DENIAL OF SERVICE AND INTRUSION DETECTION

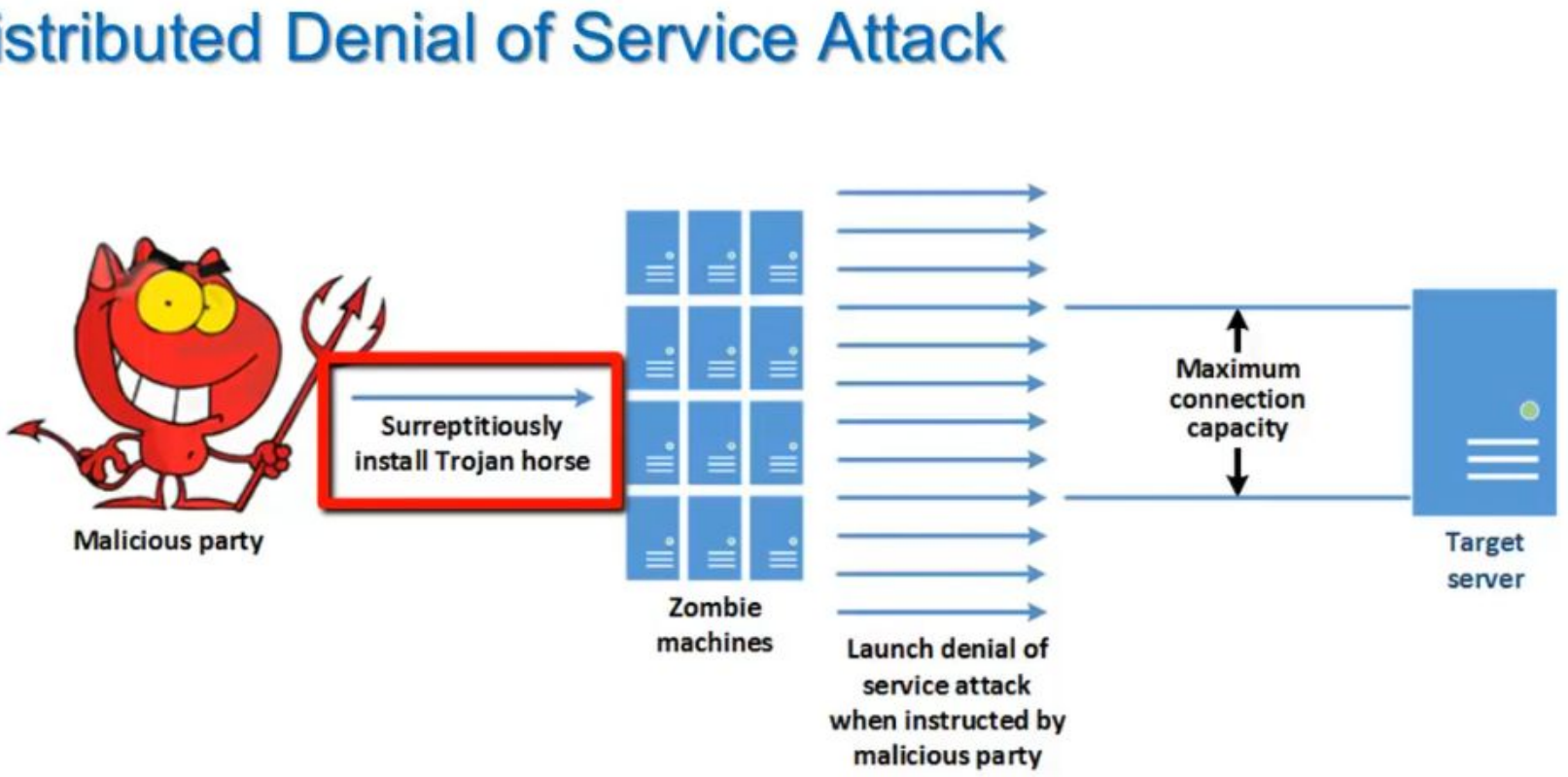
DISTRIBUTED DENIAL OF SERVICE

- An attacker uses any convenient method to distribute a trojan horse to as many target machine as possible
- Each of the target machine becomes a zombie and can be controlled remotely by the malicious party.
- After choosing a victim, a signal is transmitted from the attacker to each zombie machine to initiate the attack
- The trojan horse on each zombie machine then launches variety of denial of service attack on the target server or network.
- Altering a DNS table

