Analyst.Pcap

Howard Phan

Table of Contents

Analyst

Details

---

1) The 192.168.0.0/22 network is your internal network, all other addresses are external to your network.
2) All of the internal addresses are workstations, no server traffic was captured here.
3) Packets seen here are snippets of real conversations (I.E. if you see a SYN/ACK, it was in response SYN).
What (if anything) is wrong in this capture, and how would you suggest they be addressed?

1. File: Analyst.pcap
   [Computed Hashes]
   MD5 checksum: a9a8827952cb1f53dc7e89148127458b
   SHA1 checksum: bc54a8dee080492d042677f199e472643ff91d0f
   SHA256 checksum: c377a2f18bd64ee715ff54a69fb15d9241cc8931f00255ee1a88bacfb3829dc0

Analyst

Summary of Findings

Tools used for the analysis of the pcap file

- Wireshark 2.2.6 (v2.2.6-0-g32dac6a)

The analysis of the pcap file identified the following summary information in relation to the exhibit.

Packet 3. IP address 192.168.2.142 is sending a ping request to destination 5.255.255.255 through the icmp protocol

Packet 4. IP address 192.168.2.142 is sending a get request from an outside host www.claria.com\r\n to download a file called Gator-4.2.exe

Packet 5. IP address 192.168.2.142 is an Xmas tree packet, as shown by Flag:0x029 (FIN, PSH, URG). The packet is launched from 192.168.2.142 against the destination ip of 5.192.33.34 port 111

Packet 7. IP address 192.168.2.142 is attempting to test the IIS Unicode directory traversal exploit using the command GET /scripts/..%c1%1c../winnt/sysem32/cmd.exe?/c+dir

Packet 9. IP address 192.168.0.68 is sending an IRC connection request to an external IP address, with the username wks56491.

Packet 10. IP address 192.168.0.68 is using an outdated protocol (TFTP) to read request the file test.exe using the octet transfer mode.

Analyst

Timeline

11/10/2005 6:32:20 PM (2005-11-10 14:32:20 UTC)

IP address 192.168.2.142 sends out Echo (ping) request.

11/10/2005 6:48:12 PM (2005-11-10 14:48:12 UTC)

IP address 192.168.2.142 GET /update/Gator-4.2.exe HTTP/1.1.

11/10/2005 6:58:16 PM (2005-11-10 14:58:16 UTC)

IP address 192.168.2.142 Xmas Tree Scan on destination 5.192.33.34 port 111.

11/10/2005 8:01:49 PM (2005-11-10 16:01:49 UTC)

IP address 192.168.2.142 attempts to test the IIS unicode directory traversal exploit.

11/10/2005 8:51:43 PM (2005-11-10 16:51:43 UTC)

IP address 192.168.0.68 sends an IRC connection request to an external IP address.

11/10/2005 9:45:25 PM (2005-11-10 17:45:25 UTC)

IP address 192.168.0.68 sends a read request for file text.exe using the octet transfer mode.

Analyst

Issues that should be addressed

On Packet 3, the IP address 192.168.2.142 is sending a ping request to destination 5.255.255.255 through the icmp protocol, but is not getting a response. An ICMP echo request can be used to DOS other IPs so it is normal for a corporate network to not allow ICMP echo request packets.

There is a get request being sent from an outside host (www.claria.com\r\n) to download an executable file labeled Gator-4.2.exe. It is unusual for a corporate network to allow downloads from outside sources, unless it has been whitelisted by the IT department.

Looking at Packet 5, there is an Xmas scan as shown by Flag:0x029 (FIN,PSH,URG). The packet is launched from 192.168.2.142 against the destination ip of 5.192.33.34 port 111, which is a unix port commonly used for enumerating services and ports on the machine, may be a packet of interest as it could be linked to malicious activity. The Xmas tree packet should be addressed because the attack is normally used for reconnaissance on the network.
A suggestion to address this is to set up firewall rules that flag/drop all packets with FIN, URG, and PSH.

The workstation assigned to the IP address 192.168.2.142 is attempting to test the IIS Unicode directory traversal exploit using the command:
GET/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir
The command can be run maliciously through scripts already in the scripts directory of the web server. This exploit allows the attacker to create a copy of the cmd.exe in the scripts directory and send DOS commands through a url.
The workstation assigned to the ip address should be blocked and isolated from the rest of the network and undergo forensic examination.

