0DAY_THM

Enumuration

GObuster reveleade some directories

Tried downloading the turtle pic and then extracting its info but all that was a rabbit hole

Nikto showed that site is potentially vulnerable to a shellshock vulneribility

Nmap

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 57:20:82:3c:62:aa:8f:42:23:c0:b8:93:99:6f:49:9c (DSA)
|   2048 4c:40:db:32:64:0d:11:0c:ef:4f:b8:5b:73:9b:c7:6b (RSA)
|   256 f7:6f:78:d5:83:52:a6:4d:da:21:3c:55:47:b7:2d:6d (ECDSA)
|_  256 a5:b4:f0:84:b6:a7:8d:eb:0a:9d:3e:74:37:33:65:16 (ED25519)
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: 0day
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.10 - 3.13 (95%), Linux 5.4 (95%), ASUS RT-N56U WAP (Linux 3.4) (95%), Linux 3.16 (95%), Linux 3.1 (93%), Linux 3.2 (93%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (92%), Sony Android TV (Android 5.0) (92%), Android 5.0 - 6.0.1 (Linux 3.4) (92%), Android 5.1 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 22/tcp)
HOP RTT       ADDRESS
1   202.21 ms 10.4.0.1
2   ... 3
4   457.75 ms 10.10.253.58

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.11 seconds
```

SSH:22

HTTP:80

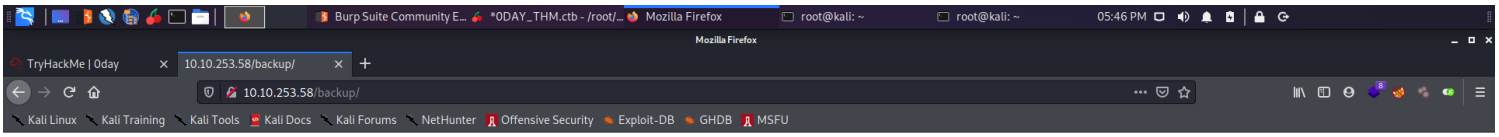
Gobuster

