Evading IDS, Firewalls,  
and Honeypots

Module Flow  
  
 To understand IDSes, firewalls, and honeypots, evasion techniques used by the attackers to break into the target network or system, it is necessary to understand these mechanisms and how they prevent intrusions and offer protection. So, let us begin with basic IDS, firewall, and honeypot concepts.

This section introduces you with the basic IDS, firewall, and honeypot concepts.

Intrusion Detection Systems (IDSes) and their Placement

An intrusion detection system is used to monitor and protect networks or systems for malicious activities. To alert security personnel about intrusions, intrusion detection systems are highly useful. IDSes are used to monitor network traffic. An IDS checks for suspicious activities. It notifies the administrator about intrusions immediately.

a) An intrusion detection system (IDS) gathers and analyzes information from within a computer or a network, to identify the possible violations of security policy, including unauthorized access, as well as misuse

b) An IDS is also referred to as a "packet-sniffer," which intercepts packets traveling along various communication mediums and protocols, usually TCP/IP

c) The packets are analyzed after they are captured  
d) An IDS evaluates a suspected intrusion once it has taken place and signals an alarm

How an IDS Works

The main purposes of IDSes are that they not only prevent intrusions but also alert the administrator immediately when the attack is still going on. The administrator could identify methods and techniques being used by the intruder and also the source of attack.

An IDS works in the following way:  
a) IDSes have sensors to detect signatures and some advanced IDSes have behavioral activity detection to determine malicious behavior. Even if signatures don't match this activity detection system can alert administrators about possible attacks.  
b) If the signature matches, then it moves to the next step or the connections are cut down from that IP source, the packet is dropped, and the alarm notifies the admin and the packet can be dropped.  
c) Once the signature is matched, then sensors pass on anomaly detection, whether the received packet or request matches or not.  
d) If the packet passes the anomaly stage, then stateful protocol analysis is done. After that through switch the packets are passed on to the network. If anything mismatches again, the connections are cut down from that IP source, the packet is dropped, and the alarm notifies the admin and packet can be dropped.

Types of Intrusion Detection Systems

Network Intrusion Detection System

The NIDS checks every packet entering the network for the presence of anomalies and incorrect data. Unlike the firewalls that are confined to the filtering of data packets with vivid malicious content, the NIDS checks every packet thoroughly. An NIDS captures and inspects all traffic, regardless of whether it is permitted. Based on the content, at either the IP or application-level, an alert is generated. Network-based intrusion detection systems tend to be more distributed than host-based IDSes. The NIDS is basically designed to identify the anomalies at the router- and host-level. The NIDS audits the information contained in the data packets, logging information of malicious packets. A threat level is assigned to each risk after the data packets are received. The threat level enables the security team to be on alert. These mechanisms typically consist of a black box that is placed on the network in the promiscuous  
mode, listening for patterns indicative of an intrusion.

Host Based Intrusion detection System

In the host-based system, the IDS analyzes each system's behavior. The HIDS can be installed on any system ranging from a desktop PC to a server. The HIDS is more versatile than the NIDS. One example of a host-based system is a program that operates on a system and  
receives application or operating system audit logs. These programs are highly effective for detecting insider abuses. Residing on the trusted network systems themselves, they are close to the network's authenticated users. If one of these users attempts unauthorized activity, host- based systems usually detect and collect the most pertinent information promptly. In addition to detecting unauthorized insider activity, host-based systems are also effective at detecting unauthorized file modification. HIDSes are more focused on changing aspects of the local systems. HIDS is also more platform-centric, with more focus on the Windows OS, but there are other HIDSes for UNIX platforms. These mechanisms usually include auditing for events that occur on a specific host. These are not as common, due to the overhead they incur by having to monitor each system event.

Intrusion Detection Tools

In addition, to the previously mentioned intrusion detection tools, there are few more tools that can be used for detecting intrusions:  
() Check Point Threat Prevention Appliance available at http://www.checkpoint.com  
() Fragroute available at http://www.monkey.org  
() Next-Generation Intrusion Prevention System (NGIPS) available at http://www.sourcefire.com  
() Outpost Network Security available at http://www.agnitum.com  
() Check Point IPS-1 available at http://www.checkpoint.com  
() FortiGate available at http://www.fortinet.com  
() Enterasys® Intrusion Prevention System available at http://www.enterasys.com  
() StoneGate Virtual IPS Appliance available at http://www.stonesoft.com  
() Cyberoam Intrusion Prevention System available at http://www.cyberoam.com  
() McAfee Host Intrusion Prevention for Desktops available at http://www.mcafee.