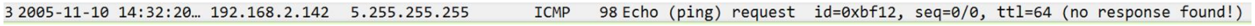
A review is needed for Packet 9, as the ip address 192.168.0.68 is sending an IRC connection request to an external IP address with the username wks56491. More information about the network is needed before concluding on whether it is malicious or not.

The IP address in Packet 10 is using an outdated protocol (TFTP) to read request the file test.exe using the octet transfer mode.

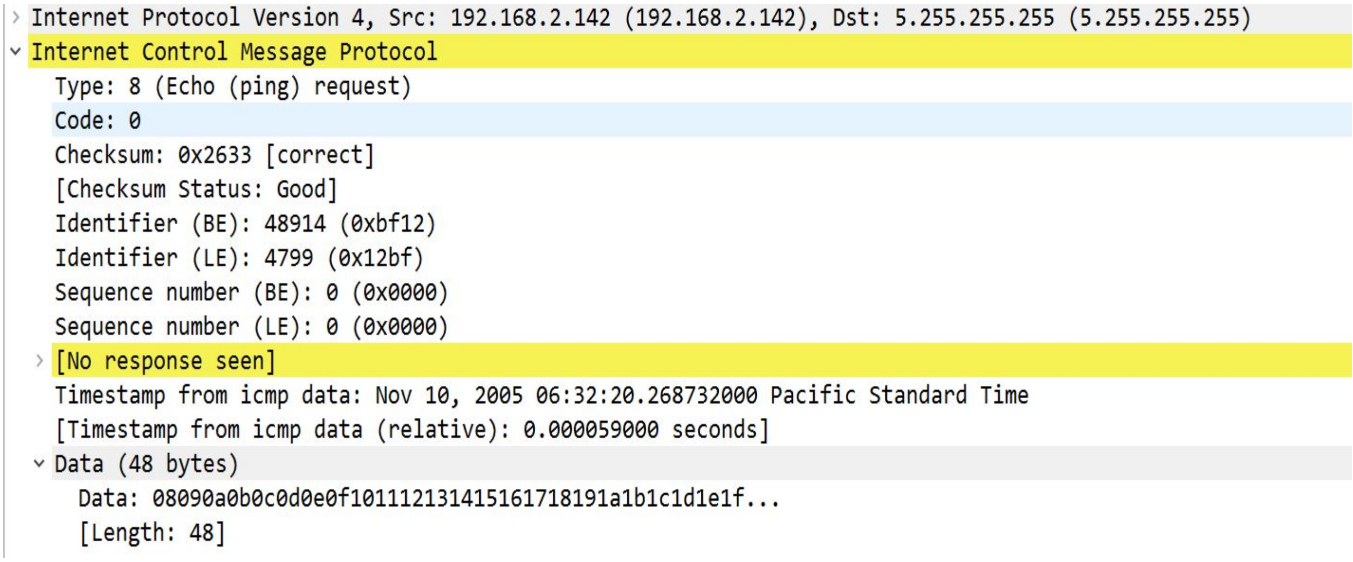
Analyst.Pcap evidence:

1.1

Name: Packet 3
Created: 11/10/2005 6:32:20 PM (2005-11-10 14:32:20 UTC)
Item: 1
Category: Pcap
P-Size: 98 bytes on wire



```
3 2005-11-10 14:32:20… 192.168.2.142   5.255.255.255       ICMP    98 Echo (ping) request  id=0xbf12, seq=0/0, ttl=64 (no response found!)
```

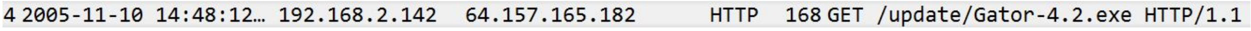


```
> Internet Protocol Version 4, Src: 192.168.2.142 (192.168.2.142), Dst: 5.255.255.255 (5.255.255.255)
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x2633 [correct]
    [Checksum Status: Good]
    Identifier (BE): 48914 (0xbf12)
    Identifier (LE): 4799 (0x12bf)
    Sequence number (BE): 0 (0x0000)
    Sequence number (LE): 0 (0x0000)
  > [No response seen]
    Timestamp from icmp data: Nov 10, 2005 06:32:20.268732000 Pacific Standard Time
    [Timestamp from icmp data (relative): 0.000059000 seconds]
  v Data (48 bytes)
      Data: 08090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f...
      [Length: 48]
```

