Chapter 12: Evading IDS, Firewall and Honeypots

Technology Brief

IDS, Firewall and Honeypot Concepts

As the awareness of cyber and network security is increasing day by day, it is very important to understand the core concepts of Intrusion Detection/Defense System (IDS) as well as Intrusion Prevention System(IPS). IDS and IPS often create confusion as both modules are created by multiple vendors and different terminologies used to define the technical concepts are also same. Sometimes the same technology may be used for detection and prevention of some threat.

Just like other products, Cisco also has developed a number of solutions for implementing IDS/IPS for the security of the network. In the first phase of this section, different concepts will be discussed before moving to the different implementation methodologies.

Intrusion Detection Systems (IDS)

The placement of sensor within a network differentiates the functionality of IPS over the IDS. When sensor is placed in line with the network, i.e., the common in/out of specific network segment terminates on a hardware or logical interface of the sensor and goes out from second hardware or logical interface of the sensor, then every single packet will be analyzed and pass through sensor only if does not contain anything malicious. By dropping the traffic malicious traffic, the trusted network or a segment of it can be protected from known threats and attacks. This is the basic working of Intrusion Prevention System (IPS). However, the inline installation and inspection of traffic may result in a slighter delay. IPS may also become a single point of failure for the whole network. If 'fail-open' mode is used, the good and malicious traffic will be allowed in case of any kind of failure within IPS sensor. Similarly, if 'fail-close' mode is configured, the whole IP traffic will be dropped in case of sensor's failure.

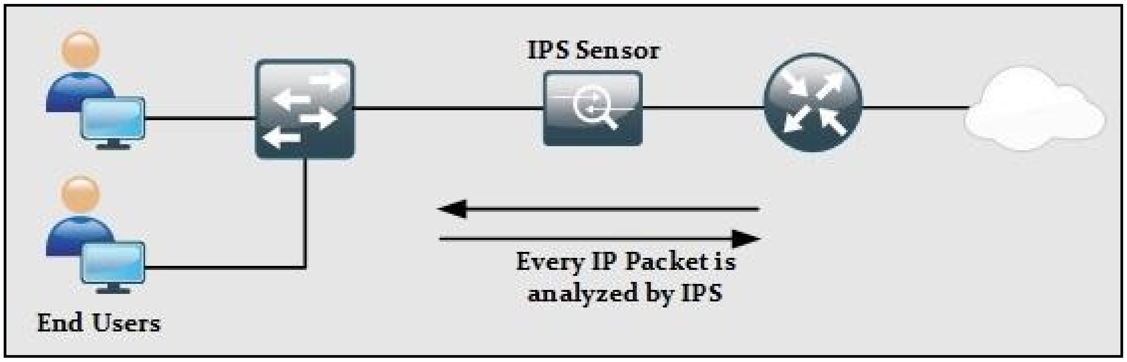


Figure 12-01. In-line Deployment of IPS Sensor

If a sensor is installed in the position as shown below, a copy of every packet will be sent to the sensor to analyze any malicious activity.

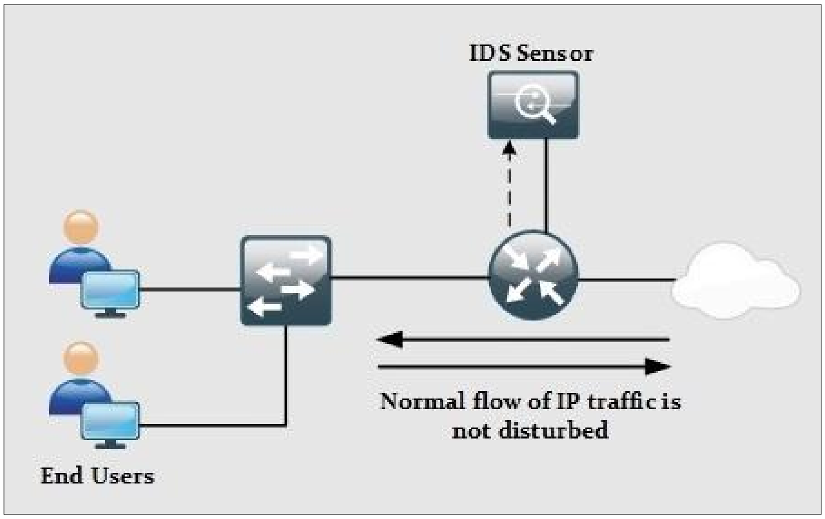


Figure 12-02. Sensor deployment as IDS

In other means, the sensor, running in promiscuous mode will perform the detection and generate an alert if required. As the normal flow of traffic is not disturbed, no end-to-end delay will be introduced by implementing IDS. The only downside of this configuration is that IDS will not be able to stop malicious packets from entering the network because IDS is not controlling the overall path of traffic.

The following table summarizes and compares various features of IDS and IPS.

Feature	IPS	IDS
Positioning	In-line with the network. Every packet goes through it.	Not in-line with the network. It receives the copy of every packet.
Mode	In-line/Tap	Promiscuous
Delay	Introduces delay because every packet is analyzed before forwarded to the destination	Does not introduce delay because it is not in-line with the network.
Point of failure?	Yes. If the sensor is down, it may drop as well as malicious traffic from entering the network, depending on one of the two modes configured on it, namely fail-open or fail-close	No impact on traffic as IDS is not in-line with the network
Ability to mitigate an attack?	Yes. By dropping the malicious traffic, attacks can be readily	IDS cannot directly stop an attack. However, it

	reduced on the network. If deployed in TAP mode, then it will get a copy of each packet but cannot mitigate the attack	assists some in-line device like IPS to drop certain traffic to stop an attack.
Can do packet manipulation?	Yes. Can modify the IP traffic according to a defined set of rules.	No. As IDS receive mirrored traffic, so it can only perform the inspection.

Table 12-01. IDS/IPS Comparison

Ways to Detect an Intrusion

When a sensor is analyzing traffic for something strange, it uses multiple techniques base on the rules defined in the IPS/IDS sensor. Following tools and techniques can be used in this regard:

- Signature-based IDS/IPS
- Policy-based IDS/IPS
- Anomaly-based IDS/IPS
- Reputation-based IDS/IPS

Signature-based IDS/IPS: A signature looks for some specific string or behavior in a single packet or stream of packets to detect the anomaly. Cisco IPS/IDS modules, as well as next-generation firewalls, come with preloaded digital signatures which can be used to mitigate against already discovered attacks. Cisco constantly updates the signatures set which also needs to upload to a device by the network administrator.

Not all signatures are enabled by default. If some signature is generating an alert for traffic which is intended to be allowed due to some business needs, the network administrator needs to tune the IPS/IDS module so that false positive generated for legitimate traffic must not be generated.

Policy-Based IDS/IPS: As the name suggests, policy-based IDS/IPS module works based on the policy or SOP of an organization. For example, if an organization has a security policy that every management session with networking devices as well as end-devices must not initiate via TELNET protocol. A custom rule specifying this policy needs to be defined on sensors. If it is configured on IPS, whenever TELNET traffic hits the IPS, an alert will be generated followed by the drop of packets. If it is implemented on IDS based sensor, then an alert will generate for it, but traffic keeps flowing because IDS works in promiscuous mode.

Anomaly-Based IDS/IPS: In this type, a baseline is created for specific kind of traffic. For example, after analyzing the traffic, it is noticed that 30 half-open TCP sessions are created every minute. After deciding the baseline, say 35 half-open TCP connections in a minute, assume the number of half-open TCP connected has increased to 150 then based on this anomaly, IPS will drop the extra half-open connections and generate alert for it.

Reputation-Based IDS/IPS: If there is some sort of global attack, For example, recent DDoS attacks on servers of twitter and some other social websites. It would be great to filter out the known traffic which results in propagation of these attacks before it hits the organizations critical infrastructure. Reputation-based IDS/IPS collect information from systems participating in global correlation. Reputation-based IDS/IPS include relative descriptors like known URLs, domain names, etc. Global correlation services are maintained by Cisco Cloud Services.

The following table summarizes the different technologies used in IDS/IPS along with some advantages over disadvantages.

IDS/IPS Technology	Advantages	Disadvantages
Signature-Based	Easier Implementation and management.	Does not detect the attacks which can bypass the signatures. May require some tweaking to stop generating false positive for legitimate traffic.
Anomaly-Based	Can detect malicious traffic based on the custom baseline. It can deny any kind of latest attacks as they will not be defined within the scope of baseline policy.	It requires baseline policy. Difficult to baseline large network designs. It may generate false positives due to misconfigured baseline.
Policy-Based	It is a simple implementation with reliable results. Everything else outside the scope of defined policy will be dropped.	It requires manual implementation of policy. Any slighter change within a network will require a change in policy configured in IPS/IDS module
Reputation-Based	Uses the information provided by Cisco Could Services in which systems share their experience with network	Requires regular updates and participation in Cisco Could service of global correlation in which systems share their experience with other members.

	attacks. Someone's experience become protection for organization's	

Table 12-02. Comparison of Techniques used by IDS/IPS sensors

Types of Intrusion Detection Systems

Depending on the network scenario, IDS/IPS modules are deployed in one of the following configurations:

- Host-based Intrusion Detection
- Network-based Intrusion Detection

Host-based IPS/IDS is normally deployed for the protection of specific host machine, and it works closely with the Operating System Kernel of the host machine. It creates a filtering layer and filters out any malicious application call to the OS. There are four major types of Host-based IDS/IPS:

- **File System Monitoring:** In this configuration, IDS/IPS works by closely comparing the versions of files within some directory with the previous versions of same file and checks for any unauthorized tampering and changing within a file. Hashing algorithms are often used to verify the integrity of files and directories which gives an indication of possible changes which are not supposed to be there.

- **Log Files Analysis:** In this configuration, IDS/IPS works by analyzing the log files of the host machine and generates warning for system administrators who are responsible for machine security. Several tools and applications are available which works by analyzing the patterns of behavior and further correlate it with actual events.

- **Connection Analysis:** IDS/IPS works by monitoring the overall network connections being made with the secure machine and tries to figure out which of them are legitimate and how many of them are unauthorized. Examples of techniques used are open ports scanning, half open and rogue TCP connections and so forth.

- **Kernel Level Detection:** In this configuration, the kernel of OS itself detects the changing within the system binaries, and an anomaly in system calls to detect the intrusion attempts on that machine.