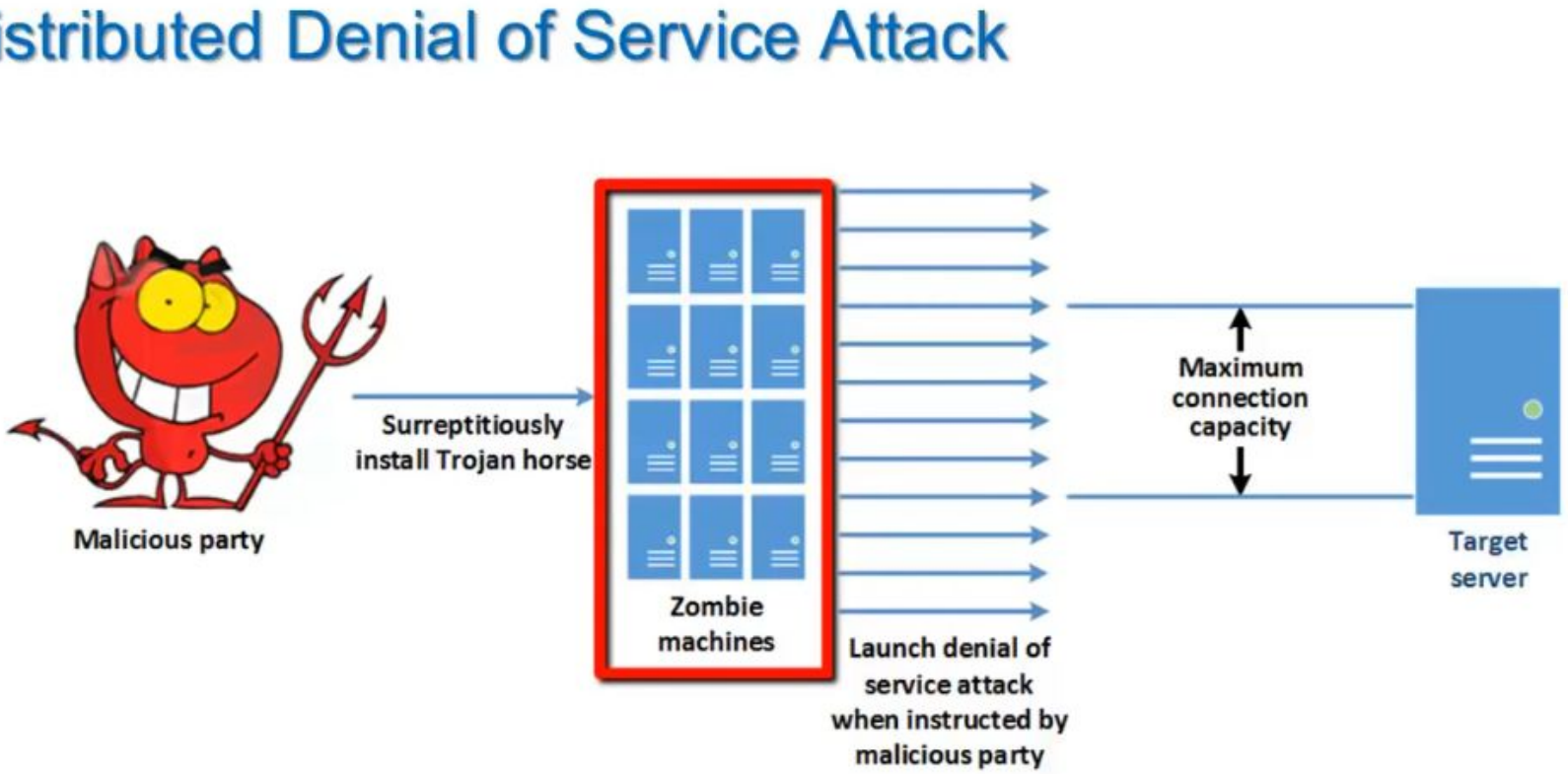
DISTRIBUTED DENIAL OF SERVICE

- If a sufficient large number of zombie machine and a sufficient large variety of denial of service techniques in a DoS attack then the attack will be quite successful.
- This is because with many different machine attack the machine from potentially all over the world using a variety of techniques it becomes difficult for security personnel to distinguish and isolate attackers from legitimate users.

