Global Information Assurance Certification Paper

The Lone Packet

Denial of Service Against Kerio Personal Firewall

Prepared by:

Gerald Batten, CISSP, SCSP
GCIH Certification Practical
Version 4, Option 1

January 20th, 2005

Abstract/Summary

This paper represents the practical assignment portion of the SANS Track 4 course, as part of the GCIH certification. The first portion details the actual exploit, and provides a technical description of the cause of the exploit, how it can be successfully executed, as well as some background information.

The second portion details the steps in which a malicious user may go about researching a vulnerability (in this case the Kerio Personal Firewall Denial of Service vulnerability) with a suitable exploit for their environment, and the successful execution of the exploit.

The third portion details the steps in which a response team may respond to an attack as described in the second portion. It details how the team goes through the steps of the incident handling process given their environment and limitations.

Table of Contents

Statement of Purpose

The attack I have chosen for this exercise is the successful execution of a denial of service attack against the Kerio Personal Firewall. Versions 4.1.1 and prior appear to be vulnerable to this specific attack. The denial of service attack consists of sending a single packet to the target machine with a TCP option length of zero.

Being somewhat limited in actual available computer equipment and configurations, I planned on performing the exercise with two separate systems. It should be noted that the attacking system as well as the victim system will both be virtual machines within VM Ware. Figure 1 presents the physical layout, as well as the host and virtual operating systems.

The attacking system is currently running Windows 2000 Pro, with service pack 4 installed. Ethereal 0.10.7 and VMWare 4 are installed. This instance of VMWare is used to load and utilize Knoppix-STD 0.1b within a virtual machine. It is not possible to natively use Knoppix-STD on this system, since it is a laptop, and therefore does not recognize the native network or video services, which are critical to the success of this exercise.

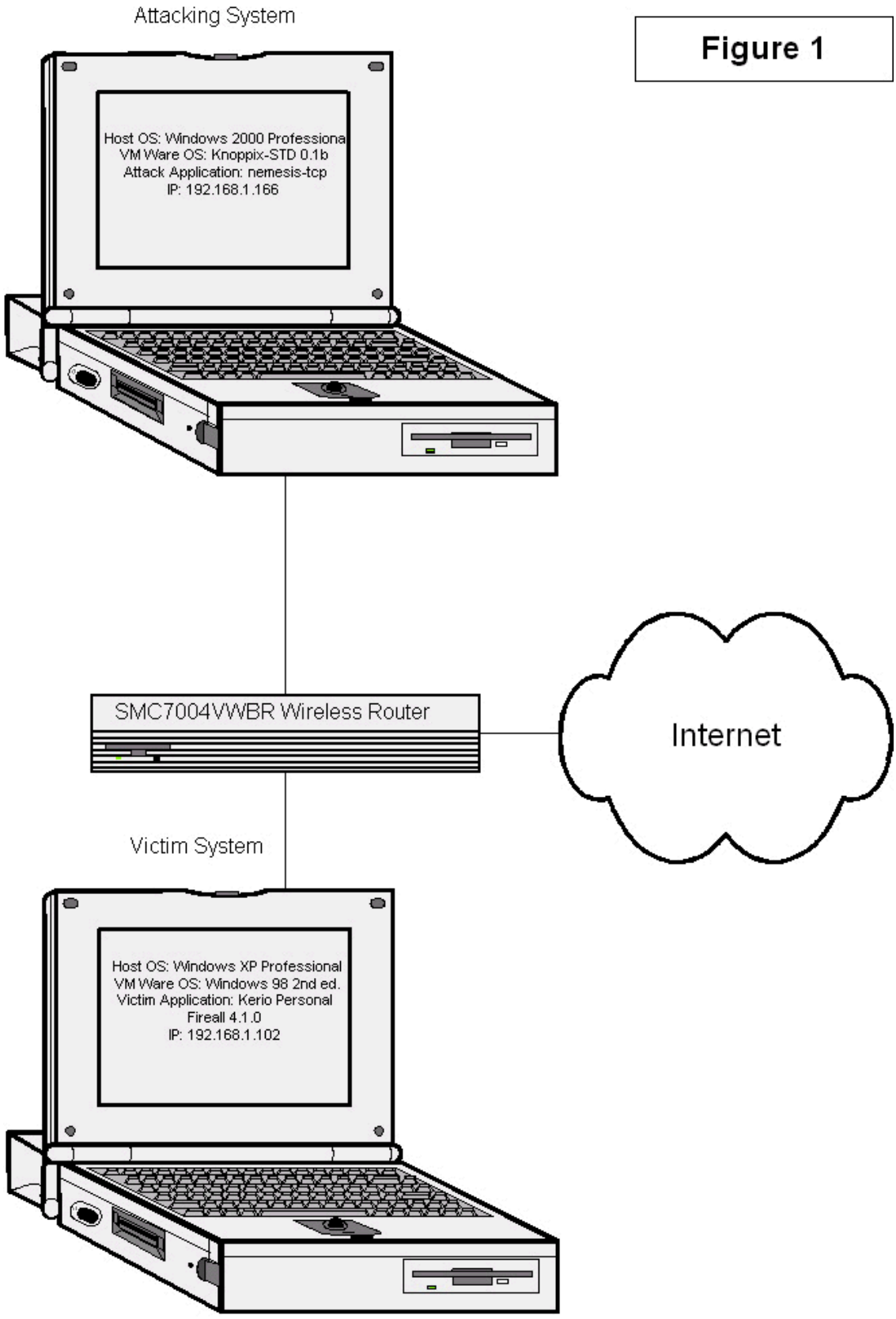
The victim system is currently running Windows XP Pro SP1, with all other security updates installed (with the exception of SP2) as of the time of this exercise. A full list is available in the References section of this document. VMWare 4 is installed, and Windows 98 Second Edition is installed and enabled on the VMWare virtual machine. The only additional piece of software installed on the Windows 98 virtual machine is the Kerio Personal Firewall v4.1.0.

The attacking system and the victim system are both attached to an SMC 7004VWBR wireless router. It should be noted that the systems are wired to the wireless router, because various low-level network tools such as Ethereal do not always behave as desired in a wireless environment.

From the attacking system, the intention is to capture all relevant packets with Ethereal. This will be accomplished by setting a capture filter for the IP address of the victim system (192.168.1.102), so that only traffic with a source IP or target IP of the victim system will be captured.

From the victim system, the intention is to use the ping command to establish a heartbeat to the attacking system. When the victim system stops sending icmp packets, this will demonstrate within the ethereal logs that the denial of service attack was successful.

Figure 1



The Exploit
In this section, we will be discussing the various details of the exploit. This includes a technical description of the exploit, an analysis of the tools used in the successful execution of the exploit, as well as a description of the environment that ensures a system is vulnerable to this exploit.

Name
Kerio Personal Firewall Denial Of Service Vulnerability

- EEye Advisory #: AD20041109
- Secunia Advisory #: 13030
- CVE Advisory #: CAN-2004-1109
- SecurityFocus Advisory #: 11639
- ISS Xforce Advisory #: 17992

Operating Systems

- Windows '98
- Windows '98 Second Edition
- Windows Millennium Edition
- Windows 2000 Professional
- Windows XP Home
- Windows XP Pro

Protrocols/Services/Applications

- Kerio Personal Firewall 4.0.6
- Kerio Personal Firewall 4.0.7
- Kerio Personal Firewall 4.0.8
- Kerio Personal Firewall 4.0.9
- Kerio Personal Firewall 4.0.10
- Kerio Personal Firewall 4.0.16
- Kerio Personal Firewall 4.1
- Kerio Personal Firewall 4.1.1
- TCP, UDP or ICMP options length value must be 0, where the TCP, UDP or ICMP options are greater than 0.

Description
Kerio Personal Firewall, from version 4.0.6 until 4.1.1 inclusive, is vulnerable to a denial of service attack. This particular vulnerability was discovered by eEye Digital Security on October 30, 2004. Kerio released an updated version of their firewall product, which mitigated the vulnerability on November 9th, 2004, 10 days later.

The exploit can be conducted remotely or locally. However, in a real-world situation, it would be highly unlikely that this exploit would be conducted locally. Because Kerio Personal Firewall accepts and interprets all packets under any

condition, this exploit will succeed even if the Kerio Personal Firewall is configured to reject or ignore all packets. The exploit consists of a single packet, using TCP. The sources referenced indicate that UDP and ICMP options may work as well, however this exercise will only utilize the TCP options field. The actual exploit consists of a falsified value in the options field. Specifically, the field length value must be 0, when the options field is greater than 0 bytes.

When Kerio Personal Firewall decodes a packet laced with the falsified options length value, it immediately causes an infinite loop to occur, taking up all CPU cycles. The problem occurs when Kerio Personal Firewall realizes that there are extensions, however the offset, or length, indicates that there are no options. Kerio reads the falsified option length, and is programmed to move the memory pointer that many bytes. Since the value is zero, it does not move. Since it is in the same place, it will read the value, and attempt to move that any bytes, thus the infinite loop. Curiously, the exploit works even when the Kerio Personal Firewall is configured to deny any and all traffic. This occurs because the logic that dictates which packets to ignore is preceded by the logic that captures and decodes the network traffic.

Signatures of the Attack

Empirical evidence of a successful execution of this exploit can be observed as a system that no longer responds to any interaction. If a user's system suddenly and mysteriously stops responding to keystrokes, mouse gestures, remote network access or swearing, this is a good indication that the system has fallen victim to someone exploiting the denial of service vulnerability within Kerio Personal Firewall. This is assuming, of course, that Kerio Personal Firewall is installed and in use at the time.

A successful attack does not leave any signatures on the victim system. It does, however, leave a fairly specific signature when the attacking packet is sniffed from the network. The key factor in this exploit is a TCP options length of zero, when the actual options length field is greater than 0. This signature may be detected by a network intrusion detection program such as Snort.

When using Snort to effectively detect this exploit, Snort should be started with the –b option in order to enable it to log the full binary packet. The following Snort rule should detect the packet:
alert tcp any any -> any any (contents:"|01 01 05 00|"; msg:"Possible Null TCP Options Length";)

This rule will cause an alert to be generated if it finds the hexadecimal string "01 01 05 00" anywhere within any packet that Snort is capable of detecting. The "01 01 05 00" string is indicative of the TCP options indicated in the eEye advisory number AD20040423. This advisory is for a different product, but the vulnerability and exploit are identical to the Kerio Personal Firewall advisory.

