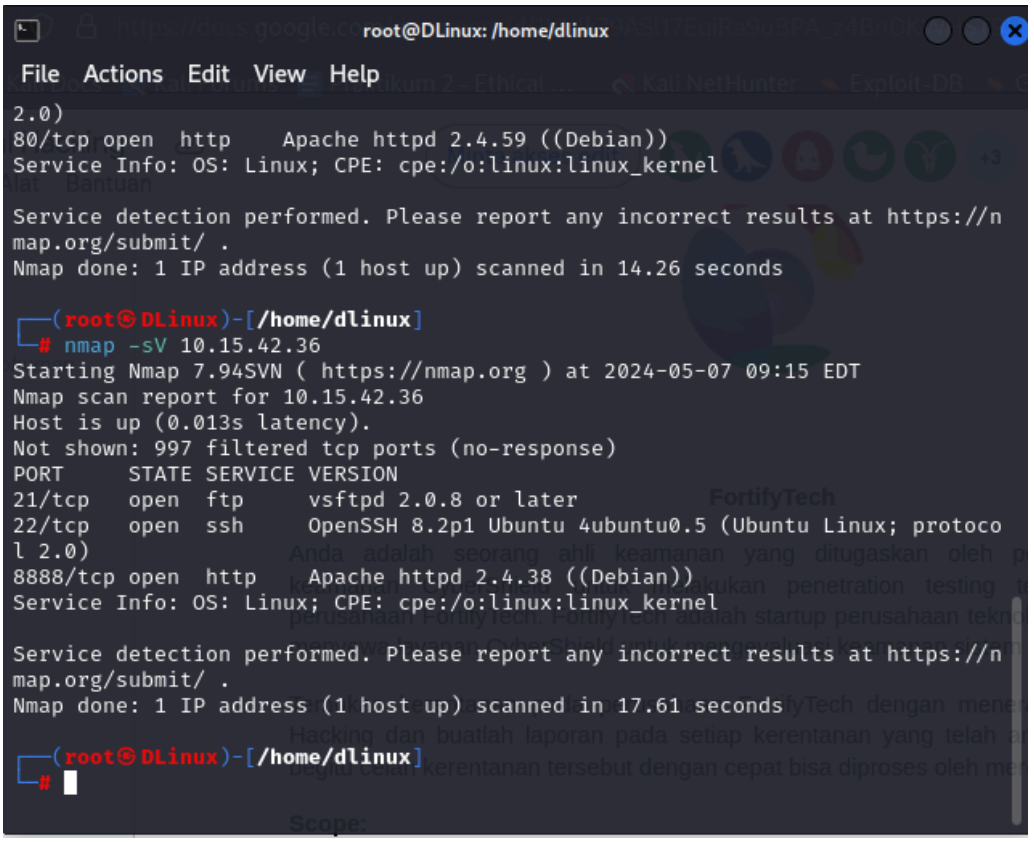
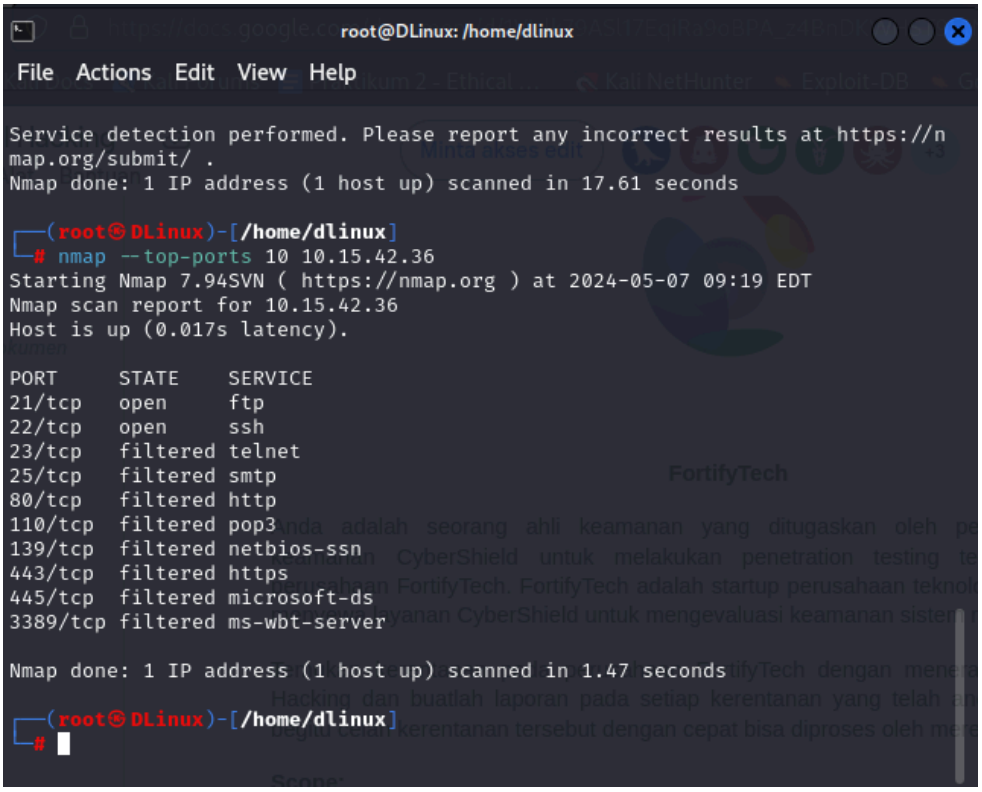
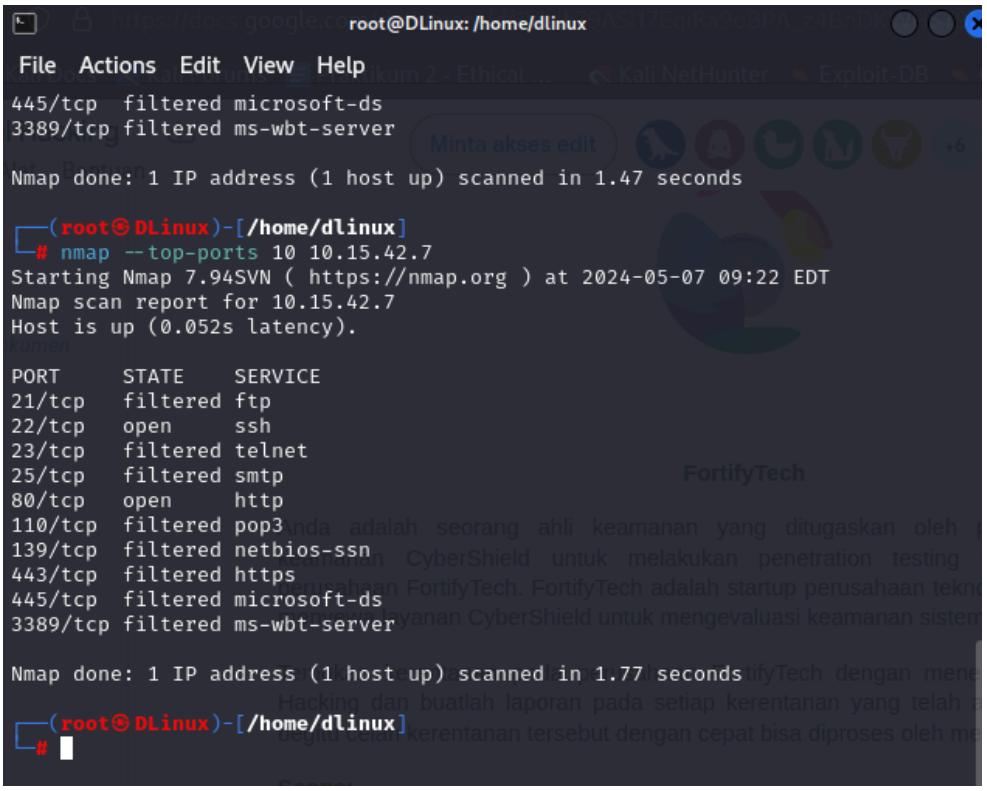
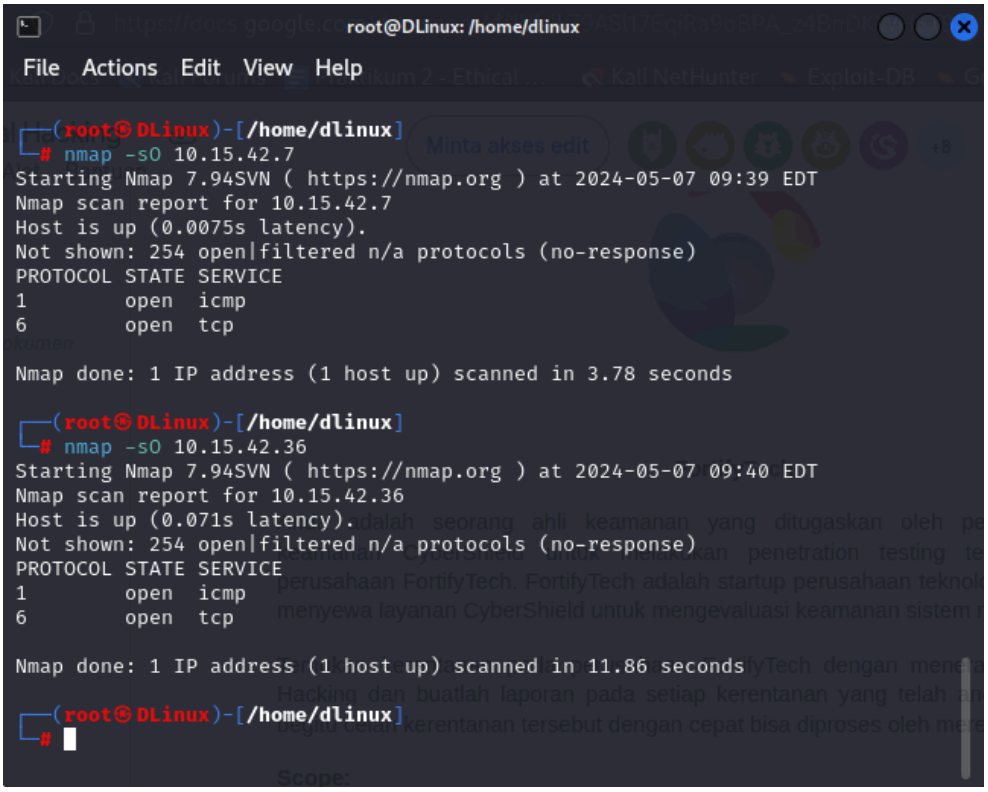
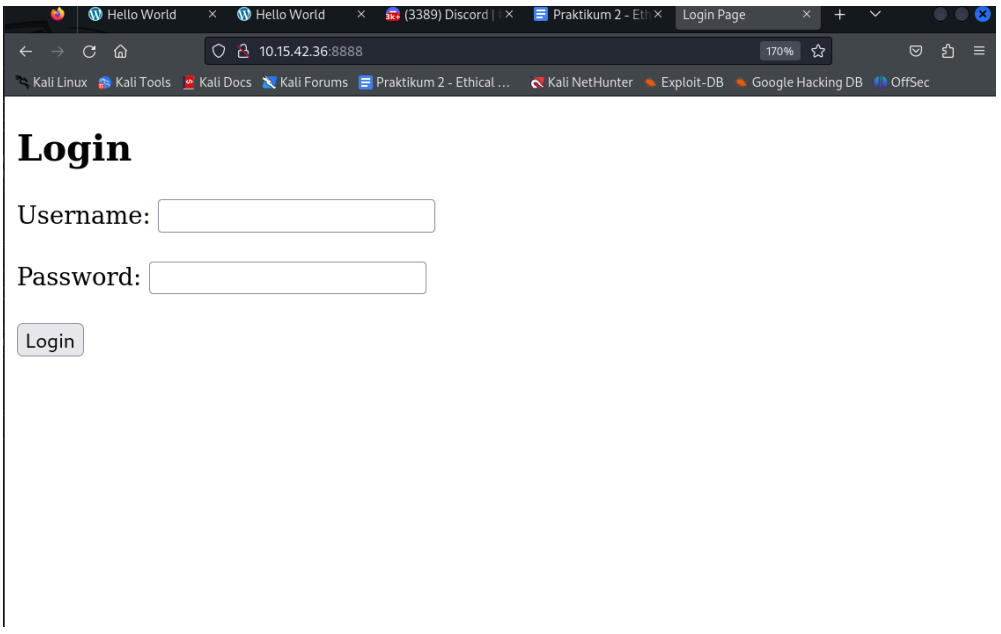

root@DLinux: /home/dlinux
File Actions Edit View Help
┌──(dlinux㉿DLinux)-[~]
└─$ sudo su
[sudo] password for dlinux:
┌──(root㉿DLinux)-[/home/dlinux]
└─# nmap -sV 10.15.42.7
Starting Nmap 7.94SVN (https://nmap.org) at 2024-05-07 09:15 EDT
Nmap scan report for 10.15.42.7
Host is up (0.014s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
