Threats

An event, the occurrence of which could have an undesirable impact on the well-being of an **asset**.

(ISC)^2

International Information Systems Security Certification Consortium

Any circumstances or event that has the potential to cause harm to a system or network. That means, that even the existence of an (unknown) vulnerability implies a threat by definition.

[CERT]

Understanding Threats

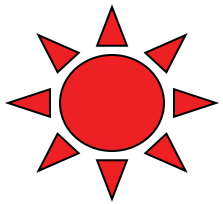
Threat Source	Attackers Motives/Goals	Attack methods
•Employees •Malicious intended guys •Ignorant •Non-employees •Outside attackers •Natural disasters	•Disruption of Service •Expose sensitive information •Alter information •Damage information •Delete information •Funny jokes •Publicity, peer recognition •Monetary gain •Revenge/Defaming others •Political means •Terrorism •Curiosity, testing skills/system	•Social Engineering •Virus, Trojan horses, worms •Key-loggers •Exploitation of vulnerabilities •Packet replay •Packet modification •IP spoofing •Mail bombing •Various hacking tools •Password cracking •Cross-site scripting •SQL injection

Classification of Information Security Threats

- **Transmission Threats**
  - Eavesdropping/Sniffer
  - DoS/DDoS
  - Covert channel
  - Spoofing
  - Tunneling
  - Masquerading/man-in-the middle attacks
- **Malicious Code Threats**
  - Virus
  - Worms
  - Trojans
  - Spyware/Adware
  - Logic Bombs
  - Backdoors
  - Bots
- **Password Threats**
  - Password crackers
- **Social engineering**
  - Dumpster diving
  - Impersonation
  - Shoulder surfing

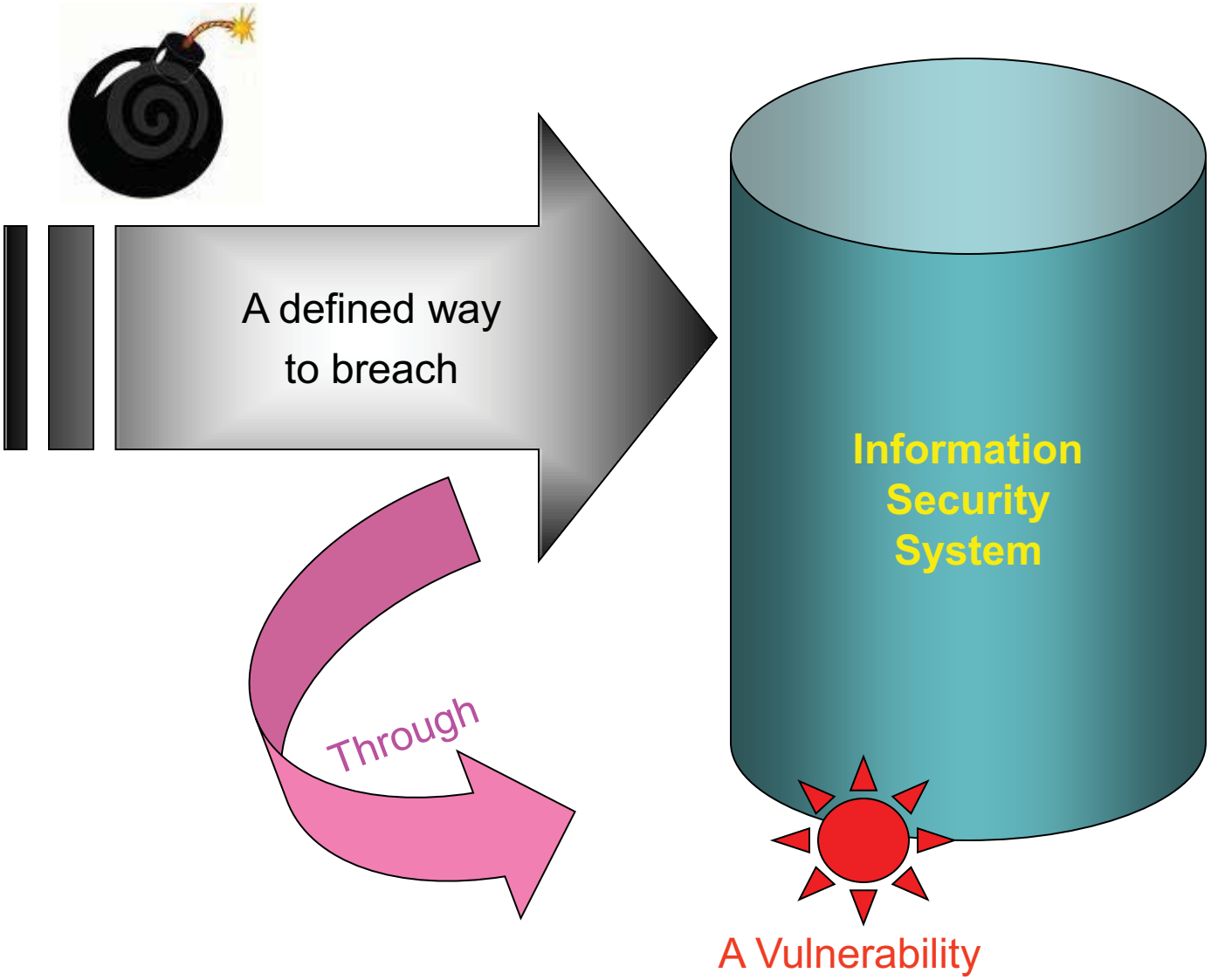
- **Physical Threats**
  - Physical access
  - Spying
- **Application Threats**
  - Buffer overflows
  - SQL Injection
  - Cross-site Scripting
- **Improper usage/Un-authorized access**
  - Hackers
  - Greyhats, Whitehats, Black hats
  - Internal intruders
  - Defacement
  - Open Proxy- Spam
  - Phishing
- **Other Threats**
  - Mobile code