Unfortunately, according to the Snort documentation, it is possible to create a rule which filters on what IP Options are in use, but not for TCP Options. It also does not specify if it can detect a zero-length options field. Therefore, this rule may cause false positive conditions.

What is a denial of service attack?

A denial of service attack is an unauthorized exploitation of a system or service within a system, with the intent of reducing or eliminating its desired or intended functionality. Such attacks are by definition malicious in nature. The immediately apparent resulting effect of a successful denial of service attack is the lack of availability for a particular system or service. Depending on the system or service, there may be significant financial consequences as well.

One of the most famous denial of service attacks happened in February 2000, when a Montreal-area teen, whose Internet alias was Mafiaboy, successfully executed denial of service attacks against several high-profile e-commerce sites, potentially resulting in millions of dollars of lost revenue for the affected companies.

What are TCP Options?

In a rare demonstration of foresight, the designers of TCP/IP included TCP options in the original design of the protocol. They realized that somebody in the future might want to improve or tweak the protocol without having to re-develop the protocol from the ground up. TCP options allow for improvements in TCP while ensuring backwards compatibility.

Stages Of The Attack Process

In this section, we will be discussing the attacker's (Sam from Sales) point of view with regards to this exploit. We will discuss, in a semi-fictional scenario, how Sam acquires his victim through reconnaissance and scanning. The scenario is based on actual events that the author of this paper has witnessed during his career, and identifying information has been removed to protect the guilty, as well as the innocent. We will then discuss how Sam uses this information to exploit the system and gain access. A discussion on possible ways for Sam to maintain his desired state will be theorized, as well as possible ways for Sam to obfuscate or otherwise cover his tracks.

Reconnaissance

The Kerio Personal Firewall software effectively blocks all typical reconnaissance methods. For example, the following command was executed from the attacking system in an attempt to obtain information against the victim:
Nmap –sS –sV –O –v –v 192.168.1.102 –oN ./scankerio.txt

The results were as follows:
nmap 3.70 scan initiated Fri Dec 10 15:04:24 2004 as: nmap -sV -O -v -v -oN /temp/scankerio.txt 192.168.1.102
Warning: OS detection will be MUCH less reliable because we did not find at least 1 open and 1 closed TCP port
All 1660 scanned ports on 192.168.1.102 (192.168.1.102) are: filtered
MAC Address: 00:0C:29:F8:E2:08 (VMware)
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SInfo(V=3.70%P=i686-pc-linux-gnu%D=1/11%Time=41E43176%O=-1%C=-1)
T5(Resp=N)
T6(Resp=N)
T7(Resp=N)
PU(Resp=N)
# Nmap run completed at Fri Dec 10 15:05:10 2005 -- 1 IP address (1 host up) scanned in 45.779 seconds.

The nmap scan above is attempting to do several things.

- The –sS option indicates that we are performing a SYN scan, which is the default when the user has root or equivalent privileges.
- The –sV option tells nmap that we wish to perform a version scan. A version scan attempts to guess what product and version is running on a discovered port. For example, let us suppose for an instant that we are running a SYN scan against a server running Microsoft IIS. A version scan will attempt to determine what version of IIS is running on the target system.
- The –O option indicates to nmap that we wish to guess what the operating.
- The –v options indicate to nmap that we wish very verbose output.

- The IP address of the target system may appear in between any option.
- The –oN option indicates to nmap that we wish to save the output in human-readable format. The option is followed by the file name containing the command's output.

In order to establish that the system is actually turned on, an attempt to simply ping the victim machine resulted in the following:

```
PING 192.168.1.102 (192.168.1.102) 56(84) bytes of data.
64 bytes from 10.165.21.171: icmp_seq=1 ttl=128 time=5.90 ms
64 bytes from 10.165.21.171: icmp_seq=2 ttl=128 time=0.133 ms
64 bytes from 10.165.21.171: icmp_seq=3 ttl=128 time=0.171 ms
64 bytes from 10.165.21.171: icmp_seq=4 ttl=128 time=0.133 ms
64 bytes from 10.165.21.171: icmp_seq=5 ttl=128 time=0.161 ms

--- 192.168.1.102 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4025ms
rtt min/avg/max/mdev = 0.133/1.300/5.906/2.303 ms
```

Kerio Personal Firewall, in its default configuration, allows ICMP echo requests, but effectively ignores port scans. Therefore, in this scenario, traditional reconnaissance techniques are ineffective. For the purposes of this paper, we will assume that Sam from Sales is a technically proficient disgruntled employee of Acme Widgets, Inc., and that Kerio Personal Firewall is a corporate standard that is installed on all desktops. Fortunately for Sam, the corporate IT department is slightly behind in their patch management.

The attacker therefore, must perform a different kind of reconnaissance, and research what vulnerabilities exist within the products currently installed on his or her desktop. This may be accomplished by researching vulnerabilities on the web sites of specific vendors, such as http://www.microsoft.com or http://www.kerio.com. Additional information, such as specific details regarding vulnerabilities may be found at http://www.securityfocus.com, http://www.secunia.com, and the Bugtraq full disclosure mailing list, archived at http://seclists.org/#fulldisclosure.

Scanning

Kerio Personal Firewall, in its default configuration, detects and blocks port scans, as demonstrated in the Reconnaissance section above. Therefore, the assumption can be made that since there do not appear to be any ports open on the victim system, and yet it responds to ping requests, that this particular system is protected by the corporate desktop firewall.

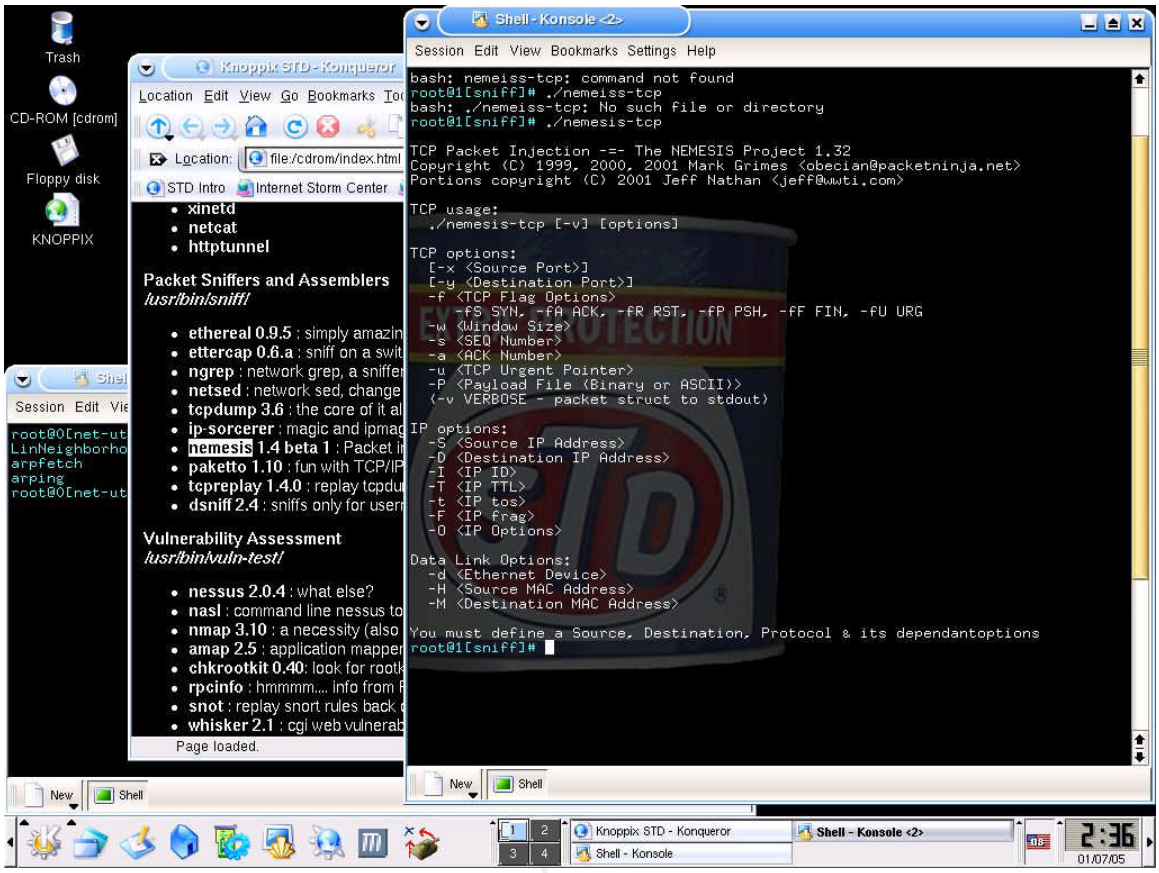
Exploiting the system

Once a vulnerability has been discovered, in this case the Kerio Personal Firewall Denial of Service vulnerability, Sam must determine what resources are required in order to successfully execute the exploit.