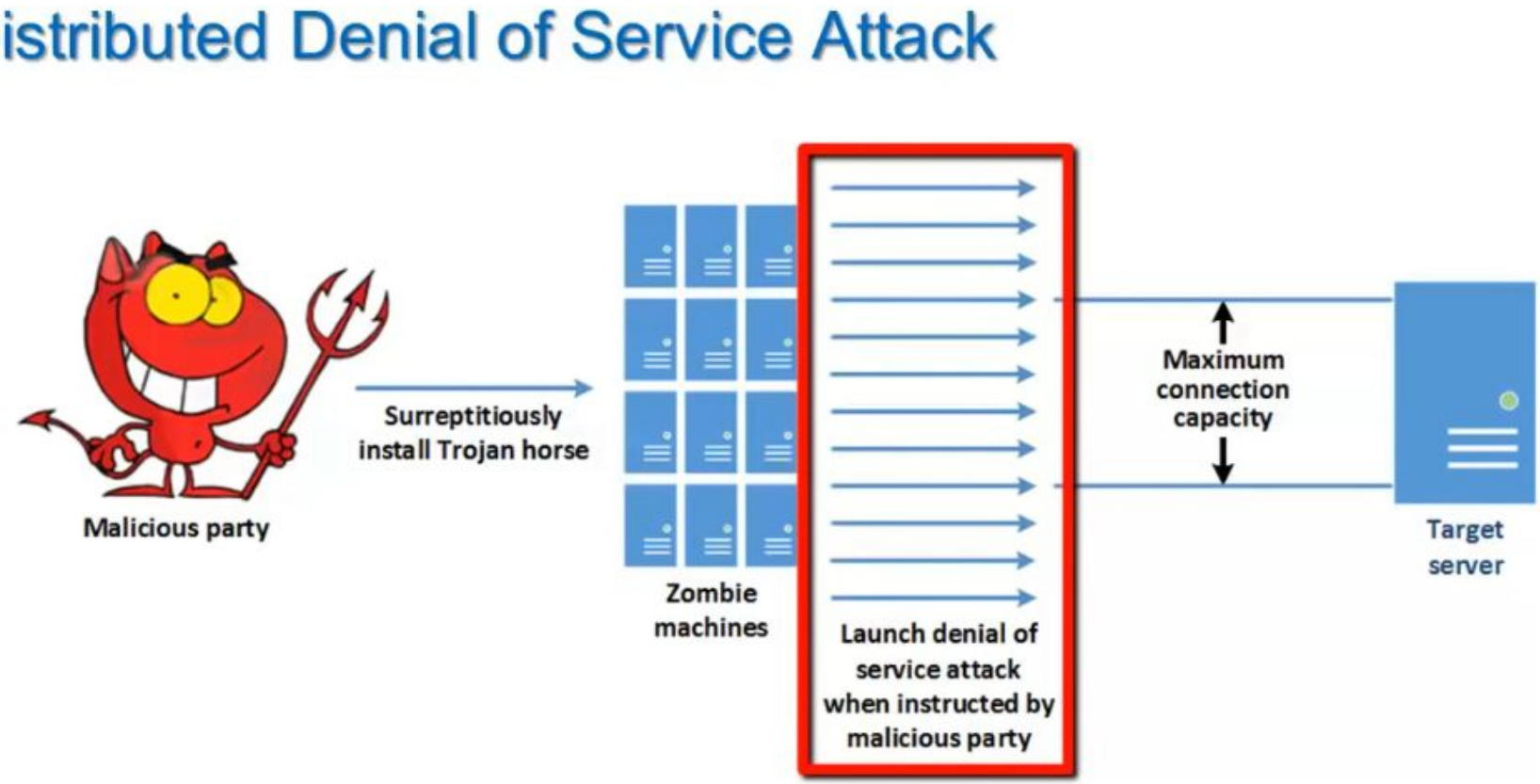
DISTRIBUTED DENIAL OF SERVICE



DISTRIBUTED DENIAL OF SERVICE



DISTRIBUTED DENIAL OF SERVICE



INTRUSION DETECTION SYSTEM

INTRUSION DETECTION SYSTEM

- It is better to prevent an attack than to detect it after it has already succeeded.
- An Intrusion Detection System (IDS) is a device that monitors system activities with a view toward detecting malicious or suspicious events.
- Intrusion Detection Systems attempt to dedtect:
  - Outsiders breaking into a system
  - Insiders attempting to perform inappropriate actions (actions could be intentionally or unintentionally)

INTRUSION DETECTION SYSTEM TERMINOLOGIES

Common terms associated with the use of intrusion detection system:

- Anomaly

- It refers to abnormal or unusual behavior that is occurring on the network

- Misuse

- An activity which violates the network or system security policy.

