Task 1

A small company, ACME, has a network as shown in Figure 1 with IP addresses as indicated. The packet filtering firewall, FW, is also an Internet access gateway. Collab, is an external partner to ACME and they both share component design files on the sever NAS but share no other data. NAS also hosts a database that stores credit card information of ACME's customers. Web is the company web site using HTTP for ACME's general Internet presence and also to process online sales made by credit card.

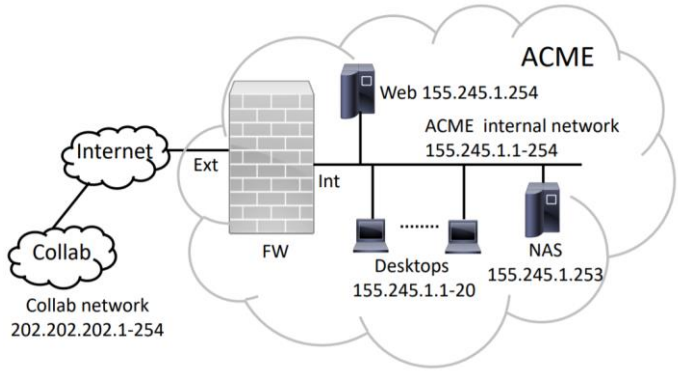

Figure 1

ACME requires the following border control policy:

- *Web should serve HTTP traffic to the Internet (HTTP uses port 80)*
- *Desktops should be able to access TCP servers in the Internet except Telnet servers in the Internet (Telnet uses port 23)*
- *Collab should be able to access NAS on TCP port 445*
- *spoofed IP addresses from the Internet should be blocked*
- *any other traffic must be blocked.*

Task 1(a)

Design the firewall rules in FW that meet the specifications above. The firewall FW is a stateless packet filter. Your answer does not need to be in the format of any particular firewall system, but should describe the required firewall rule parameters and indicate the order of the rules. Every firewall rule must have a description that explains the fields.

- the number for the rule,

IPort, OPort - the physical port i.e. internal, external or admin

Flags - TCP flags such as SYN, ACK, RST, FIN, EST (EST means match any)

SPort, Dport - TCP or UDP source and destination ports

IPort Physcial input port
OPort Physcial input port

IPSrc
IPDst

Proto (TCP/UDP/ICMP)
SPort (TCP/UDP source port)
DPort (TCP/UDP destination port)

Flags (TCP flags, none relevant in UDP)

IPort OPort IPsrc IPDst Proto Sport DPort Flags Action

Spoofed IP addresses from the Internet should be blocked
1. ext * * 155.245.1.1-254 * * * * * deny

Web should serve HTTP traffic to the Internet (HTTP uses port 80)
2. ext int * 155.245.1.254 * * 80 * allow

Web should serve HTTP traffic to the Internet (HTTP uses port 80)
3. int ext 155.245.1.254 * * 80 * EST allow

Desktops should not be able to access Telnet servers in the Internet (Telnet uses port 23).
4. int ext 155.245.1.1-20 * TCP * 23 * deny

Desktops should be able to access TCP servers in the Internet
5. int ext 155.245.1.1-20 * TCP * * * allow

Desktops should be able to access TCP servers in the Internet
6. ext int * 155.245.1.1-20 TCP * * EST allow

Collab should be able to access NAS on TCP port 445
7. ext int 202.202.202.1-254 155.245.1.253 TCP * 445 * allow

Collab should be able to access NAS on TCP port 445
8. int ext 155.245.1.253 202.202.202.1-254 TCP 445 * EST allow

any other traffic must be blocked.
9. * * * * * * * * deny

Task 1 (b)

The network architecture described above is very poor from a security perspective. Design a better architecture and explain why it improves the security. Your design should introduce as little new equipment as possible, as would suit a small company.

Internet <--> extDMZFW <-> DMZ <-> intDMZFW <-> internal <-> intFW <-> DBNet

extDMZFW - a firewall that exists inbetween the Internet and the DMZ packet filtering firewall, this will limit access from the Internet to only the traffic relevant for each server in DMZ.

DMZ – the demilitarized zone.

