The Nessus Client/Server Communication: NTP 1.2 Protocol Analysis

1. Overview

The Nessus communication protocol NTP (Nessus Transfer Protocol) is not well documented and not easy to understand. This document shows examples of a Nessus client/server communication on a NessusWX client (version 1.4.4) with a Nessus server (version 2.2.0). For simplification and readability, the communication examples were taken from unencrypted connections by setting the option “ssl_version=none” in <nessus-home>/etc/nessus/nessusd.conf. Encrypted communication is identical and just runs on top of a SSL protocol connection.

The packet examples have been generated with tcpdump from live connections and have been filtered and exported with Ethereal (version 0.10.8) using the “print” option (Settings: “Plain Text”, “Output to File”, “Packet Summary Line”, “Output Bytes”). In most instances below, ACK packets have been intentionally left out to further shorten the text and improve readability, as they are only packet receipts of little educational relevance.

The packet data has been colored for better readability using the following code:

A grey header bar indicates a new packet and shows the direction with the source & destination IP address	▨	(Grey 30%)
Control character/terminator (newline '\n' – hex: 0a):	🟦	(Tourqoise 3)
NTP protocol control strings (commands, markers):	🟩	(Green 4)
NTP protocol data (plugins, preferences, rules, etc):	🟧	(Orange 4)

Author: Frank4DD, January 6th, 2005 http://www.frank4dd.com

2. Nessus client: Successful login and server configuration dump

Here is a example of a sucessful client login with IP 192.168.11.12 to a Nessus server with IP 192.168.11.8 on the standard Nessus port TCP/1241.

Initialisation Phase 0: Standard TCP 3-Way Syn/SYN-ACK/ACK Handshake between client and server.

```
No.    Time         Source                 Destination            Protocol
1      0.000000     192.168.11.12          192.168.11.8           TCP

2204 > 1241 [SYN] Seq=0 Ack=0 Win=65535 Len=0 MSS=1260

0000   00 00 39 ae d6 25 00 02 b3 da 4b 8d 08 00 45 00   ..9..%....K...E.
0010   00 30 ad 9a 40 00 80 06 b5 c8 c0 a8 0b 0c c0 a8   .0..@...........
0020   0b 08 08 9c 04 d9 db 44 ff f8 00 00 00 00 70 02   .......D......p.
0030   ff ff 03 d0 00 00 02 04 04 ec 01 01 04 02         ..............
```

```
No.    Time         Source                 Destination            Protocol
2      0.000112     192.168.11.8           192.168.11.12          TCP

1241 > 2204 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460

0000   00 02 b3 da 4b 8d 00 00 39 ae d6 25 08 00 45 00   ....K...9..%..E.
0010   00 30 4b 96 40 00 40 06 57 cd c0 a8 0b 08 c0 a8   .0K.@.@.W.......
0020   0b 0c 04 d9 08 9c 6d 9e bd d0 db 44 ff f9 70 12   ......m....D..p.
0030   16 d0 c0 b7 00 00 02 04 05 b4 01 01 04 02         ..............
```

```
No.    Time          Source                Destination           Protocol
3      0.000238      192.168.11.12         192.168.11.8          TCP

2204 > 1241 [ACK] Seq=1 Ack=1 Win=65535 Len=0

0000   00 00 39 ae d6 25 00 02 b3 da 4b 8d 08 00 45 00   ..9..%....K...E.
0010   00 28 ad 9b 40 00 80 06 b5 cf c0 a8 0b 0c c0 a8   .(..@...........
0020   0b 08 08 9c 04 d9 db 44 ff f9 6d 9e bd d1 50 10   .......D..m...P.
0030   ff ff 04 4c 00 00 00 00 00 00 00 00               ...L........
```

Initialisation Phase 1: The client sends its NTP version string (12 bytes) to the server, terminated by newline '\n' (hex: 0a).

```
No.    Time          Source                Destination           Protocol
4      0.000636      192.168.11.12         192.168.11.8          TCP

2204 > 1241 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=12

0000   00 00 39 ae d6 25 00 02 b3 da 4b 8d 08 00 45 00   ..9..%....K...E.
0010   00 34 ad 9c 40 00 80 06 b5 c2 c0 a8 0b 0c c0 a8   .4..@...........
0020   0b 08 08 9c 04 d9 db 44 ff f9 6d 9e bd d1 50 18   .......D..m...P.
0030   ff ff 88 3b 00 00 3c 20 4e 54 50 2f 31 2e 32 20   ...;..< NTP/1.2 
0040   3e 0a                                             >.
```

Initialisation Phase 2: The server responds with its NTP version string (12 bytes) to the client, terminated by a newline '\n' (hex: 0a).

```
No.    Time          Source                Destination           Protocol
6      0.002200      192.168.11.8          192.168.11.12         TCP

1241 > 2204 [PSH, ACK] Seq=1 Ack=13 Win=5840 Len=12

0000   00 02 b3 da 4b 8d 00 00 39 ae d6 25 08 00 45 00   ....K...9..%..E.
0010   00 34 4b 98 40 00 40 06 57 c7 c0 a8 0b 08 c0 a8   .4K.@.@.W.......
0020   0b 0c 04 d9 08 9c 6d 9e bd d1 db 45 00 05 50 18   ......m....E..P.
0030   16 d0 71 5f 00 00 3c 20 4e 54 50 2f 31 2e 32 20   ..q_..< NTP/1.2 
0040   3e 0a                                             >.
```

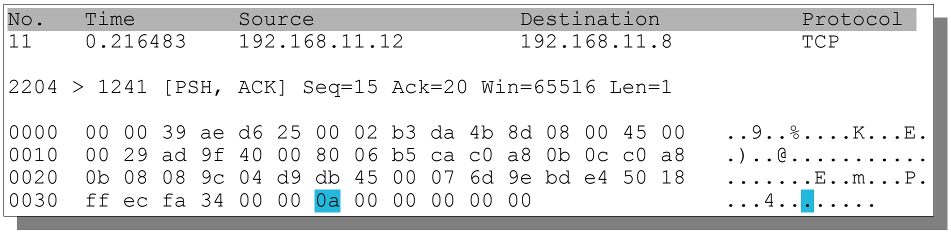
Initialisation Phase 3: The server continues to send the User prompt (7 bytes) to client, not terminated but including a trailing space ' ' (hex: 20) at the end.

```
No.    Time          Source                Destination           Protocol
8      0.176395      192.168.11.8          192.168.11.12         TCP

1241 > 2204 [PSH, ACK] Seq=13 Ack=13 Win=5840 Len=7

0000   00 02 b3 da 4b 8d 00 00 39 ae d6 25 08 00 45 00   ....K...9..%..E.
0010   00 2f 4b 99 40 00 40 06 57 cb c0 a8 0b 08 c0 a8   ./K.@.@.W.......
0020   0b 0c 04 d9 08 9c 6d 9e bd dd db 45 00 05 50 18   ......m....E..P.
0030   16 d0 f2 34 00 00 55 73 65 72 20 3a 20            ...4..User : 
```

Initialisation Phase 4: The client sends the username 'fm' to the server (3 bytes), with a newline '\n' (hex: 0a). The termination at the end is transmitted in a subsequent packet on its own.

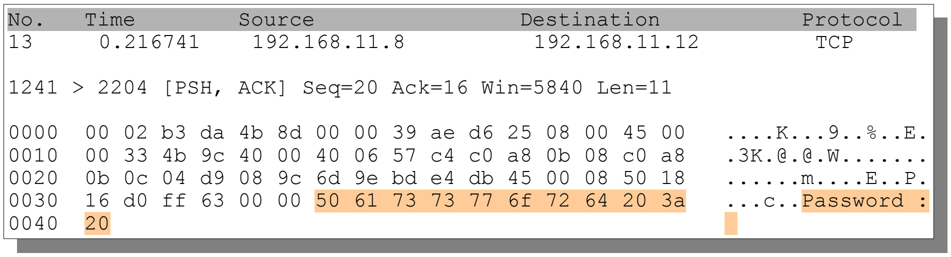
```
No.    Time          Source                Destination           Protocol
9      0.176581      192.168.11.12         192.168.11.8          TCP

2204 > 1241 [PSH, ACK] Seq=13 Ack=20 Win=65516 Len=2

0000   00 00 39 ae d6 25 00 02 b3 da 4b 8d 08 00 45 00   ..9..%....K...E.
0010   00 2a ad 9e 40 00 80 06 b5 ca c0 a8 0b 0c c0 a8   .*..@...........
0020   0b 08 08 9c 04 d9 db 45 00 05 6d 9e bd e4 50 18   .......E..m...P.
0030   ff ec 9d c8 00 00 66 6d 00 00 00 00               ......fm....
```

Initialisation Phase 4: The client sends the remaining newline '\n' termination for the username.



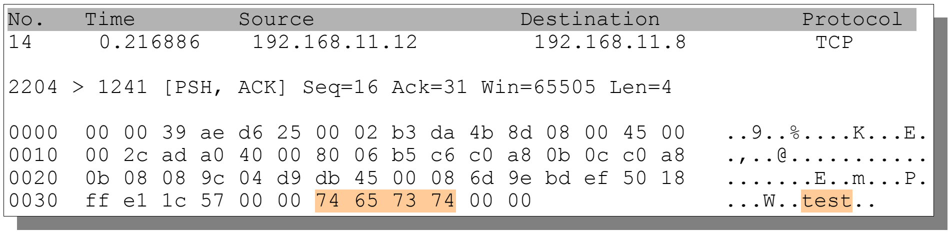
```
No.    Time         Source                Destination           Protocol
11     0.216483     192.168.11.12         192.168.11.8          TCP

2204 > 1241 [PSH, ACK] Seq=15 Ack=20 Win=65516 Len=1

0000   00 00 39 ae d6 25 00 02 b3 da 4b 8d 08 00 45 00   ..9..%....K...E.
0010   00 29 ad 9f 40 00 80 06 b5 ca c0 a8 0b 0c c0 a8   .)..@...........
0020   0b 08 08 9c 04 d9 db 45 00 07 6d 9e bd e4 50 18   .......E..m...P.
0030   ff ec fa 34 00 00 0a 00 00 00 00 00               ...4........
```

Initialisation Phase 5: The server sends the password prompt (11 bytes), with a space ' ' (hex: 20) and no newline termination at the end.