The network-based IPS solution works as in-line with the perimeter edge device or some specific segment of the overall network. As network-based solution works by monitoring the overall network traffic (or data packets in specific) so it should be as fast as possible in terms of processing power so that overall latency may not be introduced in the network.

Depending on vendor and series of IDS/IPS, it may use one of above technologies in its working.

The following table summarizes the difference between the host based and network-based IDS/IPS solution:

Feature	Host-based IDS/IPS	Network-based IDS/IPS
Scalability	Not scalable as the number of secure hosts increases	Highly scalable. Normally deployed at perimeter gateway.
Cost-effectiveness	Low. More systems mean more IDS/IPS modules	High. One pair can monitor the overall network.
Capability	Capable of verifying if an attack was succeeded or not	Only capable of generating an alert of an attack
Processing Power	The processing power of host device is used.	Must have high processing power to overcome latency issues

Table 12-03. Host-based vs. Network-based IDS/IPS solution.

Firewall

The primary function of using a dedicated device named as the firewall at the edge of the corporate network is isolation. A firewall prevents the direct connection of internal LAN with internet or outside world. This isolation can be performed in multiples way but not limited to:

- **A Layer 3 device** using an Access List for restricting the specific type of traffic on any of its interfaces.
- **A Layer 2 device** using the concept of VLANs or Private VLANs (PVLAN) for separating the traffic of two or more networks.
- **A dedicated host device** with software installed on it. This host device, also acting as a proxy, filters the desired traffic while allowing the remaining traffic.

Although the features above provide isolation in some sense, The following are the few reasons a dedicated firewall appliance (either in hardware or software) is preferred in production environments:

Risks	Protection by firewall
Access by untrusted entities	Firewalls try to categorize the network into different portions. One portion is considered as a trusted portion of internal LAN. Public internet and interfaces connected to are considered as an untrusted portion. Similarly, servers accessed by untrusted entities are placed in a special segment known as a demilitarized

	zone (DMZ). By allowing only specific access to these servers, like port 90 of the web server, firewall hide the functionality of network device which makes it difficult for an attacker to understand the physical topology of the network.
Deep Packet Inspection and protocols exploitation	One of the interesting features of the dedicated firewall is their ability to inspect the traffic more than just IP and port level. By using digital certificates, Next Generation Firewalls available today can inspect traffic up to layer 7. A firewall can also limit the number of established as well as half-open TCP/UDP connections to mitigate DDoS attacks
Access Control	By implementing local AAA or by using ACS/ISE servers, the firewall can permit traffic based on AAA policy.
Antivirus and protection from infected data	By integrating IPS/IDP modules with firewall, malicious data can be detected and filtered at the edge of the network to protect the end-users

Table 12-04. Firewall Risk Mitigation Features

Although firewall provides great security features as discussed in the table above, any misconfiguration or bad network design may result in serious consequences. Another important deciding factor of deploying a firewall in current network design depends on whether current business objectives can bear the following limitations:

- **Misconfiguration and Its Consequences:** The primary function of a firewall is to protect network infrastructure in a more elegant way than a traditional layer3/2 devices. Depending on different vendors and their implementation techniques, many features need to be configured for a firewall to work properly. Some of these features may include Network Address Translation (NAT), Access-Lists(ACL), AAA base policies and so on. Misconfiguration of any of these features may result in leakage of digital assets which may have a financial impact on business. In short, complex devices like firewall also requires deep insight knowledge of equipment along with the general approach to deployment.
- **Applications and Services Support:** Most of the firewalls use different techniques to mitigate the advanced attacks. For example, NATing is one of the most commonly used features in firewalls, and it is used to mitigate the reconnaissance attacks. In situations where network infrastructure is used to support custom-made applications, it may be required to re-write the whole application in order to work properly under new network changes.

- **Latency:** Just like implementing NATing on a route adds some end to end delay, firewall along with heavy processing demanding features add a noticeable delay over the network. Applications like Voice Over IP (VOIP) may require special configuration to deal with it.

Another important factor to be considered while designing the security policies of network infrastructure uses the layered approach instead of relying on a single element. For example, consider the following scenario:

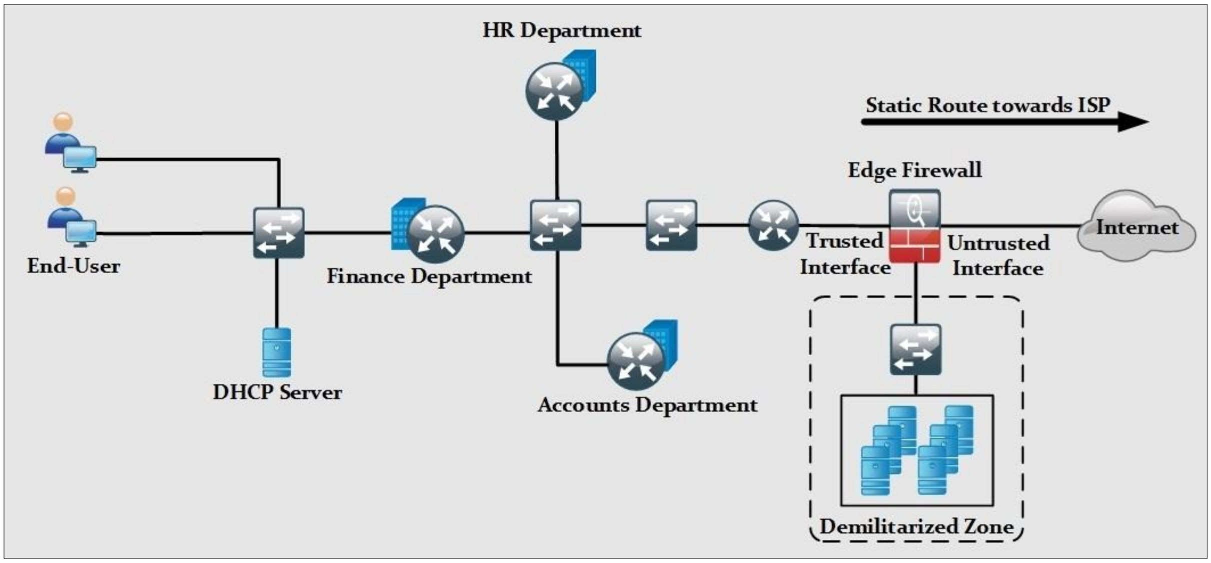


Figure 12-03. Positioning Firewall in a production environment

The previous figure shows a typical scenario of SOHO and mid-sized corporate environment where whole network infrastructure is supported by a couple of routers and switches. If the edge firewall is supposed to be the focal point of security implementation, then any slighter misconfiguration may result in high scale attacks. In general, a layered security approach is followed, and packet passes through multiple security checks before hitting the intended destination.

The position of firewall varies in different design variants. In some designs, it is placed on the perimeter router of the corporation while in some designs it is placed at the edge of the network as shown in the last figure. Irrelevant to the position, it is a good practice to implement the layered security in which some of the features like unicast reverse path forwarding, access-lists, etc. are enabled on perimeter router. Features like deep packet inspection, digital signatures are matched on the firewall. If everything looks good, the packet is allowed to hit the intended destination address.

Network layer firewalls permit or drop IP traffic based on Layer 3 and 4 information. A router with access-list configured on its interfaces is a common example of network layer firewall. Although very fast in operation and, network layer firewalls do not perform deep packet inspection techniques and detect any malicious activity.

Apart from acting as the first line of defense, network layer firewalls are also deployed within internal LAN segments for enhanced layered security and isolation.

Firewall Architecture

1. *Bastion Host*

Bastion Host is a computer system that is placed in between public and private network. It is intended to be the crossing point where all traffic is passed through. Certain roles and responsibilities are assigned to this computer to perform. Bastion host has two interfaces, one connected to the public network while the another is connected to the private network.

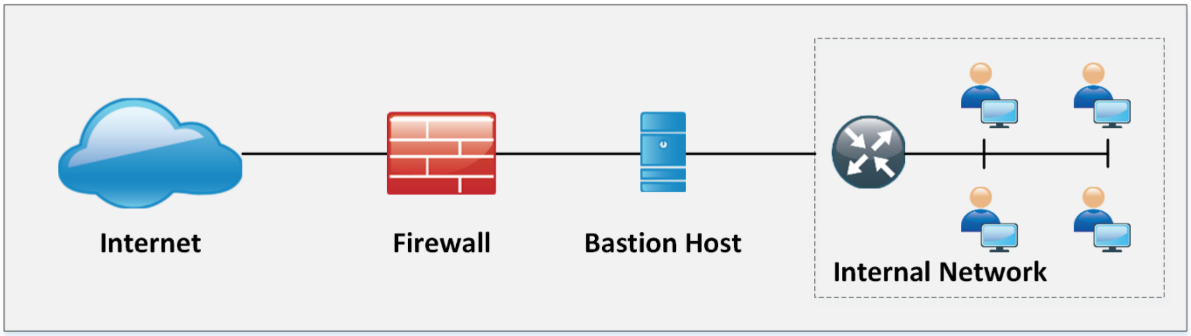


Figure 12-04. Bastion Host

2. *Screened Subnet*

Screened Subnet can be set up with a firewall with three interfaces. These three interfaces are connected with the internal private network, Public network, and Demilitarized Zone (DMZ). In this architecture, each zone is separated by another zone hence compromise of one zone will not affect another zone.

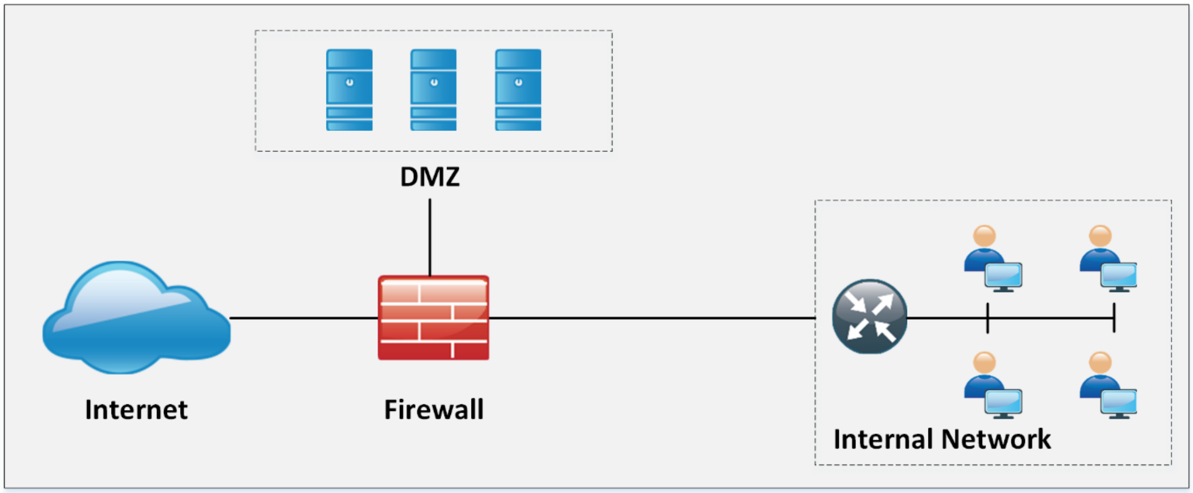


Figure 12-05. Screened Subnet

3. *Multi-homed Firewall*

Multi-homed firewall referred to two or more networks where each interface is connected to its network. It increases the efficiency and reliability of a network. A firewall with two or more interfaces allows further subdivision.