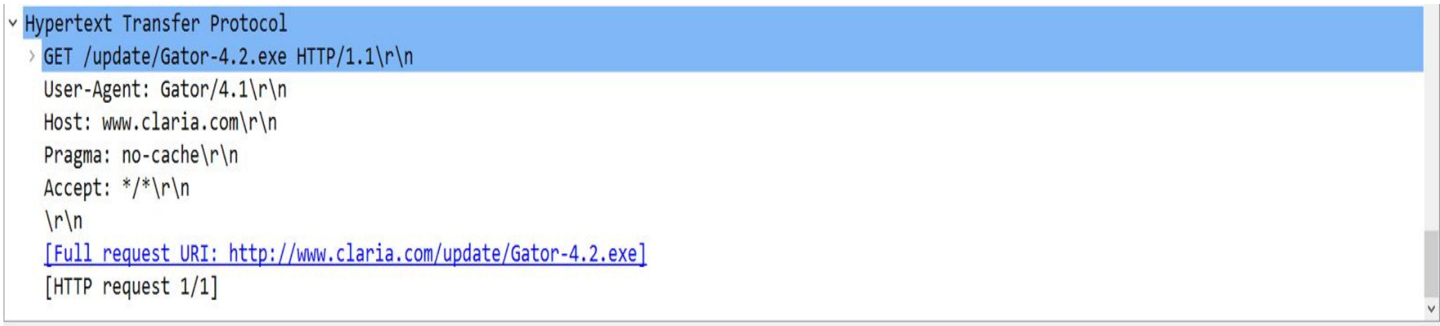
Analyst

1.2

Name: Packet 4
Created: 11/10/2005 6:48:12 PM (2005-11-10 14:48:12 UTC)
Item: 2
Category: Pcap
P-Size: 168 bytes on wire



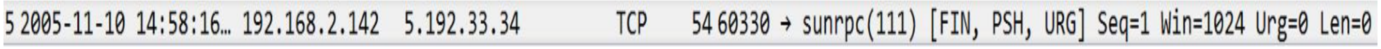
```
4 2005-11-10 14:48:12…  192.168.2.142   64.157.165.182       HTTP   168 GET  /update/Gator-4.2.exe HTTP/1.1
```



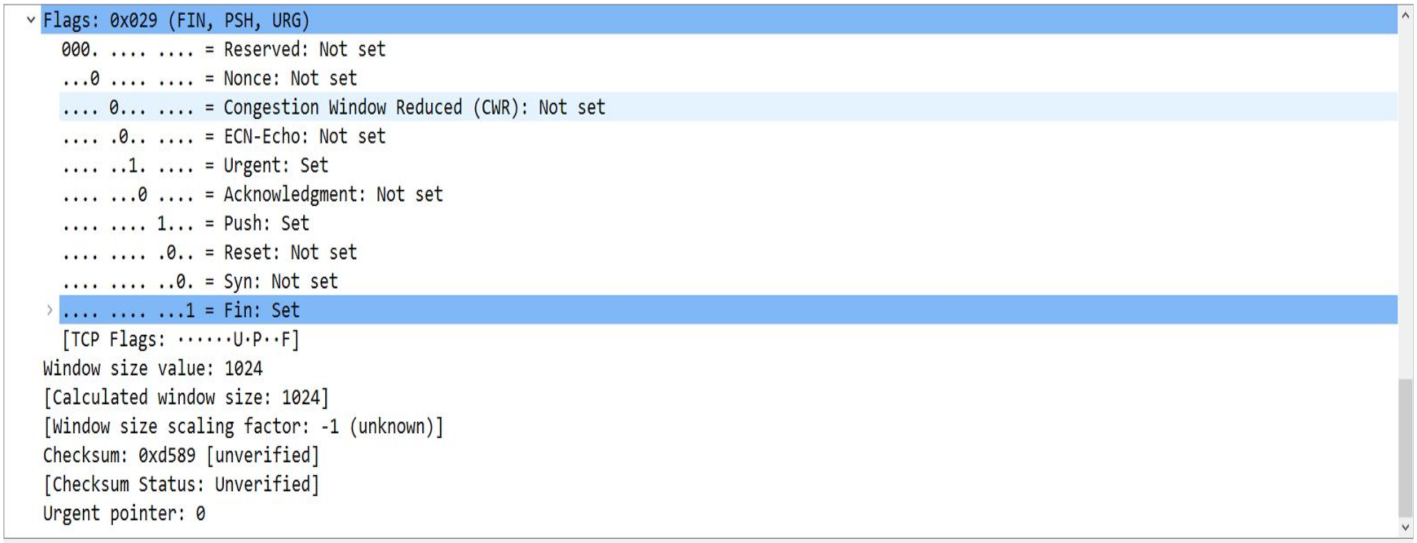
```
⌄ Hypertext Transfer Protocol
  › GET /update/Gator-4.2.exe HTTP/1.1\r\n
    User-Agent: Gator/4.1\r\n
    Host: www.claria.com\r\n
    Pragma: no-cache\r\n
    Accept: */*\r\n
    \r\n
    [Full request URI: http://www.claria.com/update/Gator-4.2.exe]
    [HTTP request 1/1]
```

