Folie 02 – Netzwerksicherheit

ICMP

Internet Control Message Protocol (ICMP) is a connectionless protocol used for IP operations, diagnostics, and errors.

Smurf-Attack

A smurf attack is an exploitation of the Internet Protocol (IP) broadcast addressing to create a denial of service. The smurf program builds a network packet that appears to originate from another address (this is known as spoofing an IP address). The packet contains an ICMP ping message that is addressed to an IP broadcast address. The echo responses to the ping message are sent back to the "victim" address. Enough pings and resultant echoes can flood the network making it unusable for real traffic.

Inverse Mapping

Inverse Mapping is a technique used to map internal networks or hosts that are protected by a filtering device.

1. Attacker sends an ICMP reply message to a range of IP addresses presumably behind a filtering device.
2. Upon receiving the series of ICMP reply messages, since the filtering device does not keep state of the list of ICMP requests, it will allow these packets to their destination.
3. If there is an internal router, the router will respond with a ICMP “Host Unreachable” for every host that it cannot reach, thus giving the attacker knowledge of all hosts which are present behind the filtering device.

ICMP Route Redirect

An ICMP Route Redirect message is sent when a gateway receives an IP traffic from a host and finds in its routing table that its next gateway to be routed to for this traffic is on the same network as the host. Allows a Man-In-The-Middle attack.

1. Attacker manages to take over a secondary gateway G1 of the source host.
2. Attacker sends a TCP open packet to source host acting as destination host.
3. While a reply is in transit from the source host to the destination host through gateway G2, the attacker sends an ICMP route redirect message to source host spoofing as G2.
4. Source host will accept the route change control message as valid and thus changes its routing table to now route all traffic bound for destination host through Gateway G1.
5. Now attacker will quietly read/modify and forward all traffic bound for destination host to Gateway G2 acting as a Man-In-The-Middle host.

Ping of death

Some computer systems were never designed to properly handle a ping packet larger than the maximum packet size because it violates the Internet Protocol documented in RFC 791. However, when the target computer reassembles the malformed packet, a buffer overflow can occur, causing a system crash and potentially allowing the injection of malicious code.

ICMP Flood

An ICMP Flood - the sending of an abnormally large number of ICMP packets of any type (especially network latency testing “ping” packets) - can overwhelm a target server that attempts to process every incoming ICMP request, and this can result in a denial-of-service condition for the target server.

IP

IP Fragmentation Attack

Form of denial of service attack, in which the perpetrator overbears a network by exploiting datagram fragmentation mechanisms. IP fragmentation: a communication procedure in which IP datagrams are broken down into small packets, transmitted across a network and then reassembled back into the original datagram. Every network has a unique limit for the size of datagrams that it can process. This limit is known as the maximum transmission unit (MTU). If a datagram is being sent that is larger than the receiving server's MTU, it has to be fragmented in order to be transmitted completely.

Teardrop attacks, these assaults target TCP/IP reassembly mechanisms, preventing them from putting together fragmented data packets. As a result, the data packets overlap and quickly overwhelm the victim's servers, causing them to fail.

Tiny Fragment Attack

If the data packet size is made small enough to force some of a TCP packet’s TCP header fields into the second data fragment, filter rules that specify patterns for those fields will not match. If the filtering implementation does not enforce a minimum fragment size, a disallowed packet might be passed because it didn’t hit a match in the filter.

UDP

UDP Flood Attack

“UDP flood” is a type of Denial of Service (DoS) attack in which the attacker overwhelms random ports on the targeted host with IP packets containing UDP datagrams.

The receiving host checks for applications associated with these datagrams and—finding none—sends back a “Destination Unreachable” packet. As more and more UDP packets are received and answered, the system becomes overwhelmed and unresponsive to other clients.

NTP Amplification Attacks

NTP amplification is a type of Distributed Denial of Service (DDoS) attack in which the attacker exploits publically-accessible Network Time Protocol (NTP) servers to overwhelm the targeted with User Datagram Protocol (UDP) traffic.

In the most basic type of NTP amplification attack, an attacker repeatedly sends the “get monlist” request to an NTP server, while spoofing the requesting server’s IP address to that of the victim server. The NTP server responds by sending the list to the spoofed IP address.

This response is considerably larger than the request, amplifying the amount of traffic directed at the target server and ultimately leading to a degradation of service for legitimate requests.

TCP

Low rate attack

These attacks often aim at leaving connections open on the target by creating a relatively low number of connections over a period of time and leaving those sessions open for as long as possible. Common methods include sending partial http requests, such as Slowloris, and Slowpost (a DDoS tool which completes the handshake) and sending small data packets or keep alives in order to keep the session from going to idle timeout.

Christmas tree packets

Christmas tree packets can be used as a method of divining the underlying nature of a TCP/IP stack by sending the packets and then awaiting and analyzing the responses. When used as part of scanning a system, the TCP header of a Christmas tree packet has the flags FIN, URG and PSH set. By observing how a host responds to an odd packet, such as a Christmas tree packet, assumptions can be made regarding the host's operating system.

A large number of Christmas tree packets can also be used to conduct a DoS attack by exploiting the fact that Christmas tree packets require much more processing by routers and end-hosts than the 'usual' packets do.

TCP session hijacking

In that the authentication check is performed only when opening the session, a pirate who successfully launches this attack is able to take control of the connection throughout the duration of the session.

Source routing: The initial hijacking method used involved using the source routing option of the IP protocol. This option made it possible to specify the path IP packets were to follow, using a series of IP addresses showing the routers to be used. By exploiting this option, the pirate could indicate a return path for packets to a router under his control.

Blind attack: When source routing is disabled, which is the case nowadays for most equipment, a second method involves sending packets as "blind attacks", without receiving a response, by trying to predict sequence numbers.

Man in the middle: Also, when the pirate is on the same network thread as his two contacts, he can monitor the network and "quiet" one of the participants by crashing his machine or by flooding the network to take his place.

Other Attacks

- TCP Session Poisoning (z.B. FIN, RST)
- TCP Sequence Number Prediction

DNS

- Mitlesen/Verändern von DNS-Requests/Replies
- Erraten der ID eines DNS-Requests
- Name Chaining (Subgroup of Cache Poisioning)
    - Victim issues a query
    - Attacker injects response, whether via packet interception, query guessing, or ..
    - Attacker's response includes one or more Resource Records (RRs) with DNS names in their RDATA; depending on which particular form this attack takes, the object may be to inject false data associated with those names into the victim's cache via the Additional section of this response, or …

Quellen

https://www.incapsula.com/ddos/attack-glossary/ip-fragmentation-attack-teardrop.html

https://www.cybrary.it/glossary/t-the-glossary/tiny-fragment-attack/

https://www.sans.org/reading-room/whitepapers/threats/icmp-attacks-illustrated-477

https://www.incapsula.com/ddos/attack-glossary/udp-flood.html

https://www.incapsula.com/ddos/attack-glossary/ntp-amplification.html

https://tools.ietf.org/html/rfc3833

https://security.radware.com/ddos-knowledge-center/ddospedia/low-rate-attack/

https://en.wikipedia.org/wiki/Christmas_tree_packet