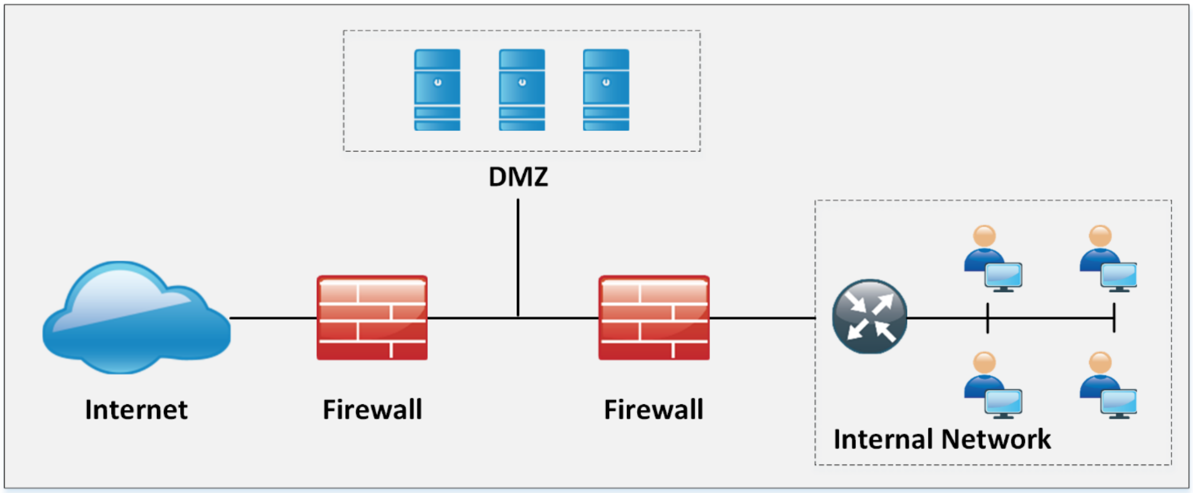


Figure 12-06. Multi-Homed Firewall

DeMilitarized Zone (DMZ)

IOS zone-based firewalls is a specific set of rules which may help to mitigate mid-level security attacks in environments where security is also meant to be implemented via routers. In zone-based firewalls(ZBF), interfaces of devices are placed to different unique zones like (inside, outside or DMZ) and then policies are applied on these zones. Naming conventions for zones must be easier to understand in order to be helpful at the hour of troubleshooting.

ZBFs also uses stateful filtering which means that if the rule is defined to permit originating traffic from one zone, say inside to another zone like DMZ, then return traffic would automatically be allowed. Traffic from different zones can be allowed using policies permiting the traffic in each direction.

One of the advantages of applying policies on zones instead of interfaces is that whenever new changes required at the interface level, then simply removing or adding interface in particular zone apply policies on it automatically.

ZBF may use the following feature set in its implementation:

- Stateful inspection
- Packet filtering
- URL filtering
- Transparent firewall
- Virtual Routing Forwarding (VRF)

This figure shows the scenario explained above:

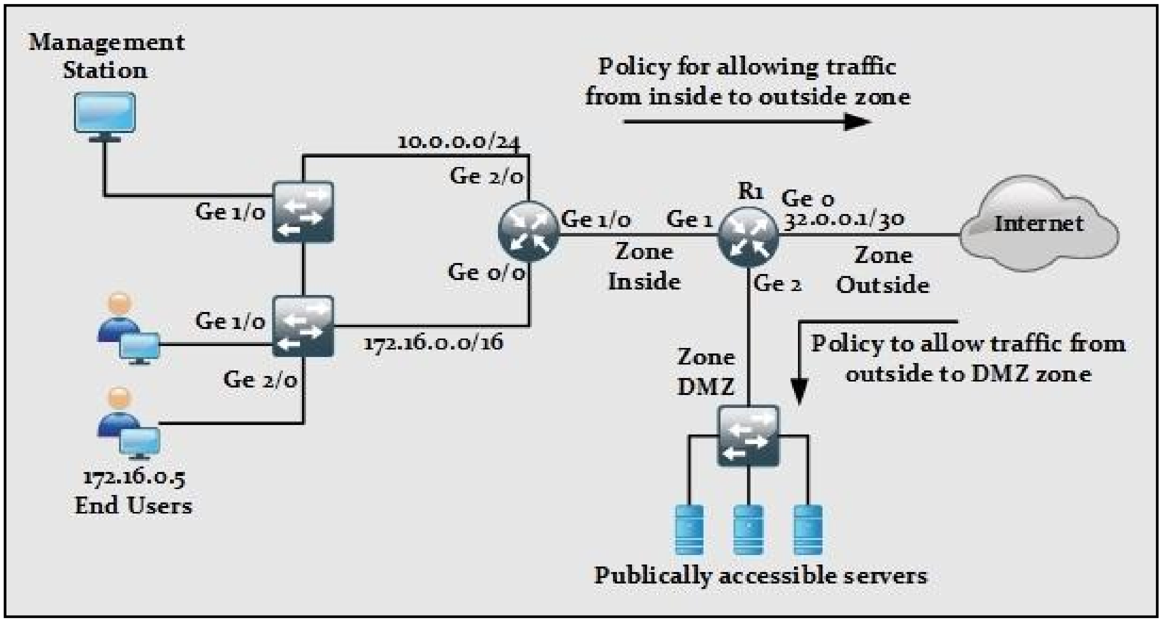


Figure 12-07. Cisco IOS Zone-Based Firewall Scenario

Types of Firewall

1. *Packet Filtering Firewall*

Packet Filtering Firewall includes the use of access-lists to permit or deny traffic based on layer 3 and layer 4 information. Whenever a packet hits an ACL configured layer 3 device's interface, it checks for a match in an ACL (starting from the first line of ACL). Using an extended ACL in Cisco device, following information can be used for matching traffic:

- Source address
- Destination address
- Source port
- Destination port
- Some extra features like TCP established sessions etc.

This table shows the advantages and disadvantages of using packet filtering techniques:

Advantages	Disadvantages
Ease of implementation by using permit and deny statements.	Cannot mitigate IP spoofing attacks. An attacker can compromise the digital assets by spoofing IP source address to one of the permit statements in the ACL
Less CPU intensive than deep packet inspection techniques	Difficult to maintain when ACLS size grows
Configurable on almost every Cisco IOS	Cannot implement filtering based on session states.

Even a mid-range device can perform ACL based filtering	Scenarios in which dynamic ports are used, a range of ports will be required to be opened in ACL which may also be used by malicious users

Table 12-05. Advantages and Disadvantages of Packet Filtering Techniques

2. *Circuit-Level Gateway Firewall*

Circuit Level gateway firewall operates at the session layer of the OSI model. They capture the packet to monitor TCP Handshaking, in order to validate if the sessions are legitimate. Packets forwarded to the remote destination through a circuit-level firewall appears to have originated from the gateway.

3. *Application-Level Firewall*

Application Level Firewall can work at layer 3 up to the layer 7 of OSI model. Normally, a specialized or open source software running on high-end server acts as an intermediary between client and destination address. As these firewalls can operate up to layer 7, more granular control of packets moving in and out of network is possible. Similarly, it becomes very difficult for an attacker to get the topology view of inside or trusted network because connection requests terminate on Application/Proxy firewalls.

Some of the advantages and disadvantages of using application/proxy firewalls are:

Advantages	Disadvantages
Granular control over the traffic is possible by using information up to layer 7 of OSI model.	As proxy and application, firewalls run in software. A very high-end machine may be required to full fill the computational requirements.
The indirect connection between end devices makes it very difficult to generate an attack.	Just like NAT, not every application has support for proxy firewalls and few amendments may be needed in current applications architecture.
Detailed logging is possible as every session involves the firewall as an intermediary.	Another software may be required for logging feature which takes extra processing power.
Any commercially available hardware can be used to install and run proxy firewalls on it.	Along with computational power, high storage may be required in different scenarios.

Table 12-06. Advantages and Disadvantages of Application/Proxy Firewalls

4. *Stateful Multilayer Inspection Firewall*

As the name depicts, this saves the state of current sessions in a table known as a stateful database. Stateful inspection and firewalls using this technique normally deny any traffic between trusted and untrusted interfaces. Whenever an end-device from trusted interface wants to communicate with some destination address attached to the untrusted interface of the firewall, its entry will be made in a stateful database table containing layer 3 and layer 2 information. Following table compares different features of stateful inspection-based firewalls.

Advantages	Disadvantages
Helps in filtering unexpected traffic	Unable to mitigate application layer attacks
Can be implemented on a broad range of routers and firewalls	Except for TCP, other protocols do not have well-defined state information to be used by the firewall
Can help in mitigating denial of service (DDoS) attacks	Some applications may use more than one port for successful operation. Application architecture review may be needed in order to work after the deployment of stateful inspection based firewall.

Table 12-07. Advantages and Disadvantages of Stateful Inspection based Firewalls

5. *Transparent firewalls*

Most of the firewalls discussed above work on layer 3 and beyond. Transparent firewalls work exactly like above-mentioned techniques, but the interfaces of the firewall itself are layer 2 in nature. IP addresses are not assigned to any interface, think of it as a switch with ports assigned to some VLAN. The only IP address assigned to the transparent firewall is for management purposes. Similarly, as there is no addition of extra hop between end-devices, the user will not be able to be aware of any new additions to network infrastructure and custom- made applications may work without any problem.