Firewalls  
A firewall is a set of related programs located at the network gateway server that protects the resources of a private network from users on other networks. Firewalls are a set of tools that monitor the flow of traffic between networks. A firewall, placed at the network level and working closely with a router, filters all network packets to determine whether or not to forward them toward their destinations. A firewall is often installed away from the rest of the network so that no incoming request can get directly to a private network resource. If configured properly, systems on one side of the firewall are protected from systems on the other side of the firewall.

a) A firewall is an intrusion detection mechanism. Firewalls are specific to an organization's security policy. The settings of the firewalls can be changed to make appropriate changes to the firewall functionality.

b) Firewalls can be configured to restrict incoming traffic to POP and SNMP and to enable email access. Certain firewalls block the email services to secure against spam.

c) Firewalls can be configured to check inbound traffic at a point called the "choke point/׳ where security audit is performed. The firewall can also act as an active "phone tap" tool in identifying the intruder's attempt to dial into the modems within the network that is secured by firewall. The firewall logs consist of logging information that reports to the administrator on all the attempts of various incoming services.

() The firewall verifies the incoming and outgoing traffic against firewall rules. It acts as a router to move data between networks. Firewalls manage access of private networks to host applications.

() All the attempts to log in to the network are identified for auditing. Unauthorized attempts can be identified by embedding an alarm that is triggered when an unauthorized user attempts to login. Firewalls can filter packets based on address and types of traffic. They identify the source, destination addresses, and port numbers while address filtering, and they identify types of network traffic when protocol filtering.  
Firewalls can identify the state and attributes of the data packets.

Types of Firewalls

A firewall refers to a hardware device or a software program used in a system to prevent malicious information from passing through and allowing only the approved information.

Firewalls are mainly categorized into four types:  
() Packet filters  
() Circuit-level gateways  
() Application-level gateways  
() Stateful multilayer inspection firewall

Packet Filtering Firewall

A packet filtering firewall investigates each individual packet passing through it and makes a decision whether to pass the packet or drop it. As you can tell from their name, packet filter-based firewalls concentrate on individual packets and analyze their header information  
and which way they are directed.

Circuit-level Gateway Firewall

Circuit-level gateways work at the session layer of the OSI model or the TCP layer of TCP/IP. A circuit-level gateway forwards data between the networks without verifying it. It blocks incoming packets into the host, but allows the traffic to pass through itself. Information passed to remote computers through a circuit-level gateway appears to have originated from the gateway, as the incoming traffic carries the IP address of the proxy (circuit-level gateway).  
A circuit-level gateway gives the controlled network connection to the network between the system, internal and external to it. For detecting whether or not a requested session is valid, it checks the TCP handshaking between the packets. Circuit-level gateways do not filter individual packets. Circuit-level gateways are relatively inexpensive and hide the information about the private network that they protect.

Application-level Firewall

־־Proxy/application-based firewalls concentrate on the Application layer rather than just the packets.  
() These firewalls analyze the application information to make decisions about whether or not to transmit the packets.  
() A proxy-based firewall asks for authentication to pass the packets as it works at the Application layer.  
() A content caching proxy optimizes performance by caching frequently accessed information instead of sending new requests for the same old data to the servers.

Stateful Multilayer Inspection Firewall

Stateful multilayer inspection firewalls combine the aspects of the other three types of firewalls. They filter packets at the network layer, to determine whether session packets are legitimate, and they evaluate the contents of packets at the application layer. The inability of the packet filter firewall to check the header of the packets to allow the passing of packets is overcome by stateful packet filtering.

Firewall Identification: Port Scanning

Systematically scanning the ports of a computer is known as port scanning. Attackers use such methods to identify the possible vulnerabilities in order to compromise a network. It is one of the most popular methods that attackers use for investigating the ports used by the victims. A tool that can be used for port scanning is Nmap.

A port scan helps the attacker find which ports are available (i.e., what service might be listening to a port); it consists of sending a message to each port, one at a time. The kind of response received indicates whether the port is used and can therefore be probed further for weakness. Some firewalls will uniquely identify themselves using simple port scans. For example: Check Point's FireWall-1 listens on TCP ports 256, 257, 258, and 259 and Microsoft's Proxy Server usually listens on TCP ports 1080 and 1745.

Firewall Identification: Firewalking

Firewalking is a method used to collect information about remote networks that are behind firewalls. It probes ACLs on packet filtering routers/firewalls. It is same as that of tracerouting and works by sending TCP or UDP packets into the firewall that have a TTL set at  
one hop greater than the targeted firewall. If the packet makes it through the gateway, it is forwarded to the next hop where the TTL equals zero and elicits a TTL "exceeded in transit" message, at which point the packet is discarded. Using this method, access information on the  
firewall can be determined if successive probe packets are sent. Firewalk is the most well-known software used for firewalking. It has two phases: a network discovery phase and a scanning phase. It requires three hosts:

() Firewalking host: The firewalking host is the system, outside the target network, from which the data packets are sent, to the destination host, in order to gain more information about the target network.