DMZ – this is a zone containing Internet facing servers:

- each server has a single purpose, and is highly secured, so that if one server is compromised, it is not directly possible to compromise another service.
- **DNS**(**dmz**) server will perform lookups for the Internet for local services, it will also provide a lookup service for local systems to find Internet IP addresses.
- **HTTPS** server, this should be changed from **HTTP** because **HTTPS** uses TLS to protect credit card details (and other user data) when they are accessing the shop. The **HTTPS** server does not hold credit card information, instead it will send it as soon as it gets it to an application server in the internal network by using a secure and thoroughly tested API service.
- **SMTPext** server that is used for email to/from the Internet
- **DMZLOG** server used for logging data (ie syslog data from the **HTTP** server and **DNS** server).
- The **DMZLOG** server is not accessible from the Internet.
- The database server holding the credit card information is not in this zone.

intDMZFW - a firewall that exists between the **DMZ** and internal network (an application layer firewall):

- Making sure the data is clean by checking the application data sent from **HTTPS** server.
- Allowing email to pass between **SMTPext** and **SMPTint,** checking that the email is clean. The email out must obey the site policy, for example, send addresses are correct.
- Performing **NAT** between the Internet and internal networks.

Internal - the network where the staff members are connected, this uses private address space (e.g. 10.0.0.0/8):

- The staff members exists in this network.
- **SMPTint** is used for internal mail.
- **DNSint** is used for internal **DNS**.
- The application server for the online shop also exists in this network, it gets data from **DMZ HTTPS**, then cleans it and sends it to **DBNet**.
- The file sharing server is also exists here.

intFW - a firewall that exists between the internal network and **DBNet**

- An application layer firewall that checks the traffic to **DBNet** where the credit card information is stored, it will decrypt the data, and check that no malicious data exists.
- Filters all of the admin data traffic.
- Only allows the application server to send information to **DBNet**, which will block everyone (systems and staff) from accessing the credit card information.

DBNet – an internal network containing the admin users and the credit card database.

- **DB**: An internal database used to store the credit card information
- **Admin**: These users can access the **DB** net, but access is otherwise restricted.

Task 2

A company finds that their only Internet connection is overwhelmed by domain name system (DNS) replies so that their main web presence is unable to provide the essential on-line sales service for the company. They analyse the DNS replies that are being sent to them and see that they result from what is called a DNS amplification attack; they are certain that the DNS replies are not generated from DNS requests coming from the company.

Explain what is meant by a DNS amplification attack and propose a solution for the company that will allow them to maintain a reliable web presence even if the attack continues. Explain how your solution operates.

The DNS amplification attack is a type of distributed denial-of-service (DDoS) attack, which leverages the functionality of open DNS resolvers in order to overwhelm a target server or network with an amplified amount of traffic, which will render the server inaccessible.

All amplification attacks exploit the bandwidth consumption between an attacker and the targeted web resource. By sending small queries that result in large responses, the malicious user is able to get more from less. The attacker is able to multiply the magnification, by making bots in a botnet issue similar requests, this means that it's not possible to identify the attacker, and in turn they can issue a larger amount of traffic.

It is possible to reduce the number of servers that can be used by attackers to generate traffic, as there are multiple mitigation techniques that are available that can reduce the overall effectiveness of such attacks, such as source IP verification. The DNS queries that are sent by the clients must have a source address spoofed to appear as the victim's system, to reducing the effectiveness of DNS amplification, a rule can be created to reject any DNS traffic with spoofed addresses. If it is not possible to reach the source address of the packet, then the packet has a spoofed source address and in turn this address should be blocked or limited.

Task 3

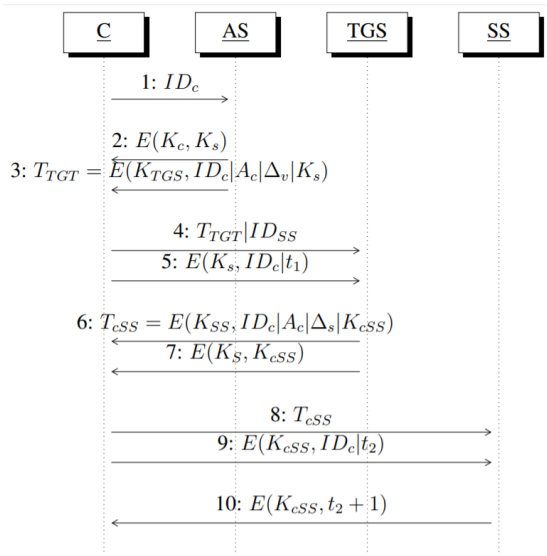

Figure 2

Figure 2 shows a simplified view of the messages between a client and a service server using Kerberos v5 to authenticate the client.