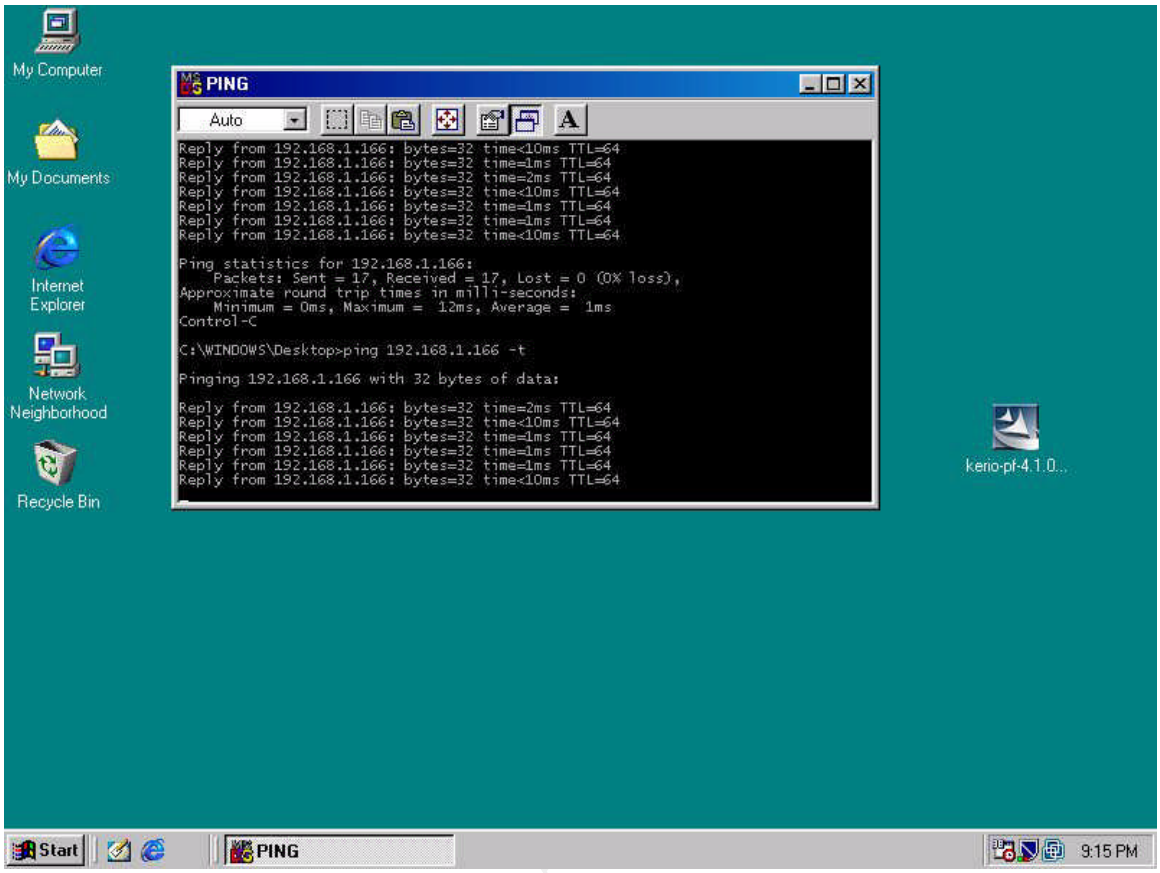
This particular exploit requires the creation of a TCP packet with a modified TCP options length value. The tools required to create such a packet are not readily available within the standard corporate desktop, or the corporate network. Therefore, additional software must be obtained. This presents Sam with a problem, because the default user configuration does not allow for third-party software to be installed by the user. This problem is resolved by the Knoppix-STD 0.1b Linux distribution. Knoppix is a fully functional Linux installation on a bootable CD-ROM. Because Knoppix is never actually installed, and bypasses the native operating system completely, the attacker is capable of using the required tools without circumventing the security of the native operating system, or potentially violating company policy (at least the part about not installing unauthorized software).

The attacker has decided to attack the system of the CEO's administrative assistant, preventing an important document from being completed. An 'nslookup' command is used to determine the IP address of the victim system. The administrative assistant's computer is running Windows '98 second edition without any security patches. It should be noted that in the author's experience, the administrative assistant of the head honcho (CEO, President, etc…) has has almost always been provided with sub-standard equipment. This is the basis for the assumption that the CEO's administrative assistant, in this case, is equipped with an un-patched, antiquated system.

Sam inserts the Knoppix-STD 0.1b CD-ROM into his computer system and re-boots. The computer boots from the CD instead of the hard drive, and loads the Knoppix graphical user interface (GUI). Sam launches the 'Sniffers and Packet Assemblers' command-line interface, as seen below.



Meanwhile, the attacker has managed to establish a heartbeat from the victim machine back to the target machine. Let us assume that the attacker is in the office after-hours and has physical access to the victim system. If the exploit is successful, the heartbeat will stop.



Unfortunately, the coding ability of Sam (and by extension, the author) prohibited the creation of a custom created tool. Therefore, the 'nemesis-tcp' tool was used to generate the desired packet. The command line that generated the packet is as follows:

nemesis-tcp -x 10 -y 10 -fS -s 10000 -u 0 -v -S 192.168.1.166 -D 192.168.1.102 -O 01010500

The command parameters provide the application with all of the information required to execute the exploit.

- The –x and –y options provides nemesis-tcp with the source and target ports, respectively.
- The –fS option informs the program that the SYN flag is to be set. This is to help ensure that any routers along the way do not reject the packet, by pretending to initiate a TCP handshake. A TCP handshake establishes a TCP connection, and follows three steps. The initiating system sends a packet with the SYN flag set. The target system then replies back with the SYN and ACK flags set, basically saying "Yes, I'm here. Are you still there?". The initiating system sends a final packet with the 'ACK' flag set basically stating, "Yes, I'm here". Routers may be configured to keep state, where they may reject any packet with a 'SYN/ACK' or 'ACK' if there is no preceding, corresponding 'SYN'.

- The –s option indicates what sequence number to use. For the purposes of this exploit, any number will suffice.
- The –u option specifies whether or not the 'urgent' pointer is used. In this case, there is no urgent pointer.
- The –v options indicate that verbose mode is to be used. This provides additional, human-readable information in the results.
- -S and –D indicate source and destination IP addresses. The source address need not be the actual source address of the attacking system.
- -O indicates what TCP options to utilize, if any. The TCP options in this situation are the cause the exploitation of the vulnerability within Kerio personal firewall. The value following the –O is actually a hexadecimal value, where the last pair of digits (00) indicates the length of the option field. This is a falsified value, since there are actually options within the options field, which are defined in this case as '010105'.

.

Once the packet has been sent, the victim system is thrown into an infinite loop, which prevents other processes from obtaining any CPU cycles. The computer is incapable of performing any other tasks, including tracking the mouse pointer when the mouse is moved. The infinite loop occurs when "the vulnerable code maintains an offset into the IP option bytes, and attempts to advance past a variable-length option by adding its length to the offset." (eEye). What this means, is that when Kerio Personal Firewall receives a packet, it must decode, or translate the packet into meaningful information. During this process, the TCP Options field is discovered. This field is a variable length field. In order for Kerio Personal firewall to continue reading and interpreting this particular field, it must add the length to its current position. If the length is zero, it will keep detecting a TCP Options field, add the length which is 0 bytes, and re-read the same data over and over. The logic within Kerio personal firewall that dictates what to do with the packet does not supersede the packet capturing logic. Because of this logic flaw, Kerio personal firewall is vulnerable to this exploit even if the 'Block All Traffic' option is enabled.

Network Diagram

The actual physical network diagram is located in the Statement of Purpose section. It indicates that two separate computers are used, each with a virtual machine. The virtual machines are in reality the target and victim systems. The main reason that the project was conducted in this manner was to ensure that proper recording of the event could take place. The alternative reason was simply a lack of available hardware.

The logical diagram below involves only the victim machine, the router, and the attacking machine, as shown here.

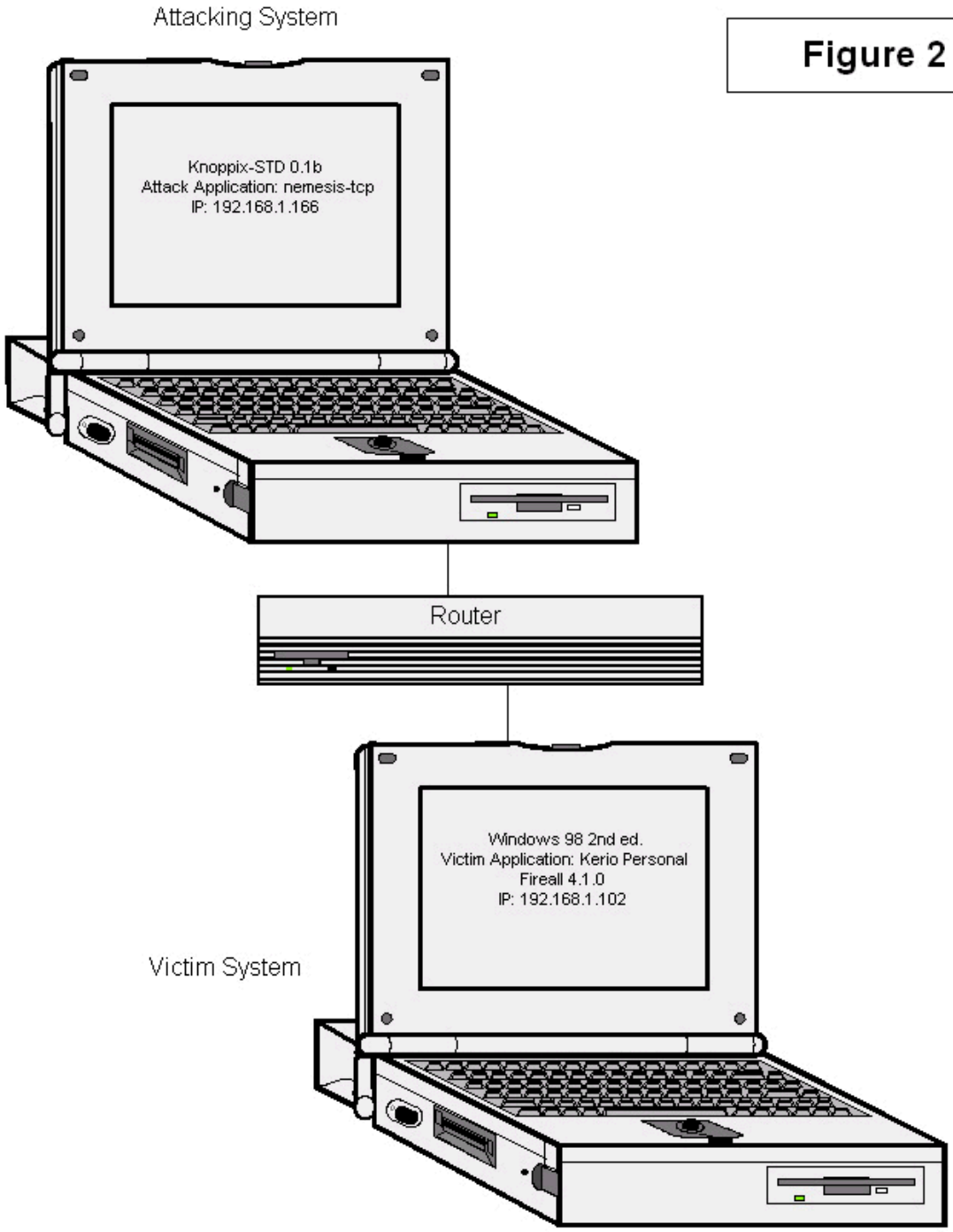


Figure 2

Keeping Access

As this is a denial of service attack that renders the victim system useless until the system is powered off, keeping access is not an issue. However, the attacker may wish to keep their victim systems in a compromised state. This may be accomplished with a simple batch file or shell script. If we program the

script in pseudo-code, it may look like this.

