Session hijacking
Network defense tools

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

SESSION HIJACKING

Session hijacking

- Intercepting legitimate communication between hosts and obtain the role of one side.
  - Network level hijacking (TCP or UDP session)
  - Application level hijacking (e.g. HTTP session)
- Spoofing vs. hijacking
  - In spoofing the attacker impersonates one side in communication
  - In hijacking the attacker enters the already active session between the two sides

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Session hijacking techniques and methodology

- Session hijacking techniques
  - Stealing
  - Guessing
  - Brute forcing
- Session hijacking process
  - Sniffing/Monitoring
  - Session ID
  - Session Desynchronization
  - Command injection
- Passive and active attacks

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Network level hijacking

- Observing the TCP sequence numbers, and injecting packets with correct address/port combination (IP spoofing required) and expected sequence numbers
  - RST hijacking
    - Sending packets with spoofed IP address with the RST flag set (e.g. hping3 tool) and predicted sequence numbers. Can cause TCP session reset
  - Blind hijacking
    - The attacker does not know the sequence numbers, and brute forces his packet using various numbers
    - Can't see the outcome of the attack
  - Source routing
  - ICMP and ARP spoofing
- UDP hijacking
  - No session, port numbers are sufficient
  - Attack effectiveness depend on the quality of the application

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Linux TCP implementation vulnerability

- Kernel version 3.6 (2012)
- Vulnerability reported in 2016: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5696
- Affected platforms: https://www.securityfocus.com/bid/91704
- The attacker can predict ACK sequence numbers and do the effective blind TCP hijack attacks (inject data or reset the connection)
- It takes about 40 to 60 seconds to finish the attack and the success rate is 88% to 97%.
- http://www.cs.ucr.edu/~zhiyunq/pub/sec16_TCP_pure_off path.pdf

ISSES

Co-funded by the Erasmus+ Programme of the European Union

Application level hijacking

- The attacker is looking for a legitimate session ID (token, cookie). If he gets it, he can create packets with the appropriate content to be injected into the session.
- Sniffing or predicting session tokens
- Entering/taking over the session

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Application level attacks

- Man in the middle
- Man in the browser (trojan, modified browser code which sends session ID to the attacker)
- Cross-site scripting XSS (create a link with the malicious script – might steal session ID)
- Cross-site request forgery
- Session Replay attack
- Session fixation (attacker creates a legitimate session and sends a link to the victim so that he/she continues the established session)

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

Session hijacking countermeasures

- Good random generators for session IDs
- Encryption
  - TLS encryption (e.g. HTTPS, SSH,…)
  - IPsec
- Encrypted (hashed) cookies
- Using network defense tools for detection and mitigation

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

NETWORK DEFENSE TOOLS

Network defense tools

- Firewalls
- Intrusion detection/prevention tools
- Network access control (policy check/preadmission and post admission checks)
- Honeypots

ISSES
Co-funded by the Erasmus+ Programme of the European Union

FIREWALL

Firewall

- A network element which routes traffic and protects the devices in the protected network – a form of IPS system
- Placed at the entry/exit point of the protected network
- Filters all the traffic and decides whether it will be passed or filtered
- Firewalls are typically configured to allow only specific kinds of traffic, such as with email protocols, web protocols, or remote access protocols.
- A firewall uses rules that determine how traffic will be handled. Rules exist for traffic entering and exiting the network, and it is possible for traffic going one way not to be allowed to go the other way.
- Firewalls can filter traffic based on a multitude of criteria, including destination, origin, protocol, content, or application.
- There are host-based firewalls.