80/tcp open http Apache httpd 2.4.59 ((Debian))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.26 seconds
┌──(root㉿DLinux)-[/home/dlinux]
└─# nmap -sV 10.15.42.36
Starting Nmap 7.94SVN (https://nmap.org) at 2024-05-07 09:15 EDT
Nmap scan report for 10.15.42.36
Host is up (0.013s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION

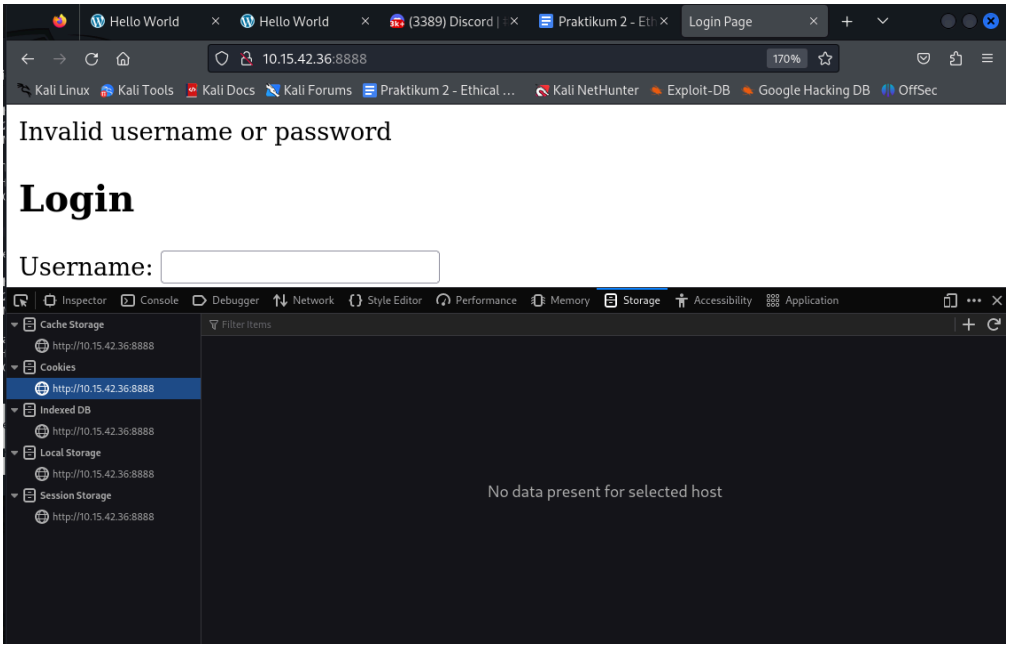

root@DLinux: /home/dlinux
File Actions Edit View Help
2.0)
80/tcp open http Apache httpd 2.4.59 ((Debian))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.26 seconds
┌──(root㉿DLinux)-[/home/dlinux]
└─# nmap -sV 10.15.42.36