 # Begin script
Obtain current IP address;
Pick random client within address space;
Randomize values (source IP, sequence number, source port, target port)
Execute nemesis-tcp with spoofed values;
Goto start of script
#End script

In this case, Sam is not capable of keeping access due to the nature of the exploit. However, he may be able to continually attack vulnerable systems at random, potentially causing a surge in calls to the corporate help desk, causing a non-IT denial of service attack in addition to his successful exploit of the corporate desktop firewall.

Covering Tracks

Kerio Personal Firewall does not record any events in its log regarding the attack. However, a packet sniffer is capable of capturing the offending packet. In this section, we shall see what the packet looks like 'on the wire', as well as options for the attacker with regards to obfuscating its source.

First, we shall have a look at what ethereal picks up on the wire. Luckily, nemesis-tcp performed where the attacker wanted it to, which is the falsified option field length:
Security (with too-short option length = 0 bytes)

The intended source and destination ports were supposed to be 10, with a sequence number of 10000. It appears that there may be either a bug in nemesis-tcp, or that it is suffering from improper documentation. In any case, for some reason, the source port, destination port and sequence number have ended up with the following values:
Transmission Control Protocol, Src Port: 0 (0), Dst Port: 10000 (10000), Seq: 0

Fortunately, such errors are forgivable since the source port, destination port and sequence numbers are irrelevant for this exploit to function. Nemesis-tcp also seems to have sent two identical packets with the same values when only one packet was requested.

Since the exploit consists of a single packet, a full TCP session is not required. The victim does not have to send any information back to the attacker, nor does the attacker have to be on the same network as the victim. As long as the victim receives a single packet, the exploit will succeed. Because nemesis-tcp is capable of creating a packet with an incorrect source IP address, an attacker can cover their tracks quite easily with this exploit.

Since Sam is a disgruntled employee, he will want to create the offending packet with a spoofed source IP address. This may be accomplished by simply using a different IP address on the nemesis-tcp command line. Depending on the spoofed IP address, Sam may make the packet appear to originate from the Internet. Alternatively, he may spoof the source IP address to appear as if the packet came from another co-worker, thereby framing them for the crime.

The Incident Handling Process

In this section, we will discuss the exploit from the point of view of the incident handler. During this exercise, we will see how the incident handler would go through the six steps in the incident handling process.

Preparation

In this section, we will discuss how the incident handling team has (or has not) prepared for this type of situation. There are 10 fundamentals of contingency planning (SANS courseware book 4.1, page 36), which are:

1. Policy;
2. People;
3. Data;
4. Software/Hardware;
5. Communications;
6. Supplies;
7. Transportation;
8. Space;
9. Power and Environmental Controls; and
10. Documentation.

Policy

The incident handling team at Acme Widgets, Inc., is more commonly known as 'tech support'. Tech support has managed to lead the initiative on corporate IT policy with the cooperation of the legal department. The basics have been covered by the following policies:

Acceptable Use

The acceptable use policy is signed by all employees upon the start of their first full day of work at Acme Widgets, Inc. It basically states that the company recognizes that employees only spend a third (ok, sometimes up to a half) of their life at work, and that sometimes things happen in their personal lives during working hours that require immediate attention. An email or phone call to a spouse or child is acceptable, as is casual Internet usage during breaks and lunch hour. As long as it is not offensive or does not cause harm to the Acme Widgets, Inc. it should be OK. If the employee has any doubt, they may communicate with their manager for clarification.

Legal Policy

The legal policy states if and when Acme Widgets, Inc. will take legal action against an employee, contractor, or any other individual who violates any of the company's rules. In this case, it states that it will most likely not sue any employee unless the damage has caused significant financial or potential financial loss to the company. However, employee dismissal will be considered if repeated violations occur, or if the transgression is serious enough. The decision of dismissing the perpetrator will be up to their manager or human resources.

Privacy Policy

The privacy policy simply states that any information gathered or otherwise obtained on company premises or equipment belongs to the company. This includes all e-mails, instant messages and telephone calls.

IT Policy

The IT policy specifically sets out rules for how computer systems supplied by Acme Widgets, Inc. will be used. Basically, what you see is what you get. No modification or installation of any software or hardware is allowed without management approval. There are, however, no indication of any remedial action should anyone violate this policy.

Warning Banners

Warning banners serve as a reminder of the above policies. The warning banners are displayed every time a user loads the native operating system of their computer system. A 10-second timer is also in place to prevent the user from simply disregarding the warning banner.

People

The incident handling team, a.k.a. tech support, consists of four people: Alice, Bob, Carol and David. They are all technically proficient, and have roughly the same qualifications. Alice is the person with the most seniority, and therefore she is the leader of the group. Since they work in a manufacturing plant (what did you expect Acme Widgets, Inc. to do? They make widgets of course!), they carry around Family Radio Service (FRS) radios at all times for instant communication. One of her duties as group leader is to liaison with other staff, such as Eve, the leader of the legal department, and Frank, leader of physical security. Lastly, Alice must also liaison with Grace, the CIO. Grace's role is to review the tech support group's performance. She recognizes their value (Bob has saved her data on more than one occasion) and gives them her full support. Henry, the human resources leader, works closely with Frank and Alice, especially when an individual happens to do something to warrant dismissal.

Data

Alice's team has a centralized backup system, with weekly full backups, and daily incremental backups. Full backups are stored off-site, usually in Bob's basement.

Software/Hardware

Alice's team has done their best in an attempt to standardize on similar hardware and software. However, with limited budgets, some hardware and software just doesn't get upgraded like it should. Take the example of the executive secretary. All she does is use a word processor and e-mail, so she hasn't been provided with any hardware or software upgrades in about five years. Even then, her hardware upgrade was a hand-me-down from one of the sales representatives. However, the data on her hard drive is very important, so it's not saved to the central server where unauthorized people may gain access. It's quite safe on her antique hard drive, or so says Peter, the President.

Communications

Alice's team relies on face-to-face, email and radio communication. They use FRS radios when they're on the shop floor.

Supplies

Having limited resources, (the widget market profit ratio just hasn't been the same since Widget-Mart became their biggest distributor), Alice's team must scrounge for spare parts and resources. Also, some of the company's systems are so old, that Alice must buy spare parts used, because new parts are no longer being manufactured. They have made a rescue kit, which includes installation disks, rescue disks, a usb drive, and various other tools of the trade, designed to help them recover data, and to restore a system to a known, clean state.

Transportation

Being a fairly liberal company, the use of roller blades on the shop floor expedites transportation of people from one area to another.

Space

Alice and her team do not have very much space. Each member has his or her own cubicle, which are located just outside the server room where the air conditioning system drowns out the noise of the computers.

Power and Environmental Controls

The server room is air conditioned with the proper (yet aging) equipment. A diesel generator is on standby in case the power goes out.

Documentation

Alice had previously come to the realization that her team would eventually change, and that the more common tasks, such as scheduling backups and changing tapes should be well documented. Alice's motto is that if any of her team has had to do anything more than once, it should be documented. Documentation consists mainly of a checklist of to-do items, and assumes that

the reader is familiar with the system. There is no specific incident handling checklist.

Identification

Because Alice and her team are usually busy 'fighting fires', there is no time for proactive identification tools such as intrusion detection systems, or regular reviews of firewall logs. In this case, the first indication that something is wrong comes from Irene, the executive assistant. Her complaint is that her system keeps 'locking up'. It's fine once it gets re-booted, but after a while it locks up again. She's quite upset, because she needs to get an important document finished. Dave is the individual closest to Irene, and proceeds to her office to identify the problem.

At 9:30am, Dave performs the following steps:

1. Re-boots computer
2. Runs a scandisk
3. Updates virus definitions
4. Scans for viruses
5. Shrugs

Dave has performed a preliminary check against Irene's computer, and everything seems fine. In reality, he's quickly performed the six incident handling steps; however they are not executed properly, as seen here.

Preparation – Already done, he can get one of his co-workers to get the rescue kit if required.
Identification – He has not identified the actual problem, but he has a good guess.
Containment – Problem seems to be isolated to Irene's computer, for the moment.
Eradication – Problem goes away once the computer has re-booted, and has not recurred in his presence.
Recovery – Irene's data seems to be intact, and he's updated the virus definitions.
Lessons Learned – Dave learns that he shouldn't be too far away in case it happens again.

At 10:00am, Dave informs Irene to let him know if it happens again.

At 11:00am, Irene calls Dave, informing him that her computer has locked up yet again. Dave believes that it must be a hardware problem, and manages to get Irene a slightly better computer. He creates an image of her hard drive and copies it to her new computer, using a bit-copying tool.

At 11:30, while Dave is busy with Irene's computer, Carol has gotten a couple of calls from irate users whose computers are exhibiting the same symptoms.

Carol and Dave decide that it probably can't be a hardware issue, given the number of failures occurring simultaneously. Carol and Dave concur that they should still give Irene the updated computer, and utilize her old one to help determine the cause of the failures. Their initial gut reaction is that a virus may be spreading.

At 11:45, Dave installs InCtrl5 from Ziff-Davis Publishing on Irene's old computer, and runs the first phase of a two-phase differential report.

At 11:55, the computer locks up.
At 11:56, Dave reboots the computer and runs InCtrl5 again to complete the differential report. Unfortunately, no significant files or registry entries have changed to suggest that a virus or worm is spreading.