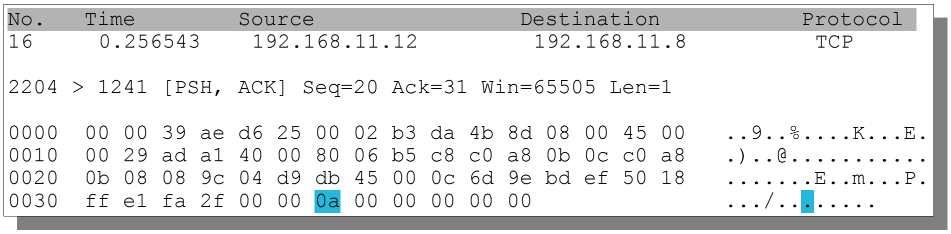
```
No.    Time         Source                Destination           Protocol
13      0.216741     192.168.11.8          192.168.11.12         TCP

1241 > 2204 [PSH, ACK] Seq=20 Ack=16 Win=5840 Len=11

0000   00 02 b3 da 4b 8d 00 00 39 ae d6 25 08 00 45 00   ....K...9..%..E.
0010   00 33 4b 9c 40 00 40 06 57 c4 c0 a8 0b 08 c0 a8   .3K.@.@.W.......
0020   0b 0c 04 d9 08 9c 6d 9e bd e4 db 45 00 08 50 18   ......m....E..P.
0030   16 d0 ff 63 00 00 50 61 73 73 77 6f 72 64 20 3a   ...c..Password :
0040   20                                                
```

Initialisation Phase 5: The client sends the password string 'test' (4 bytes) plus the newline '\n' (hex: 0a) termination in a subsequent packet.



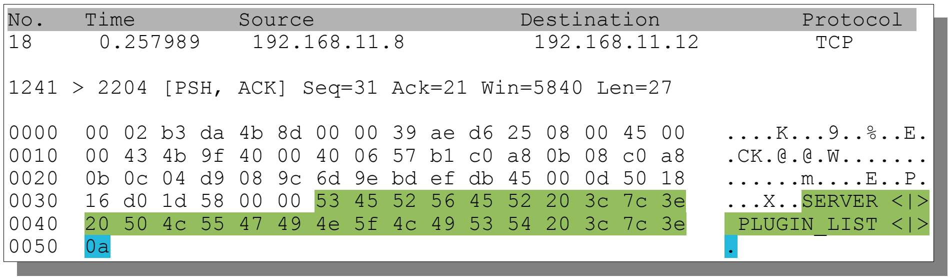
```
No.    Time         Source                Destination           Protocol
14      0.216886     192.168.11.12         192.168.11.8          TCP

2204 > 1241 [PSH, ACK] Seq=16 Ack=31 Win=65505 Len=4

0000   00 00 39 ae d6 25 00 02 b3 da 4b 8d 08 00 45 00   ..9..%....K...E.
0010   00 2c ad a0 40 00 80 06 b5 c6 c0 a8 0b 0c c0 a8   .,..@...........
0020   0b 08 08 9c 04 d9 db 45 00 08 6d 9e bd ef 50 18   .......E..m...P.
0030   ff e1 1c 57 00 00 74 65 73 74 00 00               ...W..test..
```

Initialisation Phase 5: The client sends the newline '\n' (hex: 0a) termination for the password string.



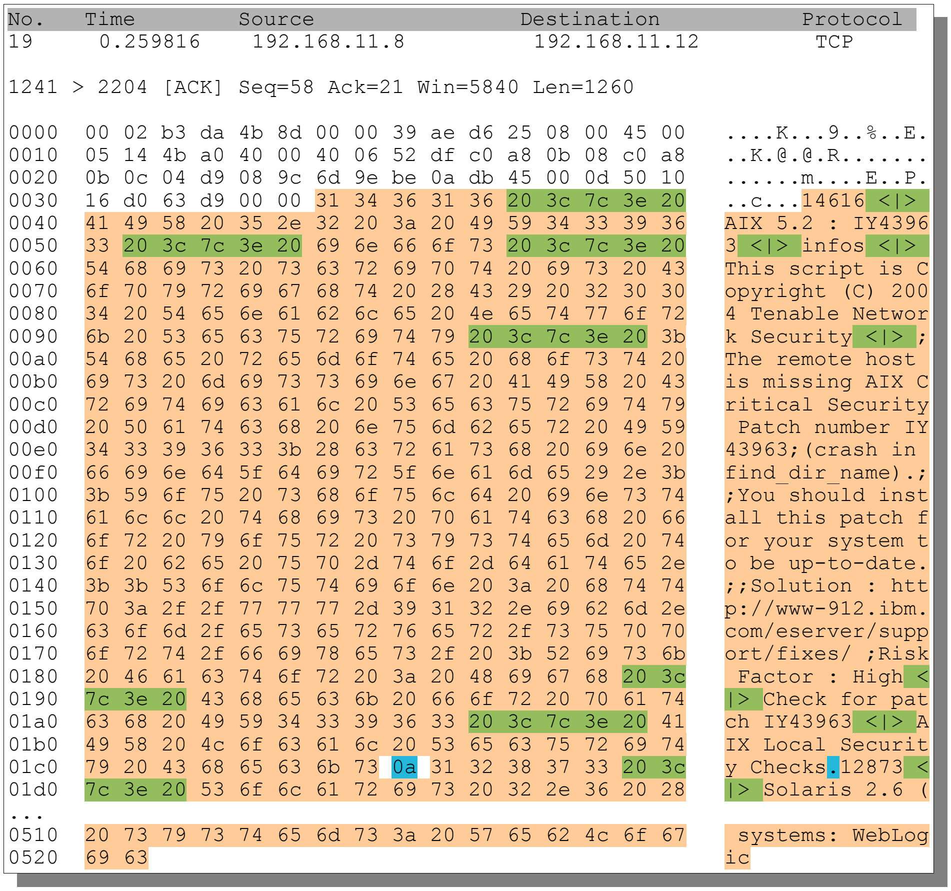
```
No.    Time         Source                Destination           Protocol
16      0.256543     192.168.11.12         192.168.11.8          TCP

2204 > 1241 [PSH, ACK] Seq=20 Ack=31 Win=65505 Len=1

0000   00 00 39 ae d6 25 00 02 b3 da 4b 8d 08 00 45 00   ..9..%....K...E.
0010   00 29 ad a1 40 00 80 06 b5 c8 c0 a8 0b 0c c0 a8   .)..@...........
0020   0b 08 08 9c 04 d9 db 45 00 0c 6d 9e bd ef 50 18   .......E..m...P.
0030   ff e1 fa 2f 00 00 0a 00 00 00 00 00               .../........
```

Initialisation Phase 6: Login Complete. The server sends a start marker (27 bytes) to dump its configuration, including the newline '\n' (hex: 0a) termination.

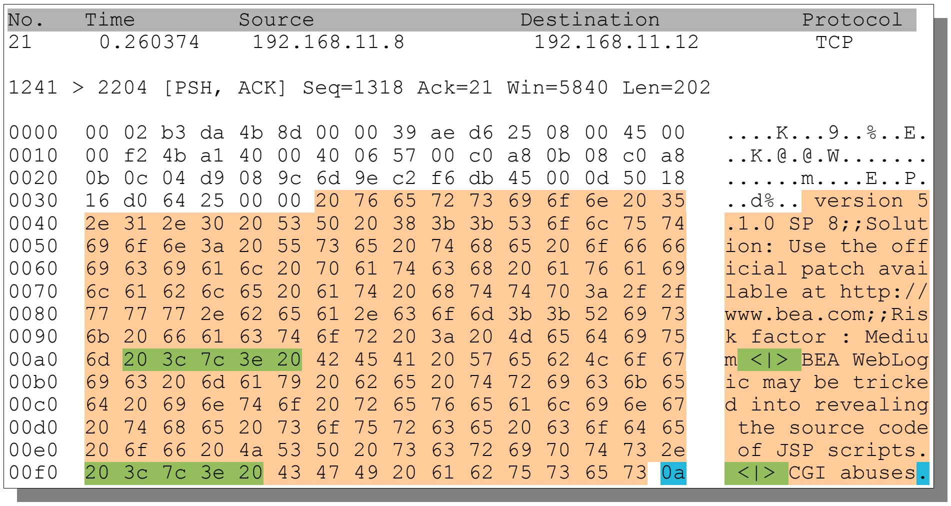


```
No.    Time         Source                Destination           Protocol
18      0.257989     192.168.11.8          192.168.11.12         TCP

1241 > 2204 [PSH, ACK] Seq=31 Ack=21 Win=5840 Len=27

0000   00 02 b3 da 4b 8d 00 00 39 ae d6 25 08 00 45 00   ....K...9..%..E.
0010   00 43 4b 9f 40 00 40 06 57 b1 c0 a8 0b 08 c0 a8   .CK.@.@.W.......
0020   0b 0c 04 d9 08 9c 6d 9e bd ef db 45 00 0d 50 18   ......m....E..P.
0030   16 d0 1d 58 00 00 53 45 52 56 45 52 20 3c 7c 3e   ...X..SERVER <|>
0040   20 50 4c 55 47 49 4e 5f 4c 49 53 54 20 3c 7c 3e    PLUGIN_LIST <|>
0050   0a                                                .
```

Initialisation complete: The server continues to dump its configuration data, starting with the plugin list. Each plugin consists of seven fields (Plugin ID, Plugin Name, Category, Author, Description, Summary and Family), which are separated by a " <|> " string (hex: 20 3c 7c 3e 20). Each plugin is terminated by a newline '\n' character.