Starting Nmap 7.94SVN (https://nmap.org) at 2024-05-07 09:15 EDT
Nmap scan report for 10.15.42.36
Host is up (0.013s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.0.8 or later
22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
8888/tcp open http Apache httpd 2.4.38 ((Debian))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.61 seconds
┌──(root㉿DLinux)-[/home/dlinux]
└─#


root@DLinux: /home/dlinux
File Actions Edit View Help
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.61 seconds
┌──(root㉿DLinux)-[/home/dlinux]
└─# nmap --top-ports 10 10.15.42.36
Starting Nmap 7.94SVN (https://nmap.org) at 2024-05-07 09:19 EDT
Nmap scan report for 10.15.42.36
Host is up (0.017s latency).
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp filtered telnet
25/tcp filtered smtp
80/tcp filtered http
110/tcp filtered pop3
139/tcp filtered netbios-ssn
443/tcp filtered https
445/tcp filtered microsoft-ds
3389/tcp filtered ms-wbt-server
Nmap done: 1 IP address (1 host up) scanned in 1.47 seconds
┌──(root㉿DLinux)-[/home/dlinux]
└─#

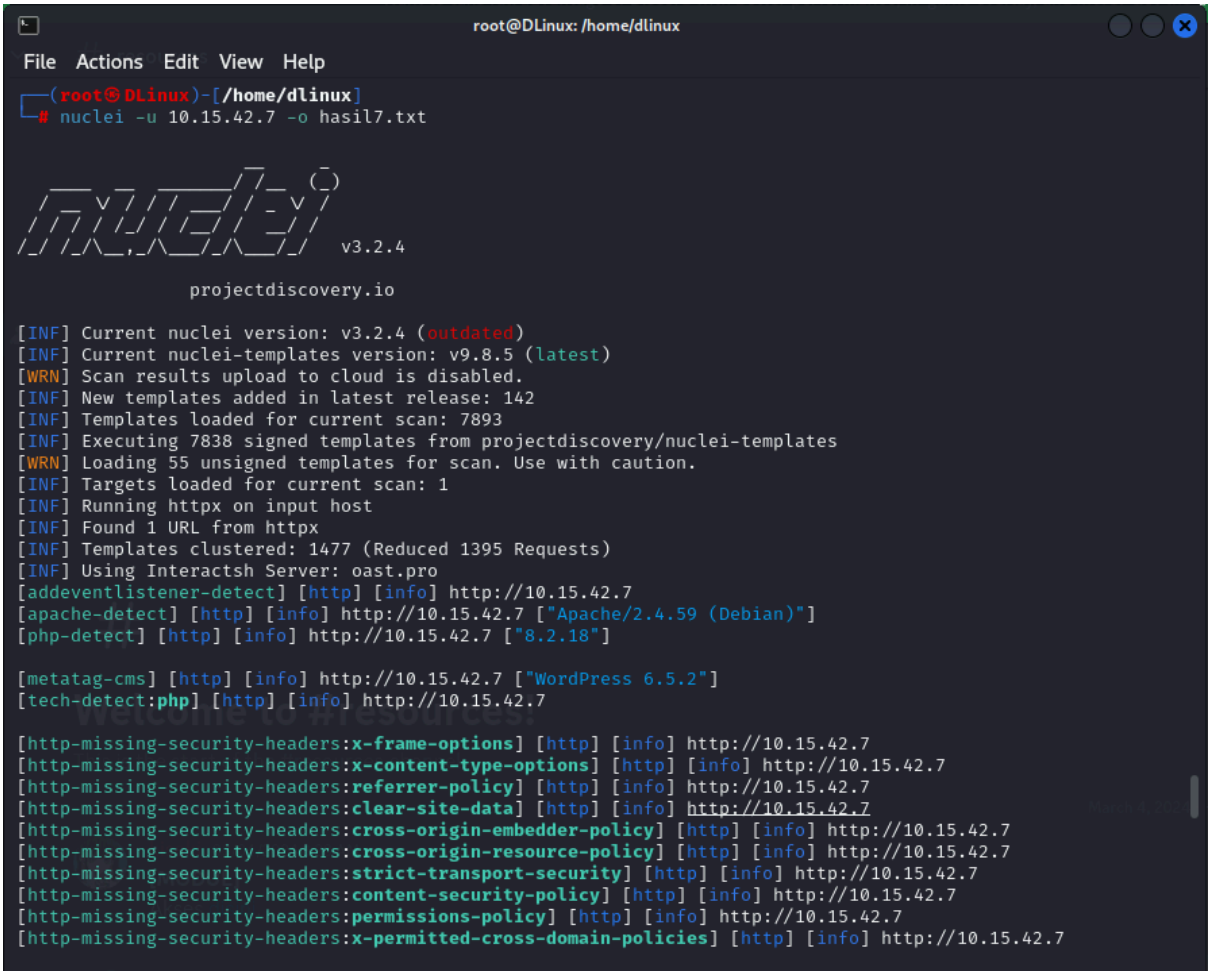

root@DLinux: /home/dlinux
File Actions Edit View Help
445/tcp filtered microsoft-ds
3389/tcp filtered ms-wbt-server