At 12:00, Dave and the rest of the team give up on lunch. The team members get together to attempt to figure out what the actual problem may be. Bob suggests using a sniffer to determine if there's any strange traffic. Meanwhile, Carol volunteers to go over the firewall logs.

At 12:20, Carol has stated that there does not seem to be anything out of the ordinary in the firewall log, but she will keep looking.

At 12:30, Bob has installed ethereal on a computer plugged into a monitoring port on one of the routers on the network backbone. He notices some strange packets going across the network, as indicated by the following ethereal log sample:

Protocol: TCP (0x06)
Header checksum: 0x754f (correct)
Source: 192.168.1.166 (192.168.1.166)
Destination: 192.168.1.102 (192.168.1.102)
Options: (4 bytes)
Security (with too-short option length = 0 bytes)
Transmission Control Protocol, Src Port: 0 (0), Dst Port: 10000 (10000), Seq: 0
Source port: 0 (0)
Destination port: 10000 (10000)
Sequence number: 0 (relative sequence number)
Header length: 0 bytes (bogus, must be at least 20)

According to the log, there are several things wrong with this packet. Firstly, the TCP Options field consists of 4 bytes; however the options field length is set to 0 bytes. Secondly, legitimate network traffic does not usually have a source port of 0. Lastly, the TCP header length is 0, when it must be at least 20 bytes long. Bob has come to the conclusion that the source IP addresses appear to vary, but the source MAC address stays the same throughout.

At 13:00, Bob discusses his findings with the group. Their own systems start to crash in the meantime. The consensus is that any such invalid traffic should be picked up by the personal firewalls. If they are not, then something must be wrong with them. Alice decides to modify the router configurations to deny all packets with a source port of 0 to help stop the lock-ups. Meanwhile, Dave has been researching vulnerabilities against Kerio Personal firewall, and he has found the following references to a vulnerability that appears to match the symptoms they are experiencing:

http://www.kerio.com/security_advisory.html
http://www.eeye.com/html/research/advisories/AD20041109.html
http://secunia.com/advisories/13030/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1109
http://www.securityfocus.com/bid/11639
http://xforce.iss.net/xforce/xfdb/17992

At 13:10, the lockups seem to have been contained to one general area. Alice and her team have now identified the vulnerability being exploited within their network. The attacking machine appears to be internal, according to the MAC address. It also appears to be coming from the general area of Sales.

Containment

In this section, we will observe what Alice and Bob discover the source of the attacks, and what they do to contain the situation.

At 13:15, Alice and Bob walk up to the affected area (appears to be coming from sales). Bob has taken the proactive step of bringing their rescue kit.

At 13:20, they arrive in the sales department. A hush sweeps the area as they enter, and several sales staff move away from one particular cubicle. It's the cubicle of Sam from Sales, who is showing off a new operating system called Knoppix. Apparently, Sam lost a large multi-million dollar sale, and was not happy about it, since he had already put a non-refundable deposit on a new yacht. Bob takes out his notebook and begins to record the date, time, and people in proximity. He also records the fact that Sam from Sales appears to be running an unauthorized operating system.

At 13:21, Alice pulls the network cable from Sam's computer. Bob records this in his notebook. Bob notes the following command on the screen:
nemesis-tcp -x 10 -y 10 -fS -s 10000 -u 0 -v -S 192.168.1.166 -D 192.168.1.102 -O 01010500

Bob recognizes the last digits of the command as TCP options and questions Sam about the command. Sam admits that he was remotely crashing the systems because he wanted the company to suffer as he had suffered

financially.

Eradication

In this section, we will observe how Alice and her team eradicate the root cause of the incident.

At 13:25, Alice calls Frank in Physical Security to come and escort Sam to Henry in HR.

At 13:45, Alice and Bob return to their cubicles. Dave reports to Alice that the issue lies in the Kerio Personal Firewall, and that a patch has been released. Alice issues the order for all PCs to be upgraded with the latest version of Kerio Personal Firewall, pending a business impact analysis.

At 14:00, Alice, Bob, Carol and Dave finally have lunch. Meanwhile, Henry has terminated Sam, and has asked Frank to escort him out of the building. Henry has sent a preliminary email to Eve detailing his knowledge of the situation.

Recovery

In this section, we will observe what recovery procedures Alice and her team implement in order to help the victims of the attack quickly and efficiently resume operations.

In order to help the affected users recover their systems, Alice uses the building's intercom system to instruct all affected users to turn off their computers, count to ten, then turn them back on again. Alice apologizes for the stereotypical solution, but assures the users that this is the simplest and most effective course of action. Alice then calls Grace, the CIO, and briefs her on the situation, promising her a full report by the end of the week.

Lessons Learned

In this section, we will observe what remedial activities Alice and her team have suggested to help mitigate the possibility of future incidents, as well as to help reduce the time and effort required to identify, contain, eradicate and recover from a similar incident.

The next day, Alice holds a team meeting to discuss the previous day's events. Alice is concerned about what she believes to be deficiencies in her team, as well as their resources. Notably, she has observed the following:

- No access to an intrusion detection system (IDS);
- Software management procedures cause a delay in awareness of critical updates;
- Lack of staff's advanced IT security knowledge;
- Lack of workstation security; and
- Grace was not pleased that she was not informed until after the fact.

After meeting with her team, the following recommendations were made:

- Improve software maintenance procedures. The goal of this initiative is to reduce the amount of time between a vendor supplied patch and the internal deployment thereof;
- Password-protect and configure BIOS/CMOS to only boot from the internal hard drive. This will help prevent situations like this from recurring. Buy not allowing a user to easily bypass the operating system, local security measures will still be in place;
- Look into the possibility of an Intrusion Detection System as an early-warning system. This will help the team identify and possibly contain many network-based attacks;
- Invest some of the training budget into advanced security courses. This will ensure that staff know what to do with the data generated from the IDS, firewall logs and other sources; and
- Inform the CIO of any confirmed malicious behavior immediately. This is to ensure that proper non-IT processes are properly executed. The CIO (or her representative) can organize the legal, HR and physical security resources required during an incident.

Extras

List of References

The following materials and tools were consulted in the preparation of this document.

Sourcefire, Inc.; Green, Chris; Roesch, Martin. Snort Users Manual 2.2.0. 10 Aug 2004. <http://www.snort.org/docs/snort_manual.pdf>.

Personal Radio Steering Group Inc. Frequently Asked Questions about The Family Radio Service (FRS) 28 Jun 2003 <http://www.provide.net/~prsg/frs-faq.htm>.

Free Software Foundation, Inc. Alice and Bob. Wikipedia. 4 Jan 2005. <http://en.wikipedia.org/wiki/Alice_and_Bob>.

InCtrl 5

Rubenking, Neil J. “Stay In Control”. PC Magazine. 5 Dec 2000 <http://www.pcmag.com/print_article2/0,2533,a=4583,00.asp>.

InCtrl 5 is a free utility by Ziff-Davis Publishing that takes a before and after snapshot of a system and provides a delta report.

Nemeisis-tcp

Nathan, Jeff. Nemesis.7 Oct. 2004. <http://nemesis.sourceforge.net/docs.html>.

The Nemesis project is a collection of tools which allow the user to create custom-designed TCP, UDP or ICMP packets, and allows the user to send them across the network.

VMWare Workstation 4.0

VMWare, Inc. VMWare Workstation. Jan, 2005. <http://www.vmware.com/products/desktop/ws_features.html>.

VMWare Workstation 4.0 (hereby known as VMWare) gives the user the ability to simultaneously run more than one operating system on an appropriately powered computer. This tool was used to create the lab environment in which the exploit was successfully executed. This was accomplished by installing a legitimate license on each laptop. Once VMWare was properly installed, a virtual machine was created on each system.

The attacking system comprised of a virtual machine with 128mb of RAM and a virtual CD-ROM. The virtual CD-ROM was actually an ISO image of Knoppix STD 0.1b.

The victim system comprised of a virtual machine with 128mb of RAM and a virtual one-gigabyte hard drive with Windows ’98 Second edition installed.

Knoppix STD 0.1b

Liller, Jason. Knoppix STD Main Page. 9 May 2004. <http://www.knoppix-std.org/>.

Knoppix is a type Linux distribution known as a live distribution. A live Linux distribution is a fully functional Linux installation that can be booted from and fully executed from a CD-ROM or DVD-ROM. With no software being actually installed on a computer, it provides an ideal environment for temporary computing, such as a lab environment.

Knoppix STD 0.1b is a live Linux distribution that provides a copy of nemesis-tcp, as well as ethereal.

Ethereal

Ethereal. Ethereal - The world's most popular network protocol analyzer. 15 Dec 2004. <http://www.ethereal.com>.

Ethereal is a network packet sniffer. It can be configured to capture network traffic that meets a certain criteria. In this case, it was configured to capture all data going to or from the VMWare virtual machine running Knoppix STD.

Windows ’98 Second Edition

Micorosoft Corporation. Microsoft Windows ’98. 31 Oct 2002. <http://www.microsoft.com/windows98>.

This particular version of Windows was chosen as the operating system for the victim VMWare machine for two reasons. First, a legitimate license was available. Second, it is a relatively light operating system, meaning that it does not take long to install and does not consume many resources. Lastly, the target application, Kerio Personal Firewall, is compatible with it.

No updates were applied to this installation of Windows.

Kerio Personal Firewall

Kerio Technologies, Inc. Kerio Personal Firewall 18 Nov 2004. <http://www.kerio.com/kpf_home.html>.

Kerio Personal Firewall version 4.1.0 is the victim program in this exercise, and was installed on the virtual Windows ’98 system on the victim machine. Kerio Personal Firewall is designed to protect individual computers from unwanted incoming connections, as well as unauthorized outgoing connections.

Windows 2000 Professional

Microsoft Corporation. Microsoft Windows 2000 Professional. 25 Nov 1999. <http://www.microsoft.com/windows2000/>.

This particular version of Windows is the host operating system of the physical attacking machine. Service pack 4 is installed.

Windows XP

Microsoft Corporation. Microsoft Windows XP. 25 Oct. 2001. <http://www.microsoft.com/windowsxp>.

