Global Information Assurance Certification Paper

Raja Azrina Raja Othman
GSEC version 1.3

Understanding the Various Types of Denial of Service Attack

1.0 Summary

This paper describes the different types of Denial of Service (DoS) attacks and Distributed Denial of Service (DDoS) attack. It will not be possible for me to go into the details for recovery from each type of attacks within this paper, since it will make it very lengthy and redundant to many other resources already available. Instead, referrals are made to other sites for more information in dealing with each specific type of attacks. However, the purpose of describing the different types of attacks is to illustrate the different approaches and variations of DoS attacks in order to provide an overall recovery steps and best practice in networking to prevent high impact disaster against such attacks by ways of technology and legal framework. This is because I believe, it is not possible to prevent DoS attack in isolated approach, for example protecting merely at the perimeter devices, such as applying CISCO ACLs, while forgoing the configurations and patches on the application hosts. This paper is also useful as reference when analyzing possible symptoms of DoS attacks. However, there is no guarantee that one will be immune to DoS attack once these preventive measures are abided to, since as long as there are human writing codes, there will be programming loopholes!

This paper concludes that Denial of Service attack cannot be merely resolved with single product solution, but rather a holistic approach is required to look into all elements of the computing, networking and system, including the design, implementation and maintenance, to ensure all measures are applied to reduce the single point of failure and to ensure resistance to attacks.

2.0 About DoS Attack

As early as November 3, 1988, Robert Morris Jr. released a worm which later penetrated hundreds of computers across United States of America, paralyzing systems in research institutions from performing the normal operations.

> On February 6th, 2000, Yahoo portal was shut down for 3 hours. Then retailer Buy.com Inc. (BUYX) was hit the next day, hours after going public. By that evening, eBay (EBAY), Amazon.com (AMZN), and CNN (TWX) had gone dark. And in the morning, the mayhem continued with online broker E*Trade (EGRP) and others having traffic to their sites virtually choked off.
>
> (Business Week Online, 12 February 2000)

The first detection of DoS attack in 1988 was instrumental to the formation of CERTCC in Carnegie Mellon US. More than a decade later, a more alarming attack occurred

identified to be due to Denial of Service Attack. For e-commerce sites, such interruptions of service meant great financial loss. The hosting service provider and Internet Service Providers (ISP) were challenged for security beef-up.

Previously, DoS attacks targeting specific hosts do not represent risk of penetrations or data tampering, thus are often not rated high priority. However, DoS attacks can generate huge audit logs or use up computing resources, which can become a nuisance or loss to businesses. In current situation where high availability is associated to information security, DoS and DDoS becomes a threat which needs to be mitigated effectively.

2.1 Differences in DoS and DDoS Attack

DoS attacks are a class of attacks initiated by individual or group of individuals exploiting aspects of the Internet Protocol to deny other users from legitimate access to systems and information. In the past DoS attacks has been associated to SMURF attacks, which were targeted at routers. If an attacker can force a router to stop forwarding packets, then all hosts behind the router are effectively disconnected. Recently though more forms of attacks are crafted to attack web servers, mail servers and other services. The book "Incident Response : Investigating Computer Crimes" [9] provides a good description of DoS attacks which are categorized in the following manner:

> **Destructive** – Attacks which destroy the ability of the device to function, such as deleting or changing configuration information or power interruptions.
>
> **Resource consumption** – Attacks which degrade the ability of the device to function, such as opening many simultaneous connections to the single device.
>
> **Bandwidth consumption** – Attacks which attempt to overwhelm the bandwidth capacity of the network device.

Network with small bandwidth may suffer from high bandwidth consumption instantaneously if it becomes target. Response rate will depend on cooperation from service providers, for example in applying filters at upstream routers.

DDoS on the other hand is a combination of DoS attacks staged or carried out in concert from various hosts to penalize the target host from further serving its function. DDoS is term coined when the source of the attack is not coming from a single source, but multiple source. DDoS cannot be eliminated with merely filtering the source IPs since it is often launched from multiple points installed with agents. Some known DDoS tools are Mstream, Trinoo, TFN2K (Tribe Flood Network), Stacheldraht and Shaft. DDoS attack is an example of a bandwidth attack. Diagram 1 depicts how DDoS works:

Distributed Denial of Service Attack

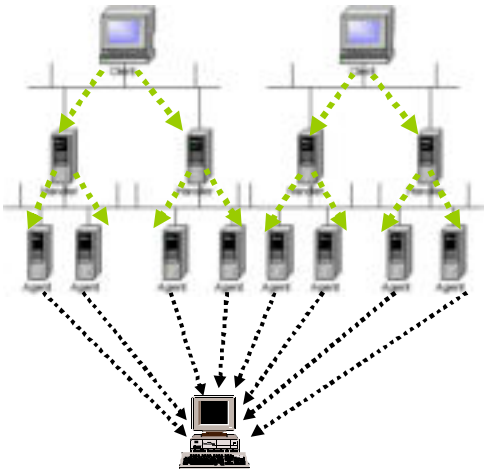

Diagram 1

2.2 Connection oriented attacks

This attack completes a three-way handshake in which it establishes connection with the requesting host. In this event, often the source is a legitimate IP. By spawning multiple established sessions to the same host, the CPU utilization rate will increase and may cause the host to fail to serve to new requests. Often, this happens when the host does not have a limit and capability to drop the overwhelming request. Fortunately, for such attack, it is often possible to identify the source IP and apply filtering to prevent the IP from further connecting to the host. However, unfortunately, filtering can only be done when the attack is already in progress. It cannot be prevented with pre-set safeguard measures. Diagram 2 is a sequential diagram describing a typical connection :

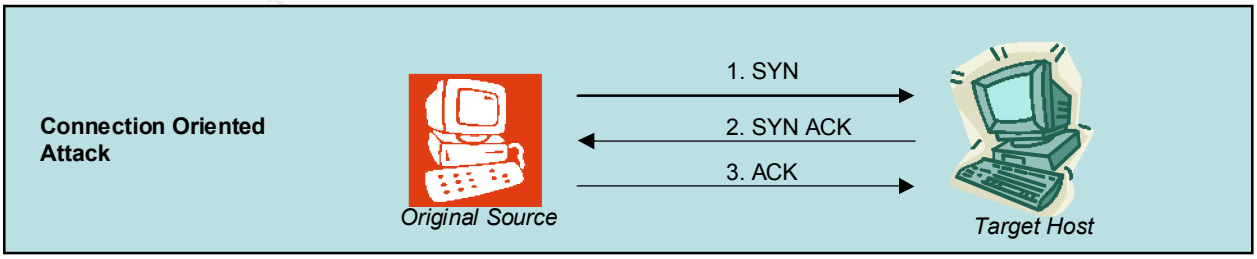

Diagram 2

2.3 Connectionless TCP attacks.

The connectionless TCP attack do not complete the three-way handshake initiated by the originator, as illustrated in diagram 3. Thus, often the packet is crafted with non-existent (spoofed) source IP. For a connectionless TCP attack, it is more difficult to filter since the source address is not necessarily the original source IP of the packet. When the host fail to find the source IP, it will wait until it times out. The most effective way of stopping such attacks is by applying rate limit. Rate limit is a method of setting threshold to an acceptable number of packets to be processed by the computer. Network Ingress filtering can also prevent their downstream networks from injecting packets with faked or "spoofed" addressed into the Internet. Although it may not stop the attack, it will make identifying the source host easier and terminate it immediately. RFC 2267 [1] provides more information on Ingress Filtering.

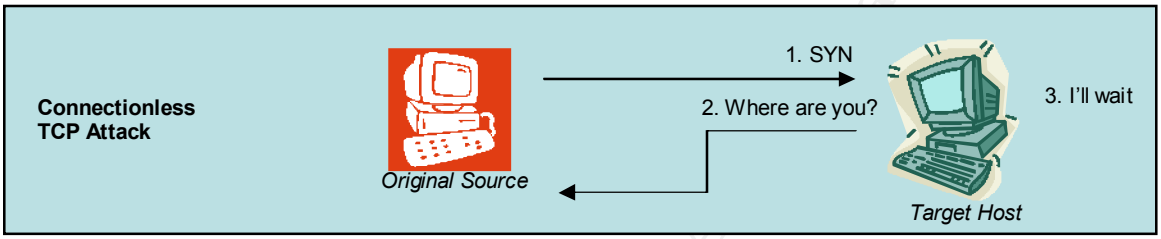

Diagram 3

3.0 Detection of DoS Attack

Initially, network administrators will first detect symptoms such as uniform degradation of network or device performance. Uniformly degraded performance could be due to resource consumption of bandwidth attack. Point-to-point attack can also occur to specific devices in the network, causing the CPU utilization to run up and failure of the host to serve other users. Investigating Denial of Service Attacks often require the use of sniffers or logging at the router to determine the extent of the attack, whether it is propagating to other hosts in the network, and to identify the pattern or signature of the attack. Analyzing router and host logs may or may not show the real nature of the attack or may cause false reporting. In some experience with organizations installing commercial network Intruder Detection System, mis-configured attack signature, provided wrong alert indicators. A sniffer at this point helps to identify the real threat.