Nmap done: 1 IP address (1 host up) scanned in 1.47 seconds
┌──(root㉿DLinux)-[/home/dlinux]
└─# nmap --top-ports 10 10.15.42.7
Starting Nmap 7.94SVN (https://nmap.org) at 2024-05-07 09:22 EDT
Nmap scan report for 10.15.42.7
Host is up (0.052s latency).
PORT STATE SERVICE
21/tcp filtered ftp
22/tcp open ssh
23/tcp filtered telnet
25/tcp filtered smtp
80/tcp open http
110/tcp filtered pop3
139/tcp filtered netbios-ssn
443/tcp filtered https
445/tcp filtered microsoft-ds
3389/tcp filtered ms-wbt-server
Nmap done: 1 IP address (1 host up) scanned in 1.77 seconds
┌──(root㉿DLinux)-[/home/dlinux]
└─#


root@DLinux: /home/dlinux
File Actions Edit View Help
┌──(root㉿DLinux)-[/home/dlinux]
└─# nmap -sO 10.15.42.7
Starting Nmap 7.94SVN (https://nmap.org) at 2024-05-07 09:39 EDT
Nmap scan report for 10.15.42.7
Host is up (0.0075s latency).
Not shown: 254 open|filtered n/a protocols (no-response)
PROTOCOL STATE SERVICE
1 open icmp
6 open tcp
Nmap done: 1 IP address (1 host up) scanned in 3.78 seconds
┌──(root㉿DLinux)-[/home/dlinux]
└─# nmap -sO 10.15.42.36
Starting Nmap 7.94SVN (https://nmap.org) at 2024-05-07 09:40 EDT
Nmap scan report for 10.15.42.36
Host is up (0.071s latency).