6. *Next Generation (NGFW) firewalls*

NGFW is relatively a new term used for latest firewalls with the advanced feature set. This kind of firewalls provides in-depth security features to mitigate against known threats and malware attacks. An example of next-generation firewalls is Cisco ASA series with FirePOWER services. NGFW provides complete visibility into network traffic users, mobile devices, virtual machine (VM) to VM data communication, etc.

7. *Personal Firewalls*

Personal Firewall is also known as desktop firewalls, helps the end-users personal computers from general attacks from intruders. Such firewalls appear to be great security line of defense for users who are constantly connected to the internet via DSL or cable modem. Personal firewalls help by providing inbound and outbound filtering, controlling internet connectivity to and from the computer (both in a domain based and workgroup mode) and altering the user for any attempts of intrusions.

Honeypot

Honeypots are the devices or system that are deployed to trap attackers attempting to gain unauthorized access to the system or network as they are deployed in an isolated environment and being monitored. Typically, honeypots are deployed in DMZ and configured identically to a server. Any probe, malware, infection, the injection will be immediately detected by this way as honeypots appear to be a legitimate part of the network.

Types of Honeypots

1. ***High-Interaction Honeypots***

High-Interaction Honeypots are configured with a verity of services which is basically enabled to waste the time of an attacker and gain more information from this intrusion. Multiple honeypots can be deployed on a single physical machine to be restored if attacker even compromised the honeypot.

2. ***Low-Interaction Honeypots***

Low-Interaction Honeypots are configured to entertain only the services that are commonly requested by the users. Response time, less complexity and few resources make Low-interaction honeypot deployment more easy as compared to High-interaction honeypots.

Detecting Honeypots

The basic logic of detecting a honeypot in a network is by probing the services. The attacker usually crafts a malicious packet to scan running services on the system and open and closed ports information. These services may be HTTPS, SMTPS or IMAPS or else. Once attacker extracts the information, it can attempt to build a connection, the actual server will complete the process of three-way handshaking but the deny of handshaking indicates the presence of a honeypot. Send-Safe Honeypot Hunter, Nessus, and Hping tools can be used to detect honeypots.

IDS, Firewall and Honeypot System

Intrusion Detection Tools

Snort

Snort is an open source intrusion prevention system which delivers the most effective and comprehensive real-time network defense solutions. Snort is capable of protocol analysis, real-time packet analysis, and logging. It can also search and filter content, detect a wide variety of attacks and probes including buffer overflows, port scans, SMB probes and much more. Snort can also be used in various forms including a packet sniffer, a packet logger, network file logging device, or as a full-blown network intrusion prevention system.

Snort Rule

Rules are a criterion for performing detection against threats and vulnerabilities to the system and network, which leads to the advantage of zero-day detection. Unlike signatures, rules are focused on detecting the actual vulnerabilities. There are two ways to get Snort rules:

1. Snort Subscribers Rule
2. Snort Community Rule

There is no much difference in between Snort Subscribers rule and Community rule. However, Subscriber rules are updated frequently and updated on the device as well. It requires a paid subscription to get real-time updates of Snort Rules. Community rules are updated by Snort Community containing all rules as the Subscribers set of the rule contains but they are not updated quickly as subscriber rule is.
Snort rules are comprised of two logical sections: -

1. ***The rule header***

The rule header contains the rule's action, protocol, source and destination IP addresses and netmasks, and the source and destination ports information.

2. ***The rule options***

The rule option section contains alert messages and information on which parts of the packet should be inspected to determine if the rule action should be taken.

Categories of Snort Rules

Snort rules are categorized into different categories and frequently updated by TALOS. Some of these categories are

Application Detection Rule Category includes the rules monitoring Controlling of traffic of certain application. These rules control the behavior and network activities of these applications.

- app-detect.rules

Black List Rules category include the URL, IP address, DNS and other rules that have been determined to be an indicator of malicious activities.

- blacklist.rules

Browsers Category include the rule for detection of vulnerabilities in certain browsers.

- browser-chrome.rules
- browser-firefox.rules
- browser-ie.rules
- browser-webkit
- browser-other

- browser-plugins

Operating System Rules category include rules looking for vulnerabilities in OS

- os-Solaris
- os-windows
- os-mobile
- os-Linux
- os-other

Similarly, there is a number of categories and types of rules.

Other Intrusion Detection Tools

- ZoneAlarm PRO Firewall 2015
- Comodo Firewall
- Cisco ASA 1000V Cloud Firewall

Firewalls for Mobile

- Android Firewall
- Firewall IP

Honeypot Tool

- KFSensor
- SPECTER
- PatriotBox
- HIHAT

Evading IDS

Insertion Attack

An Insertion attack is a type of evasion of IDS device by taking advantage of blindly believing of IDS. Intrusion Detection System (IDS) assumes that accepted packets are also accepted by the end systems, but there may be a possibility that end system may reject these packets. This type of attack is specially targeted to Signature-based IDS device in order to insert data into IDS. Taking advantage of vulnerability attacker can insert packets with a bad checksum or TTL values and send them out of order. IDS and end host, when reassembling the packet, they might have two different streams. For example, an attacker may send the following stream.

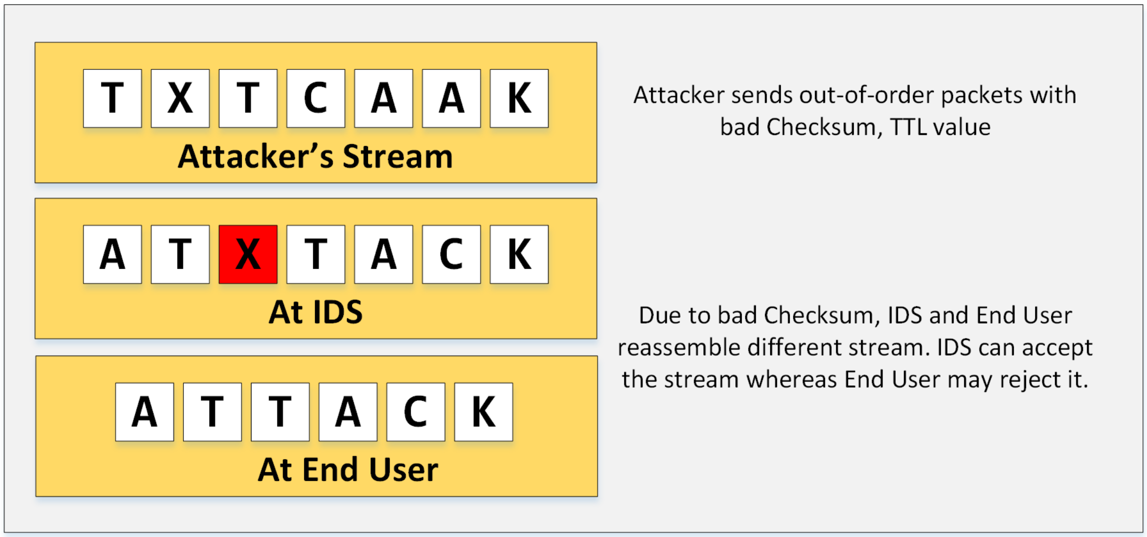

T X T C A A K
Attacker's Stream
A T X T A C K
At IDS
A T T A C K
At End User
Attacker sends out-of-order packets with bad Checksum, TTL value
Due to bad Checksum, IDS and End User reassemble different stream. IDS can accept the stream whereas End User may reject it.

Figure 12-08. Insertion attack on IDS

Evasion

Evasion is a technique intended to send the packet that is accepted by the end system which is rejected by the IDS. Evasion techniques are intended to exploit the host. An IDS that mistakenly rejects such a packet misses its contents entirely. An attacker may take advantage of this condition and exploit it.

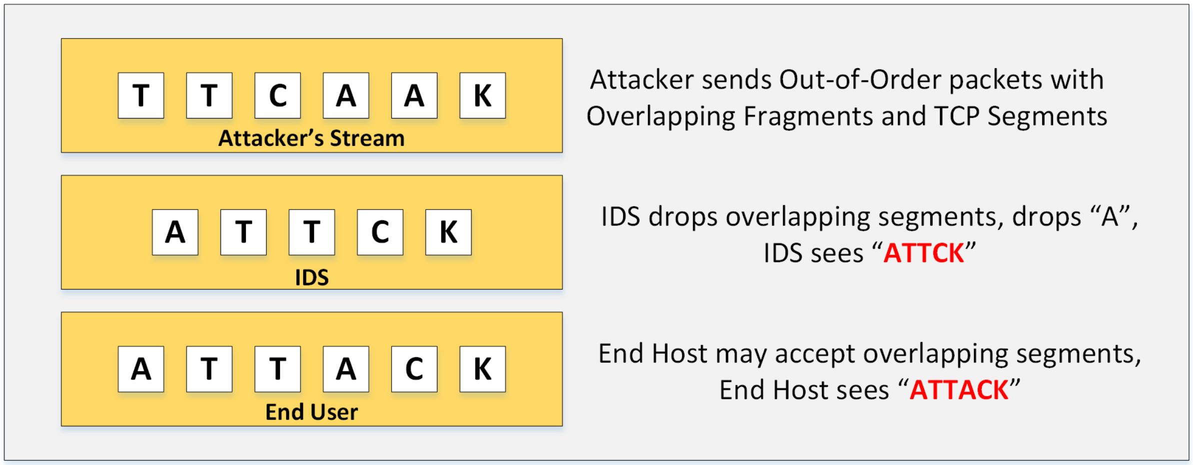

T T C A A K
Attacker's Stream
A T T C K
IDS
A T T A C K
End User
Attacker sends Out-of-Order packets with Overlapping Fragments and TCP Segments
IDS drops overlapping segments, drops "A", IDS sees "ATTCK"
End Host may accept overlapping segments, End Host sees "ATTACK"

Figure 12-09. IDS Evasion

Fragmentation Attack

Fragmentation is the process of splitting the packet into fragments. This technique is usually adopted when IDS and Host device is configured with different timeouts. For example, if an IDS is configured with 10 Seconds of timeout whereas host is configured with 20 seconds of a timeout. Sending packets with 15sec delay will bypass reassembly at IDS and reassemble at the host.

Similarly, overlapping fragments are sent. In Overlapping fragmentation, a packet with the TCP sequence number configured is overlapping. Reassembly of these overlapping, fragmented packets is based on how an operating system configured to do. Host OS may use original fragmentation whereas IOS devices may use subsequent fragment using offset.