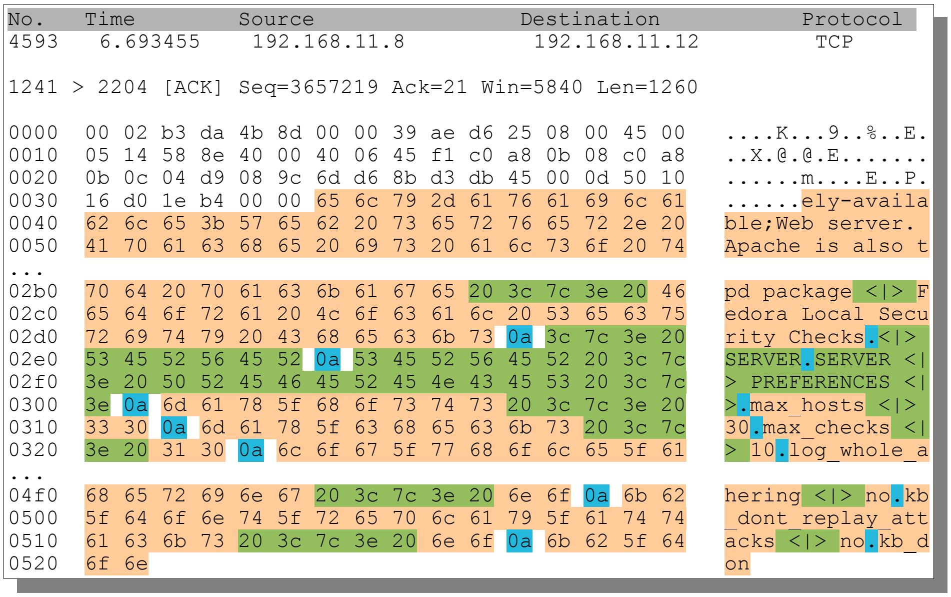


```
No.    Time          Source                       Destination                 Protocol
19      0.259816      192.168.11.8                 192.168.11.12               TCP

1241 > 2204 [ACK] Seq=58 Ack=21 Win=5840 Len=1260

0000   00 02 b3 da 4b 8d 00 00 39 ae d6 25 08 00 45 00    ....K...9..%..E.
0010   05 14 4b a0 40 00 40 06 52 df c0 a8 0b 08 c0 a8    ..K.@.@.R.......
0020   0b 0c 04 d9 08 9c 6d 9e be 0a db 45 00 0d 50 10    ......m....E..P.
0030   16 d0 63 d9 00 00 31 34 36 31 36 20 3c 7c 3e 20    ..c...14616 <|>
0040   41 49 58 20 35 2e 32 20 3a 20 49 59 34 33 39 36    AIX 5.2 : IY4396
0050   33 20 3c 7c 3e 20 69 6e 66 6f 73 20 3c 7c 3e 20    3 <|> infos <|>
0060   54 68 69 73 20 73 63 72 69 70 74 20 69 73 20 43    This script is C
0070   6f 70 79 72 69 67 68 74 20 28 43 29 20 32 30 30    opyright (C) 200
0080   34 20 54 65 6e 61 62 6c 65 20 4e 65 74 77 6f 72    4 Tenable Networ
0090   6b 20 53 65 63 75 72 69 74 79 20 3c 7c 3e 20 3b    k Security <|> ;
00a0   54 68 65 20 72 65 6d 6f 74 65 20 68 6f 73 74 20    The remote host
00b0   69 73 20 6d 69 73 73 69 6e 67 20 41 49 58 20 43    is missing AIX C
00c0   72 69 74 69 63 61 6c 20 53 65 63 75 72 69 74 79    ritical Security
00d0   20 50 61 74 63 68 20 6e 75 6d 62 65 72 20 49 59     Patch number IY
00e0   34 33 39 36 33 3b 28 63 72 61 73 68 20 69 6e 20    43963;(crash in
00f0   66 69 6e 64 5f 64 69 72 5f 6e 61 6d 65 29 2e 3b    find_dir_name).;
0100   3b 59 6f 75 20 73 68 6f 75 6c 64 20 69 6e 73 74    ;You should inst
0110   61 6c 6c 20 74 68 69 73 20 70 61 74 63 68 20 66    all this patch f
0120   6f 72 20 79 6f 75 72 20 73 79 73 74 65 6d 20 74    or your system t
0130   6f 20 62 65 20 75 70 2d 74 6f 2d 64 61 74 65 2e    o be up-to-date.
0140   3b 3b 53 6f 6c 75 74 69 6f 6e 20 3a 20 68 74 74    ;;Solution : htt
0150   70 3a 2f 2f 77 77 77 2d 39 31 32 2e 69 62 6d 2e    p://www-912.ibm.
0160   63 6f 6d 2f 65 73 65 72 76 65 72 2f 73 75 70 70    com/eserver/supp
0170   6f 72 74 2f 66 69 78 65 73 2f 20 3b 52 69 73 6b    ort/fixes/ ;Risk
0180   20 46 61 63 74 6f 72 20 3a 20 48 69 67 68 20 3c     Factor : High <
0190   7c 3e 20 43 68 65 63 6b 20 66 6f 72 20 70 61 74    |> Check for pat
01a0   63 68 20 49 59 34 33 39 36 33 20 3c 7c 3e 20 41    ch IY43963 <|> A
01b0   49 58 20 4c 6f 63 61 6c 20 53 65 63 75 72 69 74    IX Local Securit
01c0   79 20 43 68 65 63 6b 73 0a 31 32 38 37 33 20 3c    y Checks.12873 <
01d0   7c 3e 20 53 6f 6c 61 72 69 73 20 32 2e 36 20 28    |> Solaris 2.6 (
...
0510   20 73 79 73 74 65 6d 73 3a 20 57 65 62 4c 6f 67     systems: WebLog
0520   69 63                                              ic
```



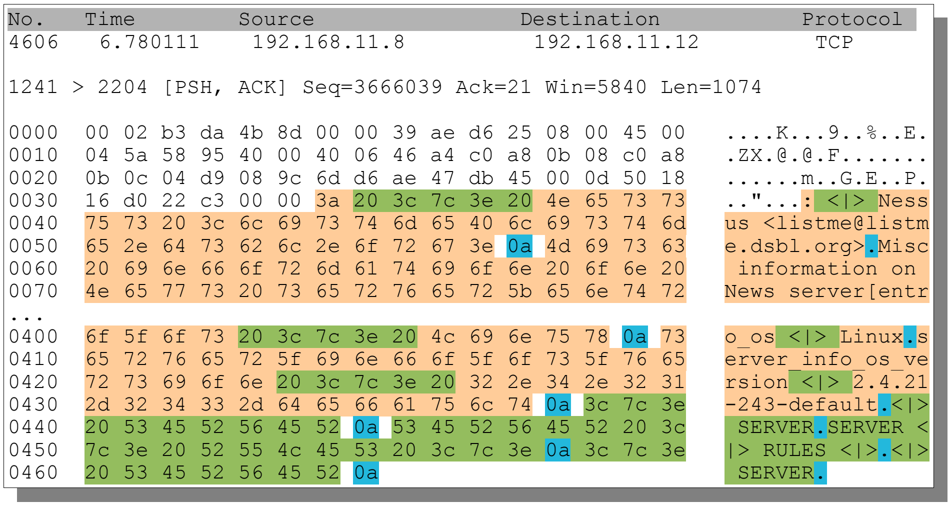
```
No.    Time          Source                       Destination                 Protocol
21      0.260374      192.168.11.8                 192.168.11.12               TCP

1241 > 2204 [PSH, ACK] Seq=1318 Ack=21 Win=5840 Len=202

0000   00 02 b3 da 4b 8d 00 00 39 ae d6 25 08 00 45 00    ....K...9..%..E.
0010   00 f2 4b a1 40 00 40 06 57 00 c0 a8 0b 08 c0 a8    ..K.@.@.W.......
0020   0b 0c 04 d9 08 9c 6d 9e c2 f6 db 45 00 0d 50 18    ......m....E..P.
0030   16 d0 64 25 00 00 20 76 65 72 73 69 6f 6e 20 35    ..d%.. version 5
0040   2e 31 2e 30 20 53 50 20 38 3b 3b 53 6f 6c 75 74    .1.0 SP 8;;Solut
0050   69 6f 6e 3a 20 55 73 65 20 74 68 65 20 6f 66 66    ion: Use the off
0060   69 63 69 61 6c 20 70 61 74 63 68 20 61 76 61 69    icial patch avai
0070   6c 61 62 6c 65 20 61 74 20 68 74 74 70 3a 2f 2f    lable at http://
0080   77 77 77 2e 62 65 61 2e 63 6f 6d 3b 3b 52 69 73    www.bea.com;;Ris
0090   6b 20 66 61 63 74 6f 72 20 3a 20 4d 65 64 69 75    k factor : Mediu
00a0   6d 20 3c 7c 3e 20 42 45 41 20 57 65 62 4c 6f 67    m <|> BEA WebLog
00b0   69 63 20 6d 61 79 20 62 65 20 74 72 69 63 6b 65    ic may be tricke
00c0   64 20 69 6e 74 6f 20 72 65 76 65 61 6c 69 6e 67    d into revealing
00d0   20 74 68 65 20 73 6f 75 72 63 65 20 63 6f 64 65     the source code
00e0   20 6f 66 20 4a 53 50 20 73 63 72 69 70 74 73 2e     of JSP scripts.
00f0   20 3c 7c 3e 20 43 47 49 20 61 62 75 73 65 73 0a     <|> CGI abuses.
```

Sending the plugin list is continued to packet 4593: Then the server sends the end marker string <|> **SERVER** and a terminating newline '\n' (hex: 0a) to end the plugin list section. After that, it sends the preferences start marker string, terminated by newline '\n' (hex: 0a).



```
No.    Time          Source               Destination          Protocol
4593    6.693455      192.168.11.8          192.168.11.12         TCP

1241 > 2204 [ACK] Seq=3657219 Ack=21 Win=5840 Len=1260

0000   00 02 b3 da 4b 8d 00 00 39 ae d6 25 08 00 45 00   ....K...9..%..E.
0010   05 14 58 8e 40 00 40 06 45 f1 c0 a8 0b 08 c0 a8   ..X.@.@.E.......
0020   0b 0c 04 d9 08 9c 6d d6 8b d3 db 45 00 0d 50 10   ......m....E..P.
0030   16 d0 1e b4 00 00 65 6c 79 2d 61 76 61 69 6c 61   ......ely-availa
0040   62 6c 65 3b 57 65 62 20 73 65 72 76 65 72 2e 20   ble;Web server. 
0050   41 70 61 63 68 65 20 69 73 20 61 6c 73 6f 20 74   Apache is also t
...
02b0   70 64 20 70 61 63 6b 61 67 65 20 3c 7c 3e 20 46   pd package <|> F
02c0   65 64 6f 72 61 20 4c 6f 63 61 6c 20 53 65 63 75   edora Local Secu
02d0   72 69 74 79 20 43 68 65 63 6b 73 0a 3c 7c 3e 20   rity Checks.<|> 
02e0   53 45 52 56 45 52 0a 53 45 52 56 45 52 20 3c 7c   SERVER.SERVER <|
02f0   3e 20 50 52 45 46 45 52 45 4e 43 45 53 20 3c 7c   > PREFERENCES <|
0300   3e 0a 6d 61 78 5f 68 6f 73 74 73 20 3c 7c 3e 20   >.max_hosts <|> 
0310   33 30 0a 6d 61 78 5f 63 68 65 63 6b 73 20 3c 7c   30.max_checks <|
0320   3e 20 31 30 0a 6c 6f 67 5f 77 68 6f 6c 65 5f 61   > 10.log_whole_a
...
04f0   68 65 72 69 6e 67 20 3c 7c 3e 20 6e 6f 0a 6b 62   hering <|> no.kb
0500   5f 64 6f 6e 74 5f 72 65 70 6c 61 79 5f 61 74 74   _dont_replay_att
0510   61 63 6b 73 20 3c 7c 3e 20 6e 6f 0a 6b 62 5f 64   acks <|> no.kb_d
0520   6f 6e                                             on
```