() Gateway host: The gateway host is the system on the target network that is connected to the Internet, through which the data packet passes on its way to the target network.

() Destination host: The destination host is the target system on the target network that the data packets are addressed to.

Firewall Identification: Banner Grabbing

Banners are messages sent out by network services during the connection to the service. Banners announce which service is running on the system. Banner grabbing is a technique generally used by the attacker for OS detection. The attacker uses banner grabbing to discover services run by firewalls. The three main services that send out banners are FTP, Telnet, and web servers.

Ports of services such as FTP, Telnet, and web servers should not be kept open, as they are vulnerable to banner grabbing. A firewall does not block banner grabbing because the connection between the attacker's system and the target system looks legitimate.

An example of SMTP banner grabbing is: telnet mail.targetcompany.org 25. The syntax is:  
“<service name>< service running> <port number>”

Banner grabbing is a mechanism that is tried and true for specifying banners and application information. For example, when the user opens a telnet connection to a known port on the target server and presses Enter a few times, if required, the following result is displayed:

C:\>telnet www.corleone.com 80  
HTTP/1.0 400 Bad Request  
Server: Netscape - Commerce/1.12

This system works with many other common applications that respond on a set port. The information generated through banner grabbing can enhance the attacker's efforts to further compromise the system. With information about the version and the vendor of the web server, the attacker can further concentrate on employing platform-specific exploit techniques.

Firewalls  
  
Firewalls provide essential protection to the computers against viruses, privacy threats, objectionable content, hackers, and malicious software when networked or connected to the Internet. A firewall monitors running applications that access the network. It analyzes downloads and warns you if downloading a malicious file, stops it from infecting your PC. A few of the firewalls that provide system protection are listed as follows:  
()Check Point Firewall Software Blade available at http://www.checkpoint.com  
() eScan Enterprise available at http://www.escanav.com  
() Jetico Personal Firewall available at http://www.ietico.com  
() Outpost Security Suite available at http://free.agnitum.com  
() Novell BorderManager available at http://www.novell.com  
() Firewall UTM available at http://www.esoft.com  
()Sonicwall available at http://www.tribecaexpress.com  
() Comodo Firewall available at <http://personalfirewall.comodo.com>

()Online Armor available at http://www.online-armor.com  
() FortiGate-5101C available at http://www.fortinet.com

Honeypot

A honeypot is a system that is intended to attract and trap people who try unauthorized or illicit utilization of the host system. Whenever there is any interaction with a honeypot, it is most likely to be a malicious activity. Honeypots are unique; they do not solve a specific problem. Instead, they are a highly flexible tool with many different security applications. Some honeypots can be used to help prevent attacks; others can be used to detect attacks; while a few honeypots can be used for information gathering and research.

Examples:  
() Installing a system on the network with no particular purpose other than to log all attempted access.

()Installing an older unpatched operating system on a network. For example, the default installation of WinNT 4 with IIS 4 can be hacked using several different techniques. A standard intrusion detection system can then be used to log hacks directed against the system and further track what the intruder attempts to do with the system once it is compromised. Install special software designed for this purpose. It has the advantage of  
making it look like the intruder is successful without really allowing him/her access to the network.

Any existing system can be "honeypot-ized." For example, on WinNT, it is possible to rename the default administrator account and then create a dummy account called "administrator" with no password. WinNT allows extensive logging of a person's activities, so this honeypot  
tracks users who are attempting to gain administrator access and exploit that access.

Types of Honeypots

Honeypots are mainly divided into two types:

Low-Interaction Honeypot

They work by emulating services and programs that would be found on an individual's system. If the attacker does something that the emulation does not expect, the honeypot will simply generate an error. They capture limited amounts of information, mainly transactional data and some limited interaction

Ex: Specter, Honeyd, and KFSensor  
Honeyd is a low-interaction honeypot. It is open source and designed to run primarily on UNIX systems. Honeyd works on the concept of monitoring unused IP space. Anytime it sees a connection attempt to an unused IP, it intercepts the connection and then interacts with the  
attacker, pretending to be the victim.

By default, Honeyd detects and logs connections to any UDP or TCP port. In addition, the user can configure emulated services to monitor specific ports, such as an emulated FTP server monitoring port 21 (TCP). When an attacker connects to the emulated service, not only does  
the honeypot detect and log the activity, but also it captures all of the attacker's interaction with the emulated service.

In the case of the emulated FTP server, an attacker's login and password can be potentially captured; the commands that were issued, what they were looking for, or their identity can be tracked. Most emulated services work the same way. They expect a specific type of behavior,  
and then are programmed to react in a predetermined way.