Based on experience, mis-configuration of devices such as hubs and routers can also cause DoS effect. Thus, it is advisable not to eliminate any possibility until the packets are thoroughly examined.

DoS attacks are often double edged sword, the source host (or spoofed host) will be affected just as much as the target host. Due to this situation, an attacker will have to have means to monitor if the attack is successful, by planting a sniffer in the spoofed network or the target network as shown in *diagram 4*. This situation is proven in incidents involving smurf attacks and syn flood attacks since these connection requests create a massive spur of return packets to the source IP, and often causing a similar impact to the source and the destination IP. Using spoofed IP, the spoofed machine will

be swamp with return packets instead. Spoofed source IP makes the attack very difficult to be traced to the originator machine. However, it is also very difficult to spoof IPs, especially when the attacker is within a network with Ingress filters at the routers.

In my experience in handling Incident Response, there were a few incidents involving both parties experiencing DoS attack reporting to us, claiming the attack was initiated vice-versa, due to the fact that their respective firewalls were logging only one direction of the traffic rather than bi-directional. Further analysis and correlation of the logs revealed that the attack was coming from one of them.

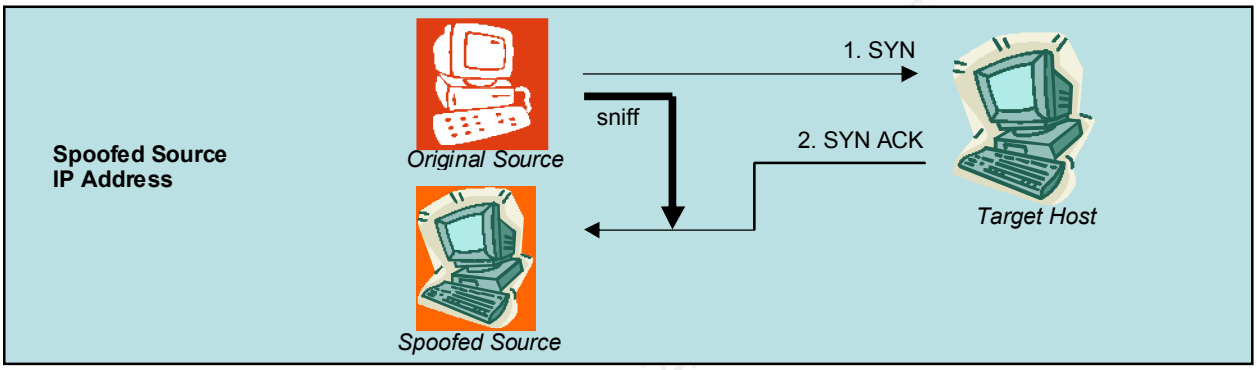

Diagram 4

The NANOG ISPSec Meeting/DDoS BoF [6] described the initial intrusions in which hosts are compromised using known exploits and later rootkit to take full control of the host, before the agents are planted on the hosts. Networks with close proximity to high-volume backbones, large population of vulnerable hosts and weak system administration make good agent sites.

Coordination and cooperation between network providers are crucial for diagnosis, tracing, and control of distributed attacks.

3.1 ICMP Attacks

"SMURF" attack [8] is one example of DoS attack, which exploits the router incapability to limit or prevent the router from performing IP broadcast and becoming an amplifier. A perpetrator sends a large amount of ICMP echo (ping) traffic at IP broadcast addresses, all of it having a spoofed source address of a victim. The traffic (echo request) will be broadcasted to the network, and most hosts within the network will reply – multiplying the responses to the spoofed source address (the victim). **"Fraggle",** which uses UDP echo packets in the same fashion as the ICMP echo packets, is a re-write of "SMURF".

A factory configuration in previous versions of Cisco routers allows the router to become the intermediary. Only Cisco IOS version 12.0 and later has "no ip directed-broadcast" as default which prevents this exploit.

RFC 2644, a Best Current Practice RFC by Daniel Senie, updates RFC 1812 to state that router software must default to denying the forwarding and receipt of directed broadcasts.