... continued to packet 4606: The server sends the end marker string **`<|> SERVER`** and a terminating newline '\n' (hex: 0a) to end the preferences section. It then sends the rules start marker string, terminated by newline '\n' (hex: 0a), and followed immediately by the end marker string, indicating that no rules data exists.



```
No.    Time          Source               Destination          Protocol
4606    6.780111      192.168.11.8          192.168.11.12         TCP

1241 > 2204 [PSH, ACK] Seq=3666039 Ack=21 Win=5840 Len=1074

0000   00 02 b3 da 4b 8d 00 00 39 ae d6 25 08 00 45 00   ....K...9..%..E.
0010   04 5a 58 95 40 00 40 06 46 a4 c0 a8 0b 08 c0 a8   .ZX.@.@.F.......
0020   0b 0c 04 d9 08 9c 6d d6 ae 47 db 45 00 0d 50 18   ......m..G.E..P.
0030   16 d0 22 c3 00 00 3a 20 3c 7c 3e 20 4e 65 73 73   ..".... : <|> Ness
0040   75 73 20 3c 6c 69 73 74 6d 65 40 6c 69 73 74 6d   us <listme@listm
0050   65 2e 64 73 62 6c 2e 6f 72 67 3e 0a 4d 69 73 63   e.dsbl.org>.Misc
0060   20 69 6e 66 6f 72 6d 61 74 69 6f 6e 20 6f 6e 20    information on 
0070   4e 65 77 73 20 73 65 72 76 65 72 5b 65 6e 74 72   News server[entr
...
0400   6f 5f 6f 73 20 3c 7c 3e 20 4c 69 6e 75 78 0a 73   o_os <|> Linux.s
0410   65 72 76 65 72 5f 69 6e 66 6f 5f 6f 73 5f 76 65   erver_info_os_ve
0420   72 73 69 6f 6e 20 3c 7c 3e 20 32 2e 34 2e 32 31   rsion <|> 2.4.21
0430   2d 32 34 33 2d 64 65 66 61 75 6c 74 0a 3c 7c 3e   -243-default.<|>
0440   20 53 45 52 56 45 52 0a 53 45 52 56 45 52 20 3c    SERVER.SERVER <
0450   7c 3e 20 52 55 4c 45 53 20 3c 7c 3e 0a 3c 7c 3e   |> RULES <|>.<|>
0460   20 53 45 52 56 45 52 0a                            SERVER.
```

This ends the first communication between the client and the server and the session is idle until the client initiates further action or the server is shut down and sends the BYE message.

3. Nessus client: Unsuccessful login

What happens if the username/password combination doesn't match or if the user does not even exist on the nessus server? See the different ending here:

Starting at packet 18, instead of sending the plugin list start marker followed by a newline terminator, the Nessus server simply sends a **`Bad Login attempt !`** string, followed by the newline terminator '\n' (hex: 0a).

```
No.    Time           Source                      Destination                 Protocol
18      0.299713       192.168.11.8                192.168.11.12               TCP

1241 > 2287 [PSH, ACK] Seq=31 Ack=21 Win=5840 Len=20

0000   00 02 b3 da 4b 8d 00 00 39 ae d6 25 08 00 45 00    ....K...9..%..E.
0010   00 3c 69 0e 40 00 40 06 3a 49 c0 a8 0b 08 c0 a8    .<i.@.@.:I......
0020   0b 0c 04 d9 08 ef 35 03 1d f3 7d b8 1d 09 50 18    ......5...}...P.
0030   16 d0 45 14 00 00 42 61 64 20 6c 6f 67 69 6e 20    ..E...Bad login 
0040   61 74 74 65 6d 70 74 20 21 0a                      attempt !.
```

There is no reason to stay connected and the server initiates the end of the TCP session with a standard FIN/ACK - ACK, FIN/ACK – ACK sequence.

```
No.    Time           Source                      Destination                 Protocol
19      0.299985       192.168.11.8                192.168.11.12               TCP

1241 > 2287 [FIN, ACK] Seq=51 Ack=21 Win=5840 Len=0

0000   00 02 b3 da 4b 8d 00 00 39 ae d6 25 08 00 45 00    ....K...9..%..E.
0010   00 28 69 0f 40 00 40 06 3a 5c c0 a8 0b 08 c0 a8    .(i.@.@.:\......
0020   0b 0c 04 d9 08 ef 35 03 1e 07 7d b8 1d 09 50 11    ......5...}...P.
0030   16 d0 06 0b 00 00                                  ......
```

```
No.    Time           Source                      Destination                 Protocol
20      0.301009       192.168.11.12               192.168.11.8                TCP

2287 > 1241 [ACK] Seq=21 Ack=52 Win=65485 Len=0

0000   00 00 39 ae d6 25 00 02 b3 da 4b 8d 08 00 45 00    ..9..%....K...E.
0010   00 28 e2 78 40 00 80 06 80 f2 c0 a8 0b 0c c0 a8    .(.x@...........
0020   0b 08 08 ef 04 d9 7d b8 1d 09 35 03 1e 08 50 10    ......}...5...P.
0030   ff cd 1d 0d 00 00 00 00 00 00 00 00                ............
```

```
No.    Time           Source                      Destination                 Protocol
21      3.326760       192.168.11.12               192.168.11.8                TCP

2287 > 1241 [FIN, ACK] Seq=21 Ack=52 Win=65485 Len=0

0000   00 00 39 ae d6 25 00 02 b3 da 4b 8d 08 00 45 00    ..9..%....K...E.
0010   00 28 e2 79 40 00 80 06 80 f1 c0 a8 0b 0c c0 a8    .(.y@...........
0020   0b 08 08 ef 04 d9 7d b8 1d 09 35 03 1e 08 50 11    ......}...5...P.
0030   ff cd 1d 0c 00 00 00 00 00 00 00 00                ............
```

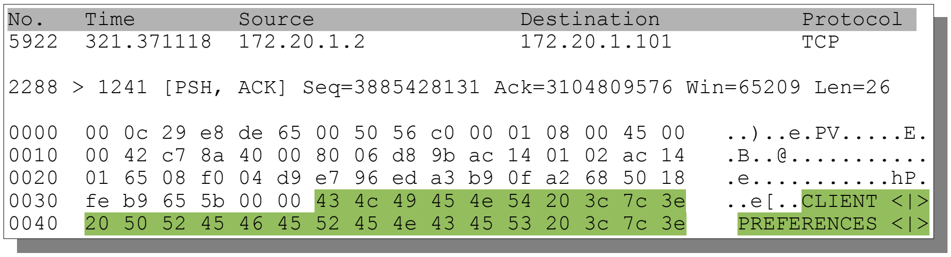
```
No.    Time           Source                      Destination                 Protocol
22      3.326853       192.168.11.8                192.168.11.12               TCP

1241 > 2287 [ACK] Seq=52 Ack=22 Win=5840 Len=0

0000   00 02 b3 da 4b 8d 00 00 39 ae d6 25 08 00 45 00    ....K...9..%..E.
0010   00 28 69 10 40 00 40 06 3a 5b c0 a8 0b 08 c0 a8    .(i.@.@.:[......
0020   0b 0c 04 d9 08 ef 35 03 1e 08 7d b8 1d 0a 50 10    ......5...}...P.
0030   16 d0 06 0a 00 00                                  ......
```

4. Nessus client: Upload a scan configuration and start a new scan

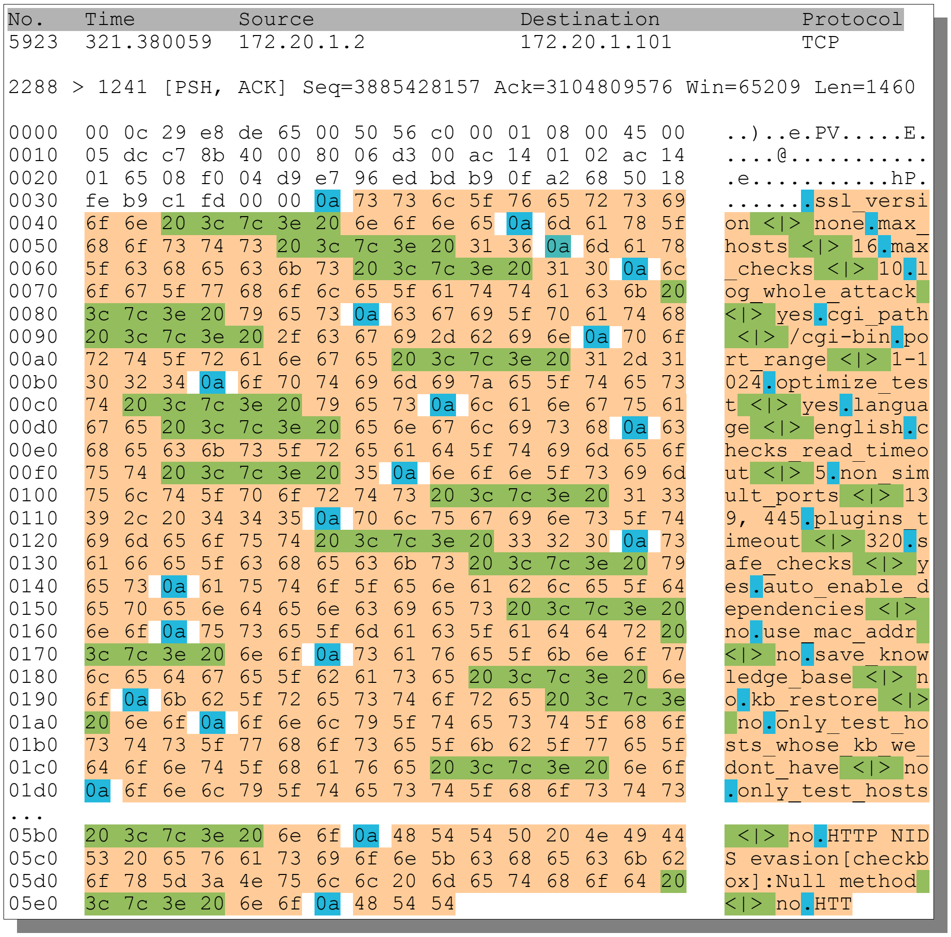
Once the client received the Nessus server plugins and settings, it can create a configuration profile and sends it back to the server. The client starts sending the preferences list first, followed by the plugin id list using the following syntax:

```
CLIENT <|> PREFERENCES <|>'\n'pref_name_1 <|> pref_value_1'\n'pref_name_2 <|>
pref_value_2'\n'pref_name_n <|> pref_value_n'\n'plugin_set <|>10715;id_2;id_n'\n'<|> CLIENT'\n'
```

According to the Nessus documentation, if the plugin id list is empty, the server will use **all** plugins available. In the examples below, the client IP is 172.20.1.2 and the Server is 172.20.1.101.