1.3

Name: Packet 5
Created: 11/10/2005 6:58:16 PM (2005-11-10 14:58:16 UTC)
Item: 3
Category: Pcap
P-Size: 54 bytes on wire



```
5 2005-11-10 14:58:16… 192.168.2.142   5.192.33.34        TCP     54 60330 → sunrpc(111) [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
```

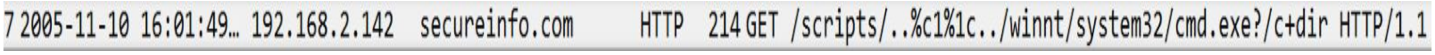


```
⌄ Flags: 0x029 (FIN, PSH, URG)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Nonce: Not set
    .... 0... .... = Congestion Window Reduced (CWR): Not set
    .... .0.. .... = ECN-Echo: Not set
    .... ..1. .... = Urgent: Set
    .... ...0 .... = Acknowledgment: Not set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
  › .... .... ...1 = Fin: Set
    [TCP Flags: ······U·P··F]
  Window size value: 1024
  [Calculated window size: 1024]
  [Window size scaling factor: -1 (unknown)]
  Checksum: 0xd589 [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
```

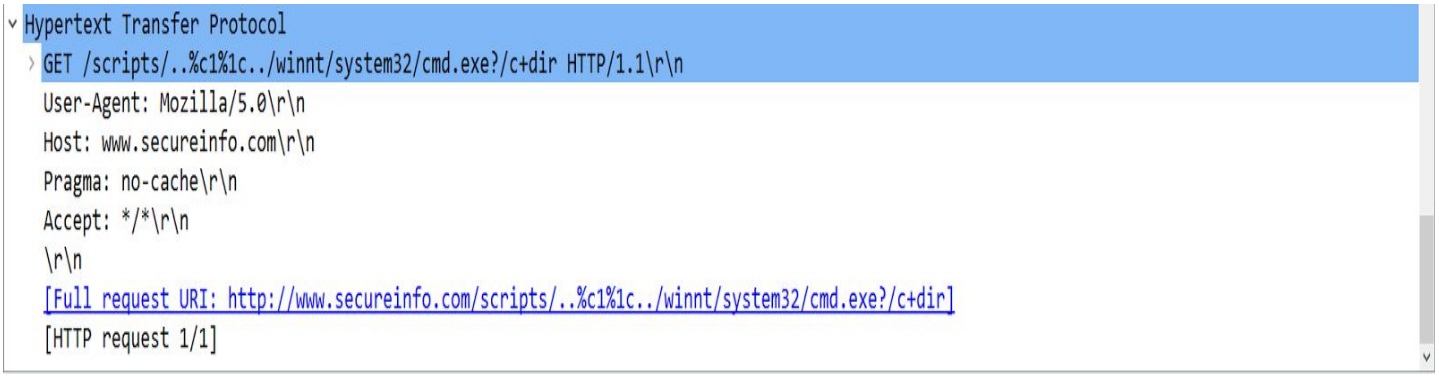
Analyst

1.4

Name: Packet 7
Created: 11/10/2005 6:58:16 PM (2005-11-10 14:58:16 UTC)
Item: 4
Category: Pcap
P-Size: 214 bytes on wire



```
7 2005-11-10 16:01:49… 192.168.2.142   secureinfo.com     HTTP   214 GET /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.1
```