Denial-of-Service Attack (DoS)

Passive IDS devices are inherently Fail-open instead of Fail-Closed. Taking advantage of this limitation, an attacker may launch a Denial-of-Service attack on the network to overload the IDS System. To perform DoS attack on IDS, an attacker may target CPU exhaustion or Memory Exhaustion techniques to overload the IDS. These can be done by sending specially crafted packet consuming more CPU resources or sending a large number of fragmented out-of-order packets.

Obfuscating

Obfuscation is the encryption of payload of a packet destined to a target in a manner that target host can reverse it but the IDS could not. It will exploit the end user without alerting the IDS using different techniques such as encoding, encryption, polymorphism. Encrypted protocols are not inspected by the IDS unless IDS is configured with the private key used by the server to encrypt the packets. Similarly, an attacker may use polymorphic shellcode to create unique patterns to evade IDS.

False Positive Generation

False Positive alert generation is the false indication of a result inspected for a particular condition or policy. An attacker may generate a large number of false positive alert by sending a Suspicious packet to manipulate and hide real malicious packet within this packet to pass IDS.

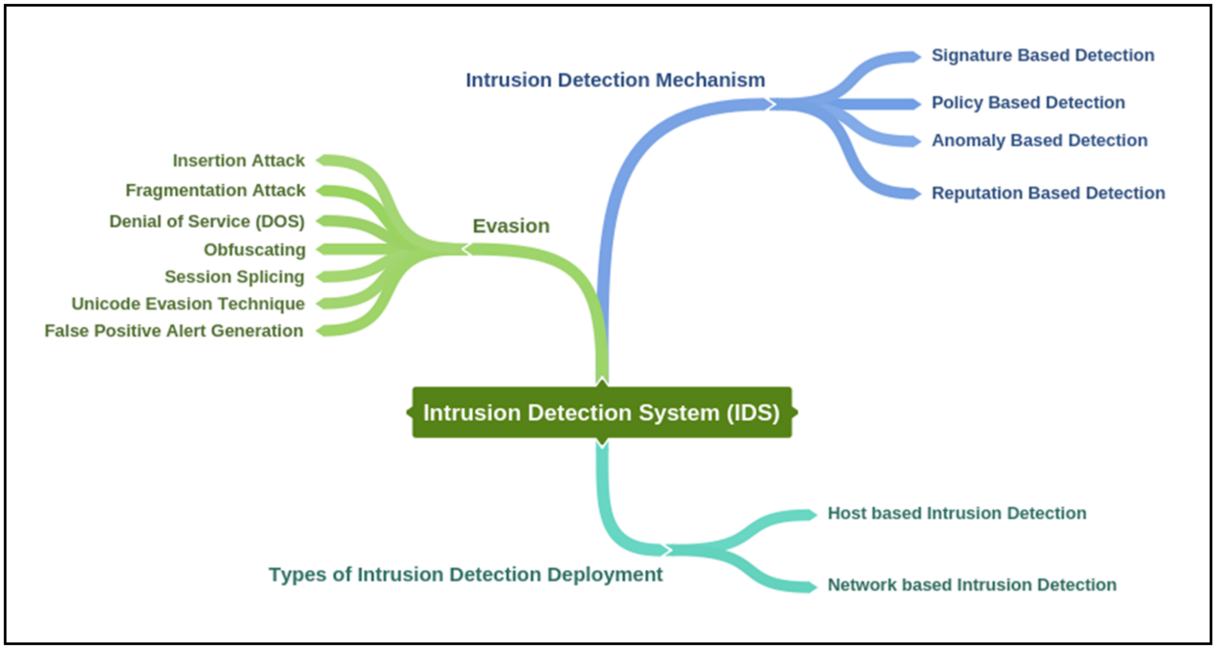
Session Splicing

Session Splicing is a technique in which attacker splits the traffic into a large number of the smaller packet in a way that not even a single packet triggers the alert. This can also be done by a slightly different technique such as adding a delay between packets. This technique is effective for those IDS which do not reassemble the sequence to check against intrusion.

Unicode Evasion Technique

Unicode evasion technique is another technique in which attacker may use Unicode to manipulate IDS. Unicode is basically a character encoding as defined earlier in HTML Encoding section. Converting string using Unicode characters can avoid signature matching and alerting the IDS, thus bypassing the detection system.

Mind Map


Intrusion Detection System (IDS)
Intrusion Detection Mechanism
Signature Based Detection
Policy Based Detection
Anomaly Based Detection
Reputation Based Detection
Evasion
Insertion Attack
Fragmentation Attack
Denial of Service (DOS)
Obfuscating
Session Splicing
Unicode Evasion Technique
False Positive Alert Generation
Types of Intrusion Detection Deployment
Host based Intrusion Detection
Network based Intrusion Detection

Evading Firewalls

Firewall Identification

Identification of firewall includes firewall fingerprinting to obtain sensitive information such as open ports, version information of services running in a network, etc. This information is extracted by different techniques such as Port scanning, Fire-walking, Banner grabbing, etc.

Port Scanning

Port Scanning is the examination procedure that is mostly used by the attackers to identify the open port. However, it may also be used by the legitimate users. Port scanning it does not always lead to an attack as it used by both of them. However, it is a network reconnaissance that can be used before an attack to collect information. In this scenario, special packets are forwarded to a particular host, whose response is examined by the attacker to get information regarding open ports.

Fire-walking

Fire-walking is a technique in which an attacker, using ICMP packet find out the location of firewall and network map by probing the ICMP echo request with TTL values exceeding one by one. It helps the attacker to find out a number of hops.

Banner Grabbing

Banner grabbing is another technique in which information from a banner is grabbed. Different devices such as routers, firewalls, and web server even display a banner in the console after login through FTP, telnet. Vendor information for a target device and firmware version information can be extracted using banner grabbing.

IP Address Spoofing

As defined earlier in the workbook, IP Address Spoofing is a technique, that is used to gain unauthorized access to machines by spoofing IP address. An attacker illicitly impersonates any user machine by sending manipulated IP packets with spoofed IP address. Spoofing process involves modification of header with a spoofed source IP address, a checksum, and the order values.

Source Routing

Source routing is a technique of sending the packet via selected route. In session hijacking, this technique is used to attempt IP spoofing as a legitimate host with the help of Source routing to direct the traffic through the path identical to the victim's path.

By passing Techniques

Bypassing Blocked Sites Using IP Address

In this technique, Blocked Website in a network is accessed using IP address. Consider a firewall blocking the incoming traffic destined to a particular domain. It can be accessed by typing IP address in URL instead of entering domain name unless IP address is also configured in access control list.

Bypass Blocked Sites Using Proxy

Accessing the blocked websites using a proxy is very common. There are a lot of online proxy solution available which hide your actual IP address to allow to access restricted websites.

Bypassing through ICMP Tunneling Method

ICMP tunneling is a technique of injecting arbitrary data in the payload of echo packet and forwarded to target host. ICMP tunneling functions on ICMP echo requests and reply packets. Basically using this ICMP tunneling, TCP communication is tunneled over ping request and replies because payload field of ICMP packets are not examined by most of the firewalls, whereas some network administrators allow ICMP because of troubleshooting purpose.

Bypassing Firewall through HTTP Tunneling Method

HTTP tunneling is another way to bypass firewalls. Consider a company with a web server listening traffic on port 80 for HTTP traffic. HTTP tunneling allows the attacker to despite the restriction imposed by the firewall by encapsulating the data in HTTP traffic.

The firewall will allow the port 80; an attacker may perform the various task by hiding into HTTP such as using FTP via HTTP protocol.

HTTP Tunneling Tools

- HTTPort
- HTTHost
- Super Network Tunnel
- HTTP-Tunnel

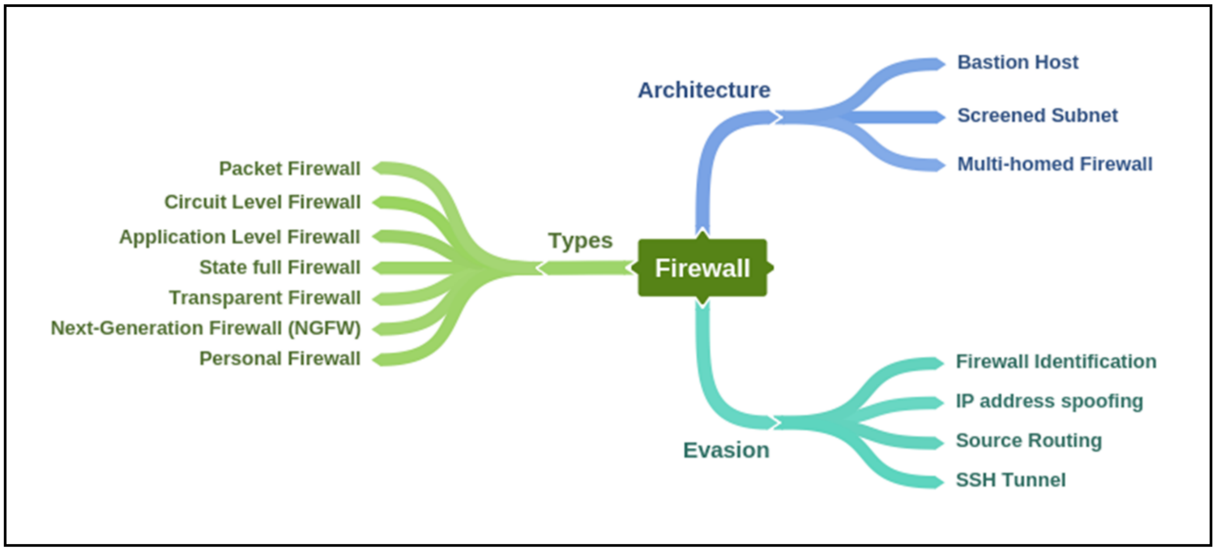
Bypassing through SSH Tunneling Method

OpenSSH is an encryption protocol that is basically used for securing the traffic from different threats and attacks such as eavesdropping, hijacking, etc. SSH connection is mostly used by applications to connect to the application servers. The attacker uses OpenSSH to encrypt the traffic to avoid detection by security devices.

Bypassing Firewall through External Systems

Bypassing through the external system is a process of hijacking a session of a legitimate user of a corporate network which is allowed to connect to an external network. An attacker can easily sniff the traffic to extract the information, stealing SessionID, cookies and impersonate him to bypass the firewall. An attacker can also infect the external system used by the legitimate user with malware or Trojan to steal information.