3.2 Internet worms

Code Red Worm and NIMDA worm which hit Internet at large end of July 2001 onwards are another breed of DoS attacks on Internet infrastructure after the Morris Worm. Code Red Worm has a fast rate of propagation and infection via network scanning to detect and automatically exploit IIS ISAPI extensions vulnerabilities. The exploit although known, and was widely exploited manually by various crackers before, was then made simple through the automated scripts in Code Red Worm codes. The effect of such high rate of scanning and propagation caused a DoS effect to many network devices and consumed high bandwidth. Due to the complexity of the attack in which the source came from various IP addresses, it was not possible to prevent the packets by analyzing the header itself. Some form of content filtering was necessary to stop the traffic from further penetrating in or out of networks. Refer to Code Red Worm [4] and NIMDA [5] advisories on how to stop such malicious traffic.

3.3 TCP and UDP Attacks

One of the most common attacks which will appear on many Intruder Detection System alerts is TCP SYN flood alerts. TCP SYN flood attacks are instigated by crafting packets from spoofed or non-existent source address and generating a high number of half-open connections. Because each connection opened must be processed to its completion (to complete the handshake or eventual timeout), the system is pinned down to perform these tasks. This problem is inherent in any network or operating system running full fledged TCP/IP design and something that is not easily rectified. Methods in handling this type of attack is available at reference [10].

Another common form of attack is UDP flooding which consist of a large number of spoofed UDP packets aimed at diagnostic ports on network devices. This attack can cause increase in CPU time responding to these packets on network devices. Methods in handling this type of attack is available at reference [11].

3.4 Mass Email Worms

Email worm is one example of an application DoS attack. Microsoft Outlook Express with its features by default installation has scripting enabled to handle VBScripts and JScripts, allowing attachments to be launched on the fly, as the message is being opened. This “feature” although had “honest” intention of providing ease of use for the users, had indirectly created a tool for exploitation. Many recent worms which spread

on a fast rate, were Melissa, Love worm, MTX Worm, Happy99, and SIRCAM which exploited this feature.

For reference on how to disable this feature please refer to
http://www.mycert.org.my/faq-safe_email_practices.htm#Q6

3.5 Buffer Overflow

DoS is not usually an attempt to intrude the host, instead, it may be a sequel to a successful intrusion! History tells us that some of the most well known DoS incidents were due to buffer overflow exploit, which enable unauthorized access to the system.

The Jargon file defines buffer overflow as:

> What happens when you try to stuff more data into a buffer (holding area) than it can handle. It could be caused by program mismatch in processing rates of the producing and consuming processes or because the buffer is simply too small to hold the data that must accumulate before a piece of it can be processed.

Failure to perform checks on the data fed can create this hole. However, it is rather unrealistic to perform checks for each and every character written to the buffer. The buffer overflow technique is often used by crackers to gain rootshell. It takes a high level of skill to implement a new buffer overflow attack. However, known tools to perform these known exploits are already wide spread on the Internet. Some of the previous worm incidents demonstrate deliberate acts to exploit these holes.

For example, not many knew that the Morris worm fast spread was due to exploit of buffer overflow in the gets() function in fingerd service. Eugene Spafford explains this in his paper “The Internet Worm: An Analysis”.

Code Red Worm and Code Red Worm II are also examples in which buffer overflow attacks were launched on exploiting IIS ISAPI extensions in order to gain access to plant the malicious codes.

4.0 Recovering

Unfortunately DoS attack requires filtering response which is very reactive in nature. The methods of filtering depends on the type and the source of attacks. As described above, some of the attacks unique identifier are in the source IP, while mass worm attacks can be detected based on the payload.

Traditional DoS attack technique most often does not involve host compromise, thus they are the most easiest to respond to. If the source IP Address or the pattern of the attack is identified it is possible to filter the traffic at the router. However, recent

development of DoS attacks, such as Code Red Worm and NIMDA attacks, have changed that perspective, since the attack also involve compromise of certain platforms of web hosts and generate various pattern of scanning and exploits.

In normal circumstances, after an attack is filtered, there is a list of other activities which require to be conducted to recover the network services. This is because filtering are only temporary solutions. Recovery and prevention steps are crucial to maintain the service.

Recovery and rectification of the host often involves the following measures:

- Implement Access Control List (ACL) to limit malicious traffic – this can be done only when the full pattern of the attack is identified, with payload if any, by applying specific "ban" of the packet based on the pattern of the header or the payload. More information about DoS attacks and countermeasures using ACLs are detailed in http://www.cisco.com/warp/public/707/22.html .

- Content Filtering Device or Proxy Servers can also be used to filter out DoS attacks which can be identified based on its unique payload.