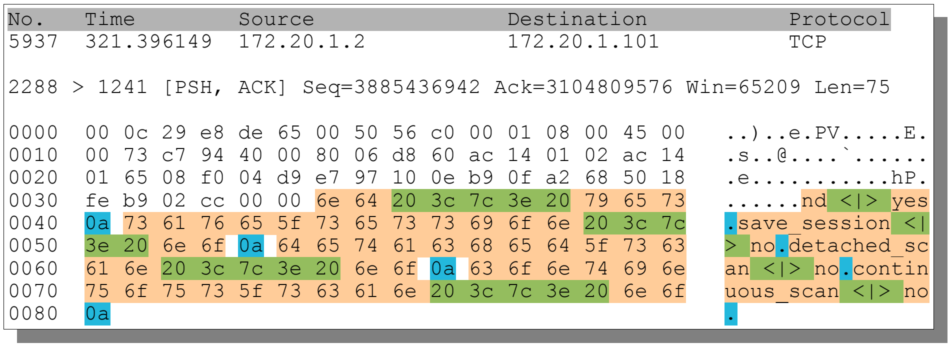


```
No.   Time        Source                Destination           Protocol
5922  321.371118  172.20.1.2            172.20.1.101          TCP

2288 > 1241 [PSH, ACK] Seq=3885428131 Ack=3104809576 Win=65209 Len=26

0000  00 0c 29 e8 de 65 00 50 56 c0 00 01 08 00 45 00   ..)..e.PV.....E.
0010  00 42 c7 8a 40 00 80 06 d8 9b ac 14 01 02 ac 14   .B..@...........
0020  01 65 08 f0 04 d9 e7 96 ed a3 b9 0f a2 68 50 18   .e...........hP.
0030  fe b9 65 5b 00 00 43 4c 49 45 4e 54 20 3c 7c 3e   ..e[..CLIENT <|>
0040  20 50 52 45 46 45 52 45 4e 43 45 53 20 3c 7c 3e    PREFERENCES <|>
```



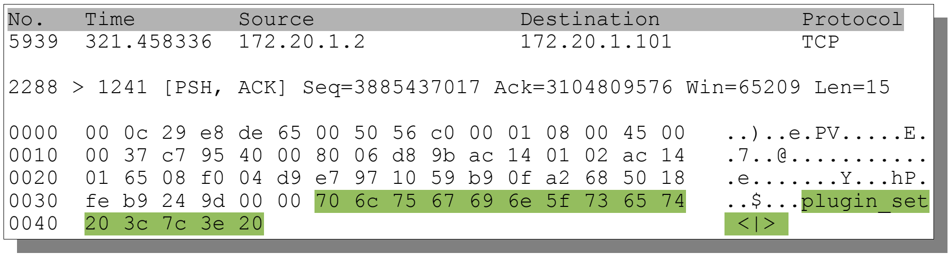
```
No.   Time        Source                Destination           Protocol
5923  321.380059  172.20.1.2            172.20.1.101          TCP

2288 > 1241 [PSH, ACK] Seq=3885428157 Ack=3104809576 Win=65209 Len=1460

0000  00 0c 29 e8 de 65 00 50 56 c0 00 01 08 00 45 00   ..)..e.PV.....E.
0010  05 dc c7 8b 40 00 80 06 d3 00 ac 14 01 02 ac 14   ....@...........
0020  01 65 08 f0 04 d9 e7 96 ed bd b9 0f a2 68 50 18   .e...........hP.
0030  fe b9 c1 fd 00 00 0a 73 73 6c 5f 76 65 72 73 69   .......ssl_versi
0040  6f 6e 20 3c 7c 3e 20 6e 6f 6e 65 0a 6d 61 78 5f   on <|> none.max_
0050  68 6f 73 74 73 20 3c 7c 3e 20 31 36 0a 6d 61 78   hosts <|> 16.max
0060  5f 63 68 65 63 6b 73 20 3c 7c 3e 20 31 30 0a 6c   _checks <|> 10.l
0070  6f 67 5f 77 68 6f 6c 65 5f 61 74 74 61 63 6b 20   og_whole_attack 
0080  3c 7c 3e 20 79 65 73 0a 63 67 69 5f 70 61 74 68   <|> yes.cgi_path
0090  20 3c 7c 3e 20 2f 63 67 69 2d 62 69 6e 0a 70 6f    <|> /cgi-bin.po
00a0  72 74 5f 72 61 6e 67 65 20 3c 7c 3e 20 31 2d 31   rt_range <|> 1-1
00b0  30 32 34 0a 6f 70 74 69 6d 69 7a 65 5f 74 65 73   024.optimize_tes
00c0  74 20 3c 7c 3e 20 79 65 73 0a 6c 61 6e 67 75 61   t <|> yes.langua
00d0  67 65 20 3c 7c 3e 20 65 6e 67 6c 69 73 68 0a 63   ge <|> english.c
00e0  68 65 63 6b 73 5f 72 65 61 64 5f 74 69 6d 65 6f   hecks_read_timeo
00f0  75 74 20 3c 7c 3e 20 35 0a 6e 6f 6e 5f 73 69 6d   ut <|> 5.non_sim
0100  75 6c 74 5f 70 6f 72 74 73 20 3c 7c 3e 20 31 33   ult_ports <|> 13
0110  39 2c 20 34 34 35 0a 70 6c 75 67 69 6e 73 5f 74   9, 445.plugins_t
0120  69 6d 65 6f 75 74 20 3c 7c 3e 20 33 32 30 0a 73   imeout <|> 320.s
0130  61 66 65 5f 63 68 65 63 6b 73 20 3c 7c 3e 20 79   afe_checks <|> y
0140  65 73 0a 61 75 74 6f 5f 65 6e 61 62 6c 65 5f 64   es.auto_enable_d
0150  65 70 65 6e 64 65 6e 63 69 65 73 20 3c 7c 3e 20   ependencies <|> 
0160  6e 6f 0a 75 73 65 5f 6d 61 63 5f 61 64 64 72 20   no.use_mac_addr 
0170  3c 7c 3e 20 6e 6f 0a 73 61 76 65 5f 6b 6e 6f 77   <|> no.save_know
0180  6c 65 64 67 65 5f 62 61 73 65 20 3c 7c 3e 20 6e   ledge_base <|> n
0190  6f 0a 6b 62 5f 72 65 73 74 6f 72 65 20 3c 7c 3e   o.kb_restore <|>
01a0  20 6e 6f 0a 6f 6e 6c 79 5f 74 65 73 74 5f 68 6f    no.only_test_ho
01b0  73 74 73 5f 77 68 6f 73 65 5f 6b 62 5f 77 65 5f   sts_whose_kb_we_
01c0  64 6f 6e 74 5f 68 61 76 65 20 3c 7c 3e 20 6e 6f   dont_have <|> no
01d0  0a 6f 6e 6c 79 5f 74 65 73 74 5f 68 6f 73 74 73   .only_test_hosts
...
05b0  20 3c 7c 3e 20 6e 6f 0a 48 54 54 50 20 4e 49 44    <|> no.HTTP NID
05c0  53 20 65 76 61 73 69 6f 6e 5b 63 68 65 63 6b 62   S evasion[checkb
05d0  6f 78 5d 3a 4e 75 6c 6c 20 6d 65 74 68 6f 64 20   ox]:Null method 
05e0  3c 7c 3e 20 6e 6f 0a 48 54 54                     <|> no.HTT
```

Sending the list of preferences is continued to packet 5937. Packet 5937 ends the list of preferences sent to the server.

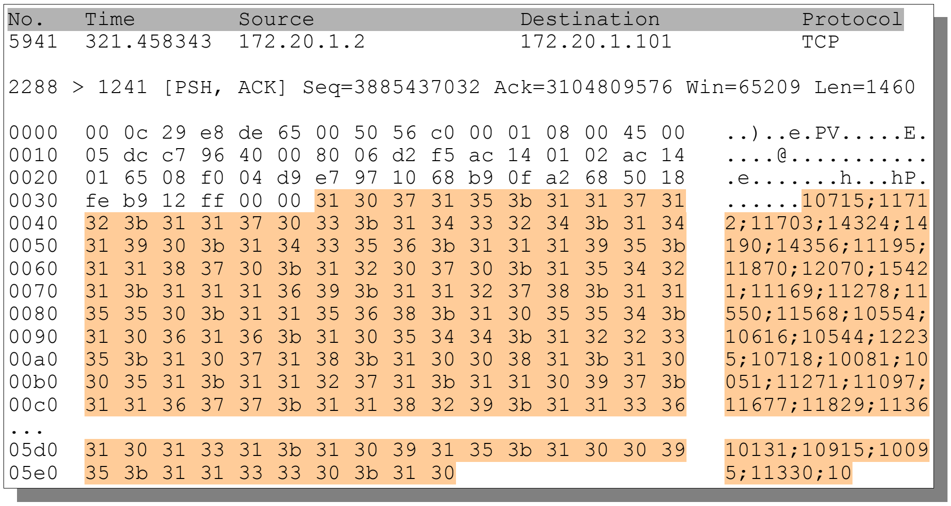


```
No.   Time        Source               Destination          Protocol
5937  321.396149  172.20.1.2           172.20.1.101         TCP

2288 > 1241 [PSH, ACK] Seq=3885436942 Ack=3104809576 Win=65209 Len=75

0000  00 0c 29 e8 de 65 00 50 56 c0 00 01 08 00 45 00   ..)..e.PV.....E.
0010  00 73 c7 94 40 00 80 06 d8 60 ac 14 01 02 ac 14   .s..@....`......
0020  01 65 08 f0 04 d9 e7 97 10 0e b9 0f a2 68 50 18   .e...........hP.
0030  fe b9 02 cc 00 00 6e 64 20 3c 7c 3e 20 79 65 73   ......nd <|> yes
0040  0a 73 61 76 65 5f 73 65 73 73 69 6f 6e 20 3c 7c   .save_session <|
0050  3e 20 6e 6f 0a 64 65 74 61 63 68 65 64 5f 73 63   > no.detached_sc
0060  61 6e 20 3c 7c 3e 20 6e 6f 0a 63 6f 6e 74 69 6e   an <|> no.contin
0070  75 6f 75 73 5f 73 63 61 6e 20 3c 7c 3e 20 6e 6f   uous_scan <|> no
0080  0a                                                .
```

Now the client sends the **`plugin_set <|>`** marker, followed by the list of plugin ID's, which are separated with a semicolon ';'.