- Intrusion

- Refers to a situation in which the system or network is been misused either by outsiders or by insiders

- Audit

- activities or actions of the user or system are evaluated and analyzed

- profiling

Refers to the process of observing legitimate users or the system in order to establish a model of what constitute a normal behaviour

Scope of Intrusion Detection Systems

Intrusion detection systems can be classified by scope

- ✔ Host-based
  - IDS runs on a host
  - IDS monitors activities on this host only

- ✔ Network based
  - The IDS is a stand-alone device
  - The IDS monitors the entire network or sub-network

Operation Mode Intrusion Detection Systems

Intrusion detection systems can be classified by their mode of operation

✔ Anomaly-based

- IDS allows only permitted behavior
- uses models of acceptable user activities
- Raises alarm upon detection of deviation from model behavior

✔ Signature-based

- The look for known attacks
- To detect an attack, current activities are matched to known attack signatures.
- Problem: unable to detect new attacks(unknown signatures)

Operation Mode Intrusion Detection Systems

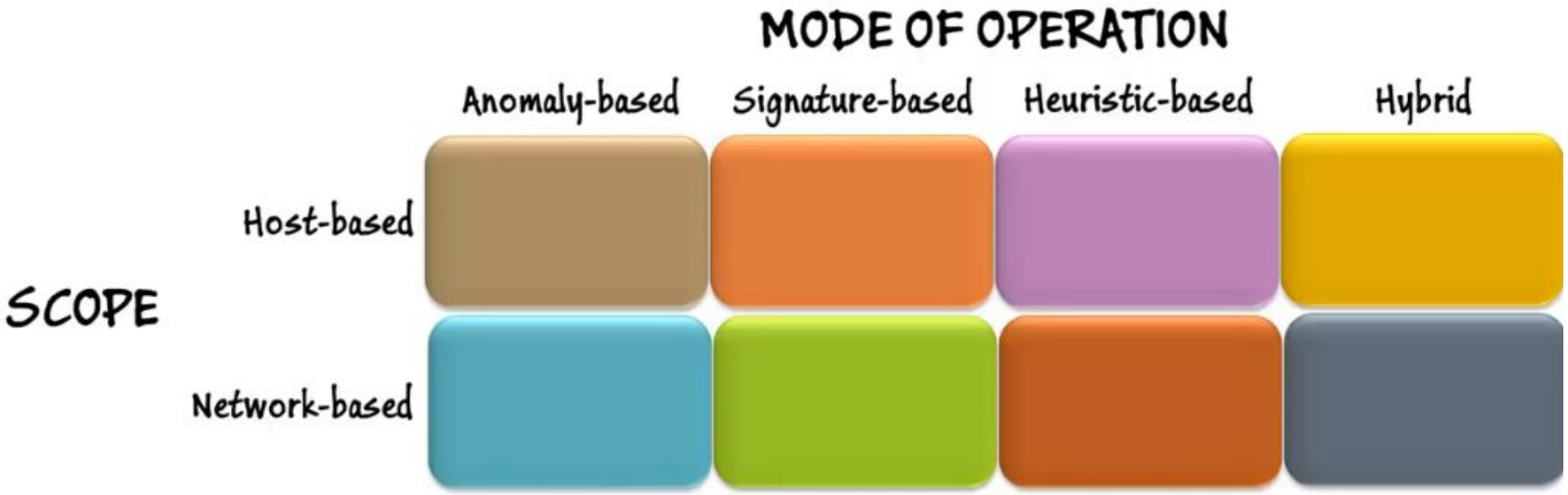
✔ Heuristic-based

- The IDS automattically construct a model of ‘normal’ system behavior
- current behaviors are compared to what is considered normal in order to identify unacceptable system activities

✔ Hybrid

- IDS is a combination of anomaly, signature, and/or heuristic-based approaches.

Classifying Intrusion Detection Systems



Goals for Intrusion Detection Systems

- Intrusion detection system have two primary goals:

✔ Detect all attacks correctly

- avoid false positive(false alarms)
- Avoid false negative(fails to detect genuin attack)

✔ Monitors systems effectively with minimal overhead and performance degradation

Intrusion Detection Systems Responses

- An IDS may trigger several different types of responses:

✔ Monitor the attack and collect data

- Invisible to the attacker

✔ Protect systems and reduce exposure

- Might respond to an attack by automatically attempting to protect information asset. example maybe to immediately disconnect critical database or block access to critical file.

- Visible to the attacker.

✔ Alert a human

- By alerting human security personnel who can make decision as the attack unfold.

END

THANK YOU