Vulnerabilities



- A feature or bug in a system or program which enables an attacker to bypass security measures.
- An aspect of a system or network that leaves it open to attack.
- Absence or weakness of a risk-reducing safeguard. It is a condition that has the potential to allow a threat to occur with greater frequency, greater impact or both.

Exploit


A defined way
to breach
Information
Security
System
Through
A Vulnerability

Vulnerability Tracking Model

Tracking various vulnerabilities regarding computer security threats such as:

- latest and zero day vulnerabilities in Microsoft OS, Office and related products
- Various network devices like Cisco routers, Juniper IPS etc
- Various Oracle products
- Different web browsers
- Various other products like Adobe/Apache/ Apple iPhone, iOS etc

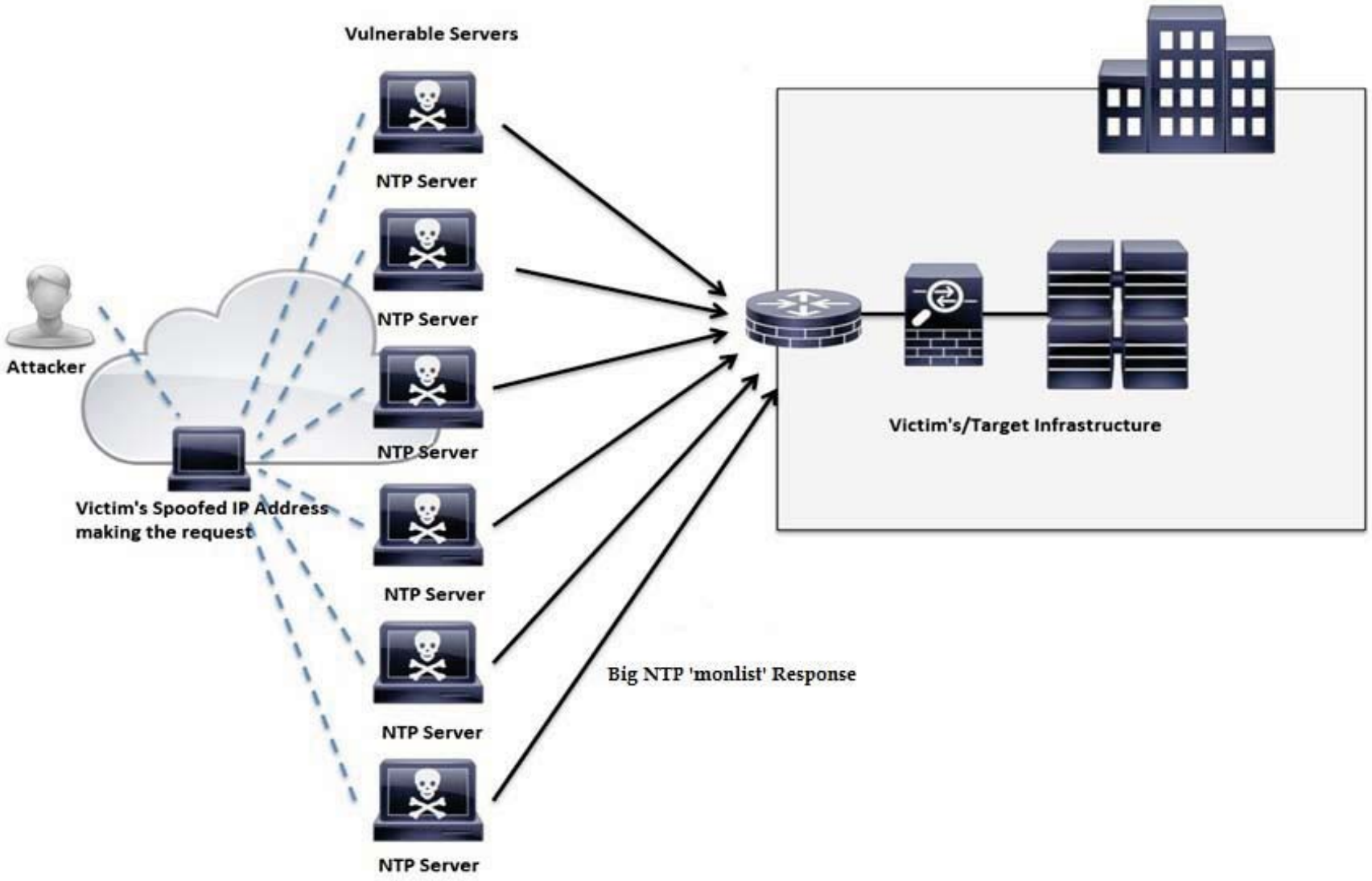
Network Time Protocol Vulnerability

- NTP can be abused to amplify denial-of-service attack traffic.
- The attacker sends a packet with their source address being the IP of a victim. The NTP server replies to this request, but the number of bytes sent in the response is an amplified amount compared to the initial request, resulting in a denial-of-service on the victim.
- Certain NTP control messages provide significant bandwidth amplification factors (BAF)

Typical ‘monlist’ response

```
root@kali:~/Desktop# ntpdc -n -c monlist 192.168.119.243
remote address          port local address      count m ver rstr avgint  lstint
===============================================================================
1.2.3.4                38419 192.168.119.243        2 3 4    0     9        7