This particular version of Windows is the host operating system of the physical victim machine. The following service packs and hotfixes are installed.

Service Pack 1
Q819696
Q823182
Q824105
Q824141
Q825119
Q826939
Q828026
Q828035
Q828741
Q833987
Q835732
Q837001
Q839645
Q840315
Q840374
Q841873
Q842773
Q883357
Q814078
Q816093
Q823353
Q867801
Q870669
Q832483

Works cited

SANS Institute & Ed Skoudis, Track 4 - Hacker Techniques, Exploits, and Incident Handling. Volume 4.1. SANS Press, 2004

Rosencrance, Linda. "'Mafiaboy' to plead guilty to hacking major Web sites" ComputerWorld. 07 Nov. 2000. <http://www.computerworld.com/securitytopics/security/story/0,10801,53492,00.html>.

eEye Digital Security. Symantec Multiple Firewall TCP Options Denial of Service. 23 Apr 2004. <http://www.eeye.com/html/research/advisories/AD20040423.html>.

eEye Digital Security. Kerio Personal Firewall Multiple IP Options Denial of Service. 9 Nov 2004. <http://www.eeye.com/html/research/advisories/AD20041109.html>.

Kerio Technologies, Inc. Advisory Number KSEC-2004-11-04-01. 4 Nov 2004. <http://www.kerio.com/security_advisory.html>.

Secunia. Kerio Personal Firewall IP Option Denial of Service Vulnerability. 7 Dec 2004. <http://secunia.com/advisories/13030/>.

The Mitre Corporation. CAN-2004-1109. 30 Nov 2004. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1109>.

SecurityFocus Symantec Corporation. Kerio Personal Firewall IP Options Denial Of Service Vulnerability.12 Nov 2004. <http://www.securityfocus.com/bid/11639>.

Internet Security Systems, Inc. Kerio Personal Firewall (KPF) packet processing denial of service. 8 Nov 2004 <http://xforce.iss.net/xforce/xfdb/17992>.

Cast of Characters

Tech Support
Alice
Bob
Carol
David

Legal
Eve

Physical Security
Frank

CIO
Grace

Human Resources
Henry

Executive Assistant
Irene

President
Peter

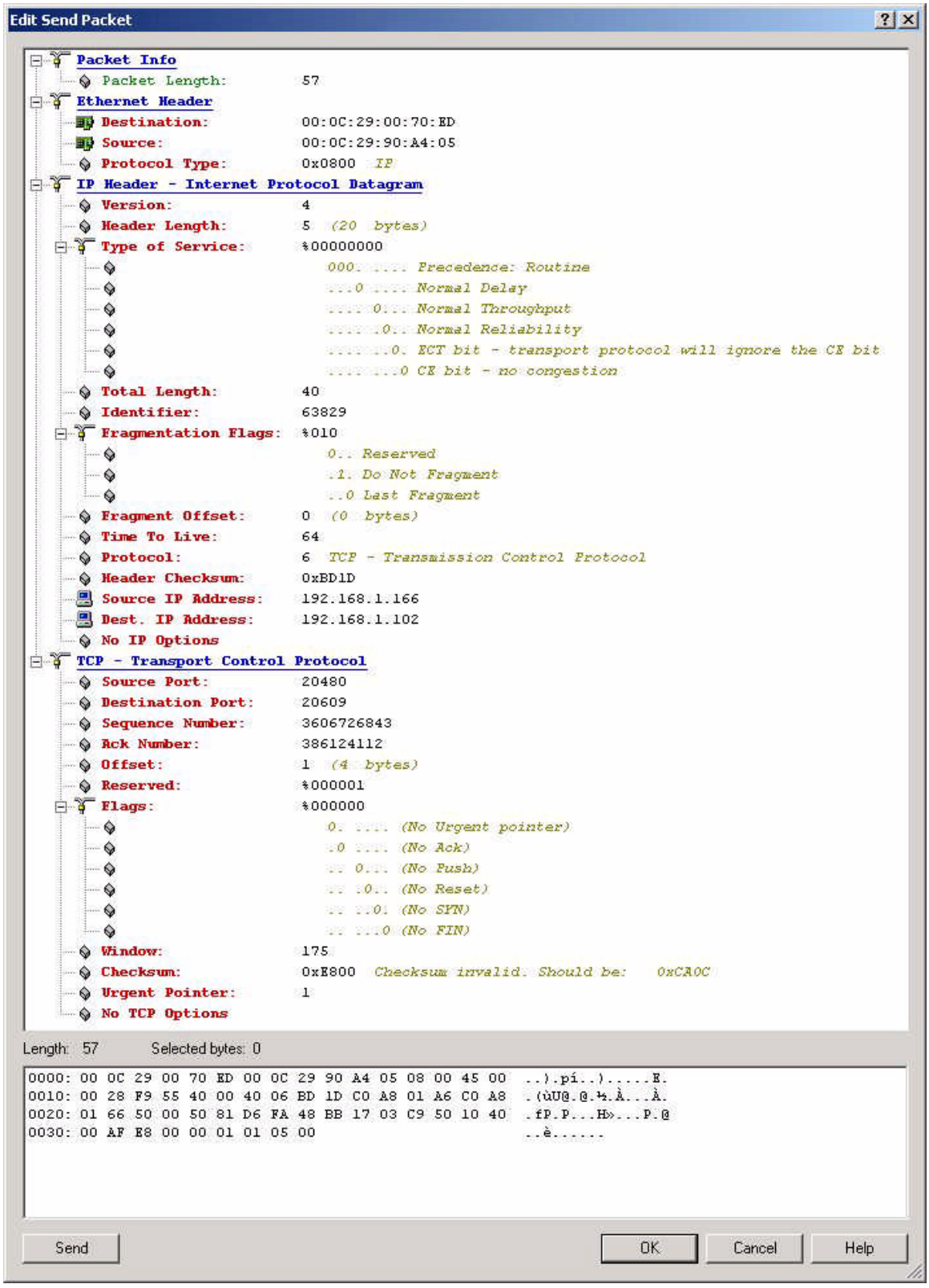
Attacker
Sam from Sales

Appendix A – Ethereal Capture 1

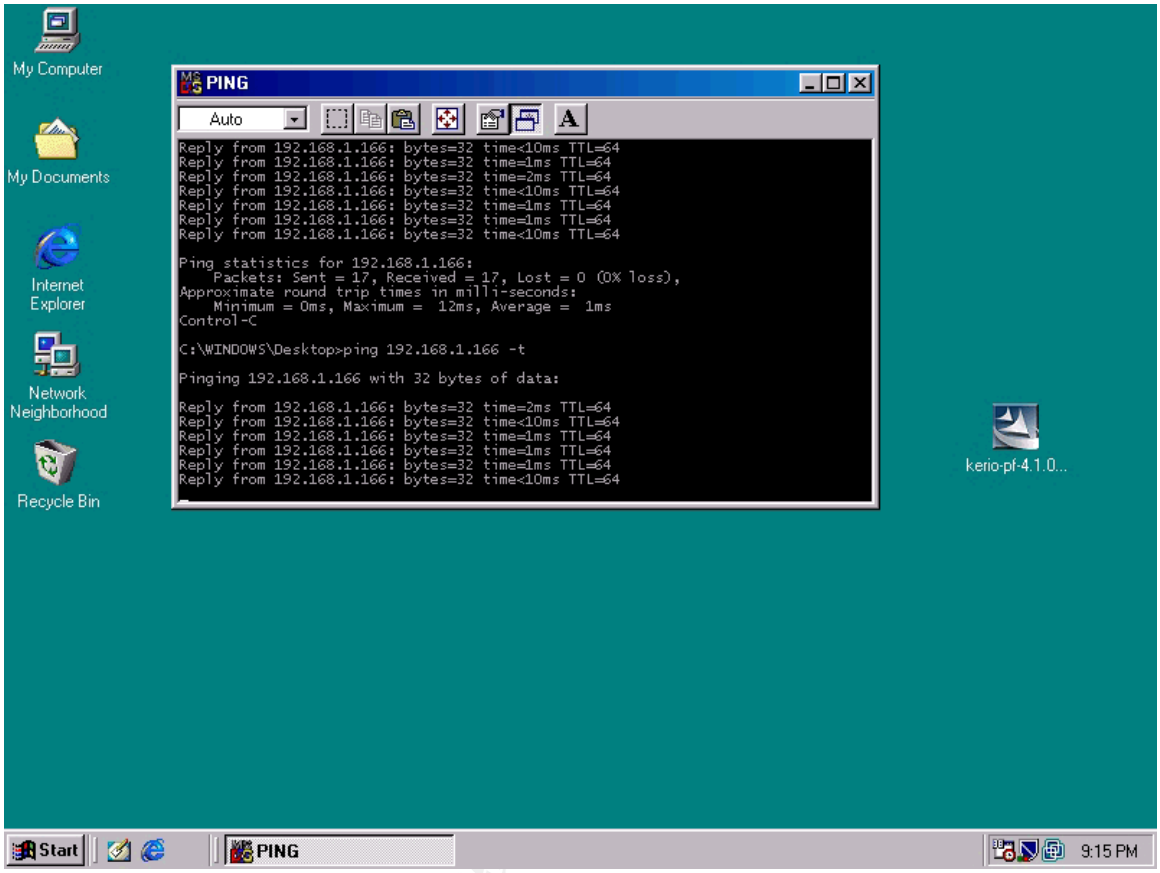
```
No.     Time        Source                Destination           Protocol Info
     79 68.506693   192.168.1.166         192.168.1.102         TCP      0 > 10000 [SYN,
RST, PSH, ACK, URG, CWR] Seq=0 Ack=1 Win=0, bogus TCP header length (0, must be at least
20)

Frame 79 (55 bytes on wire, 55 bytes captured)
    Arrival Time: Nov 30, 2004 15:17:21.510621000
    Time delta from previous packet: 0.552808000 seconds
    Time since reference or first frame: 68.506693000 seconds
    Frame Number: 79
    Packet Length: 55 bytes
    Capture Length: 55 bytes
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
    Destination: 00:0c:29:00:70:ed (192.168.1.102)
    Source: 00:0c:29:90:a4:05 (192.168.1.166)
    Type: IP (0x0800)
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
    Version: 4
    Header length: 24 bytes
    Differentiated Services Field: 0x18 (DSCP 0x06: Unknown DSCP; ECN: 0x00)
        0001 10.. = Differentiated Services Codepoint: Unknown (0x06)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 41
    Identification: 0x0000 (0)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 254
    Protocol: TCP (0x06)
    Header checksum: 0x754f (correct)
    Source: 192.168.1.166 (192.168.1.166)
    Destination: 192.168.1.102 (192.168.1.102)
    Options: (4 bytes)
        Security (with too-short option length = 0 bytes)
Transmission Control Protocol, Src Port: 0 (0), Dst Port: 10000 (10000), Seq: 0
    Source port: 0 (0)
    Destination port: 10000 (10000)
    Sequence number: 0    (relative sequence number)
    Header length: 0 bytes (bogus, must be at least 20)

No.     Time        Source                Destination           Protocol Info
     80 68.509957   192.168.1.166         192.168.1.102         TCP      0 > 10000 [SYN,
RST, PSH, ACK, URG, CWR] Seq=0 Ack=1 Win=0, bogus TCP header length (0, must be at least
20)

Frame 80 (60 bytes on wire, 60 bytes captured)
    Arrival Time: Nov 30, 2004 15:17:21.513885000
    Time delta from previous packet: 0.003264000 seconds
    Time since reference or first frame: 68.509957000 seconds
    Frame Number: 80
    Packet Length: 60 bytes
    Capture Length: 60 bytes
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
    Destination: 00:0c:29:00:70:ed (192.168.1.102)
    Source: 00:0c:29:90:a4:05 (192.168.1.166)
    Type: IP (0x0800)
    Trailer: 0000000000
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
    Version: 4
```

```
    Header length: 24 bytes
    Differentiated Services Field: 0x18 (DSCP 0x06: Unknown DSCP; ECN: 0x00)
        0001 10.. = Differentiated Services Codepoint: Unknown (0x06)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 41
    Identification: 0x0000 (0)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 254
    Protocol: TCP (0x06)
    Header checksum: 0x754f (correct)
    Source: 192.168.1.166 (192.168.1.166)
    Destination: 192.168.1.102 (192.168.1.102)
    Options: (4 bytes)
        Security (with too-short option length = 0 bytes)
Transmission Control Protocol, Src Port: 0 (0), Dst Port: 10000 (10000), Seq: 0
    Source port: 0 (0)
    Destination port: 10000 (10000)
    Sequence number: 0    (relative sequence number)
    Header length: 0 bytes (bogus, must be at least 20)
```

