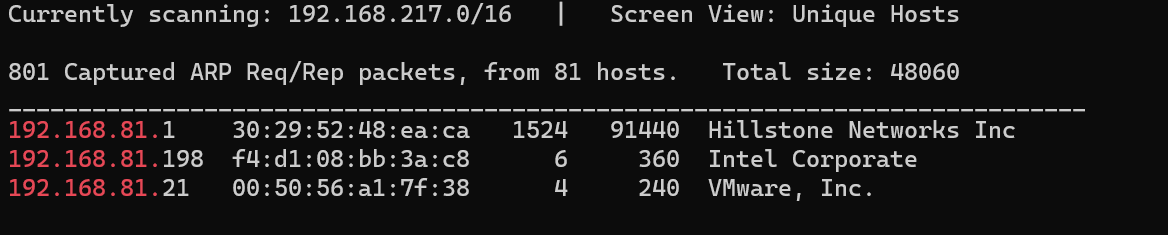
# Kotrix LV1 Write-up by Nagi

## Enumeration

* Sau bao thương đau thì cuối cùng cũng :> biết cách check IP ha :3

Netdiscover | Grep 192.168.x.x



* Scanning : có thể T4 :3 nhưng ko có ghi gì cẩn thận né các kiểu thì T1 :3

sudo nmap -sC -sV -O -p- -vvvv --min-rate=1500 192.168.66.155

PORT STATE SERVICE REASON VERSION

22/tcp open ssh syn-ack ttl 64 OpenSSH 2.9p2 (protocol 1.99)

80/tcp open http syn-ack ttl 64 Apache httpd 1.3.20 ((Unix) (Red-Hat/Linux) mod\_ssl/2.8.4 OpenSSL/0.9.6b)

| http-methods:

| Supported Methods: GET HEAD OPTIONS TRACE

|\_ Potentially risky methods: TRACE

|\_http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod\_ssl/2.8.4 OpenSSL/0.9.6b

|\_http-title: Test Page for the Apache Web Server on Red Hat Linux

111/tcp open rpcbind syn-ack ttl 64 2 (RPC #100000)

| rpcinfo:

| program version port/proto service

| 100000 2 111/tcp rpcbind

| 100000 2 111/udp rpcbind

| 100024 1 1024/tcp status

|\_ 100024 1 1024/udp status

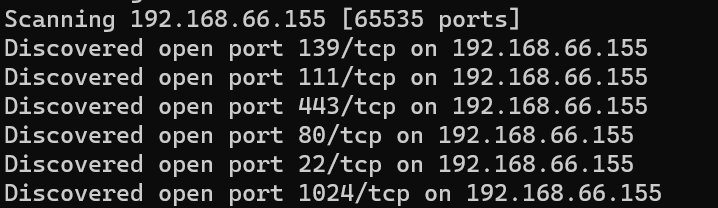
139/tcp open netbios-ssn syn-ack ttl 64 Samba smbd (workgroup: DMYGROUP)

443/tcp open ssl/https syn-ack ttl 64 Apache/1.3.20 (Unix) (Red-Hat/Linux) mod\_ssl/2.8.4 OpenSSL/0.9.6b

|\_http-title: 400 Bad Request

| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=--/emailAddress=root@localhost.localdomain/localityName=SomeCity/organizationalUnitName=SomeOrganizationalUnit