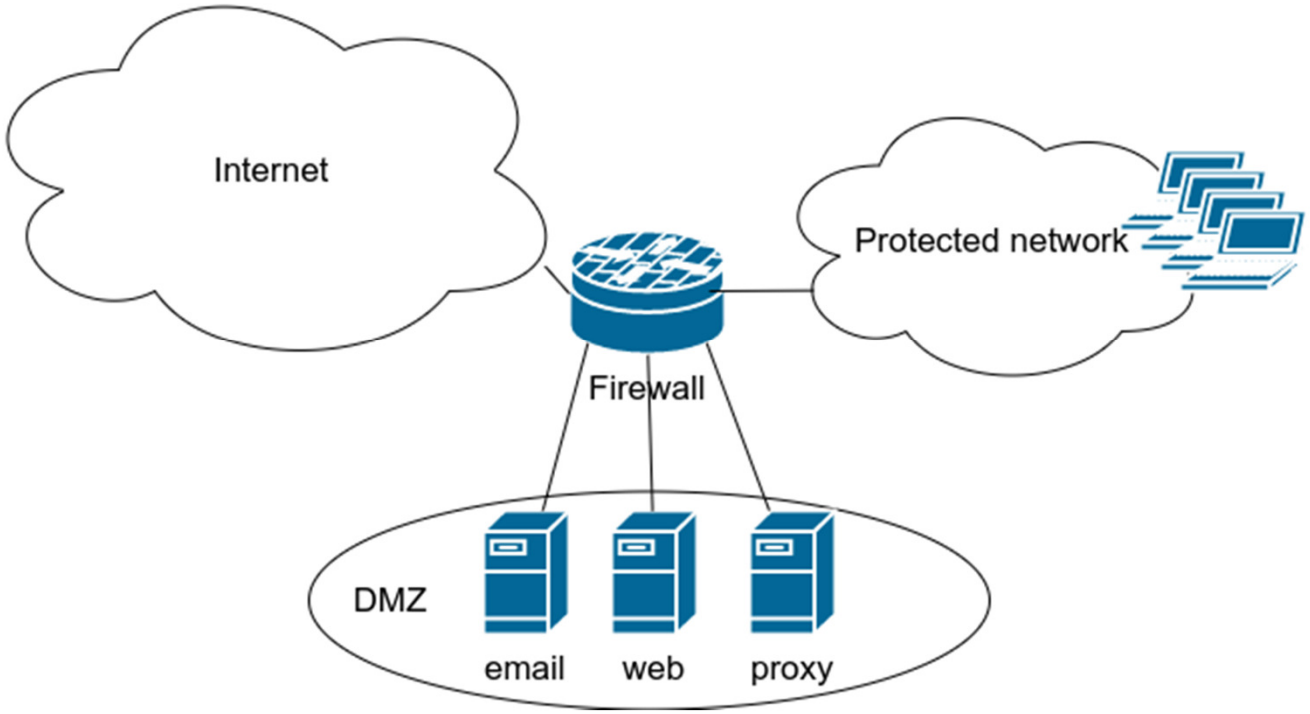
ISSES
Co-funded by the Erasmus+ Programme of the European Union

Other firewall functionalities

- Routing
- NAT
- VPN hub
- AAA access
- Malware protection
- Deep Packet Inspection
- With NFV firewall and IPS/IDS merge into a single system

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Firewall typical configuration



- DMZ – Demilitarized zone
- Multihomed firewall – multiple protected interfaces

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Types of firewalls/modes of operation (1)

- **Packet-Filtering Firewall (Access list)**
  - This firewall compares the properties of a packet such as source and destination address, protocol, and port. (layers 3 and 4)
  - If a packet doesn't match a defined rule, it is dropped.
  - If the packet matches a rule, it typically is allowed to pass.
- **Circuit-Level Gateway Firewall**
  - Layer 5 (session) operation. SOCKS proxy. Circuit proxy
  - A circuit-level firewall is able to detect whether a requested session is valid by checking the TCP handshaking between the packets.
  - Circuit-level gateways do not filter individual packets but sessions.
- **Application-Level Gateway Firewall**
  - Application proxy firewall (e.g. web proxy firewall with reputation verification)
- **Stateful Multilayer Inspection Firewall**
  - filters packets at the Network layer to determine whether session packets are legitimate, and it evaluates the contents of packets at the Application layer.

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Types of firewalls/modes of operation (2)

- **Deep Packet inspection Firewall**
  - This firewall analyzes the application information (data portion of the packet) to make decisions about whether to transmit the packets.
  - Requires a lot of processing power, no hardware acceleration
  - Adds to the delay, storage required for logs
- **Transparent firewall**
  - L2 interfaces (does not route packets, no ip addresses)
  - This firewall compares the properties of a packet such as source and destination address, protocol, and port.
- **Next generation firewall (multifunction device)**
  - Correlate data from various sources, full contextual awareness of users, infrastructure, applications, and content to detect multivector threats
  - Better infrastructure visibility
  - Example: Cisco ASA firepower.
- **Personal Firewall**
  - Active on a personal computer (Windows firewall, iptables, firewalld)

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Packet filtering - examples

- Linux iptables
- Accept all incoming packets for TCP 8080:

```
sudo iptables -I INPUT 7 -p tcp --dport   8080 -m state
--state NEW -j ACCEPT
```

- JUNOS access list---------->
- Pass TCP 20, 21, 22 and 23 to this set off addresses
- Block vs. reject

```
filter trusted-prefixes {
  term controlled-access {
   from {
     address {
                192.168.1.0/24;
                128.29.31.0/24;
                207.46.150.0/24;
                206.132.25.0/24;
                208.48.26.0/24;
                207.159.55.0/24;
               167.216.192.0/24;
               }
    protocol tcp;
    port [ ftp ftp-data telnet ssh ];
    }
 then accept;
 }
term access-denied {
   then {
        log;
       reject;
       }
   }
}
```