50.116.38.157            123 192.168.119.243       47 4 4    0    52       53
38.229.71.1              123 192.168.119.243       47 4 4    0    52       54
208.87.104.40            123 192.168.119.243       46 4 4    0    53       55
216.229.0.50             123 192.168.119.243       46 4 4    0    54       62
192.168.119.130        38419 192.168.119.243        1 3 4    0   693      693
192.168.119.243        47657 192.168.119.243        2 3 4    0   419      757
192.168.119.129        53894 192.168.119.243       44 3 4    0    56     1946
root@kali:~/Desktop#
```

NTP Vulnerability



Media Reports

InformationWeek
DARKReading CONNECTING THE INFORMATION SECURITY COMMUNITY

Home | News & Commentary | Authors | Slideshows | Video | Reports | White Papers | Events

ATTACKS/BREACHES | APP SEC | CLOUD | ENDPOINT | MOBILE | PERIMETER | RIS

ATTACKS/BREACHES

2/11/2014
12:51 PM

Mathew J. Schwartz
News

Connect Directly

6 COMMENTS
COMMENT NOW

Login

DDoS Attack Hits 400 Gbit/s, Breaks Record

A distributed denial-of-service NTP reflection attack was reportedly 33% bigger than last year's attack against Spamhaus.

A record-breaking distributed denial-of-service (DDoS) attack Monday peaked at 400 Gbit/s, which is about 100 Gbit/s more than the largest previously seen DDoS attack.

DDoS defense firm CloudFlare disclosed the attack -- against one of its customers -- Monday. "Very big NTP reflection attack hitting us right now. Appears to be bigger than the #Spamhaus attack from last year, tweeted CloudFlare CEO Matthew Prince, referring

9 Notorious Hackers Of