High-Interaction Honeypot

Honeynets are a prime example of a high-interaction honeypot. A honeynet is neither a product nor a software solution that the user installs. Instead, it is architecture, an entire network of computers designed to attack.

The idea is to have an architecture that creates a highly controlled network, one where all activity is controlled and captured. Within this network, intended victims are placed and the network has real computers running real applications.

The "bad guys" find, attack, and break into these systems on their own initiative. When they do, they do not realize they are within a honeynet. All of their activity, from encrypted SSH sessions to email and file uploads, is captured without them knowing it by inserting kernel modules on the victim's systems, capturing all of the attacker's actions.

At the same time, the honeynet controls the attacker's activity. Honeynets do this by using a honeywall gateway. This gateway allows inbound traffic to the victim's systems, but controls the outbound traffic using intrusion prevention technologies. This gives the attacker the  
flexibility to interact with the victim's systems, but prevents the attacker from harming other non-honeynet computers.

How to Set Up a Honeypot

Follow the steps here to set up a honeypot:

Step 1: Download or purchase honeypot software. Tiny Honeypot, LaBrea, and Honeyd are some of the programs available for Linux systems. KFSensor is software that works with Windows.  
Step 2: Log in as an administrator on the computer to install a honeypot onto the computer.  
Step 3: Install the software on your computer. Choose the "Full Version" to make sure every feature of the program is installed.  
Step 4: Place the honeypot software in the Program Files folder. Once you have chosen the folder, click"OK and the program will install.  
Step 5: Restart your computer for the honeypot to work.  
Step 6: Configure the honeypot to check the items that you want the honeypot to watch for, including services, applications, and Trojans, and name your domain.

Evading IDS

Insertion Attack  
The process where the attacker confuses the IDS by forcing it to read the invalid packets is known as insertion, that is, the packet would not be accepted by the system to which it is addressed. If a packet is malformed or if it does not reach its actual destination, the packet  
is invalid. Ifthe IDS read an invalid packet, the IDS will become confused.  
To understand how insertion becomes a problem for a network IDS, it is important to understand how IDSes detect attacks. The IDS employs pattern-matching algorithms to look for specific patterns of data in a packet or stream of packets. For example, IDSes might look for the  
string "phf" in an HTTP request to discover a PHF Common Gateway Interface (CGI) attack. An attacker who can insert packets into the IDS can prevent pattern matching from working. For instance, an attacker can send the string "phf" to a web server, attempting to exploit the CGI  
vulnerability, but force the IDS to read "phoneyf" (by "inserting״ the string "oney") instead. One simple insertion attack involves intentionally corrupting the IP checksum. Every packet transmitted on an IP network has a checksum that is used to verify whether the packet was  
corrupted in transit. IP checksums are 16-bit numbers that are computed by examining information in the packet. If the checksum on an IP packet does not match the actual packet, the host to which it is addressed will not accept it, while the IDS might consider it as part of the  
effective stream.

For example, the attacker can send packets whose Time to live fields have been crafted to reach the IDS but not the target computers. An attacker confronts the IDS with a stream of one- character packets (the attacker-originated data stream), in which one of the characters (the letter 'X') will be accepted only by the IDS. As a result, the IDS and the end system reconstruct two different strings.

Evasion

An "evasion" attack occurs when the IDS discards a packet that the host to which it is addressed accepts. Evasion attacks are devastating to the accuracy of the IDS. An evasion attack at the IP layer allows an attacker to attempt arbitrary attacks against hosts on a network, without the IDS ever realizing it. The attacker sends portions of the request in packets that the IDS mistakenly rejects, allowing the removal of parts of the stream from the ID system's view.

For example, if the malicious sequence is sent byte-by-byte, and one byte is rejected by the IDS, the IDS cannot detect the attack. Here, the IDS gets fewer packets than the destination. One example of an evasion attack occurs when an attacker opens a TCP connection with a data packet. Before any TCP connection can be used, it must be "opened" with a handshake between the two endpoints of the connection. A fairly obscure fact about TCP is that the handshake packets can themselves bear data. IDSes that do not accept the data in these packets are vulnerable to an evasion attack.

Denial־of־ Service Attack (DoS)

Multiple types of denial-of-service attacks are valid against IDS systems. The attacker identifies a point of network processing that requires the allocation of a resource, causing a condition to occur that consumes all of that resource. The resources that can be affected by the attacker are CPU cycles, memory, disk space, and network bandwidth. The CPU capabilities of the IDS can be monitored and affected. This is because IDS needs half of the CPU cycle to read the packets, detecting what the purpose of their existence is, and then comparing them with some location in the saved network state. An attacker can verify the most computationally expensive network processing operations and then compel the IDS to spend all its time carrying out useless work.