ISSES

Co-funded by the Erasmus+ Programme of the European Union

Application level gateways

- E.g. web and email security gateways.
- Web security gateway works as a web proxy, inspecting all web traffic, filtering malware on the pages and malicious web pages based on their reputation (daily reputation data download is needed)
- Email security gateway inspects all email traffic and filters it for malicious content
- Example Cisco Ironport/WSA/ESA

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

Stateful inspection firewall

- Stateful inspection firewall watches the status of a network connection and dynamically create filter rules based on the state of the connection:

1. Inside host S initiates the TCP handshake (SYN) to destination D with source port SP and destination port DP
2. Once the handshake is over (SYN and SYN ACK), stateful firewall creates a rule to pass the traffic belonging to this TCP session
3. FIN or timeout removes the rule

- Solution with the packet filter (permanent and much wider access):
  - permit out S:any any:DP or
  - permit in DP:any S:any

ISSES

Co-funded by the Erasmus+ Programme of the European Union

INTRUSION DETECTION SYSTEMS / INTRUSION PREVENTION SYSTEMS

Intrusion detection systems

- IDS is used to gather and analyze information that passes across a network and to identify and report on any violations or misuse of a network or host.
- IPS prevents potential threats as detected by IDS by filtering them
- Types of IDS:
  - Network IDS
  - Host IDS
  - SIEM, Log file monitors
  - File integrity checking systems

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

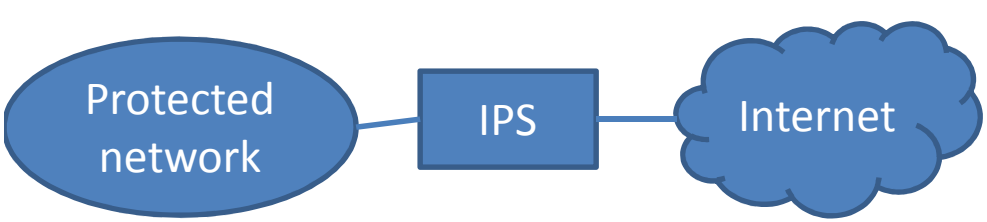
IPS vs. IDS

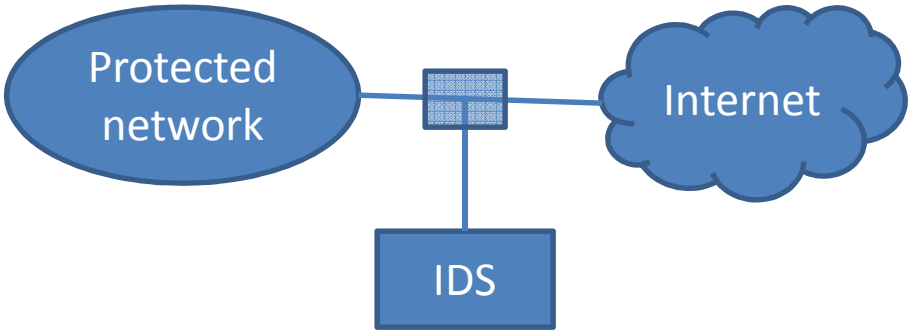
IPS

- Capable to filter traffic
- Has to be inline with the traffic
- Introduces delay
- SPOF
- Can modify packets

IDS

- Just signals that there is a suspicious activity
- Can be on a promiscuous port/tap
- Does not stop and does not affect traffic/packets





Network IDS

- The NIDS is designed to inspect every packet traversing the protected network for the presence of malicious or damaging behavior and, when malicious activity is detected, throw an alert.
- The NIDS is able to monitor traffic from the router to the host itself.
- Can be installed:
  - On the path of the traffic (traffic passes through it)
  - On the router mirror port
  - On the wire tap
- Much like a packet sniffer, an NIDS operates similarly to a network card in promiscuous mode.
- Can be dedicated computer or the more common black-box design (which is a dedicated device).

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Host IDS

- HIDS is installed on a server or computer.
- An HIDS is responsible for monitoring activities on a system and detecting misuse of a system, including insider abuses.
- HIDSs are commonly available on the Windows platform but are found on Linux and Unix systems as well.