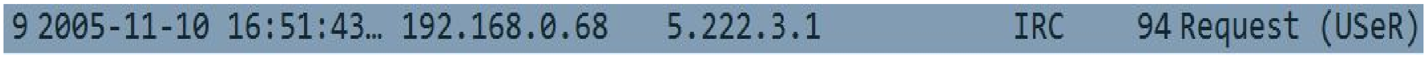


```
v Hypertext Transfer Protocol
  > GET /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.1\r\n
    User-Agent: Mozilla/5.0\r\n
    Host: www.secureinfo.com\r\n
    Pragma: no-cache\r\n
    Accept: */*\r\n
    \r\n
    [Full request URI: http://www.secureinfo.com/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir]
    [HTTP request 1/1]
```

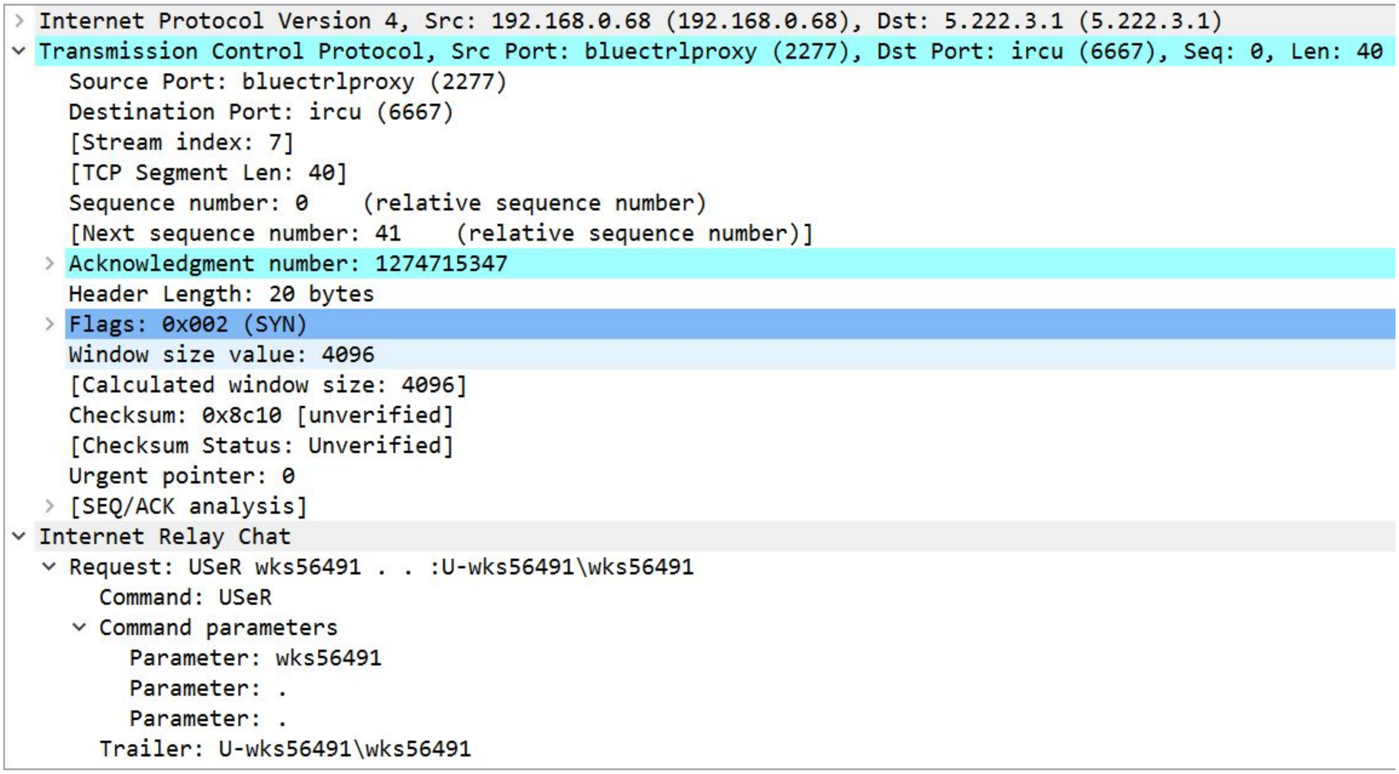
Analyst

1.5

Name: Packet 9
Created: 11/10/2005 6:58:16 PM (2005-11-10 14:58:16 UTC)
Item: 5
Category: Pcap
P-Size: 94 bytes on wire



```
9 2005-11-10 16:51:43… 192.168.0.68    5.222.3.1           IRC     94 Request (USeR)
```