An IDS requires memory for a variety of things. For generating a match for the patterns, the TCP connections should be saved, the reassembly queues should be maintained, and the buffers of the data should be generated. In the initial phase, the system requires memory so that it canread the packets. Memory is allocated by the system. It is needed for network processing operations. An attacker can verify the processing operations that require the ID system to allocate memory and force the IDS to allocate all of its memory for meaningless information.

In certain circumstances, the ID systems store activity logs on the disk. The stored events occupy most of the disk space. Most computers have limited disk space. The attackers can occupy a major part of the disk space on the IDS by creating and storing a large number of useless events. This renders the IDS useless in terms of storing real events.

Network IDS systems record the activity on the networks they monitor. They are competent because networks are hardly ever used to their full capacity; few monitoring systems can cope with an extremely busy network. The IDS system, unlike an end system, must read everyone's packets, not just those sent specifically to it. An attacker can overload the network with meaningless information and prevent the IDS system from keeping up with what is actually happening on the network.

Many IDSes today employ central logging servers that are used exclusively to store IDS alert logs. The central server's function is to centralize alert data so it can be viewed as a whole rather than on a system-by-system basis. However, if attackers know the central log server's IP address, they could slow it down or even crash it using a DoS attack. After the server is shut down, attacks could go unnoticed because the alert data is no longer being logged.

Using this evasion technique, an attacker:  
() Consumes the device's processing power and allows attacks to sneak by

() Fills up disk space causing attacks to not be logged  
() Causes more alarms than can be handled by management systems (such as databases, ticketing systems, etc.)  
() Causes personnel to be unable to investigate all the alarms.  
() Causes the device to lock up.

### Flooding

IDSs depend on resources such as memory and processor power to effectively capture packets, analyze traffic, and report malicious attacks. By flooding a network with noise traffic, an attacker can cause the IDS to exhaust its resources examining harmless traffic. In the meantime, while the IDS is distracted and occupied by the volume of noise traffic, the attacker can target its system with little or no intervention from the IDS.

### Fragmentation

Because different network media allow variable maximum transmission units (MTUs), you must allow for the fragmentation of these transmission units into differently sized packets or cells. Hackers can take advantage of this fragmentation by dividing attacking packets into smaller and smaller portions that evade the IDS but cause an attack when reassembled by a target host.

### Encryption

Network-based intrusion detection (covered later in this chapter) relies on the analysis of traffic that is captured as it traverses the network from a source to its destination. If a hacker can establish an encrypted session with its target host using Secure Shell (SSH), Secure Socket Layer (SSL), or a virtual private network (VPN) tunnel, the IDS cannot analyze the packets and the malicious traffic will be allowed to pass. Obviously, this technique requires that the attacker establish a secure encrypted session with its target host.

### Obfuscation

Obfuscation, an increasingly popular evasive technique, involves concealing an attack with special characters. It can use control characters such as the space, tab, backspace, and Delete. Also, the technique might represent characters in hex format to elude the IDS. Using Unicode representation, where each character has a unique value regardless of the platform, program, or language, is also an effective way to evade IDSs. For example, an attacker might evade an IDS by using the Unicode character c1 to represent a slash for a Web page request.

False Positive Generation  
This mode does not attack the target, but instead, it does something relatively normal. In this mode, an alarm is generated when no condition is present to warrant one.  
However, many IDSes falsely trigger on this. Another attack similar to the DoS method is to generate a large amount of alert data that must be logged. Attackers craft packets known to trigger alerts within the IDS, forcing it to generate a large number of false reports. This type of attack is designed to create a great deal of log "noise" in an attempt to blend real attacks with the false. Attackers know all too well that when looking at log data, it can be very difficult to differentiate between legitimate attacks and false positives. If attackers have knowledge of the IDS system, they can even generate false positives specific to that IDS.

Evading Firewall

IP Address Spoofing

IP address spoofing or IP spoofing is one of the ways that an attacker tries to evade firewall restrictions. IP spoofing is a technique where the attacker creates Internet protocol packets by using a forged IP address and gains access over the system or network without any authorization. The attacker spoofs the messages and they appear to be sent from a reliable source. Thus, the attacker succeeds in impersonating others׳ identities with help of IP spoofing. Hackers generally use this technique for not getting caught while spamming and various other activities.  
The following scenario shows how an attacker bypasses a firewall by impersonating a different identity with the help of th IP spoofing technique:  
() Let's consider three hosts: A, B, and C  
() Host C is a trusted machine of host B  
() Host A wants to send some packets to host B and A impersonates itself to be C by changing the IP address of these packets  
() When these packets are received, Bthinks that these packets are from C, but actually  
they are from A

Source Routing

Using this technique, the sender of the packet designates the route that a packet should take through the network in such a way that the designated route should bypass the firewall node. Using this technique the attacker can evade the firewall restrictions.  
When these packets travel through the nodes in the network, each router will check the IP address of the destination and choose the next node to forward them. In source routing, the sender makes some or all of these decisions on the router.  
The figure shows the principle of the source routing but it is an optimal way, which makes the decision of the next hop.