Not shown: 254 open|filtered n/a protocols (no-response)
PROTOCOL STATE SERVICE
1 open icmp
6 open tcp
Nmap done: 1 IP address (1 host up) scanned in 11.86 seconds
┌──(root㉿DLinux)-[/home/dlinux]
└─#

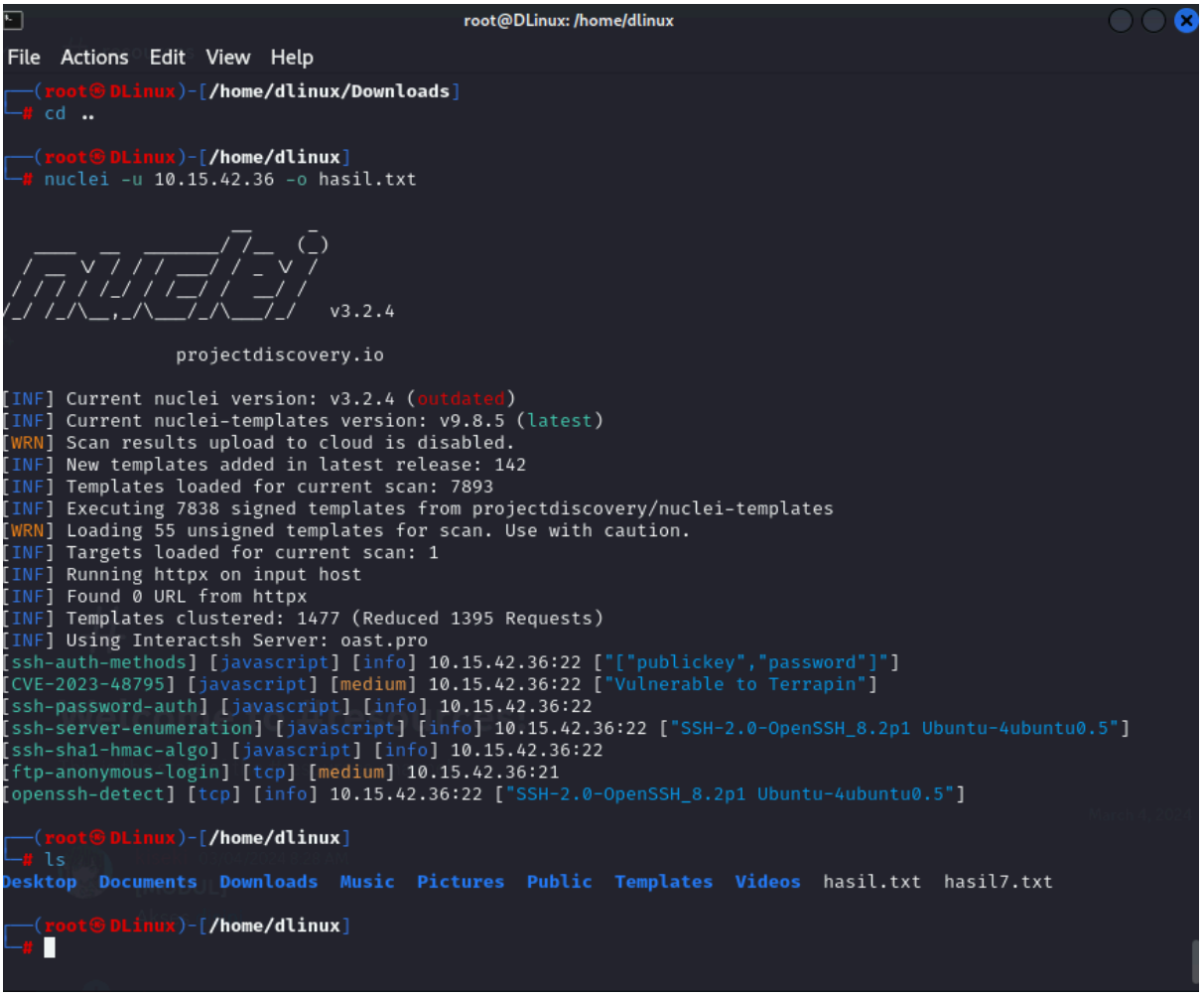

Hello World
Hello World
(3389) Discord
Praktikum 2 - Et
Login Page
10.15.42.36:8888
170%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Praktikum 2 - Ethical ...