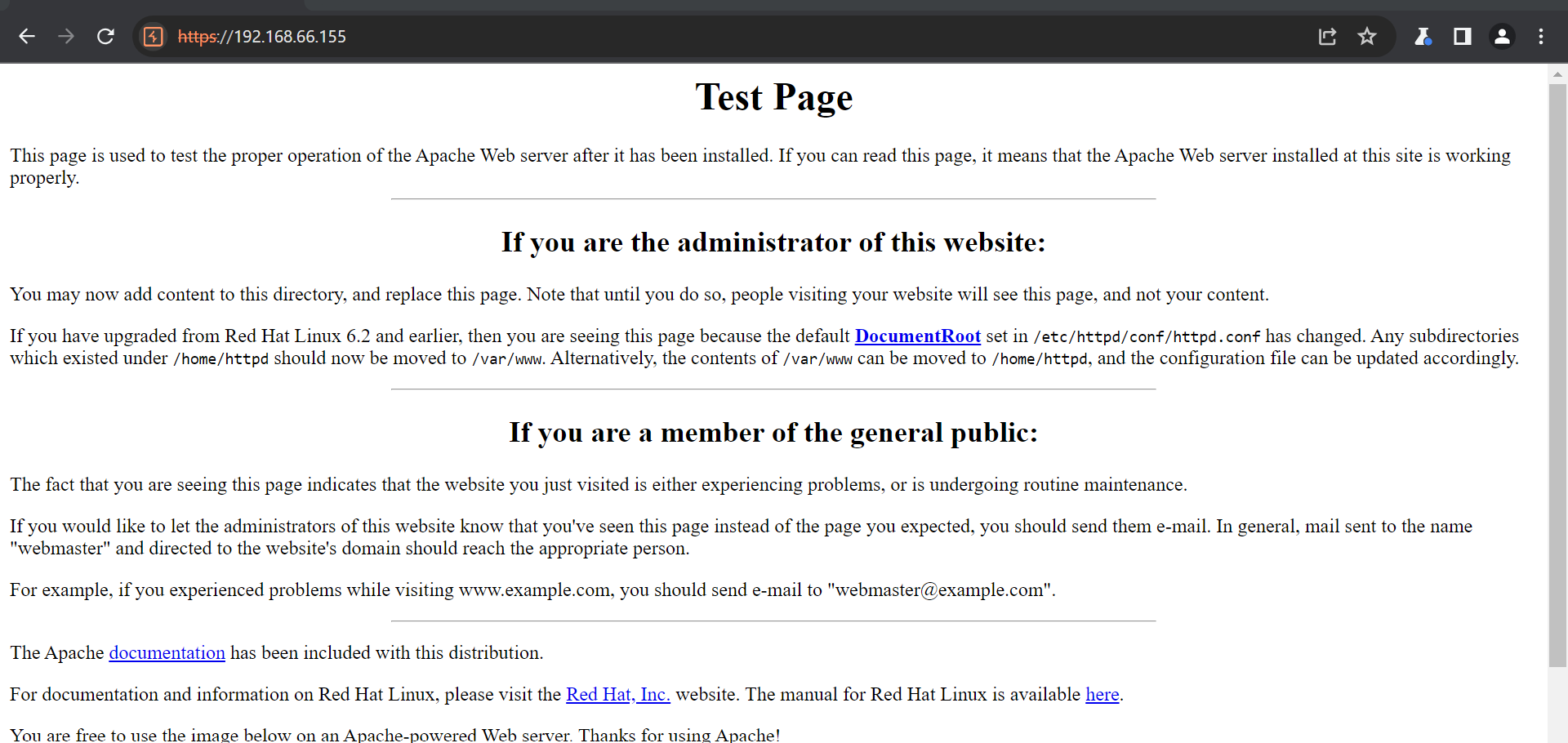
| Issuer: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=--/emailAddress=root@localhost.localdomain/localityName=SomeCity/organizationalUnitName=SomeOrganizationalUnit



Port mở : 22 , 80-443 , 139 111, 1024

Trước mắt cứ tập chung 80 và 22 trước .

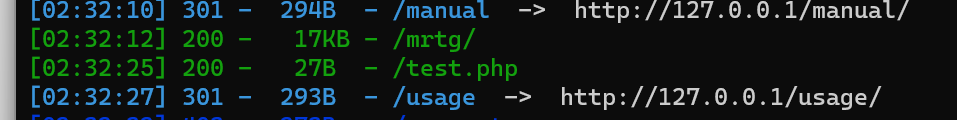
Xem web ntn



Trang test nhưng ko phải default của apache :>

Scan directory xem ntn

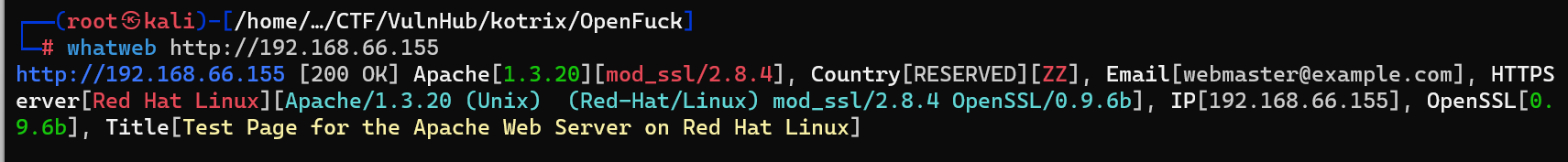
Dirsearch :3



Sau khi dirsearch và lọc hết các page và đọc mấy trang doc tôi không thấy được gì vậy tôi nghĩ rằng web sẽ chẳng có lỗ hổng về mặt code rồi