Tiny Fragments

The attacker uses the IP fragmentation technique to create extremely small fragments and force the TCP header information into the next fragment. This may result in a case whereby the TCP flags field is forced into the second fragment, and filters will be unable to check these flags in the first octet thus ignoring them in subsequent fragments.  
Attackers hope that only the first fragment is examined by the filtering router (firewall) and the remaining fragments are passed through. This attack is used to avoid user defined filtering rules and works when the firewall checks only for the TCP header information.

Bypass Blocked Sites Using IP Address in Place of URL

You can also evade firewall restrictions by typing the IP address of the blocked siteinstead of its domain names. This allows you to access the restricted or blocked sites. Youneed touse some tools to convert the target domain name into its IP address.  
For example:  
() Instead of typing www.Orkut.com, type its IP address to access Orkut  
() Host2ip can help you to find the IP address of that blocked website  
() If the blocking software can track the IP address sent to the web server, the website could not be unblocked or accessed by using this method.

Bypass Blocked Sites Using Anonymous Website Surfing Sites

Anonymous website surfing sites help you to surf the Internet anonymously and to unblock blocked sites. i.e., evade firewall restrictions. By using these sites, you can surf restricted sites anonymously, i.e., without using your IP address on the Internet. There are a number of anonymous website surfing sites available on the Internet. Some websites provide options to encrypt the URLs of websites.  
Here is a list of some of the proxy servers that can help you to unblock blocked websites:  
()http://anonvmouse.org  
() http://www.anonymizer.com  
() http://www.webproxyserver.net  
() http://www.boomproxy.com  
() http://proxify.com  
() <http://www.spysurfing.co>m

() http://alienproxv.com  
() http://zendproxy

Bypass a Firewall Using a Proxy Server

By using a proxy server, you can also bypass the firewall restriction imposed by a particular organization. To evade the firewall restrictions using a proxy server, follow these steps:  
1. Find an appropriate proxy server.  
2. On the Tools menu of any Internet browser, go to LAN of Network Connections tab, and then click LAN/Network Settings.  
3. Under Proxy server settings, select the use a proxy server for the LAN.  
4. In the Address text box, type the IP address of the proxy server.  
5. In the Port text box, type the port number that is used by the proxy server for client connections (by default, 8080).  
6. Click to select the bypass proxy server for local addresses checkbox if you do not want the proxy server computer to be used when connected to acomputer on the local network.  
7. Click OK to close the LAN Settings dialog box.  
8. Click OK again to close the Internet Options dialog box.

Bypassing a Firewall through the ICMP Tunneling Method

ICMP tunneling allows tunneling a backdoor shell in the data portion of ICMP Echo packets. RFC 792, which delineates ICMP operation, does not define what should go in the data portion. The payload portion is arbitrary and is not examined by most of the firewalls, thus any data can be inserted in the payload portion of the ICMP packet, including a backdoor application. Some administrators keep ICMP open on their firewall because it is useful for tools like ping and traceroute. Assuming that ICMP is allowed through a firewall, use Loki ICMP tunneling to execute commands of choice by tunneling them inside the payload of ICMP echo packets

Bypassing a Firewall through the ACK Tunneling Method

ACK tunneling allows tunneling a backdoor application with TCP packets with the ACK bit set. The ACK bit is used to acknowledge receipt of a packet. Some firewalls do not check packets with the ACK bit set because ACK bits are supposed to be used in response to legitimate traffic  
that is already being allowed through. Attackers use this as an advantage to perform ACK tunneling. Tools such as AckCmd (http://ntsecurity.nu) can be used to implement ACK tunneling.

Bypassing a Firewall through the HTTP Tunneling Method

This method can be implemented if the target company has a public web server with port 80 used for HTTP traffic, that is unfiltered on its firewall. Many firewalls do not examine the payload of an HTTP packet to confirm that it is legitimate HTTP traffic, thus it is possible to tunnel traffic inside TCP port 80 because it is already allowed. Tools such as HTTPTunnel.

(http://www.nocrew.org) use this technique of tunneling traffic across TCP port 80. HTTPTunnel is a client/server application, the client application is called htc, and the server is hts. Upload the server onto the target system and tell it which port is to be redirected through TCP port 80.