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Login
Username:
Password:
Login



ketika coba untuk cek dari console bagian storage tidak menemukan data apapun tapi ada site cookies




root@DLinux: /home/dlinux
File Actions Edit View Help
[apache-detect] [http] [info] http://10.15.42.7 ["Apache/2.4.59 (Debian)"]
[php-detect] [http] [info] http://10.15.42.7 ["8.2.18"]
[metatag-cms] [http] [info] http://10.15.42.7 ["WordPress 6.5.2"]
[tech-detect:php] [http] [info] http://10.15.42.7
[http-missing-security-headers:x-frame-options] [http] [info] http://10.15.42.7
[http-missing-security-headers:x-content-type-options] [http] [info] http://10.15.42.7
[http-missing-security-headers:referrer-policy] [http] [info] http://10.15.42.7
[http-missing-security-headers:clear-site-data] [http] [info] http://10.15.42.7
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] http://10.15.42.7
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] http://10.15.42.7
[http-missing-security-headers:strict-transport-security] [http] [info] http://10.15.42.7
[http-missing-security-headers:content-security-policy] [http] [info] http://10.15.42.7
[http-missing-security-headers:permissions-policy] [http] [info] http://10.15.42.7
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://10.15.42.7
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://10.15.42.7
[mixed-passive-content:img] [http] [info] http://10.15.42.7 ["http://10.15.42.7/wp-content/themes/twentytwentyfour/assets/images/tourist-and-building.webp","http://10.15.42.7/wp-content/themes/twentytwentyfour/assets/images/windows.webp","http://10.15.42.7/wp-content/themes/twentytwentyfour/assets/images/building-exterior.webp"]
[wordpress-login] [http] [info] http://10.15.42.7/wp-login.php
[wordpress-readme-file] [http] [info] http://10.15.42.7/readme.html
[robots-txt-endpoint] [http] [info] http://10.15.42.7/robots.txt
[missing-sri] [http] [info] http://10.15.42.7 ["http://10.15.42.7/wp-includes/blocks/navigation/view.min.js?ver=6.5.2"]
[wordpress-detect:version_by_js] [http] [info] http://10.15.42.7 ["6.5.2"]
[waf-detect:apachegeneric] [http] [info] http://10.15.42.7
[wordpress-forminator:outdated_version] [http] [info] http://10.15.42.7/wp-content/plugins/forminator/readme.txt ["1.24.6"] [last_version="1.28.0"]
[wordpress-user-enum] [http] [info] http://10.15.42.7/?author=1 ["author/admin"]
[wordpress-rdf-user-enum] [http] [info] http://10.15.42.7/feed/rdf/ ["admin"]
[wordpress-xmlrpc-listmethods] [http] [info] http://10.15.42.7/xmlrpc.php
[wp-license-file] [http] [info] http://10.15.42.7/license.txt
[wp-user-enum:usernames] [http] [low] http://10.15.42.7/wp-json/wp/v2/users/ ["admin"]
[wordpress-xmlrpc-file] [http] [info] http://10.15.42.7/xmlrpc.php
[CVE-2023-48795] [javascript] [medium] 10.15.42.7:22 ["Vulnerable to Terrapin"]
[ssh-auth-methods] [javascript] [info] 10.15.42.7:22 ["["publickey","password"]"]
[ssh-password-auth] [javascript] [info] 10.15.42.7:22
[ssh-server-enumeration] [javascript] [info] 10.15.42.7:22 ["SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5"]



menemukan vulnerable to terrapin dengan CVE
https://nvd.nist.gov/vuln/detail/CVE-2023-48795