- Reformat and reinstall the operating system and relevant applications on the computer to ensure complete elimination of malicious codes.

- Removal of unnecessary listening services, since these services cause the device to respond to unnecessary requests which can trigger an attack.

- Upgrade software to the latest version, since often times, DoS effect are due to software vulnerabilities (i.e. buffer overflow) which causes malfunction or misbehavior of the service.

- Fine tune respective Internet applications to prevent the system from consuming too many simultaneous sessions. AS/400 for example has a DoS limit of number of timeouts request and HTTP servers has limit to the number of simultaneous session it can handle.

- Restrict access to listening services on the host using host ACLs, this can be done using tools such as TCPwrappers on the respective hosts.

In most situation, to respond to DoS attacks which cause high resource and bandwidth utilization, require cooperation from the Internet Service Providers in providing the filtering mechanism at the upstream router, where the network bandwidth can be consumed by the ISP, but not by the last mile, small bandwidth and multiple targets at the customer end.

5.0 Prevention

What makes DoS attacks so difficult to prevent is because it not only affect open services on devices, but also closed ports, as long as the service request reaches the device, the bandwidth utilization will be effected. Due to the nature of the attack which can be crafted in many forms, targeted at many services and devices, it is most difficult to prevent devices from being susceptible to such attack.

Even a legitimate request packet can turn into malicious traffic if it creates recursive effect such as opening multiple simultaneous connections. That is another reason why DoS is very difficult to prevent. However, like other network threats, there is no silver bullet solution to the problem. Prevention of DoS requires combination of the following actions:

- **High redundancy and high availability network design**
  In order to prevent a network from falling trap into a DoS attack it is crucial to design the network as such that there is not a single point of failure. However, such high availability will incur additional cost, especially in maintaining dual connection to the Internet. It is also desired that ISPs provide load balancing on the upstream router to load share the redundant link.

- **Perimeter Defense**
  The router and firewalls should pass through only legitimate packets to reach its internal network. An example is, limiting the internal web server from initiating port 80 connection destined to external hosts. Such filtering can prevent propagation of Code Red Worm attacks which causes a stream of scanning to various IP Addresses on port 80.

  Preventing IP Address Spoofing using egress [2] and ingress filtering [1] are examples of filtering at the gateway or router level to prevent packet spoofing from internal hosts, and to internal hosts respectively. However, it will not prevent attacks from legitimate IP Addresses within the network. Every interface on a router should prohibit packets that logically could not come from that network interface.

- **Defense In-depth**
  Implementation of Intruder Detection System (IDS) will allow detection of "slave", "master" or "agent" machines communications. Action can be taken to remove those infected host from the network. However, IDS may be able to detect known attacks but not new variations of these attacks.

- **Host Hardening**
  Hardening the respective device on the network will prevent the host from DoS attack. Host hardening involves upgrading the operating system, applying relevant patches for the operating system and required applications, closing irrelevant services, customizing and tightening configurations, and applying Access Control Lists on the required services. Changing default passwords and

applying good password policies. Known buffer overflow attacks can be prevented by keeping the host up to date with patches or version upgrades.

- **Malware Detection and Prevention**
  The hosts and the network must have antivirus installed and scanning any introduction of new data, while file integrity checkers is used to detect any unauthorized attempt to change the original data. This will prevent infection of malicious codes and attempts to rootkit the host. Compromised host could make the host a potent host to become handlers for malicious users who wish to conduct DoS attack.

- **Periodic Scanning**
  Periodic network vulnerability scanning will detect vulnerable host and detect new infection. It is necessary to conduct periodic vulnerability since in any network, there are always new production host going on-line, or new devices being connected to the network.

- **Policy Enforcement**
  Last but not least is having a strong policy enforcement on acceptable use and management of computing resources. It is also a daunting task to ensure that all in house and outsource code development apply good programming practices to avoid loopholes such as buffer overflow and DoS. Rigorous testing of pre-production system is inevitable to avoid unwanted loopholes.

Despite applying all these measures there is still no guarantee that one will be immune to any DoS attacks but it will mitigate the effect of DoS attacks. However, applying the above recommendations would also mitigate other forms of malicious activities such as session hi-jacking, buffer overflow attacks and reconnaissance. It will not only prevent your network from becoming targets of DoS attacks, but also prevent it from becoming the launching pad for such attacks.