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Host IDS types

- File system monitoring – keeping track of and comparing the file versions
- Log files analysis
- Connection analysis – monitoring network connections of a host
- Kernel level detection – detecting system binary changes and anomalies in system calls which indicate intrusions

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

SIEM, LFM and file-integrity check

- SIEM - Security Information and Event Management tools
  - Log file monitors (LFMs) monitor log files created by network services.
  - The LFM IDS searches through the logs and identifies malicious events.
  - Like NIDSs, these systems look for patterns in the log files that suggest an intrusion.
  - Example:
    - Parse HTTP server log files that look for intruders who try well-known security holes, such as the phf attack.
    - Parse log of login attempts, look for brute force attacks, repeated failed attacks from a specific host
- Splunk, ELK stack (Elastic Search, Logstash, kibana)
- File integrity-checking mechanisms, check for Trojan horses or files that have otherwise been modified indicating an intrusion:
  - https://github.com/Tripwire/tripwire-open-source

ISSES
Co-funded by the Erasmus+ Programme of the European Union

IPS/IDS detection methods (1)

- Signature based
  - Parse the traffic and look for a specific pattern (string, order of packets) in it
  - Good for already known and described attacks
  - Not good for zero day attacks
  - Attacker who knows signatures can change the pattern of the attack
  - False alarms from the probability that some random packets can contain attack pattern
  - Requires daily signature updates
  - https://www.snort.org/

```
alert tcp $HOME_NET any -> any any (msg:"Command Shell Access";
content:"C:\\Users\\Administrator\\Desktop\\hfs2.3b"; sid:1000004;
rev:1;)
```

ISSES
Co-funded by the Erasmus+ Programme of the European Union

IPS/IDS detection methods (2)

- Policy based
  - Detect deviations from the company policy (per-host allowed/expected behavior)
  - Can detect zero-day attacks
  - Require reconfiguration upon policy change

ISSES
Co-funded by the Erasmus+ Programme of the European Union

IPS/IDS detection methods (3)

- Anomaly based
  - Detect deviations from the baseline
    - Increased and unexplained use of network bandwidth
    - Probes or services on systems on the network
    - Connection requests from unknown IPs outside the local network
    - Repeated login attempts from remote hosts
  - Can detect zero-day attacks
  - Can work in two phases – learning phase (creating baseline) and detection phase
  - Problem – what is the baseline, when is it recorded?
  - Protocol anomaly detection – looking for unusual behavior in some specific protocol

ISSES
Co-funded by the Erasmus+ Programme of the European Union

IPS/IDS detection methods (4)

- Reputation based:
  - Companies track websites and IP locations globally and rate them based on the previous behavior
  - Access to the low-rated locations is prevented
  - Requires regular/daily updates

ISSES
Co-funded by the Erasmus+ Programme of the European Union

HONEYPOTS

Honeypot

- Honeypot is a system deliberately left for hackers to exploit in order to detect their behaviour, new exploits etc
- Honeypot can be:
  - Server
  - Desktop computer/host
  - File
- KFSensor, HoneyBOT, and HoneyDrive

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

Honeypot types

- **Low-interaction honeypots** rely on the emulation of service and programs that would be found on a vulnerable system. If attacked, the system detects the activity and throws an error that can be reviewed by an administrator.
- **High-interaction honeypots** are more complex in that they are no longer a single system that looks vulnerable but an entire network typically known as a *honeynet*.
- Any activity that happens in this tightly controlled and monitored environment is reported. One other difference in this setup is that in lieu of emulation, real systems with real applications are present.

ISSES
Co-funded by the Erasmus+ Programme of the European Union

EVADING NETWORK DEFENSE

Avoiding/passing through firewalls

- Firewall identification (for non-transparent FW)
  - Port scanning
  - Fire walking
  - Banner grabbing
- Address spoofing
- Source routing
- Fragmentation
- Bypassing WAF with IP address instead of URL
- Bypass using proxy (e.g. for geo-restriction)
- ICMP, HTTP, DNS tunneling

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

Avoiding/passing through firewalls

- Detect firewall using nmap or similar tool
- Some firewalls such as Check Point FireWall-1 and Microsoft Proxy Server listen on ports TCP 256–259 and TCP 1080 and 1745
- Firewalk tool – similar to nmap – probe FW to detect the ACL configuration. Sends packets with varying SRC and DST port combinations with TTL+1 than the TTL of FW. Based on ICMP Time Exceeded messages creates a map of the ACL

```
firewalk -S1-1024 -i <interface> -n -pTCP <gateway IP> <target IP>
```

```
nmap --script=firewalk --traceroute <target ip-address>
```

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Avoiding/passing through IDS/IPS