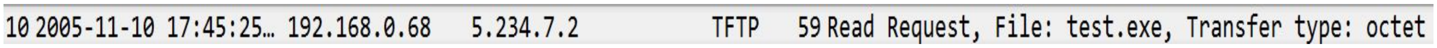


```
> Internet Protocol Version 4, Src: 192.168.0.68 (192.168.0.68), Dst: 5.222.3.1 (5.222.3.1)
v Transmission Control Protocol, Src Port: bluectrlproxy (2277), Dst Port: ircu (6667), Seq: 0, Len: 40
    Source Port: bluectrlproxy (2277)
    Destination Port: ircu (6667)
    [Stream index: 7]
    [TCP Segment Len: 40]
    Sequence number: 0    (relative sequence number)
    [Next sequence number: 41    (relative sequence number)]
  > Acknowledgment number: 1274715347
    Header Length: 20 bytes
  > Flags: 0x002 (SYN)
    Window size value: 4096
    [Calculated window size: 4096]
    Checksum: 0x8c10 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > [SEQ/ACK analysis]
v Internet Relay Chat
  v Request: USeR wks56491 . . :U-wks56491\wks56491
      Command: USeR
    v Command parameters
        Parameter: wks56491
        Parameter: .
        Parameter: .
      Trailer: U-wks56491\wks56491
```

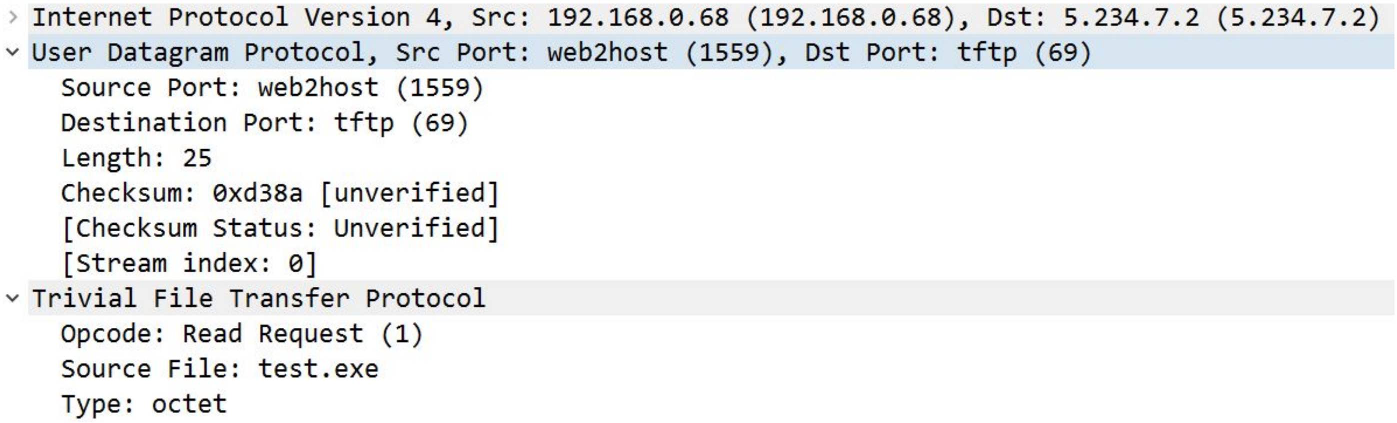
Analyst

1.6

Name: Packet 10
Created: 11/10/2005 6:58:16 PM (2005-11-10 14:58:16 UTC)
Item: 6
Category: Pcap
P-Size: 59 bytes on wire



```
10 2005-11-10 17:45:25… 192.168.0.68    5.234.7.2          TFTP    59 Read Request, File: test.exe, Transfer type: octet
```



```
> Internet Protocol Version 4, Src: 192.168.0.68 (192.168.0.68), Dst: 5.234.7.2 (5.234.7.2)
v User Datagram Protocol, Src Port: web2host (1559), Dst Port: tftp (69)
    Source Port: web2host (1559)
    Destination Port: tftp (69)
    Length: 25
    Checksum: 0xd38a [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
v Trivial File Transfer Protocol
    Opcode: Read Request (1)
    Source File: test.exe
    Type: octet
```