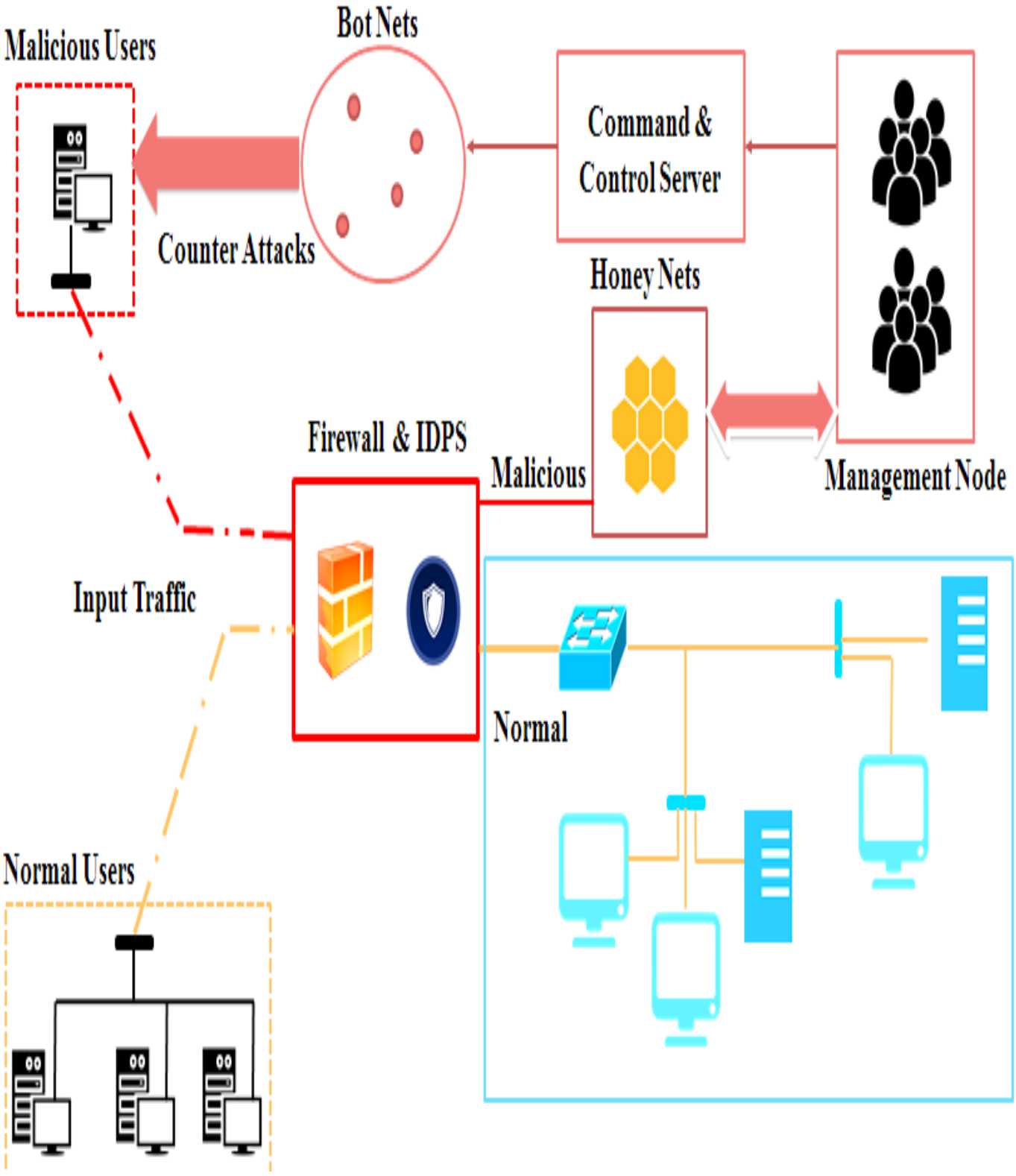