Task 3 (a)

By explaining one of the ticket exchanges in Figure 2, show how Kerberos stops a malicious user from impersonating the client and thus using a ticket to maliciously obtain access to the service server.

Client C shares a key Kc with the Authentication server (AS). The client (C) wants to access the service server (SS). Kc is derived from the user's password. The client sends an ID to AS, and AS then responds with an encrypted session key Ks (encrypted Kc). AS also sends a ticket Ttgt. This ticket is encrypted by a key Ktgs, which is only known by the AS and the ticket granting service (TGS). The client cannot decrypt the ticket.

The ticket contains:

- client id
- client address (IP address)
- validity period
- session key Ks

This ticket is enough to get a service server ticket.

The Client can request a SS ticket, this is where the client sends an authenticator and the ticket, where the ID of the SS authenticator is the ID of the client, which are timestamped and encrypted with the session key. In turn, this will guarantee that only a valid client can send the ticket.

The client then receives the SS ticket Tss, and a SS key Kcss. Kcss is generated and also shared between the client and SS. Now, the client sends Tss and authenticator to the SS. The SS will then check if the client is valid, and issue a reply which is timestamp authenticated with Kcss.

Task 3 (b)

A malicious user has been able to gain valid Kerberos tickets by using a dictionary attack. Explain how a malicious user may be able to carry out this attack. Your answer should include the description of a dictionary attack and why it is important to the malicious user that it can be performed offline. Furthermore, propose a method to stop the attack you have described.

A dictionary attack is a type of brute-force attack, that is performed by obtaining a ciphertext that is generated using the password-derived key, and then trying each password against the ciphertext. This category of attack is invisible to Kerberos and can be performed much faster than an online attack.

When a client C sends the first message which is just an ID in plain text. AS will then reply with a Ticket which contains a session key encrypted with the client key Kc. This means that attacker would only have to send the client ID to get back the last message. With the last message, the attacker is able to perform a dictionary attack where they can try to determine the key Kc. A dictionary attack is likely to successful for about 25% of users. This means that the attacker can perform a dictionary attack even if they can't access the network, which means that it is important for them to perform the attack whilst offline in order to avoid detection.

One method that can be used to stop this type of attack was introduced in Kerberos v5, which makes use of pre-authentication. The user will encrypt a timestamp and ID with their key, and send this as the first message instead of just the ID. The AS can then check if it is really a valid user. This can be used to stop an active attacker, as the AS will only sends back the second message with the encrypted session key if the first message was encrypted with a valid password.

Task 4

A new networked application is required to send traffic over the Internet between two hosts each of which is within two different partner networks. It is important that confidentiality and integrity is maintained over the whole of the network path between the hosts. Additionally, it is important that the IP addresses of the two hosts in the partner networks are kept private from snooping systems in the Internet.

The networked application must use widely standardised protocols to achieve these aims. Design a solution that meets the requirements above and describe how the systems within your design achieve confidentiality, integrity and privacy

The best solution that would meet the set requirements would be for both of the clients to make use of IPsec, using a VPN tunnel with NAT enabled. This is the most secure method of communication, as making use of the VPN tunnel will ensure that the IP addresses of the two hosts in the partner networks are kept private from any snooping systems on the Internet.

IPsec supports VPNs through tunnelling. In tunnelling, the original IP header is preserved, and an additional header is then added. This extra header is ignored as the packet passes through the public Internet is removed at an IPsec enabled gateway, as the packet enters a network. The payload may also be decrypted at the same time. IPsec provides a method for both of the users to securely communicate over the public Internet, which in turn helps to guarantee the confidentiality of the communications.

A VPN connects various types of external network connections to one another. These connections are made by cryptographic tunnel through the public Internet. The VPN tunnel ensures that confidentiality is maintained over the whole of the network path between the hosts, as it is not possible to access the VPN tunnel externally. Tunnelling mode allows for the VPN and will also provide a limited amount of security against traffic analysis. An IPsec-enabled gateway must keep a SA database if multiple connections occur. Looking up each SA in the database is the main overhead from IPsec, which can slow down the communications, but in turn helps to improve the integrity of the communications. In tunnelling mode, the inner IP packet is encapsulated within the outer headers. The gateway will then remove the IPsec additions.

Network Address Translation (NAT) is a way of sharing a single NAT router's IP address between a set of private IP addresses. NATs pose a problem for VPNs because incoming connections that have not been initiated within the private network or one-off messages may well be blocked. In order to guarantee the privacy of the users, an SSL connection can be used to tunnel all traffic between two NAT-enabled private networks.