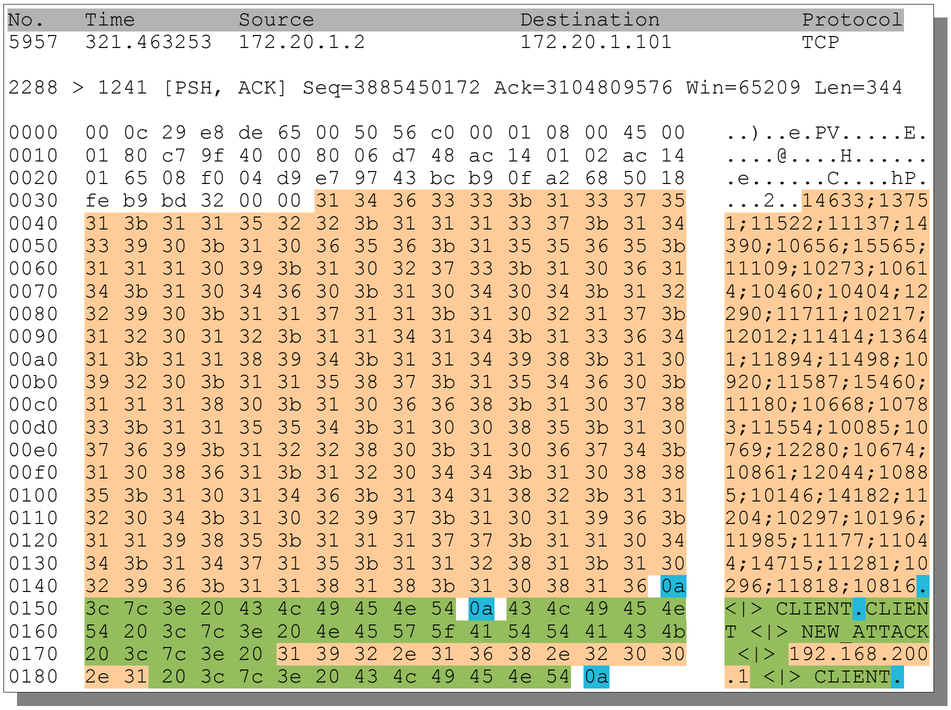


```
No.   Time         Source                 Destination            Protocol
5939  321.458336   172.20.1.2             172.20.1.101           TCP

2288 > 1241 [PSH, ACK] Seq=3885437017 Ack=3104809576 Win=65209 Len=15

0000  00 0c 29 e8 de 65 00 50 56 c0 00 01 08 00 45 00   ..)..e.PV.....E.
0010  00 37 c7 95 40 00 80 06 d8 9b ac 14 01 02 ac 14   .7..@...........
0020  01 65 08 f0 04 d9 e7 97 10 59 b9 0f a2 68 50 18   .e.......Y...hP.
0030  fe b9 24 9d 00 00 70 6c 75 67 69 6e 5f 73 65 74   ..$...plugin_set
0040  20 3c 7c 3e 20                                     <|>
```



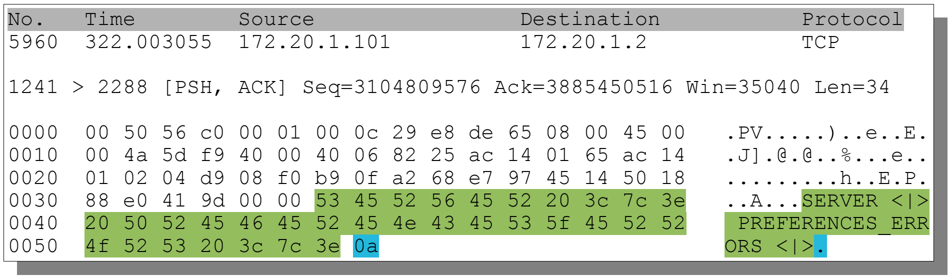
```
No.   Time         Source                 Destination            Protocol
5941  321.458343   172.20.1.2             172.20.1.101           TCP

2288 > 1241 [PSH, ACK] Seq=3885437032 Ack=3104809576 Win=65209 Len=1460

0000  00 0c 29 e8 de 65 00 50 56 c0 00 01 08 00 45 00   ..)..e.PV.....E.
0010  05 dc c7 96 40 00 80 06 d2 f5 ac 14 01 02 ac 14   ....@...........
0020  01 65 08 f0 04 d9 e7 97 10 68 b9 0f a2 68 50 18   .e.......h...hP.
0030  fe b9 12 ff 00 00 31 30 37 31 35 3b 31 31 37 31   ......10715;1171
0040  32 3b 31 31 37 30 33 3b 31 34 33 32 34 3b 31 34   2;11703;14324;14
0050  31 39 30 3b 31 34 33 35 36 3b 31 31 31 39 35 3b   190;14356;11195;
0060  31 31 38 37 30 3b 31 32 30 37 30 3b 31 35 34 32   11870;12070;1542
0070  31 3b 31 31 31 36 39 3b 31 31 32 37 38 3b 31 31   1;11169;11278;11
0080  35 35 30 3b 31 31 35 36 38 3b 31 30 35 35 34 3b   550;11568;10554;
0090  31 30 36 31 36 3b 31 30 35 34 34 3b 31 32 32 33   10616;10544;1223
00a0  35 3b 31 30 37 31 38 3b 31 30 30 38 31 3b 31 30   5;10718;10081;10
00b0  30 35 31 3b 31 31 32 37 31 3b 31 31 30 39 37 3b   051;11271;11097;
00c0  31 31 36 37 37 3b 31 31 38 32 39 3b 31 31 33 36   11677;11829;1136
...
05d0  31 30 31 33 31 3b 31 30 39 31 35 3b 31 30 30 39   10131;10915;1009
05e0  35 3b 31 31 33 33 30 3b 31 30                     5;11330;10
```

Fast forward to packet 5957, which terminates the **`CLIENT <|> PREFERENCES <|>`** section and starts a new scan using the **`CLIENT <|> NEW_ATTACK <|> 'IP Address' <|> CLIENT'\n'`** command for IP 192.168.200.1.

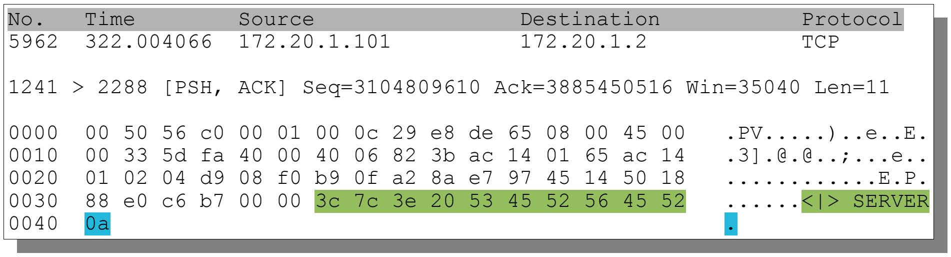


```
No.   Time         Source                 Destination            Protocol
5957  321.463253   172.20.1.2             172.20.1.101           TCP

2288 > 1241 [PSH, ACK] Seq=3885450172 Ack=3104809576 Win=65209 Len=344

0000  00 0c 29 e8 de 65 00 50 56 c0 00 01 08 00 45 00   ..)..e.PV.....E.
0010  01 80 c7 9f 40 00 80 06 d7 48 ac 14 01 02 ac 14   ....@....H......
0020  01 65 08 f0 04 d9 e7 97 43 bc b9 0f a2 68 50 18   .e......C....hP.
0030  fe b9 bd 32 00 00 31 34 36 33 33 3b 31 33 37 35   ...2..14633;1375
0040  31 3b 31 31 35 32 32 3b 31 31 31 33 37 3b 31 34   1;11522;11137;14
0050  33 39 30 3b 31 30 36 35 36 3b 31 35 35 36 35 3b   390;10656;15565;
0060  31 31 31 30 39 3b 31 30 32 37 33 3b 31 30 36 31   11109;10273;1061
0070  34 3b 31 30 34 36 30 3b 31 30 34 30 34 3b 31 32   4;10460;10404;12
0080  32 39 30 3b 31 31 37 31 31 3b 31 30 32 31 37 3b   290;11711;10217;
0090  31 32 30 31 32 3b 31 31 34 31 34 3b 31 33 36 34   12012;11414;1364
00a0  31 3b 31 31 38 39 34 3b 31 31 34 39 38 3b 31 30   1;11894;11498;10
00b0  39 32 30 3b 31 31 35 38 37 3b 31 35 34 36 30 3b   920;11587;15460;
00c0  31 31 31 38 30 3b 31 30 36 36 38 3b 31 30 37 38   11180;10668;1078
00d0  33 3b 31 31 35 35 34 3b 31 30 30 38 35 3b 31 30   3;11554;10085;10
00e0  37 36 39 3b 31 32 32 38 30 3b 31 30 36 37 34 3b   769;12280;10674;
00f0  31 30 38 36 31 3b 31 32 30 34 34 3b 31 30 38 38   10861;12044;1088
0100  35 3b 31 30 31 34 36 3b 31 34 31 38 32 3b 31 31   5;10146;14182;11
0110  32 30 34 3b 31 30 32 39 37 3b 31 30 31 39 36 3b   204;10297;10196;
0120  31 31 39 38 35 3b 31 31 31 37 37 3b 31 31 30 34   11985;11177;1104
0130  34 3b 31 34 37 31 35 3b 31 31 32 38 31 3b 31 30   4;14715;11281;10
0140  32 39 36 3b 31 31 38 31 38 3b 31 30 38 31 36 0a   296;11818;10816.
0150  3c 7c 3e 20 43 4c 49 45 4e 54 0a 43 4c 49 45 4e   <|> CLIENT.CLIEN
0160  54 20 3c 7c 3e 20 4e 45 57 5f 41 54 54 41 43 4b   T <|> NEW_ATTACK
0170  20 3c 7c 3e 20 31 39 32 2e 31 36 38 2e 32 30 30    <|> 192.168.200
0180  2e 31 20 3c 7c 3e 20 43 4c 49 45 4e 54 0a         .1 <|> CLIENT.
```

Once the client sent the new scan configuration and the scan target, the Nessus server replies with an error list message that contains possible errors, or nothing if no error occurred.