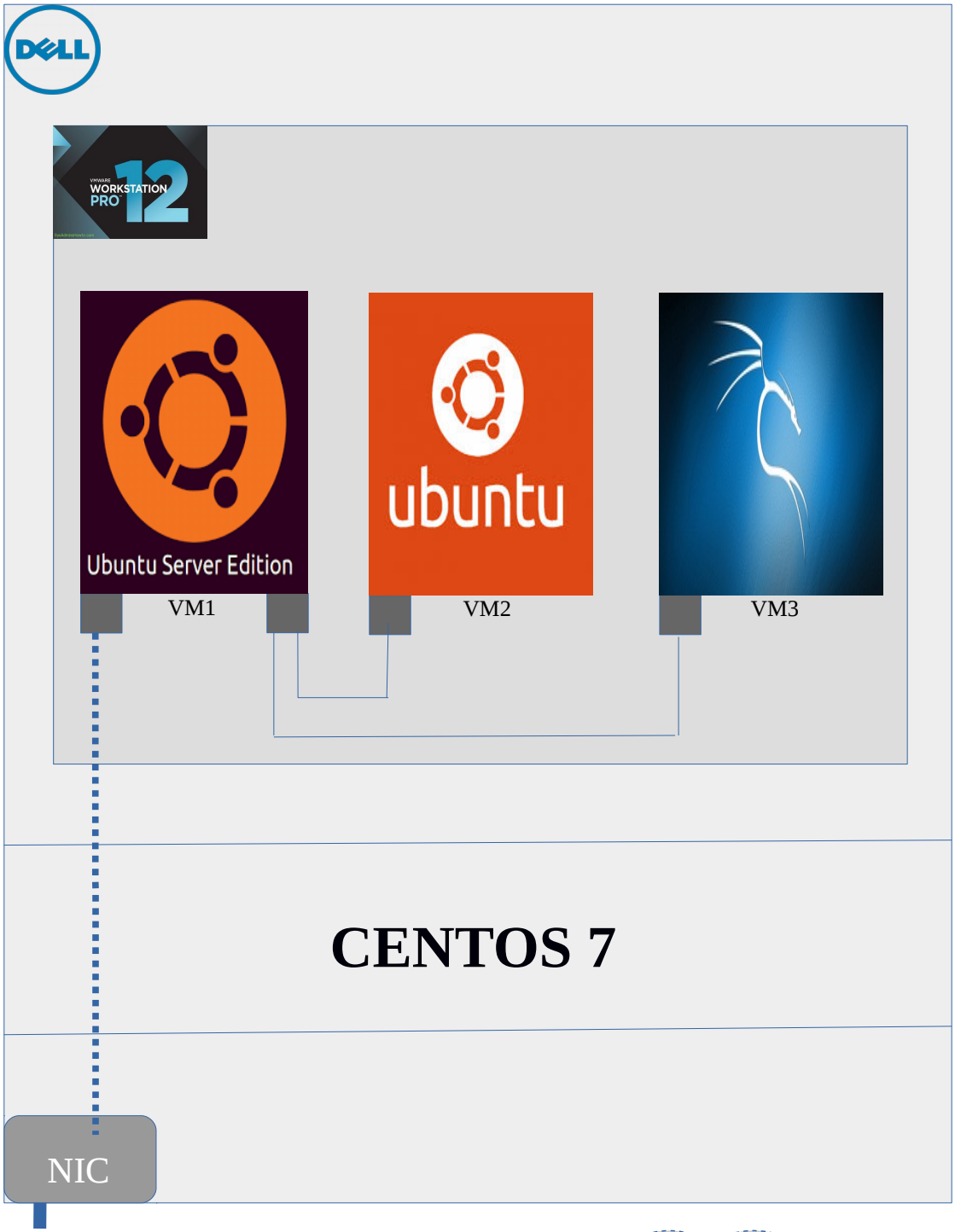
OVERALL ARCHITECTURE