```
/.htpasswd (Status: 403)
/.htaccess (Status: 403)
/.hta (Status: 403)
/admin (Status: 301)
/backup (Status: 301)
/cgi-bin (Status: 301)
/cgi-bin/ (Status: 403)
```

/css (Status: 301)
/img (Status: 301)
/index.html (Status: 200)
/js (Status: 301)
/robots.txt (Status: 200)
/secret (Status: 301)
/server-status (Status: 403)
/uploads (Status: 301)

/backup

#



-----BEGIN RSA PRIVATE KEY----- Proc-Type: 4,ENCRYPTED DEK-Info: AES-128-CBC,82823EE792E75948EE2DE731AF1A0547 T7+F+3ilm5FcFZx24mnrugMY455vI461ziMb4NYk9YJV5uwcrx4QflP2Q2Vk8phx
H4P+PLb79nCc0SrBOPBlB0V3pjLJbf2hKbZazFLtq4FjZq66aLLIr2dRw74MzHSM FznFI7jsxYFwPUqZtkz5sTcX1afch+IU5/Id4zTTsCO8qqs6qv5QkMXVGs77F2kS
Lafx0mJdcuu/5aR3NjNVtluKZyiXInskXiC01+Ynhkqjl4Iy7fEzn2qZnKKPVPv8 9zlECjERSysbUKYccnFknB1DwuJExD/erGRiLBYOGuMatc+EoagKkGpSZm4FtcIO
IrwxeyChI32vJs9W93PUqHMgCJGXEpY7/INMUQahDf3wnlVhBC10UWH9piIOupNN SkjSbrIxOgWJhIcpE9BLVUE4ndAMi3t05MY1U0ko7/vvhzndeZcWhVJ3SdcIAx4g /5D/YqcLtt
/tKbLyuyggk23NzuspnbUwZWoo5fvg+jEgRud90s4dDWMEURGdB2Wt w7uYJFhjijw8tw8WwaPHHQeYtHgrtwhmC/gLj1gxAq532QAgmXGoazXd3IeFRtGB 6+HLDl8VRDz1/4iZhafDC2gihKeWOjmLh83QqKwa4s1XIB6BKPZS
/OgyM4RMnN3u Zmv1rDPL+0yzt6A5BHENXfkNfFWRWQxvKtiGlSLmywPP5OHnv0mzb16QG0Es1FPl xhVyHt/WKlaVZfTdrJneTn8Uu3vZ82MFf+evbdMPZMx9Xc3Ix7/hFeIxCdoMN4i6 8BoZFQBcoJaOufnLkTC0hHxN7T/t