Mind Map



IDS/Firewall Evasion Counter-measures

Managing and preventing an evasion technique is a great challenge. There are so many techniques to make it difficult for an attacker to evade detection. These defensive and monitoring techniques ensure the detection system to protect the network and have more control over traffic. Some of these techniques are basic troubleshooting and monitoring, whereas some techniques are focused on proper configuration of IPS/IDS and firewalls. Initially, observe and troubleshoot the firewall by

- Port scanning
- Banner grabbing
- Fire-walking
- IP address spoofing
- Source routing
- Bypassing firewall using IP in URL
- Attempt a fragmentation attack
- Troubleshooting behavior using proxy servers
- Troubleshooting behavior using ICMP tunneling

Shutting down the unused ports, ports that are associated with known attacks in an effective step to prevent evasion. Perform in-depth analysis, resetting the malicious session, updating patches, IDS deployment, fragmented packet normalization, increasing TTL expiry, blocking TTL expired packet, reassembly of the packet at IDS, hardening the security and correctly enforcement of policies are effective step of preventing these attacks.

Lab 12-1: Configuring Honeypot on Windows Server 2016

Machines:

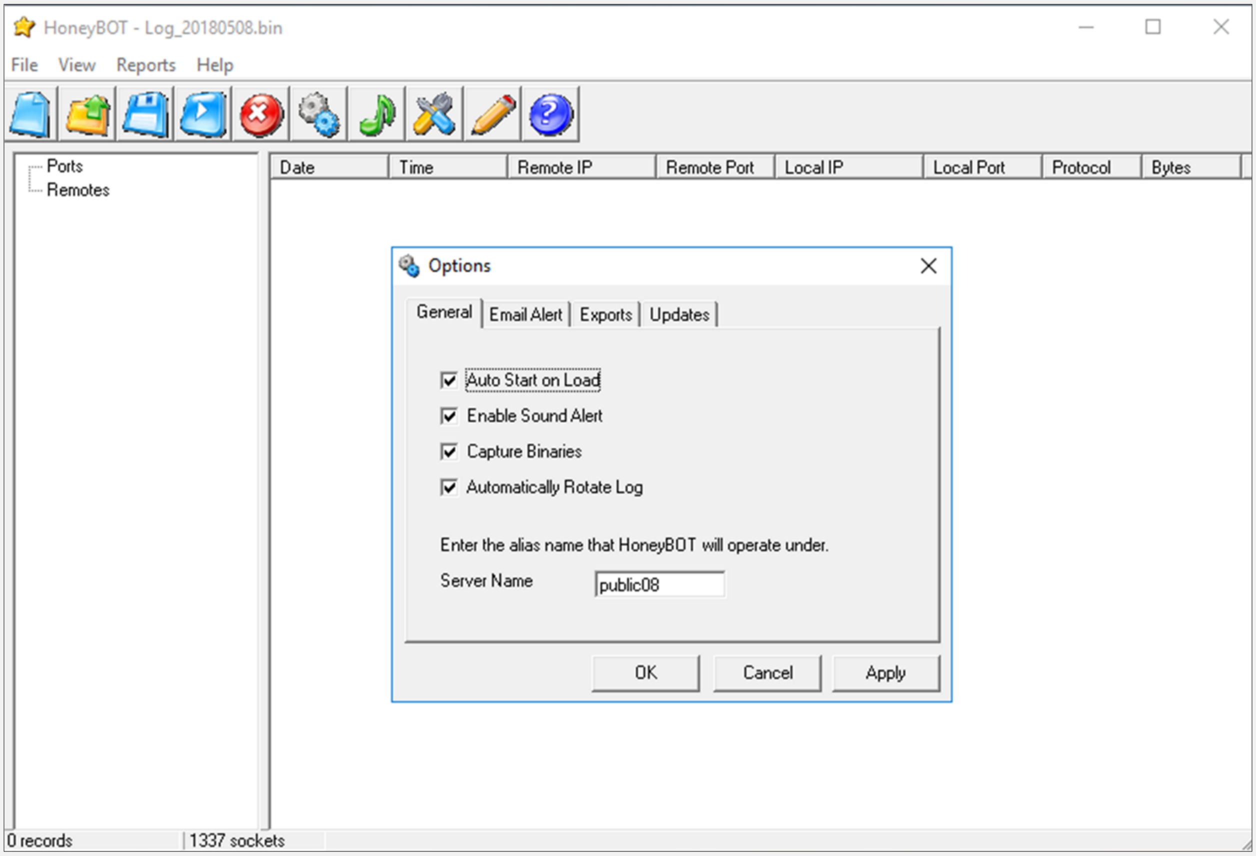
- Windows Server 2016 (VM)
- Windows 7 (VM)

Software used:

- HoneyBots (https://www.atomicsoftwaresolutions.com)

Procedure:

1. Open HoneyBot Application
2. Set parameters or leave it to default



HoneyBOT - Log_20180508.bin
File View Reports Help
Ports
Remotes
Date Time Remote IP Remote Port Local IP Local Port Protocol Bytes
Options
General Email Alert Exports Updates
OK Cancel Apply
0 records
1337 sockets

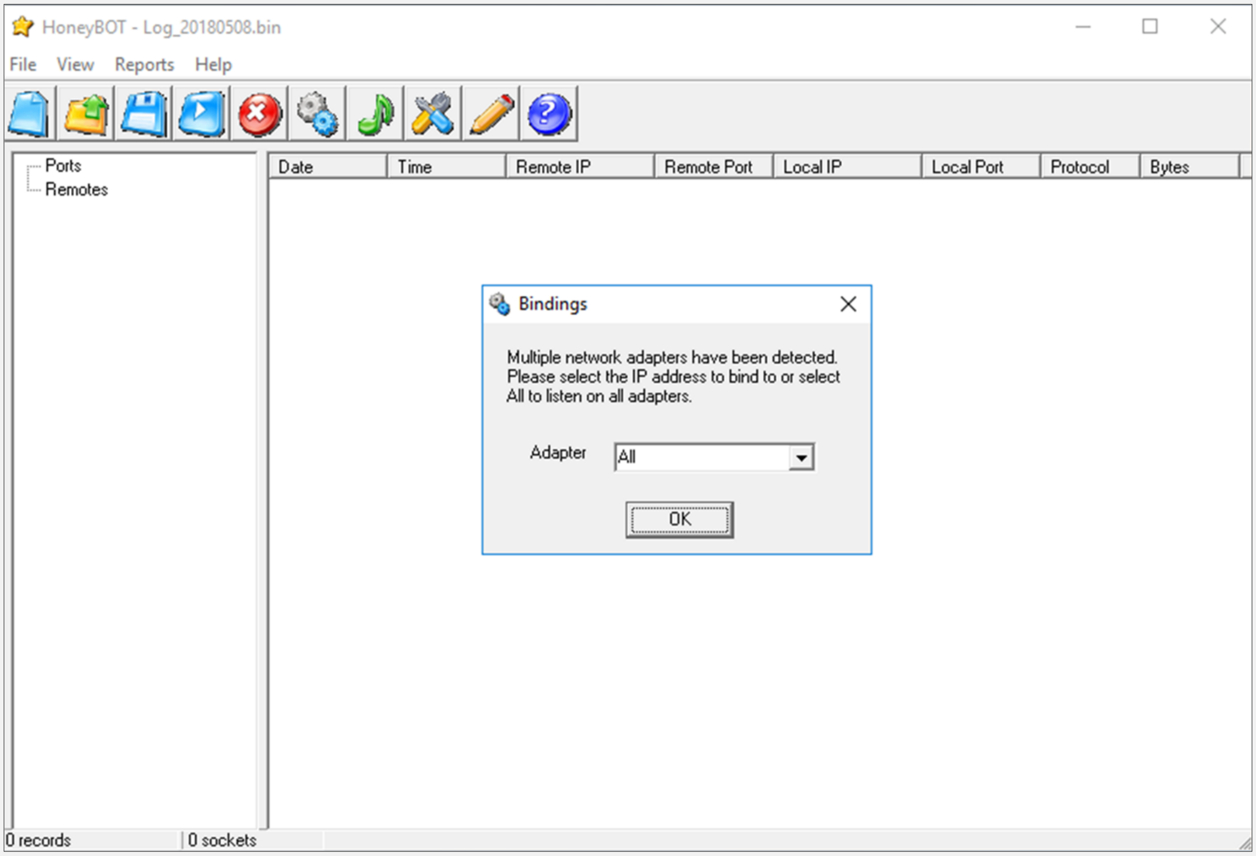
☑ Auto Start on Load
☑ Enable Sound Alert
☑ Capture Binaries
☑ Automatically Rotate Log

Enter the alias name that HoneyBOT will operate under.

Server Name: public08

Figure 12-10. HoneyBot Application

3. Select Adapters

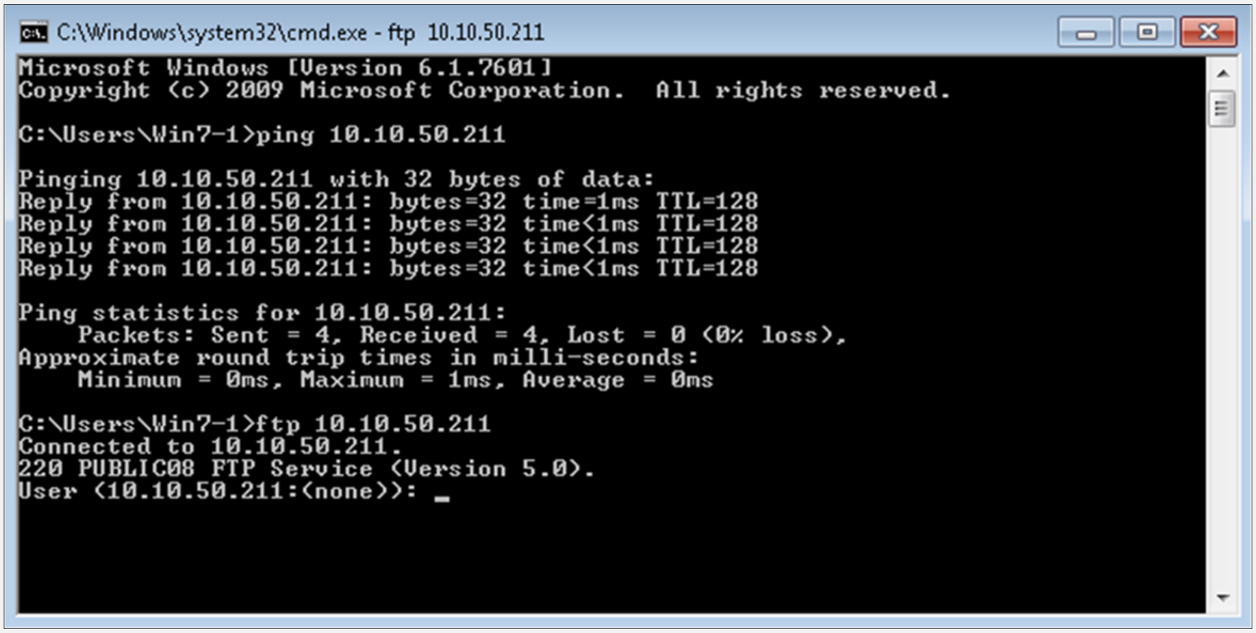


Multiple network adapters have been detected. Please select the IP address to bind to or select All to listen on all adapters.