ENVIRONMENT SETUP



SYSTEM REQUIREMENTS

SERVER USED : DELL PowerEdgeR730 **MEMORY** : 64GB			
SPECIFICATIONS	**KALI LINUX**	**UBUNTU SERVER**	**UBUNTU DESKTOP**
Memory	10GB	15GB	10GB
Hard Disk	100GB	150GB	100GB
Services	-	DHCP,BIND9, APACHE WEB SERVER	-
Role	Attacker	Server	User
Network Adapter(NA) Mode	Host-Only	NA1-Bridged NA2-Host-only	Host-Only
Processors	1	2	1

ATTACK DESCRIPTION

Ping Flood

An evolved version of ICMP flood, this DDoS attack is also application specific. When a server receives a lot of spoofed Ping packets from a very large set of source IP it is being targeted by a Ping Flood attack. Such an attack's goal is to flood the target with ping packets until it goes offline. It is designed to consume all available bandwidth and resources in the network until it is completely drained out and shuts down. This type of DDoS attack is also not easy to detect as it can easily resemble legitimate traffic.

SYN Flood

This attack exploits the design of the three-way TCP communication process between a client, host, and a server. In this process, a client initiates a new session by generating a SYN packet. The host assigns and checks these sessions until they are closed by the client. To carry out a SYN Flood attack, an attacker sends a lot of SYN packets to the target server from spoofed IP addresses. This attack goes on until it exhausts a server's connection table memory –stores and processes these incoming SYN packets. The result is a server unavailable to process legitimate requests due to exhausted resources until the attack lasts.

SYN-ACK Flood

The second step of the three-way TCP communication process is exploited by this DDoS attack. In this step, a SYN-ACK packet is generated by the listening host to acknowledge an incoming SYN packet. A large amount of spoofed SYN-ACK packets is sent to a target server in a SYN-ACK Flood attack. The attack tries to exhaust a server's resources – its RAM, CPU, etc. as the server tries to process this flood of requests. The result is a server unavailable to process legitimate requests due to exhausted resources until the attack lasts.

ACK Fragmentation Flood

Fragmented ACK packets are used in this bandwidth consuming version of the ACK & PUSH ACK Flood attack. To execute this attack, fragmented packets of 1500 bytes are sent to the target server. It is easier for these packets to reach their target undetected as they are not normally reassembled by routers at the IP level. This allows an attacker to send few packets with irrelevant data through routing devices to consume large amounts of bandwidth. This attack affects all servers within the target network by trying to consume all available bandwidth in the network.

RST/FIN Flood

After a successful three or four-way TCP-SYN session, RST or FIN packets are exchanged by servers to close the TCP-SYN session between a host and a client machine. In an RST or FIN Flood attack, a target server receives a large number of spoofed RST or FIN packets that do not belong to any session on the target server. The attack tries to exhaust a server's resources – its RAM, CPU, etc. as the server tries to process these invalid requests. The result is a server unavailable to process legitimate requests due to exhausted resources.

PSH/ACK Flood

When connecting with a server, the client can ask for confirmation that the information was received by setting the ACK flag, or it can force the server to process the information in the packet by setting the PUSH flag. Both requests require the server to do more work than with other types of requests.By flooding a server with spurious PUSH and ACK requests, an attacker can prevent the server from responding to valid traffic. This technique is called a PUSH or ACK flood.

Multiple SYN-ACK Spoofed Session Flood

This version of a fake session attack contains multiple SYN and multiple ACK packets along with one or more RST or FIN packets. A Multiple SYN-ACK Fake Session is another example of an evolved DDoS attack. They are changed up to bypass defense mechanisms which rely on very specific rules to prevent such attacks. Like the Fake Session attack, this attack can also exhaust a target's resources and result in a complete system shutdown or unacceptable system performance.

Multiple ACK Spoofed Session Flood

SYN is completely skipped in this version of Fake Session. Multiple ACK packets are used to begin and carry an attack. These ACK packets are followed by one or more RST or FIN packets to complete the disguise of a TCP session. These attacks tend to be more successful at staying under the radar as they generate low TCP-SYN traffic compared to the original SYN-Flood attacks. Like its source, the Multiple ACK Fake Session attack can also exhaust a target's resources and result in a complete system shutdown or unacceptable system performance.

UDP Flood

As the name suggests, in this type of DDoS attack a server is flooded with UDP packets. Unlike TCP, there isn't an end to end process of communication between client and host. This makes it harder for defensive mechanisms to identify a UDP Flood attack. A large number of spoofed UDP packets are sent to a target server from a massive set of source IP to take it down. UDP flood attacks can target random servers or a specific server within a network by including the target server's port and IP address in the attacking packets. The goal of such an attack is to consume the bandwidth in a network until all available bandwidth has been exhausted.

Christmas Tree Attack

A Christmas tree attack sends a large number of Christmas tree packets to an end device. A Christmas tree packet has all the options set so that any protocol can be used. The name is derived from the idea that all the settings are turned to "on" within the packet so it is lit up like a Christmas tree.Christmas tree packets require much more processing by routers and end devices than other packets. Large numbers of these packets can use up so much processing power that it ties up these devices effectively making any other task nearly impossible thus denying service to legitimate traffic.