Appendix B – Intended Packet



Appendix C – Victim Post Exploit



Appendix D – Inctrl5 Report

```
Installation Report: (two-phase mode)
Generated by InCtrl5, version 1.0.0.0
Install program:
1/15/2005 10:35 AM

------------------------------------------------------------
Registry
********

Keys ignored: 0
---------------
       * (none)

Keys added: 0
-------------

Keys deleted: 0
---------------

Values changed: 0
-----------------
------------------------------------------------------------
Disk contents
*************

Drives tracked: 1
-----------------
       * c:\

Files added: 0
--------------


Files deleted: 0
----------------


Files changed: 0
----------------


------------------------------------------------------------
INI file
********

Ini files tracked: 2
--------------------
       * c:\windows\system.ini
       * c:\windows\win.ini
------------------------------------------------------------
Text file
*********

Text files tracked: 2
---------------------
       * c:\autoexec.bat
       * c:\config.sys
------------------------------------------------------------
       InCtrl5, Copyright © 2000 by Ziff Davis Media, Inc.
       Written by Neil J. Rubenking
       First published in PC Magazine, December 5, 2000.
```

Appendix E – Ethereal Packet Summary

```
No.     Time        Source                Destination           Protocol Info
      1 0.000000    192.168.1.102         Broadcast             ARP      Who has
192.168.1.166?  Tell 192.168.1.102

Frame 1 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: 00:0c:29:00:70:ed, Dst: ff:ff:ff:ff:ff:ff
Address Resolution Protocol (request)

No.     Time        Source                Destination           Protocol Info
      2 0.001384    192.168.1.166         192.168.1.102         ARP      192.168.1.166 is
at 00:0c:29:90:a4:05

Frame 2 (42 bytes on wire, 42 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Address Resolution Protocol (reply)

No.     Time        Source                Destination           Protocol Info
      3 0.004222    192.168.1.166         192.168.1.102         ARP      192.168.1.166 is
at 00:0c:29:90:a4:05

Frame 3 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Address Resolution Protocol (reply)

No.     Time        Source                Destination           Protocol Info
      4 0.012571    192.168.1.102         192.168.1.166         ICMP     Echo (ping)
request

Frame 4 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:00:70:ed, Dst: 00:0c:29:90:a4:05
Internet Protocol, Src Addr: 192.168.1.102 (192.168.1.102), Dst Addr: 192.168.1.166
(192.168.1.166)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
      5 0.021001    192.168.1.166         192.168.1.102         ICMP     Echo (ping) reply

Frame 5 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
      6 0.021554    192.168.1.166         192.168.1.102         ICMP     Echo (ping) reply

Frame 6 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
      7 1.013031    192.168.1.102         192.168.1.166         ICMP     Echo (ping)
request

Frame 7 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:00:70:ed, Dst: 00:0c:29:90:a4:05
Internet Protocol, Src Addr: 192.168.1.102 (192.168.1.102), Dst Addr: 192.168.1.166
(192.168.1.166)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
      8 1.014084    192.168.1.166         192.168.1.102         ICMP     Echo (ping) reply
```

```
Frame 8 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
      9 1.014502    192.168.1.166         192.168.1.102         ICMP     Echo (ping) reply

Frame 9 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     10 2.021384    192.168.1.102         192.168.1.166         ICMP     Echo (ping)
request

Frame 10 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:00:70:ed, Dst: 00:0c:29:90:a4:05
Internet Protocol, Src Addr: 192.168.1.102 (192.168.1.102), Dst Addr: 192.168.1.166
(192.168.1.166)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     11 2.021481    192.168.1.166         192.168.1.102         ICMP     Echo (ping) reply

Frame 11 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     12 2.021791    192.168.1.166         192.168.1.102         ICMP     Echo (ping) reply

Frame 12 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     13 3.060261    192.168.1.102         192.168.1.166         ICMP     Echo (ping)
request

Frame 13 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:00:70:ed, Dst: 00:0c:29:90:a4:05
Internet Protocol, Src Addr: 192.168.1.102 (192.168.1.102), Dst Addr: 192.168.1.166
(192.168.1.166)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     14 3.060347    192.168.1.166         192.168.1.102         ICMP     Echo (ping) reply

Frame 14 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     15 3.060668    192.168.1.166         192.168.1.102         ICMP     Echo (ping) reply

Frame 15 (74 bytes on wire, 74 bytes captured)
```

```
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     16 4.032899    192.168.1.102         192.168.1.166         ICMP     Echo (ping)
request

Frame 16 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:00:70:ed, Dst: 00:0c:29:90:a4:05
Internet Protocol, Src Addr: 192.168.1.102 (192.168.1.102), Dst Addr: 192.168.1.166
(192.168.1.166)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     17 4.033019    192.168.1.166         192.168.1.102         ICMP     Echo (ping) reply

Frame 17 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     18 4.033356    192.168.1.166         192.168.1.102         ICMP     Echo (ping) reply

Frame 18 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     19 4.995991    192.168.1.102         192.168.1.166         ICMP     Echo (ping)
request

Frame 19 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:00:70:ed, Dst: 00:0c:29:90:a4:05
Internet Protocol, Src Addr: 192.168.1.102 (192.168.1.102), Dst Addr: 192.168.1.166
(192.168.1.166)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     20 4.996077    192.168.1.166         192.168.1.102         ICMP     Echo (ping) reply

Frame 20 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     21 4.996375    192.168.1.166         192.168.1.102         ICMP     Echo (ping) reply

Frame 21 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     22 5.020228    192.168.1.166         192.168.1.102         ARP      Who has
192.168.1.102?  Tell 192.168.1.166

Frame 22 (42 bytes on wire, 42 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
```

```
Address Resolution Protocol (request)

No.     Time        Source                Destination           Protocol Info
     23 5.020656    192.168.1.166         192.168.1.102         ARP      Who has
192.168.1.102?  Tell 192.168.1.166

Frame 23 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Address Resolution Protocol (request)

No.     Time        Source                Destination           Protocol Info
     24 5.021021    192.168.1.102         192.168.1.166         ARP      192.168.1.102 is
at 00:0c:29:00:70:ed

Frame 24 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: 00:0c:29:00:70:ed, Dst: 00:0c:29:90:a4:05
Address Resolution Protocol (reply)

No.     Time        Source                Destination           Protocol Info
     25 6.034782    192.168.1.102         192.168.1.166         ICMP     Echo (ping)
request

Frame 25 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:00:70:ed, Dst: 00:0c:29:90:a4:05
Internet Protocol, Src Addr: 192.168.1.102 (192.168.1.102), Dst Addr: 192.168.1.166
(192.168.1.166)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     26 6.034967    192.168.1.166         192.168.1.102         ICMP     Echo (ping) reply

Frame 26 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     27 6.035305    192.168.1.166         192.168.1.102         ICMP     Echo (ping) reply

Frame 27 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     28 7.024425    192.168.1.102         192.168.1.166         ICMP     Echo (ping)
request

Frame 28 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:00:70:ed, Dst: 00:0c:29:90:a4:05
Internet Protocol, Src Addr: 192.168.1.102 (192.168.1.102), Dst Addr: 192.168.1.166
(192.168.1.166)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     29 7.024553    192.168.1.166         192.168.1.102         ICMP     Echo (ping) reply

Frame 29 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     30 7.024857    192.168.1.166         192.168.1.102         ICMP     Echo (ping) reply
```

```
Frame 30 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     31 8.090226    192.168.1.102         192.168.1.166         ICMP     Echo (ping)
request

Frame 31 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:00:70:ed, Dst: 00:0c:29:90:a4:05
Internet Protocol, Src Addr: 192.168.1.102 (192.168.1.102), Dst Addr: 192.168.1.166
(192.168.1.166)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     32 8.090445    192.168.1.166         192.168.1.102         ICMP     Echo (ping) reply

Frame 32 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     33 8.090787    192.168.1.166         192.168.1.102         ICMP     Echo (ping) reply

Frame 33 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     34 9.066595    192.168.1.102         192.168.1.166         ICMP     Echo (ping)
request

Frame 34 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:00:70:ed, Dst: 00:0c:29:90:a4:05
Internet Protocol, Src Addr: 192.168.1.102 (192.168.1.102), Dst Addr: 192.168.1.166
(192.168.1.166)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     35 9.066766    192.168.1.166         192.168.1.102         ICMP     Echo (ping) reply

Frame 35 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     36 9.068103    192.168.1.166         192.168.1.102         ICMP     Echo (ping) reply

Frame 36 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     37 10.078279   192.168.1.102         192.168.1.166         ICMP     Echo (ping)
request
```

```
Frame 37 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:00:70:ed, Dst: 00:0c:29:90:a4:05
Internet Protocol, Src Addr: 192.168.1.102 (192.168.1.102), Dst Addr: 192.168.1.166
(192.168.1.166)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     38 10.078358   192.168.1.166         192.168.1.102         ICMP     Echo (ping) reply