Adapter: All

Figure 12-11. HoneyBot Application

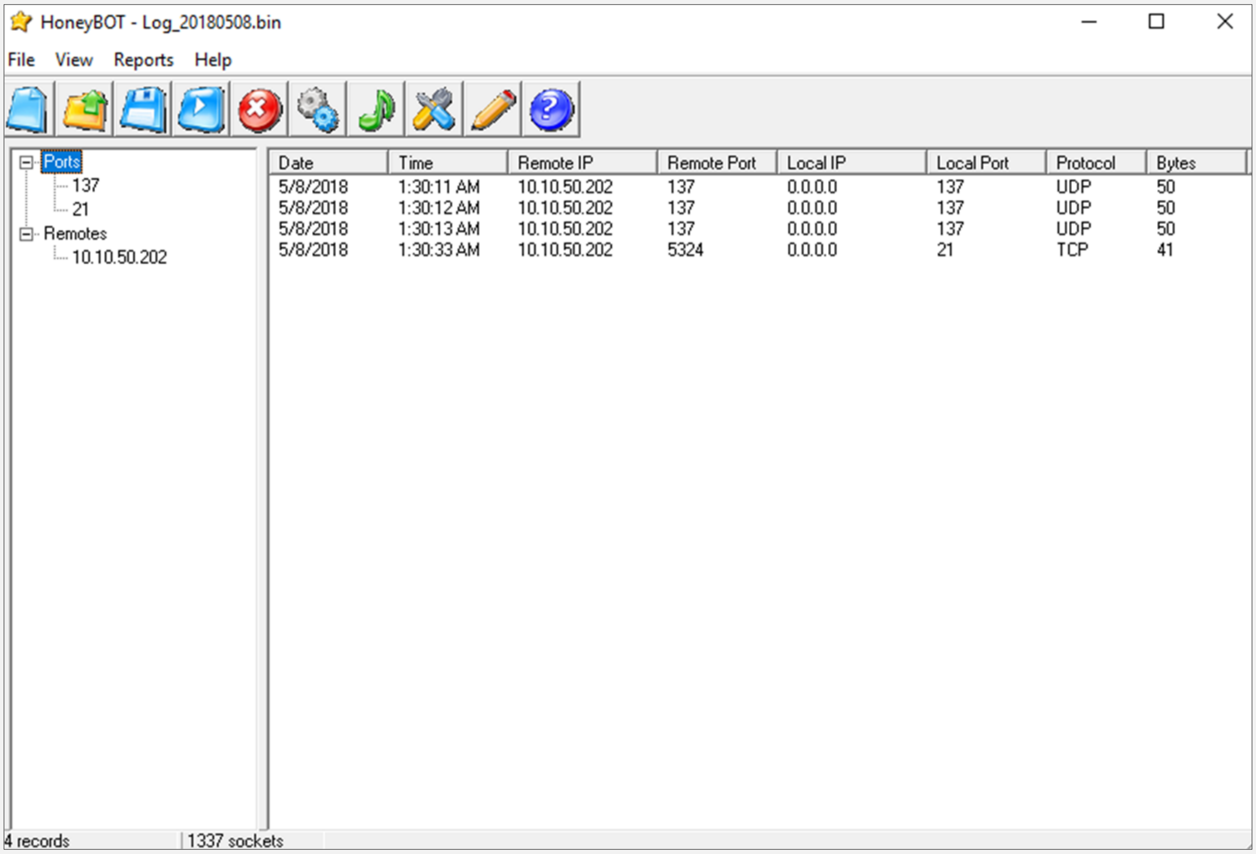
4. Go to Windows 7 machine
5. Open Command Prompt
6. Generate some traffic like FTP.



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Win7-1>ping 10.10.50.211

Pinging 10.10.50.211 with 32 bytes of data:
Reply from 10.10.50.211: bytes=32 time=1ms TTL=128
Reply from 10.10.50.211: bytes=32 time<1ms TTL=128
Reply from 10.10.50.211: bytes=32 time<1ms TTL=128
Reply from 10.10.50.211: bytes=32 time<1ms TTL=128