Bypassing a Firewall through External Systems

Attackers can bypass firewall restrictions through external systems as follows:  
1. Legitimate user works with some external system to access the corporate network.  
2. Attacker sniffs the user traffic, and steals the session ID and cookies.  
3. Attacker accesses the corporate network bypassing the firewall and gets Windows ID of the running Netscape 4.x/ Mozilla process on user's system.  
4. Attacker then issues an openURL() command to the found window.  
5. User's web browser connects with the attacker's WWW server.  
6. Attacker inserts malicious payload into the requested web page (Java applet) and thus the attacker's code gets executed on the user's machine.

Bypassing a Firewall through a MITM Attack  
The following steps illustrate an example scenario of how an attackerbypasses a firewall through an MITM attack:  
1. Attacker performs DNS server poisoning.  
2. User A requests WWW.juggyboy.com to the corporate DNS server.  
3. Corporate DNS server sends the IP address (127.22.16.64) of the attacker.  
4. User A accesses the attacker's malicious server.  
5. Attacker connects with the real host and tunnels the user's HHTP traffic.  
6. Attacker inserts malicious payload into the requested web page (Java applet),and thus  
the attacker's code is executed on the user's machine.

## Honeypots Detection Techniques

Honeypot is designed primarily for tracking or attacking attackers during their attempts to break into an organization system. Attackers would try to detect the presence of honeypots on the network by propping services running on the system. These probs would include crafting malicious packets such as HTTPS, SMTPS, etc. For example. Ports that should a running service but deny a three-way handshake might indicate the presence of honeypot.

Attackers can also defeat honeypots by using multi-proxies (TORs) and hiding their conversations using encryption and steganography techniques. However, they are Some techniques used to identify and defeat the honeypots system, as discussed below.

Detecting the presence of Tar Pits :

Tar Pits are security entities similar to honeypots. Tar Pits are designed to respond slowly to incoming requests, which would slow down attacks attempts. Tart Pits might present at Layer7, layer 4, and laye7 based on the attacking vector.

o  Layer 7 Tar Pits: Malicious Incoming SMTP/HTTP commands by an attacker, the system would slow down response. Thus Tar Pits could be identified by the latency of the response

o  Layer 4 Tar Pits manipulate TCP/IP stack, where the system would accept TCP/IP connection and switch to a zero-windows size. In such a way, the attacker blocked from sending other data.

o  Layer 2 Tar Pits: Attack has launched on the same network. The attacker can identify the presence of this daemon by looking at the responses with the unique MAC address 0:0:f:ff:ff:ff, which acts as a kind of black hole. An attacker can also identify the presence of these tar pits by analyzing the ARP responses.

·      Detecting Honeypots Running on VMware:

Attackers can detect instances that are running on the VMWare virtual machine by analyzing the MAC address. Referring to IEEE standards for the current range of MAC addresses assigned to VMWare Inc., an attacker can identify the presence of VMWare-based honeypots.

·      Detecting the presence of Honeyd Honeypot:

Honeyd is a simulator honeypot engine that can create thousands of honeypots easily. The honeyd would respond to received SMTP requests with fake responses. An attacker can identify the presence of honeyd honeypot by performing time-based TCP fingerprinting methods.

·      Detecting the presence of User-Mode Linux (UML) Honeypot:

Attackers can identify the presence of UML honeypots by analyzing files such as /proc/mounts, /proc/interrupts, and /proc/cmdline, which contain UML-specific information.

·      Detecting the presence of Sebek-based Honeypots:

Attackers can detect the existence of Sebek-based honeypots by analyzing the congestion in the network layer, as Sebek data communication is usually unencrypted. Since Sebek logs everything that is accessed via reading () call before transferring to the network, it causes the congestion effect

·      Detecting the presence of Snort\_inline Honeypot:

Attackers can identify these honeypots by analyzing the outgoing packets. If an outgoing packet is dropped, it might look like a black hole to an attacker. When the snort\_inline modifies an outgoing packet, the attacker can capture the modified packet through another host system and identify the packet modification.

·      Detecting the presence of Fake AP:

Fake access points send only beacon frames but do not produce any traffic on the access points, and an attacker can detect and monitor the network traffic and quickly note the presence of fake AP.

As discussed upper, the detection of honeypots would depend on analyzing responses, and its diversion from a typical system would act. These analyses would take much time for attackers to detect and ensure the existence of a honeypot inside the organization network.

Honeypot Detection Tool

Send-safe Honeypot Hunter is a honeypot detection tool designed for checking lists of https and socks proxies for honeypots.

Some of the Send-Safe honeypots Huter feature include:

() Check lists of HTTPS,SOCKS5 and SOCKS5 proxies with any ports

() Can check several remote or local proxy lists at once

() Can process proxy lists automatically every specified period of time

() May be used for ususal proxy list validating as well.