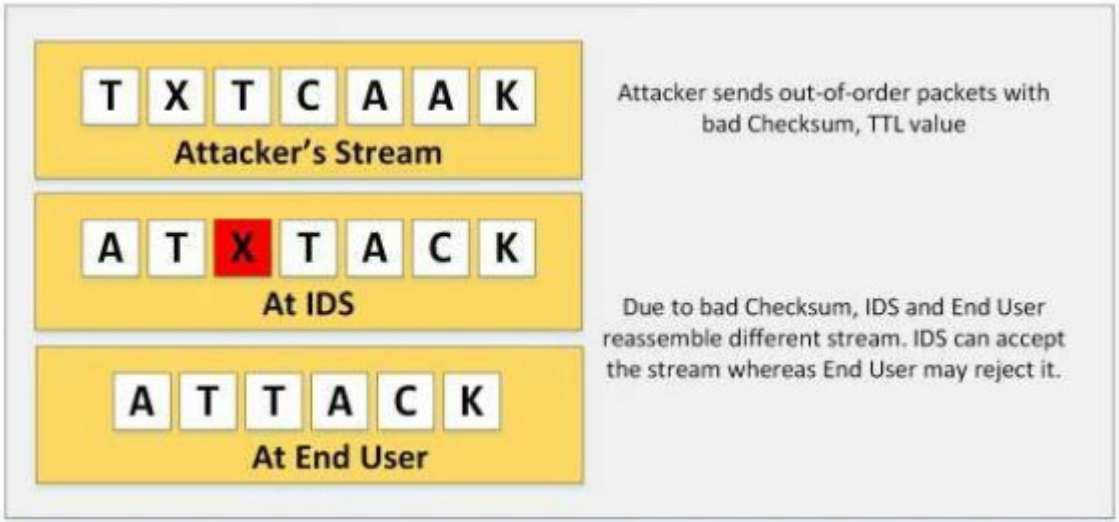
- Insertion *
- Evasion *
- Fragmentation *
- DoS attack on the IPS
- Obfuscating (encrypted payloads pass through the IDS)
- False positive generation (mask an attack with a flood of false positives)
- Session Splicing (split the malicious content into multiple packets)
- Unicode evasion technique (converting strings to avoid signature matching)

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

Insertion attack

- Target: signature based systems
- Attacker sends out of order packets, adds fake packets with bad checksums,…
- Only required packets pass through the IDS and the victim rearranges them.

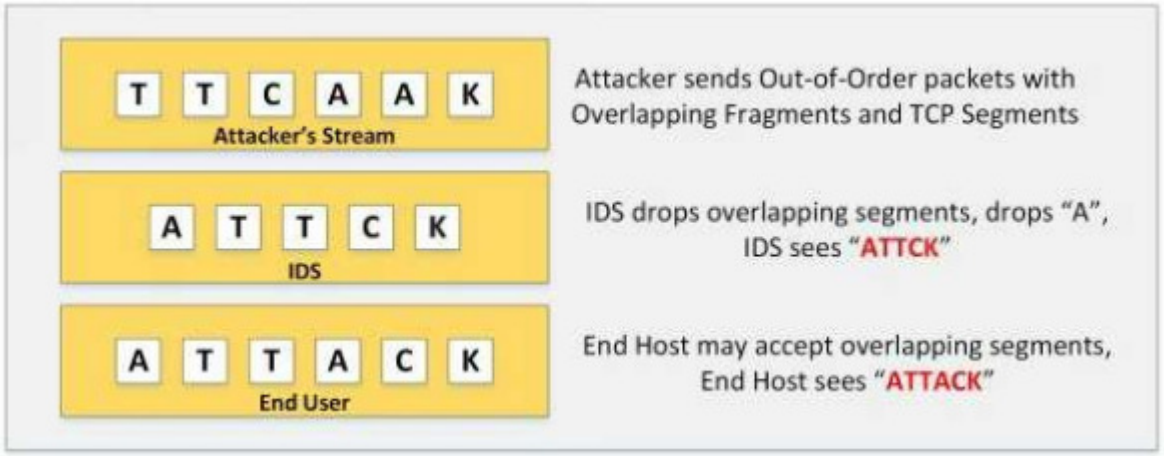


ISSES

Co-funded by the Erasmus+ Programme of the European Union

Evasion attack

- Send some packets which are accepted by the end system, but rejected by the IDS
- IDS and end host do not see the same packet stream



ISSES
Co-funded by the Erasmus+ Programme of the European Union

Fragmentation attack

- Can be successful when end point and IDS have different reassembly timeouts (end point has higher)
- If fragments of a packet are sent with the interarival time which is higher than the time to reassemble at IDS but lower than that time at the end point, a malicious packet might pass through/unnoticed

ISSES
Co-funded by the Erasmus+ Programme of the European Union