6.0 Legal infrastructure

The legal framework in handling DoS and DDoS attacks differ based on the country's legal establishment. However, one common issue is that the legal definition of threats often miss out on DoS attack. The legal framework often defines "destruction of a communication device" as a crime, which defines it as a hardware . In a DoS and DDoS attack, the system may be recovered easily after a simple reboot, without damaging the hardware device. The legal framework should define attacks as such attacks which causes failure of devices to function, or attacks which degrade the ability of the device to function, or attacks which attempt to overwhelm the bandwidth capacity of the network device to reflect DoS and DDoS attacks instead.

Another issue is spoofed IP addresses in DoS and using multiple points of attacks such as in DDoS, increases complexity of determining the original attacker's machine. It is

often difficult to obtain the information from the infected host, unless with full cooperation from the affected organization and acted upon in a short period of time. Prolonged delay in investigation may cause the data to be lost. Even after the relevant information are being preserved, and analyzed, the integrity of the data will be questioned. These factors make it difficult to identify the person behind the computer. Legal proceedings require such information to be entangled and objectively determined and analyzed. Applying computer forensics procedures are crucial in the early process of evidence gathering.

Conclusion

The DoS and DDoS attacks in combination with malicious codes implantations, are easily launched but difficult to completely stop. With the nature of TCP/IP and programming issues that are often overlooked, the current Internet is still vulnerable to various forms of DoS and DDoS attacks. There is no "silver bullet" solution to this, like many other security issues. However, in mitigating DoS or DDoS attacks, it requires good network design to be able to control the point of entry or the gateway. As for mitigating new attacks, it is essential to have filtering capability based on packet header and content within the network or at the critical gateways in order to filter malicious traffic as a response to such attacks while waiting for a permanent solution from suppliers to be applied to the devices. Applying all known patches and fixes to all devices in the network to prevent known attacks is necessary. Finally it is important to have the relevant referrals in the policy and legislations to address the issue of DoS and DDoS to ensure an effective cooperation between service providers and law enforcement agencies.

Whether you choose to downplay the effect of DoS and DDoS to your business or otherwise, is a choice made in your organization's policy. However, the effect is real. If we plan to conduct on-line, almost everything that we do in life, it is crucial to consider the responses and preventive measures to these threats.

References

[1] RFC 2267 network ingress filtering http://RFC.net/rfc2267.html (4 Jan. 2002)

[2] Brenton, Chris. "Egress Filtering v 0.2". 29 February 2000. URL: http://www.sans.org/y2k/egress.htm (1 Dec. 2001)

[3] Cisco. "Strategies to Protect Against Distributed Denial of Service Attacks". 17 February 2000. URL: http://www.cisco.com/warp/public/707/newsflash.html (4 Jan. 2002)

[4] Malaysian Computer Emergency Response Team. "MSA 029.072001: MyCERT Special Alert - Code Red Worm". 20 July 2001. URL: http://www.mycert.org.my/alerts/mycert_adv/MSA-029.072001.html (4 Jan. 2002)

[5] Malaysian Computer Emergency Response Team. "MA-034.092001 : NIMDA Worm". 19 September 2001. URL: http://www.mycert.org.my/advisory/MA-034.092001.html (4 Jan. 2002)

[6] Dittrich, Dave. "NANOG ISPSec Meeting/DDoS BoF". 7 February, 2000. URL: http://staff.washington.edu/dittrich/talks/nanog/ (4 Jan. 2002)

[7] Anonymous. Maximum Security: A Hacker's Guide to protecting your Internet site and network. Indianapolis: Sams.net Publishing, 1997.

[8] Huegen, Craig A. "The Latest in Denial of Service Attacks: "Smurfing" Description and Information to Minimize Effects". 8 February 2000. URL: http://www.pentics.net/denial-of-service/white-papers/smurf.cgi (4 Jan. 2002)

[9] Mandia, Kevin & Prosise, Chris. Incident Response : Investigating Computer Crime. Berkeley: Osborne/McGraw-Hill, 2001. 360-361.

[10] CISCO. "Defining Strategies to Protect Against TCP SYN Denial of Service Attacks". September 17, 1996. URL: http://cio.cisco.com/warp/public/707/4.html (4 Jan. 2002)

[11] CISCO. "Defining Strategies to Protect Against UDP Diagnostic Port DoS Attacks". September 17, 1996. URL : http://cio.cisco.com/warp/public/707/3.html (4 Jan. 2002)

[12] Raymond, Eric S. "Jargon File". April 2001. URL : http://www.tuxedo.org/~esr/jargon/ (4 Jan. 2002)