Ping statistics for 10.10.50.211:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Win7-1>ftp 10.10.50.211
Connected to 10.10.50.211.
220 PUBLIC08 FTP Service (Version 5.0).
User (10.10.50.211:(none)): _
```

Figure 12-12. Command Prompt (Windows 7)

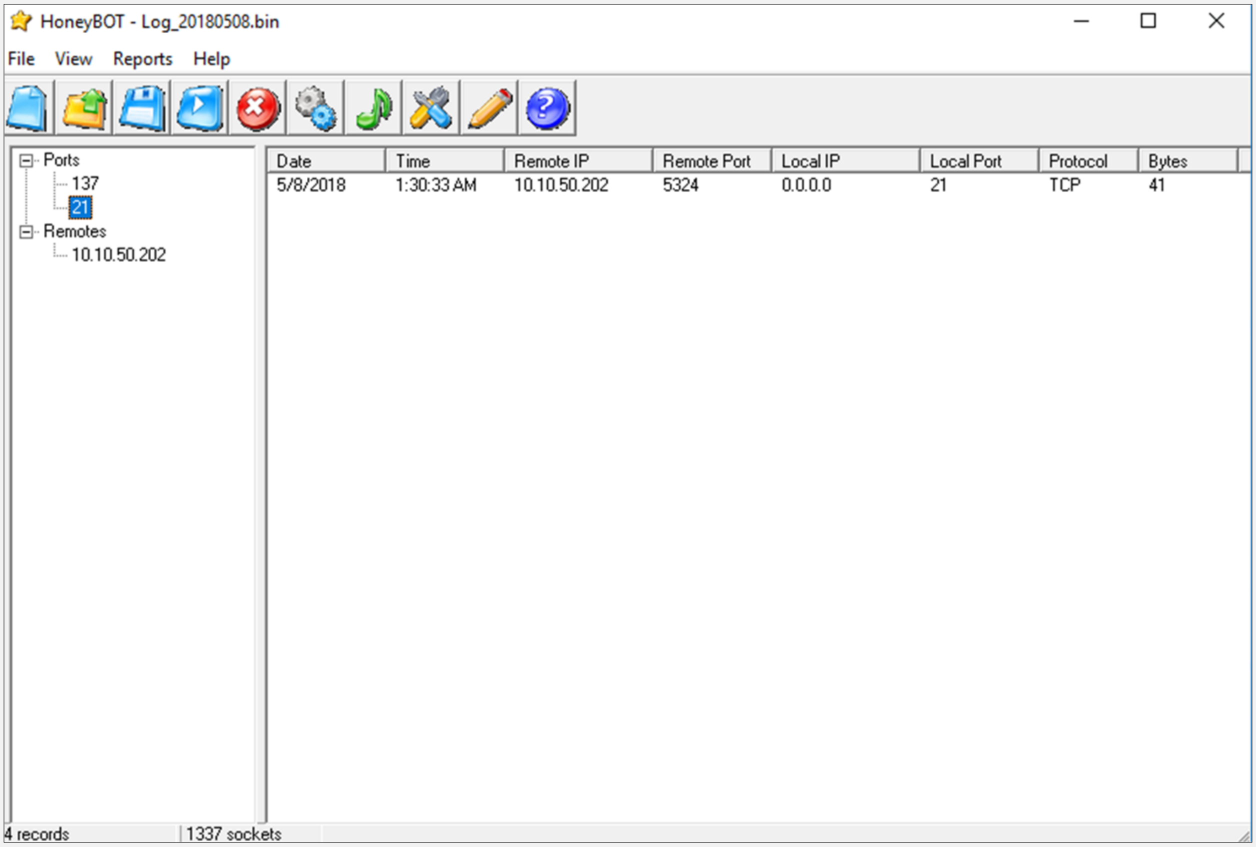
7. Back to Windows Server 2016 and observe the logs



Date	Time	Remote IP	Remote Port	Local IP	Local Port	Protocol	Bytes
5/8/2018	1:30:11 AM	10.10.50.202	137	0.0.0.0	137	UDP	50
5/8/2018	1:30:12 AM	10.10.50.202	137	0.0.0.0	137	UDP	50
5/8/2018	1:30:13 AM	10.10.50.202	137	0.0.0.0	137	UDP	50
5/8/2018	1:30:33 AM	10.10.50.202	5324	0.0.0.0	21	TCP	41

Figure 12-13. Logs

8. Click on Port > 21 and select the log

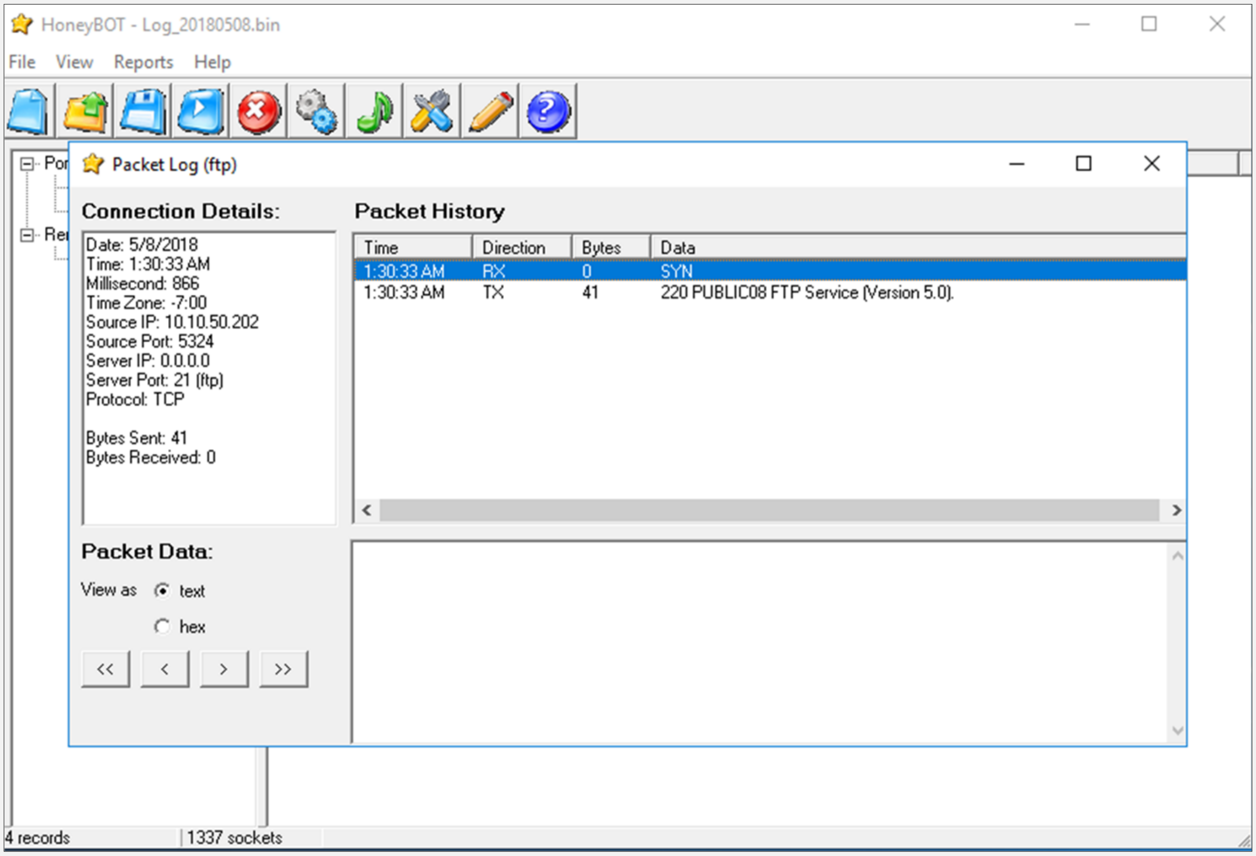


Date	Time	Remote IP	Remote Port	Local IP	Local Port	Protocol	Bytes
5/8/2018	1:30:33 AM	10.10.50.202	5324	0.0.0.0	21	TCP	41

4 records | 1337 sockets

Figure 12-14. logs

9. Right click and go to View Details



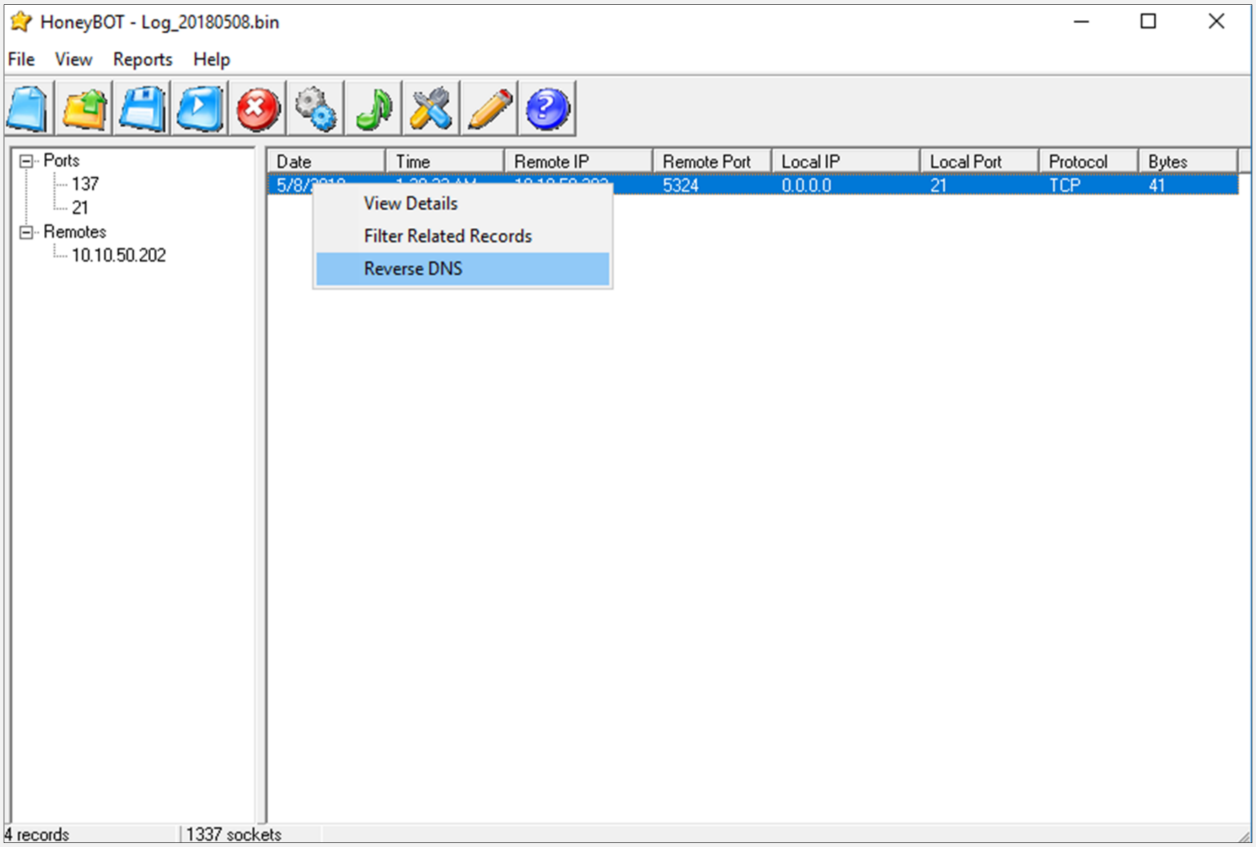
Date: 5/8/2018
Time: 1:30:33 AM
Millisecond: 866
Time Zone: -7:00
Source IP: 10.10.50.202
Source Port: 5324
Server IP: 0.0.0.0
Server Port: 21 (ftp)
Protocol: TCP

Bytes Sent: 41
Bytes Received: 0

Time	Direction	Bytes	Data
1:30:33 AM	RX	0	SYN
1:30:33 AM	TX	41	220 PUBLIC08 FTP Service (Version 5.0).

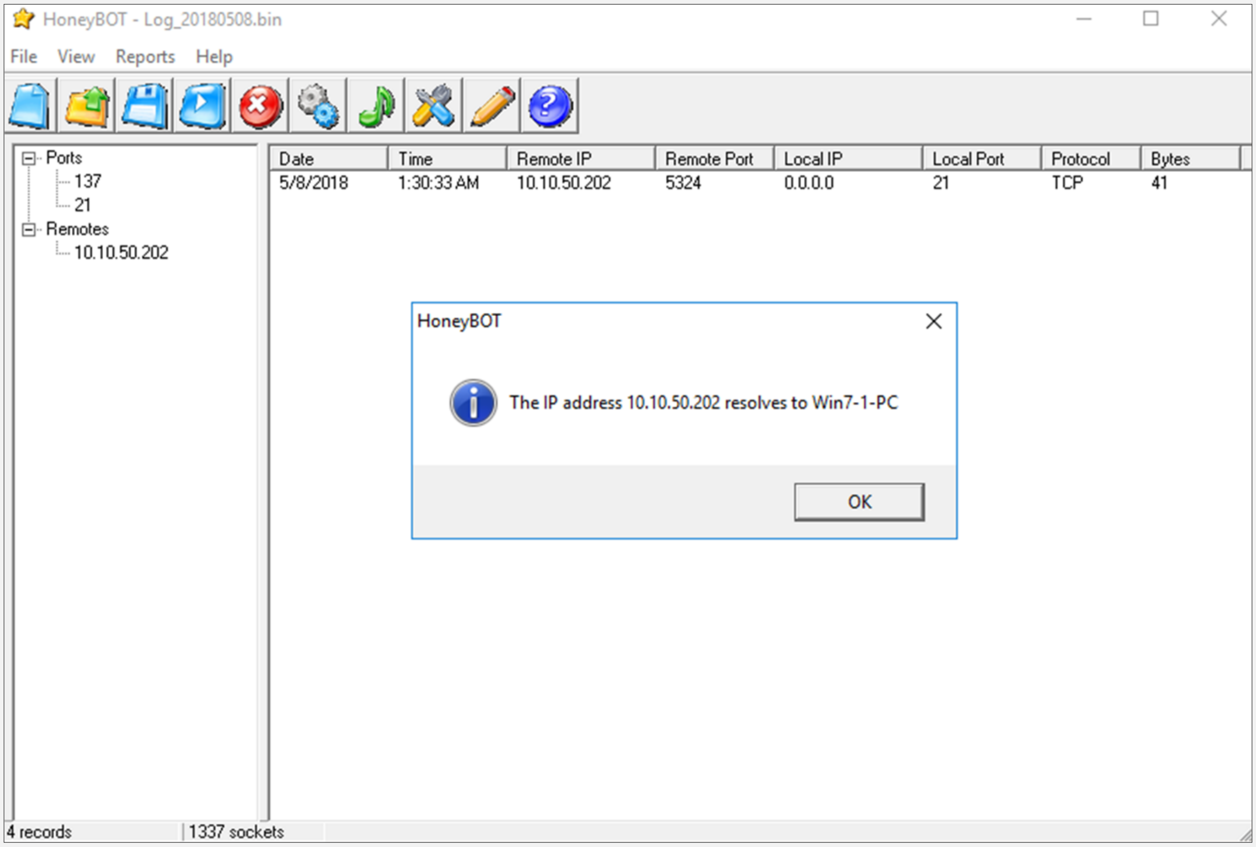
Figure 12-15. Detail of log entry

10. Right click and go to Reverse DNS



Date	Time	Remote IP	Remote Port	Local IP	Local Port	Protocol	Bytes
5/8/2018	1:28:22 AM	10.10.50.202	5324	0.0.0.0	21	TCP	41

Figure 12-16. Reverse DNS



Date	Time	Remote IP	Remote Port	Local IP	Local Port	Protocol	Bytes
5/8/2018	1:30:33 AM	10.10.50.202	5324	0.0.0.0	21	TCP	41

The IP address 10.10.50.202 resolves to Win7-1-PC

4 records | 1337 sockets

Figure 12-17. Reverse DNS