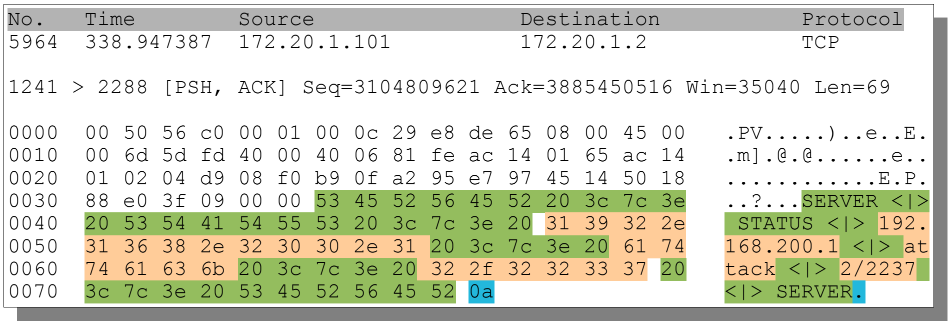
```
No.     Time          Source                Destination           Protocol
5960    322.003055    172.20.1.101          172.20.1.2            TCP

1241 > 2288 [PSH, ACK] Seq=3104809576 Ack=3885450516 Win=35040 Len=34

0000    00 50 56 c0 00 01 00 0c 29 e8 de 65 08 00 45 00    .PV.....)..e..E.
0010    00 4a 5d f9 40 00 40 06 82 25 ac 14 01 65 ac 14    .J].@.@..%...e..
0020    01 02 04 d9 08 f0 b9 0f a2 68 e7 97 45 14 50 18    .........h..E.P.
0030    88 e0 41 9d 00 00 53 45 52 56 45 52 20 3c 7c 3e    ..A...SERVER <|>
0040    20 50 52 45 46 45 52 45 4e 43 45 53 5f 45 52 52     PREFERENCES_ERR
0050    4f 52 53 20 3c 7c 3e 0a                            ORS <|>.
```



```
No.     Time          Source                Destination           Protocol
5962    322.004066    172.20.1.101          172.20.1.2            TCP

1241 > 2288 [PSH, ACK] Seq=3104809610 Ack=3885450516 Win=35040 Len=11

0000    00 50 56 c0 00 01 00 0c 29 e8 de 65 08 00 45 00    .PV.....)..e..E.
0010    00 33 5d fa 40 00 40 06 82 3b ac 14 01 65 ac 14    .3].@.@..;...e..
0020    01 02 04 d9 08 f0 b9 0f a2 8a e7 97 45 14 50 18    ............E.P.
0030    88 e0 c6 b7 00 00 3c 7c 3e 20 53 45 52 56 45 52    ......<|> SERVER
0040    0a                                                 .
```

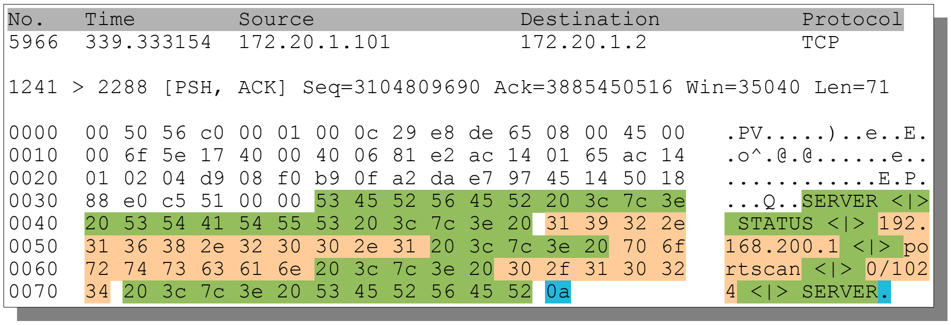
5. Nessus Server: Start the scan and report findings

With no error message reported, the server begins to scan the target and starts sending **`SERVER <|> STATUS <|>`** messages about the scan progress and **`SERVER <|> INFO <|>`** or **`SERVER <|> HOLE <|>`** messages for scan findings.



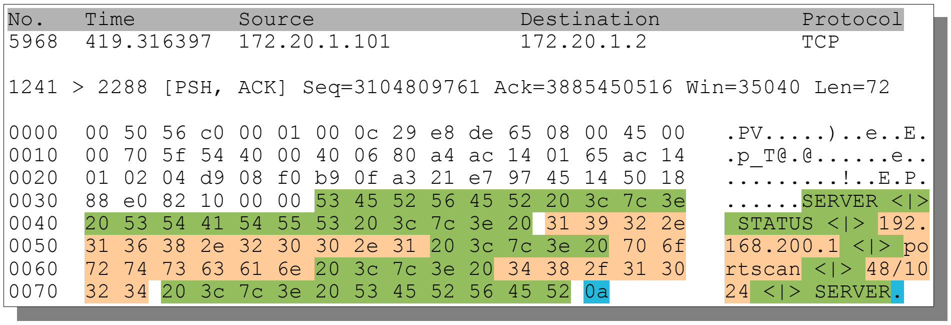
```
No.     Time          Source                Destination           Protocol
5964    338.947387    172.20.1.101          172.20.1.2            TCP

1241 > 2288 [PSH, ACK] Seq=3104809621 Ack=3885450516 Win=35040 Len=69

0000    00 50 56 c0 00 01 00 0c 29 e8 de 65 08 00 45 00    .PV.....)..e..E.
0010    00 6d 5d fd 40 00 40 06 81 fe ac 14 01 65 ac 14    .m].@.@......e..
0020    01 02 04 d9 08 f0 b9 0f a2 95 e7 97 45 14 50 18    ............E.P.
0030    88 e0 3f 09 00 00 53 45 52 56 45 52 20 3c 7c 3e    ..?...SERVER <|>
0040    20 53 54 41 54 55 53 20 3c 7c 3e 20 31 39 32 2e     STATUS <|> 192.
0050    31 36 38 2e 32 30 30 2e 31 20 3c 7c 3e 20 61 74    168.200.1 <|> at
0060    74 61 63 6b 20 3c 7c 3e 20 32 2f 32 32 33 37 20    tack <|> 2/2237
0070    3c 7c 3e 20 53 45 52 56 45 52 0a                   <|> SERVER.
```

After starting the scan, the server sends updates about the scan progress:



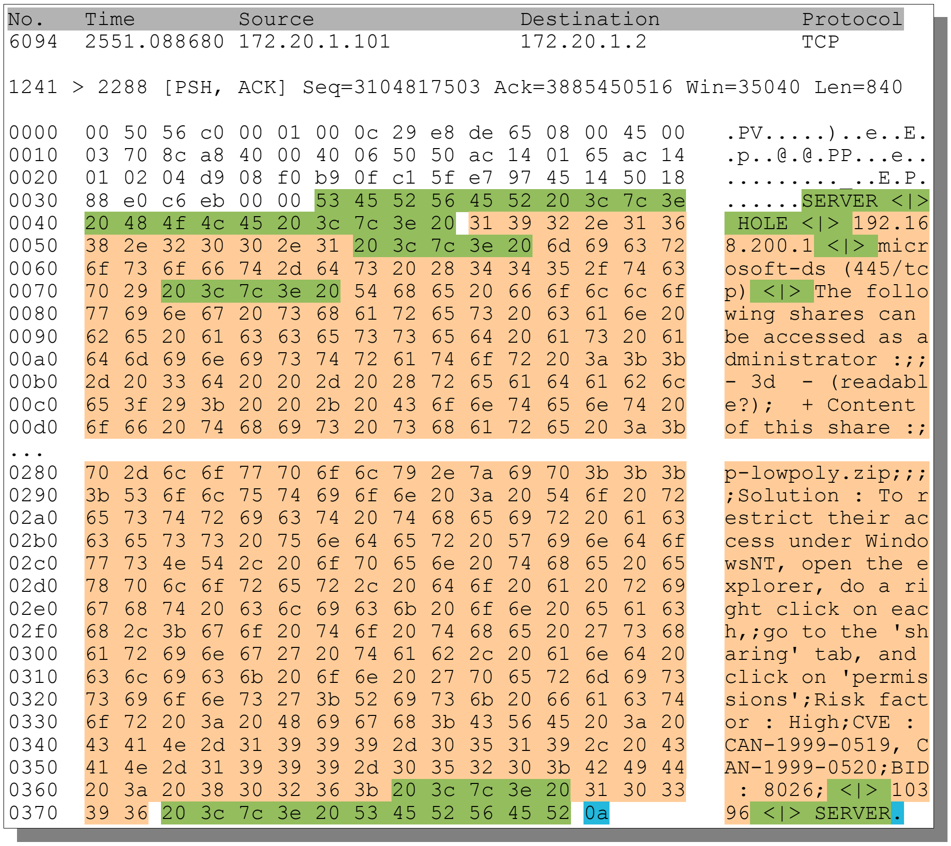
```
No.     Time          Source                Destination           Protocol
5966    339.333154    172.20.1.101          172.20.1.2            TCP

1241 > 2288 [PSH, ACK] Seq=3104809690 Ack=3885450516 Win=35040 Len=71

0000    00 50 56 c0 00 01 00 0c 29 e8 de 65 08 00 45 00    .PV.....)..e..E.
0010    00 6f 5e 17 40 00 40 06 81 e2 ac 14 01 65 ac 14    .o^.@.@......e..
0020    01 02 04 d9 08 f0 b9 0f a2 da e7 97 45 14 50 18    ............E.P.
0030    88 e0 c5 51 00 00 53 45 52 56 45 52 20 3c 7c 3e    ...Q..SERVER <|>
0040    20 53 54 41 54 55 53 20 3c 7c 3e 20 31 39 32 2e     STATUS <|> 192.
0050    31 36 38 2e 32 30 30 2e 31 20 3c 7c 3e 20 70 6f    168.200.1 <|> po
0060    72 74 73 63 61 6e 20 3c 7c 3e 20 30 2f 31 30 32    rtscan <|> 0/102
0070    34 20 3c 7c 3e 20 53 45 52 56 45 52 0a             4 <|> SERVER.
```

Here comes another example of a scan progress update:



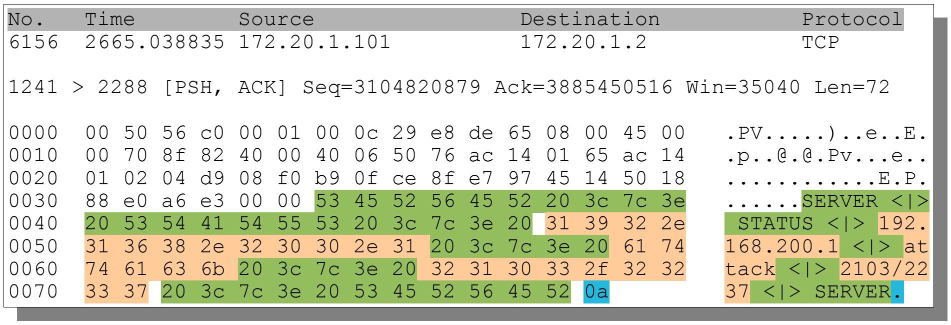
```
No.   Time        Source                Destination           Protocol
5968  419.316397  172.20.1.101          172.20.1.2            TCP

1241 > 2288 [PSH, ACK] Seq=3104809761 Ack=3885450516 Win=35040 Len=72

0000  00 50 56 c0 00 01 00 0c 29 e8 de 65 08 00 45 00   .PV.....)..e..E.
0010  00 70 5f 54 40 00 40 06 80 a4 ac 14 01 65 ac 14   .p_T@.@......e..
0020  01 02 04 d9 08 f0 b9 0f a3 21 e7 97 45 14 50 18   .........!..E.P.
0030  88 e0 82 10 00 00 53 45 52 56 45 52 20 3c 7c 3e   ......SERVER <|>
0040  20 53 54 41 54 55 53 20 3c 7c 3e 20 31 39 32 2e    STATUS <|> 192.
0050  31 36 38 2e 32 30 30 2e 31 20 3c 7c 3e 20 70 6f   168.200.1 <|> po
0060  72 74 73 63 61 6e 20 3c 7c 3e 20 34 38 2f 31 30   rtscan <|> 48/10
0070  32 34 20 3c 7c 3e 20 53 45 52 56 45 52 0a         24 <|> SERVER.
```