Firewall evasion tool: Traffic IQ professional

Traffic IQ professional enable security professional to audit and validate the behaviour of security devices by generating the standard application traffic traffic between two.virtual machines.percent packet transmission capabilities of traffic it professional make the task of reliable e-auditing validating and proving security compliance easy and quick to complete it can be used to access Audit and test the behaviour characteristics of any known proxy packet filtering device including application layer firewalls intrusion detection system intrusion prevent printing systems and routers and switches.

Firewall Evasion Tool: tcp-over-dns

tcp-over-dns contains a special server and a special dns client. The client an server work in tandem to provide a TCP (and UDP!) tunnel through the standard DNS protocol.It is similar to  
the defunct NSTX dns tunneling software.the purpose of this office to succeed there any tax paid on the stakes are disconnect with internal factors in real-world situation TCP or DNS is returned to [the.at](http://the.at) the same time providing acceptable bandwidth [speed it](http://speed.it) features include.

()Windows Linux OS compatibility

()sliding windows packet transfers for increase speed and reliability

()runtime selective LZMA compression

()TCP and udp traffic tunneling.

Firewall Evasion Tools

Firewall Evasion tools help in breching a Firewall from [inside as](http://inside.as) well as exporting data with innocent looking packets that contain insufficient data for sniffers of firewall to analyse.Firewall evasion tools are listed as follows

() SnareAgent for windows

() AckCmd

()Hotspot Shield

() Tomahawk

()Proxifier

()Freenet

Packet Fragment Generator

Packet fragment generators allows you to edit and send packets via your wireless network adaptor. They allow you to hide your network files transfer across the internet by utilising a packet forgery .these tool hide your file transfer by clocking in seemingly harmless data. A few packet fragment generators are listed as follows.

Colasoft packet builder

Common view

hping3

Multi generator

Net inspect

Nconvert

Net scan post Pro

Packet maker

Countermeasures

The following a few countermeasures that provide protection against the envading IDS firewalls and honeypots

() administrative shutdown switch port interference interface associate with the system from which attacks are print launched

()look for the north of code other than 0 x 90 to defend against the polymorphic shellcode problem

()perform bifurcating analysis in which the monitor deals with the ambitious traffic exchange by an instant tainting separate analysis test for each possible interpretation of the MP3 used traffic

()Maintain security vulnerability a dispatch vulnerabilities as soon as possible and wisely choose the ideas based on the network topology and network traffic received

()GeneralTCP RST packets to Tear down malicious TCP sessions any issue or several available icmp error code packets in response to malicious udp traffic

()interact with external Firewall router to add a general rule to block all communication from individual IP addresses or entire networks

()implement a traffic normalizer a network forwarding element that attempts to eliminate ambiguous network traffic and reduced amount connection state that the monitor must maintain

()ensure that IDSss is normalised fragmented packets and allow those packets to the assembled in the proper order which enables the ideas to look at the information just as the and host can see it

()keep updating the idea system and Firewall software regularly

Firewall IDS Penetration testing

Firewall IDS Penetration testing is conducted to identify if there is any security vulnerability related to hardware software and its configuration.and how to protect the network from outside net attackers. It helps in evaluating security by testers ingress nd egress vulnerabilities.and proper rules set of the entire network with respect to the possibility of Entry from an external location.Firewall Penetration testing.as a pen tester you should implement a following steps.to conduct penetration testing on a Firewall.

step 1 footprint the target.

you should put print the target by using various tools.such as fan speed NS lookup traceroute and map and neotrace.to learn about a system its remote access capabilities.its port and services and the other aspects of it security

step 2 perform port scanning

you should perform port scanning to detect the firewall to determine.available ports and unique play identify the firewall.if Firewall is detected.disable the trusted host or perform.banner grabbing to detect the firewall.

step3 perform banner grabbing.

perform banner grabbing technique to detect the services run by the firewall.if Firewall is detected.then disable trusted host.aur perform firewalking to detect the firewall.

step4 perform fire working

you should use the firewalking technique to determine access information on the firewall.when Pro packets are sent.a Firewall is detected that disable the trusted host.

step 5 disable the trusted host

step 6 perform IP address spoofing

you should perform IP address going to gain unauthorised access to a computer on the network.

step 7 perform source routing

step 8 use an IP address in place of URL

step 9 perform of fragmentation attac

.you should perform and IP fragmentation attack to Pota TCP header information.into the next fragment in order to bypass the firewall

step 10.use anonymous website shopping sites.you should use anonymous websites offering size to hide your identity from the internet.

step 11 use proxy servers.

you should use proxy servers that block the actual IP address.and display another.thereby allowing access to a blocked website

step 12 perform icmp tunneling

you should perform icmp tunneling to tunnel backdoor application in the data portion of icmp packets.

step13 perform ACK tunneling

you should perform ACK tunnelling using tools such as AckCmd to tunnel backdoor application.with TCP packets with the ACK bit set