Frame 38 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     39 10.078657   192.168.1.166         192.168.1.102         ICMP     Echo (ping) reply

Frame 39 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     40 11.117219   192.168.1.102         192.168.1.166         ICMP     Echo (ping)
request

Frame 40 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:00:70:ed, Dst: 00:0c:29:90:a4:05
Internet Protocol, Src Addr: 192.168.1.102 (192.168.1.102), Dst Addr: 192.168.1.166
(192.168.1.166)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     41 11.117365   192.168.1.166         192.168.1.102         ICMP     Echo (ping) reply

Frame 41 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     42 11.117973   192.168.1.166         192.168.1.102         ICMP     Echo (ping) reply

Frame 42 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     43 12.123845   192.168.1.102         192.168.1.166         ICMP     Echo (ping)
request

Frame 43 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:00:70:ed, Dst: 00:0c:29:90:a4:05
Internet Protocol, Src Addr: 192.168.1.102 (192.168.1.102), Dst Addr: 192.168.1.166
(192.168.1.166)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     44 12.124036   192.168.1.166         192.168.1.102         ICMP     Echo (ping) reply

Frame 44 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
```

```
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     45 12.124353   192.168.1.166         192.168.1.102         ICMP     Echo (ping) reply

Frame 45 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     46 13.108799   192.168.1.102         192.168.1.166         ICMP     Echo (ping)
request

Frame 46 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:00:70:ed, Dst: 00:0c:29:90:a4:05
Internet Protocol, Src Addr: 192.168.1.102 (192.168.1.102), Dst Addr: 192.168.1.166
(192.168.1.166)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     47 13.108876   192.168.1.166         192.168.1.102         ICMP     Echo (ping) reply

Frame 47 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     48 13.109183   192.168.1.166         192.168.1.102         ICMP     Echo (ping) reply

Frame 48 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     49 14.122927   192.168.1.102         192.168.1.166         ICMP     Echo (ping)
request

Frame 49 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:00:70:ed, Dst: 00:0c:29:90:a4:05
Internet Protocol, Src Addr: 192.168.1.102 (192.168.1.102), Dst Addr: 192.168.1.166
(192.168.1.166)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     50 14.123007   192.168.1.166         192.168.1.102         ICMP     Echo (ping) reply

Frame 50 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     51 14.123283   192.168.1.166         192.168.1.102         ICMP     Echo (ping) reply

Frame 51 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
```

```
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     52 15.159624   192.168.1.102         192.168.1.166         ICMP     Echo (ping)
request

Frame 52 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:00:70:ed, Dst: 00:0c:29:90:a4:05
Internet Protocol, Src Addr: 192.168.1.102 (192.168.1.102), Dst Addr: 192.168.1.166
(192.168.1.166)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     53 15.159706   192.168.1.166         192.168.1.102         ICMP     Echo (ping) reply

Frame 53 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     54 15.160036   192.168.1.166         192.168.1.102         ICMP     Echo (ping) reply

Frame 54 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     55 16.132806   192.168.1.102         192.168.1.166         ICMP     Echo (ping)
request

Frame 55 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:00:70:ed, Dst: 00:0c:29:90:a4:05
Internet Protocol, Src Addr: 192.168.1.102 (192.168.1.102), Dst Addr: 192.168.1.166
(192.168.1.166)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     56 16.132902   192.168.1.166         192.168.1.102         ICMP     Echo (ping) reply

Frame 56 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     57 16.133853   192.168.1.166         192.168.1.102         ICMP     Echo (ping) reply

Frame 57 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     58 62.903604   192.168.1.102         192.168.1.166         ICMP     Echo (ping)
request

Frame 58 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:00:70:ed, Dst: 00:0c:29:90:a4:05
Internet Protocol, Src Addr: 192.168.1.102 (192.168.1.102), Dst Addr: 192.168.1.166
(192.168.1.166)
Internet Control Message Protocol
```

```
No.     Time        Source                Destination           Protocol Info
     59 62.903723   192.168.1.166         192.168.1.102         ICMP     Echo (ping) reply

Frame 59 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     60 62.904056   192.168.1.166         192.168.1.102         ICMP     Echo (ping) reply

Frame 60 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     61 63.897396   192.168.1.102         192.168.1.166         ICMP     Echo (ping)
request

Frame 61 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:00:70:ed, Dst: 00:0c:29:90:a4:05
Internet Protocol, Src Addr: 192.168.1.102 (192.168.1.102), Dst Addr: 192.168.1.166
(192.168.1.166)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     62 63.897479   192.168.1.166         192.168.1.102         ICMP     Echo (ping) reply

Frame 62 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     63 63.897778   192.168.1.166         192.168.1.102         ICMP     Echo (ping) reply

Frame 63 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     64 64.920650   192.168.1.102         192.168.1.166         ICMP     Echo (ping)
request

Frame 64 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:00:70:ed, Dst: 00:0c:29:90:a4:05
Internet Protocol, Src Addr: 192.168.1.102 (192.168.1.102), Dst Addr: 192.168.1.166
(192.168.1.166)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     65 64.920753   192.168.1.166         192.168.1.102         ICMP     Echo (ping) reply

Frame 65 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
```

```
     66 64.921106   192.168.1.166         192.168.1.102         ICMP     Echo (ping) reply

Frame 66 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     67 65.956456   192.168.1.102         192.168.1.166         ICMP     Echo (ping)
request

Frame 67 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:00:70:ed, Dst: 00:0c:29:90:a4:05
Internet Protocol, Src Addr: 192.168.1.102 (192.168.1.102), Dst Addr: 192.168.1.166
(192.168.1.166)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     68 65.956594   192.168.1.166         192.168.1.102         ICMP     Echo (ping) reply

Frame 68 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     69 65.956898   192.168.1.166         192.168.1.102         ICMP     Echo (ping) reply

Frame 69 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     70 66.935903   192.168.1.102         192.168.1.166         ICMP     Echo (ping)
request

Frame 70 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:00:70:ed, Dst: 00:0c:29:90:a4:05
Internet Protocol, Src Addr: 192.168.1.102 (192.168.1.102), Dst Addr: 192.168.1.166
(192.168.1.166)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     71 66.936035   192.168.1.166         192.168.1.102         ICMP     Echo (ping) reply

Frame 71 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     72 66.936357   192.168.1.166         192.168.1.102         ICMP     Echo (ping) reply

Frame 72 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     73 67.908043   192.168.1.166         192.168.1.102         ARP      Who has
192.168.1.102?  Tell 192.168.1.166
```

```
Frame 73 (42 bytes on wire, 42 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Address Resolution Protocol (request)

No.     Time        Source                Destination           Protocol Info
     74 67.908452   192.168.1.166         192.168.1.102         ARP      Who has
192.168.1.102?  Tell 192.168.1.166

Frame 74 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Address Resolution Protocol (request)

No.     Time        Source                Destination           Protocol Info
     75 67.908776   192.168.1.102         192.168.1.166         ARP      192.168.1.102 is
at 00:0c:29:00:70:ed

Frame 75 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: 00:0c:29:00:70:ed, Dst: 00:0c:29:90:a4:05
Address Resolution Protocol (reply)

No.     Time        Source                Destination           Protocol Info
     76 67.953136   192.168.1.102         192.168.1.166         ICMP     Echo (ping)
request

Frame 76 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:00:70:ed, Dst: 00:0c:29:90:a4:05
Internet Protocol, Src Addr: 192.168.1.102 (192.168.1.102), Dst Addr: 192.168.1.166
(192.168.1.166)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     77 67.953216   192.168.1.166         192.168.1.102         ICMP     Echo (ping) reply

Frame 77 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     78 67.953885   192.168.1.166         192.168.1.102         ICMP     Echo (ping) reply

Frame 78 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
Internet Control Message Protocol

No.     Time        Source                Destination           Protocol Info
     79 68.506693   192.168.1.166         192.168.1.102         TCP      0 > 10000 [SYN,
RST, PSH, ACK, URG, CWR] Seq=0 Ack=1 Win=0, bogus TCP header length (0, must be at least
20)

Frame 79 (55 bytes on wire, 55 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
Transmission Control Protocol, Src Port: 0 (0), Dst Port: 10000 (10000), Seq: 0

No.     Time        Source                Destination           Protocol Info
     80 68.509957   192.168.1.166         192.168.1.102         TCP      0 > 10000 [SYN,
RST, PSH, ACK, URG, CWR] Seq=0 Ack=1 Win=0, bogus TCP header length (0, must be at least
20)

Frame 80 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: 00:0c:29:90:a4:05, Dst: 00:0c:29:00:70:ed
```

```
Internet Protocol, Src Addr: 192.168.1.166 (192.168.1.166), Dst Addr: 192.168.1.102
(192.168.1.102)
Transmission Control Protocol, Src Port: 0 (0), Dst Port: 10000 (10000), Seq: 0
```