Next is an example of a scan finding report:



```
No.   Time        Source                Destination           Protocol
6094  2551.088680 172.20.1.101          172.20.1.2            TCP

1241 > 2288 [PSH, ACK] Seq=3104817503 Ack=3885450516 Win=35040 Len=840

0000  00 50 56 c0 00 01 00 0c 29 e8 de 65 08 00 45 00   .PV.....)..e..E.
0010  03 70 8c a8 40 00 40 06 50 50 ac 14 01 65 ac 14   .p..@.@.PP...e..
0020  01 02 04 d9 08 f0 b9 0f c1 5f e7 97 45 14 50 18   ........._..E.P.
0030  88 e0 c6 eb 00 00 53 45 52 56 45 52 20 3c 7c 3e   ......SERVER <|>
0040  20 48 4f 4c 45 20 3c 7c 3e 20 31 39 32 2e 31 36    HOLE <|> 192.16
0050  38 2e 32 30 30 2e 31 20 3c 7c 3e 20 6d 69 63 72   8.200.1 <|> micr
0060  6f 73 6f 66 74 2d 64 73 20 28 34 34 35 2f 74 63   osoft-ds (445/tc
0070  70 29 20 3c 7c 3e 20 54 68 65 20 66 6f 6c 6c 6f   p) <|> The follo
0080  77 69 6e 67 20 73 68 61 72 65 73 20 63 61 6e 20   wing shares can
0090  62 65 20 61 63 63 65 73 73 65 64 20 61 73 20 61   be accessed as a
00a0  64 6d 69 6e 69 73 74 72 61 74 6f 72 20 3a 3b 3b   dministrator :;;
00b0  2d 20 33 64 20 20 2d 20 28 72 65 61 64 61 62 6c   - 3d  - (readabl
00c0  65 3f 29 3b 20 20 2b 20 43 6f 6e 74 65 6e 74 20   e?);  + Content
00d0  6f 66 20 74 68 69 73 20 73 68 61 72 65 20 3a 3b   of this share :;
...
0280  70 2d 6c 6f 77 70 6f 6c 79 2e 7a 69 70 3b 3b 3b   p-lowpoly.zip;;;
0290  3b 53 6f 6c 75 74 69 6f 6e 20 3a 20 54 6f 20 72   ;Solution : To r
02a0  65 73 74 72 69 63 74 20 74 68 65 69 72 20 61 63   estrict their ac
02b0  63 65 73 73 20 75 6e 64 65 72 20 57 69 6e 64 6f   cess under Windo
02c0  77 73 4e 54 2c 20 6f 70 65 6e 20 74 68 65 20 65   wsNT, open the e
02d0  78 70 6c 6f 72 65 72 2c 20 64 6f 20 61 20 72 69   xplorer, do a ri
02e0  67 68 74 20 63 6c 69 63 6b 20 6f 6e 20 65 61 63   ght click on eac
02f0  68 2c 3b 67 6f 20 74 6f 20 74 68 65 20 27 73 68   h,;go to the 'sh
0300  61 72 69 6e 67 27 20 74 61 62 2c 20 61 6e 64 20   aring' tab, and
0310  63 6c 69 63 6b 20 6f 6e 20 27 70 65 72 6d 69 73   click on 'permis
0320  73 69 6f 6e 73 27 3b 52 69 73 6b 20 66 61 63 74   sions';Risk fact
0330  6f 72 20 3a 20 48 69 67 68 3b 43 56 45 20 3a 20   or : High;CVE :
0340  43 41 4e 2d 31 39 39 39 2d 30 35 31 39 2c 20 43   CAN-1999-0519, C
0350  41 4e 2d 31 39 39 39 2d 30 35 32 30 3b 42 49 44   AN-1999-0520;BID
0360  20 3a 20 38 30 32 36 3b 20 3c 7c 3e 20 31 30 33    : 8026; <|> 103
0370  39 36 20 3c 7c 3e 20 53 45 52 56 45 52 0a         96 <|> SERVER.
```

Forward to packet 6156, which contains the last status update.



```
No.   Time        Source                Destination           Protocol
6156  2665.038835 172.20.1.101          172.20.1.2            TCP

1241 > 2288 [PSH, ACK] Seq=3104820879 Ack=3885450516 Win=35040 Len=72

0000  00 50 56 c0 00 01 00 0c 29 e8 de 65 08 00 45 00   .PV.....)..e..E.
0010  00 70 8f 82 40 00 40 06 50 76 ac 14 01 65 ac 14   .p..@.@.Pv...e..
0020  01 02 04 d9 08 f0 b9 0f ce 8f e7 97 45 14 50 18   ............E.P.
0030  88 e0 a6 e3 00 00 53 45 52 56 45 52 20 3c 7c 3e   ......SERVER <|>
0040  20 53 54 41 54 55 53 20 3c 7c 3e 20 31 39 32 2e    STATUS <|> 192.
0050  31 36 38 2e 32 30 30 2e 31 20 3c 7c 3e 20 61 74   168.200.1 <|> at
0060  74 61 63 6b 20 3c 7c 3e 20 32 31 30 33 2f 32 32   tack <|> 2103/22
0070  33 37 20 3c 7c 3e 20 53 45 52 56 45 52 0a         37 <|> SERVER.
```

The Scan of a particular host is ending with a **SERVER <|> FINISHED <|> IP_address <|> SERVER** message.

```
No.   Time        Source                Destination           Protocol
6158  2780.479897 172.20.1.101          172.20.1.2            TCP

1241 > 2288 [PSH, ACK] Seq=3104820951 Ack=3885450516 Win=35040 Len=49

0000  00 50 56 c0 00 01 00 0c 29 e8 de 65 08 00 45 00   .PV.....)..e..E.
0010  00 59 8f c1 40 00 40 06 50 4e ac 14 01 65 ac 14   .Y..@.@.PN...e..
0020  01 02 04 d9 08 f0 b9 0f ce d7 e7 97 45 14 50 18   ............E.P.
0030  88 e0 f8 a7 00 00 53 45 52 56 45 52 20 3c 7c 3e   ......SERVER <|>
0040  20 46 49 4e 49 53 48 45 44 20 3c 7c 3e 20 31 39    FINISHED <|> 19
0050  32 2e 31 36 38 2e 32 30 30 2e 31 20 3c 7c 3e 20   2.168.200.1 <|>
0060  53 45 52 56 45 52 0a                              SERVER.
```

Having finished the scan for all hosts, the server sends the **SERVER <|> BYE <|> BYE <|> SERVER'\n'** message.

```
No.   Time        Source                Destination           Protocol
6160  2780.750832 172.20.1.101          172.20.1.2            TCP

1241 > 2288 [PSH, ACK] Seq=3104821000 Ack=3885450516 Win=35040 Len=34

0000  00 50 56 c0 00 01 00 0c 29 e8 de 65 08 00 45 00   .PV.....)..e..E.
0010  00 4a 8f c2 40 00 40 06 50 5c ac 14 01 65 ac 14   .J..@.@.P\...e..
0020  01 02 04 d9 08 f0 b9 0f cf 08 e7 97 45 14 50 18   ............E.P.
0030  88 e0 48 4b 00 00 53 45 52 56 45 52 20 3c 7c 3e   ..HK..SERVER <|>
0040  20 42 59 45 20 3c 7c 3e 20 42 59 45 20 3c 7c 3e    BYE <|> BYE <|>
0050  20 53 45 52 56 45 52 0a                            SERVER.
```

Now the client ends the connection by initiating the final FIN-ACK/FIN-ACK/ACK sequence.

```
No.   Time        Source                Destination           Protocol
6162  3482.819770 172.20.1.2            172.20.1.101          TCP

2288 > 1241 [FIN, ACK] Seq=3885450516 Ack=3104821034 Win=64660 Len=0

0000  00 0c 29 e8 de 65 00 50 56 c0 00 01 08 00 45 00   ..)..e.PV.....E.
0010  00 28 cb 96 40 00 80 06 d4 a9 ac 14 01 02 ac 14   .(..@...........
0020  01 65 08 f0 04 d9 e7 97 45 14 b9 0f cf 2a 50 11   .e......E....*P.
0030  fc 94 95 ff 00 00 00 00 00 00 00 00               ............
```

```
No.   Time        Source                Destination           Protocol
6163  3482.857691 172.20.1.101          172.20.1.2            TCP

1241 > 2288 [FIN, ACK] Seq=3104821034 Ack=3885450517 Win=35040 Len=0

0000  00 50 56 c0 00 01 00 0c 29 e8 de 65 08 00 45 00   .PV.....)..e..E.
0010  00 28 8f c3 40 00 40 06 50 7d ac 14 01 65 ac 14   .(..@.@.P}...e..
0020  01 02 04 d9 08 f0 b9 0f cf 2a e7 97 45 15 50 11   .........*..E.P.
0030  88 e0 09 b3 00 00                                 ......
```

```
No.   Time        Source                Destination           Protocol
6164  3482.858770 172.20.1.2            172.20.1.101          TCP

2288 > 1241 [ACK] Seq=3885450517 Ack=3104821035 Win=64660 Len=0

0000  00 0c 29 e8 de 65 00 50 56 c0 00 01 08 00 45 00   ..)..e.PV.....E.
0010  00 28 cb 97 40 00 80 06 d4 a8 ac 14 01 02 ac 14   .(..@...........
0020  01 65 08 f0 04 d9 e7 97 45 15 b9 0f cf 2b 50 10   .e......E....+P.
0030  fc 94 95 fe 00 00 00 00 00 00 00 00               ............
```

This concludes the look at the Nessus NTP protocol. I hope the examples, while not complete for all circumstances, give a basic understanding on how a Nessus client communicates with a Nessus server and give some guidance on how to figure out the rest. Getting started was the hardest part. Good Luck!

Frank