/QvcaIsWSFWdgwwnYFaJncHeEj7d1hnmsAii b79Dfy384/lnjZMtX1NXIEghzQj5ga8TFnHe8umDNx5Cq5GpYN1BUtfWFYqtkGcn vzLSJM07RAgqA+SPAY8lCnXe8gN+Nv/9+/+/uiefeFtOmrpDU2kRfr9JhZYx9TkL
wTqOP0XWjqufWNEIXXIpwXFctpZaEQcC40LpbBGTDiVWTQyx8AuI6YOflt+k64fG rtfjWPVv3yGOJmiqQOa8/pDGgtNPgnJmFFrBy2d37KzSoNpTlXmeT/drkeTaP6YW
RTz8Ieg+fmVtsgQelZQ44mhy0vE48o92Kxj3uAB6jZp8jxgACpcNBt3isg7H/dq6 oYiTtCJrL3IctTrEuBW8gE37UbSRqTuj9Foy+ynGmNPx5HQeC5aO/GoeSH0FelTk cQKiDDxHq7mLMJZJO0oqdJfs6Jt/JO4gzdBh3Jt0gBoKnXMVY7P5u8da
/4sV+kJE 99x7Dh8YXnj1As2gY+MMQHVuvCpnwRR7XLmK8Fj3TZU+WHK5P6W5fLK7u3MVt1eq Ezf26lghbnEUn17KKu+VQ6EdIPL150HSks5V+2fC8JTQ1fl3rI9vowPPuC8aNj+Q
Qu5m65A5Urmr8Y01/Wjqn2wC7upxzt6hNBIMbcNrndZkg80feKZ8RD7wE7Exll2h v3SBMMCT5ZrBFq54ia0ohThQ8hklPqYhdSebkQtU5HPYh+EL/vU1L9PfGv0zipst
gbLFOSPp+GmklnRpihaXaGYXsoKfXvAxGCVIhbaWLAp5AybIiXHyBWsbhbSRMK+P -----END RSA PRIVATE KEY-----

#

Exploitation

Enumuration confirmed that machine is vulnerable to cve-2014-6278

Researching showed us that we can use msf for this so i did this metasploit way

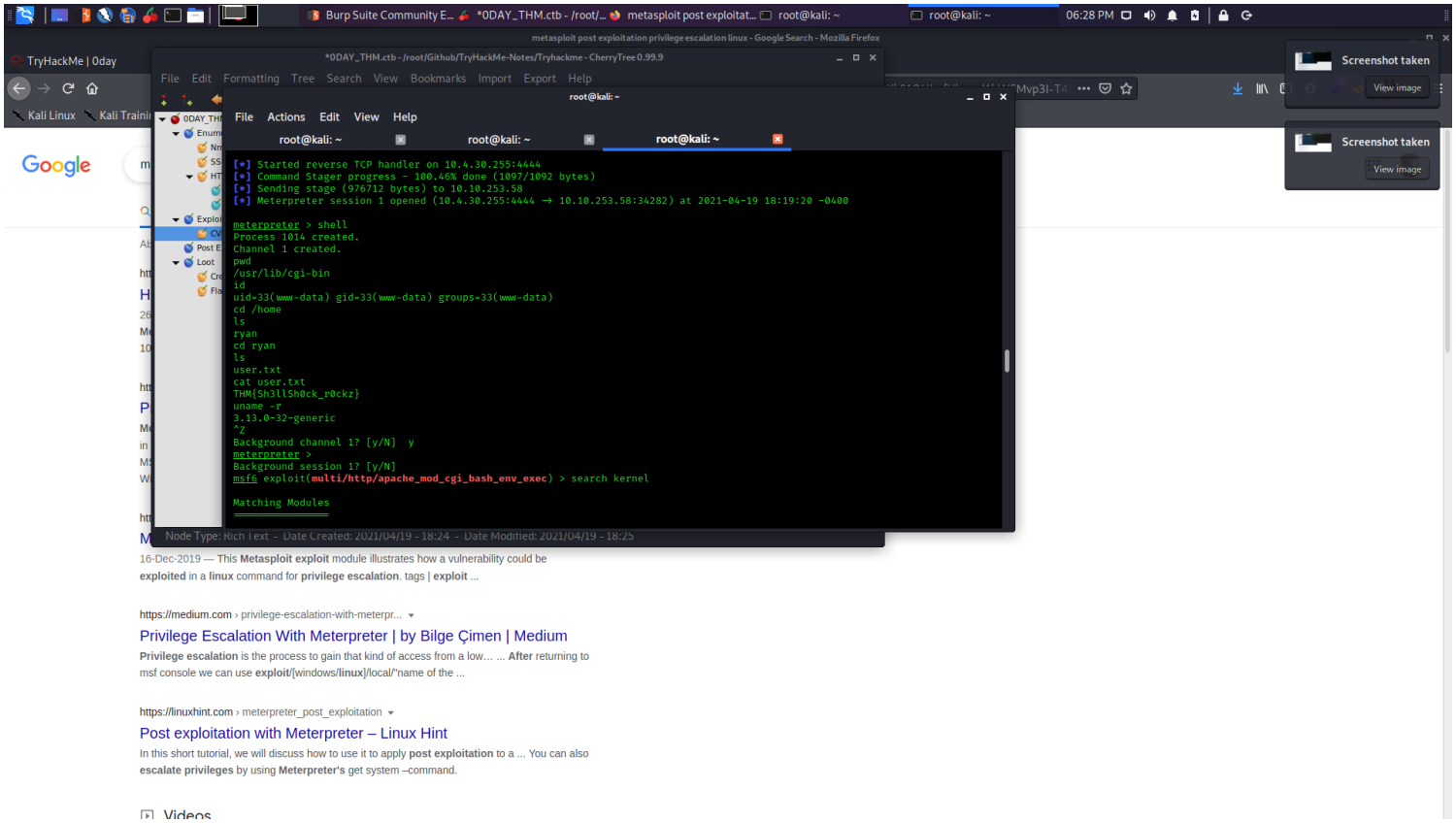
There were many exploits and i tried and got lucky with exploit/multi/http/apache_mod_cgi_bash_env_exec