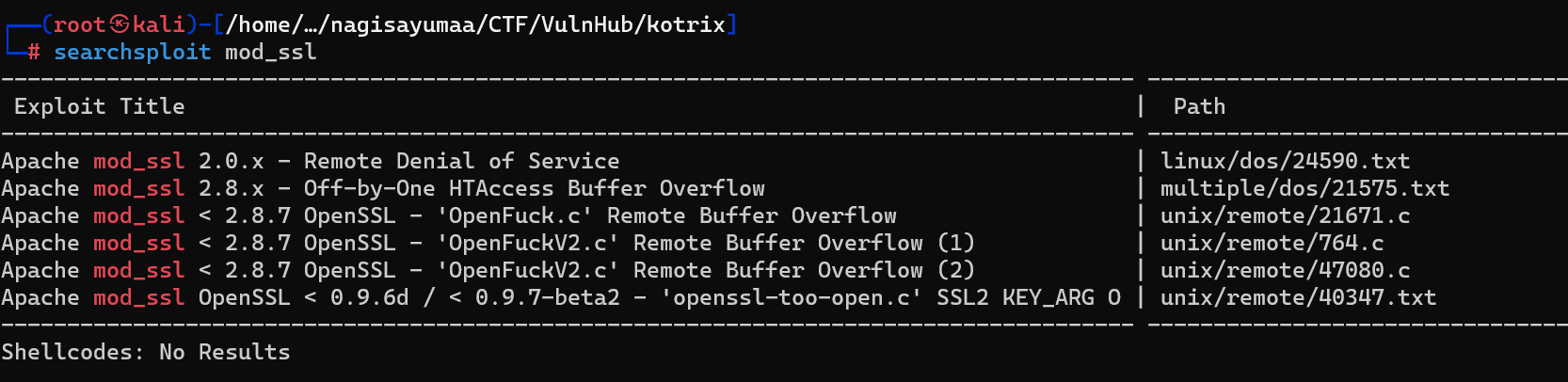
Vậy lỗ hổng ở phiên bản

Oke whatweb

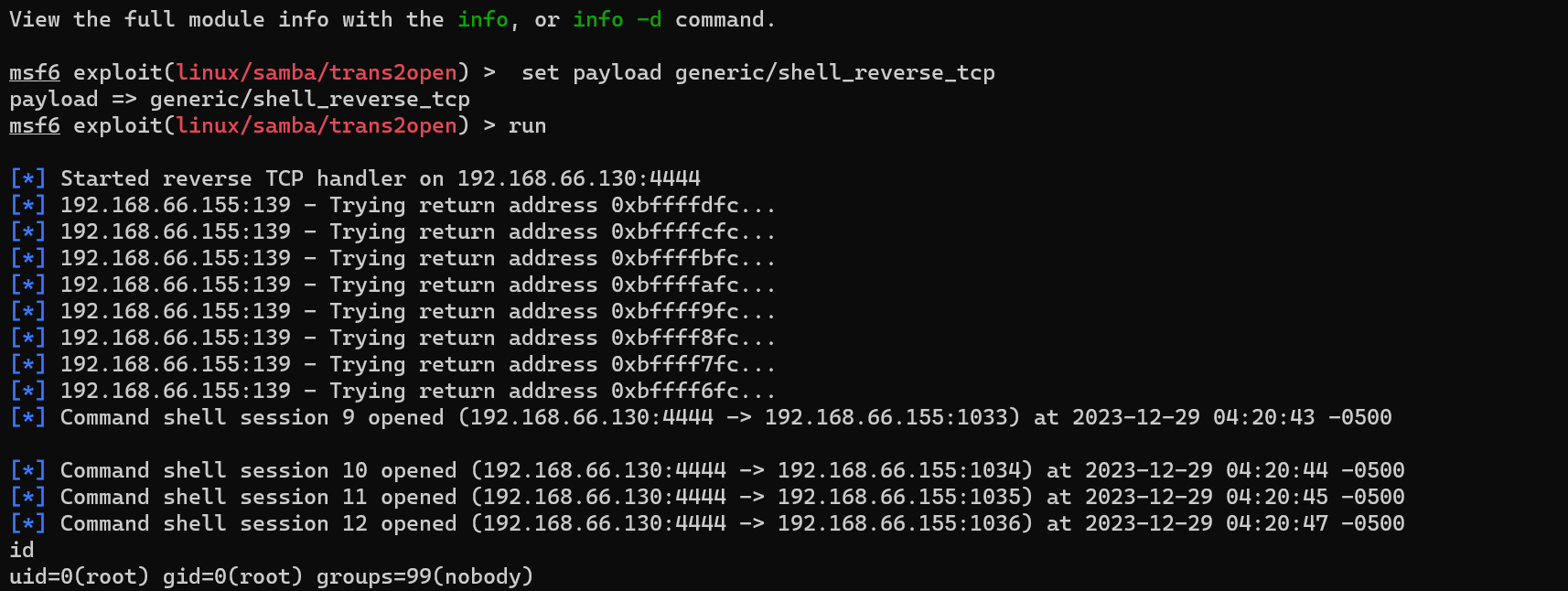


Rồi sau khi search phiên bản thì apache có vẻ ổn

Thì đến version mod\_ssl thì nó bị lỗ hổng và search ra Openfuck code và sau khi search ra từ code này thì vuln 2003-0201



Và bum metasploits thôi



Yah easy to root