CVE -2014-6278

We use metasploit module for this exploit

exploit/multi/http/apache_mod_cgi_bash_env_exec

we get a meterpreter session Exploit MOdule used multi/http/apache_mod_cgi_bash_env_exec



Got the user flag

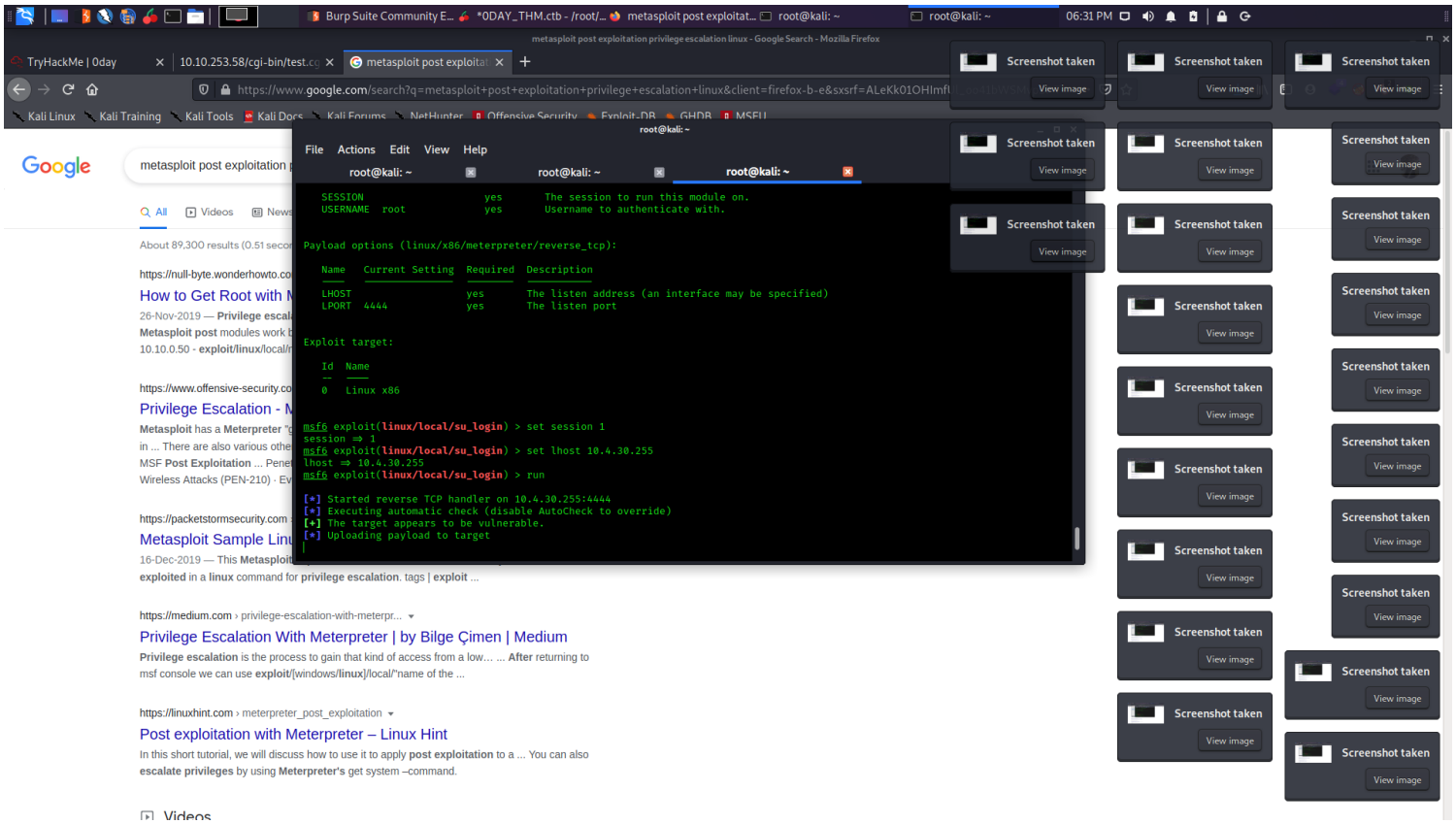
Now using local exploit suggestor of msf for privesc as system version is very old running on the box

Post Exploitation

To get root we see that kernel is very old

We use msf local exploit suggestor to get some local exploits for privesc

#



We use linux/local/overlayfs_priv_esc module but the exploit failed at first.Then i checked targets and this exploit targeted two different vulneribilities so i switched and selected the target to 0 which was cve-2015-1328 [linux/local/overlayfs_priv_esc]

Exploit worked and we got root

linux/local/overlayfs_priv_esc

As linux version is 3.13.0-32-generic its a old version and is likely vulerable to kernel exploits

linux/local/overlayfs_priv_esc is module which suggester showed us and is likely vulnerable

#

we set target to 0 which is cve-2015-1328

we run this and get root

Loot

Credentials

Flags

#User Flag

THM{Sh3llSh0ck_r0ckz}

Root Flag

THM{g00d_j0b_0day_is_Pleased}