Evading IDS, Firewalls, and Honeypots

Michael J. Teske

Principal Author Evangelist-Pluralsight

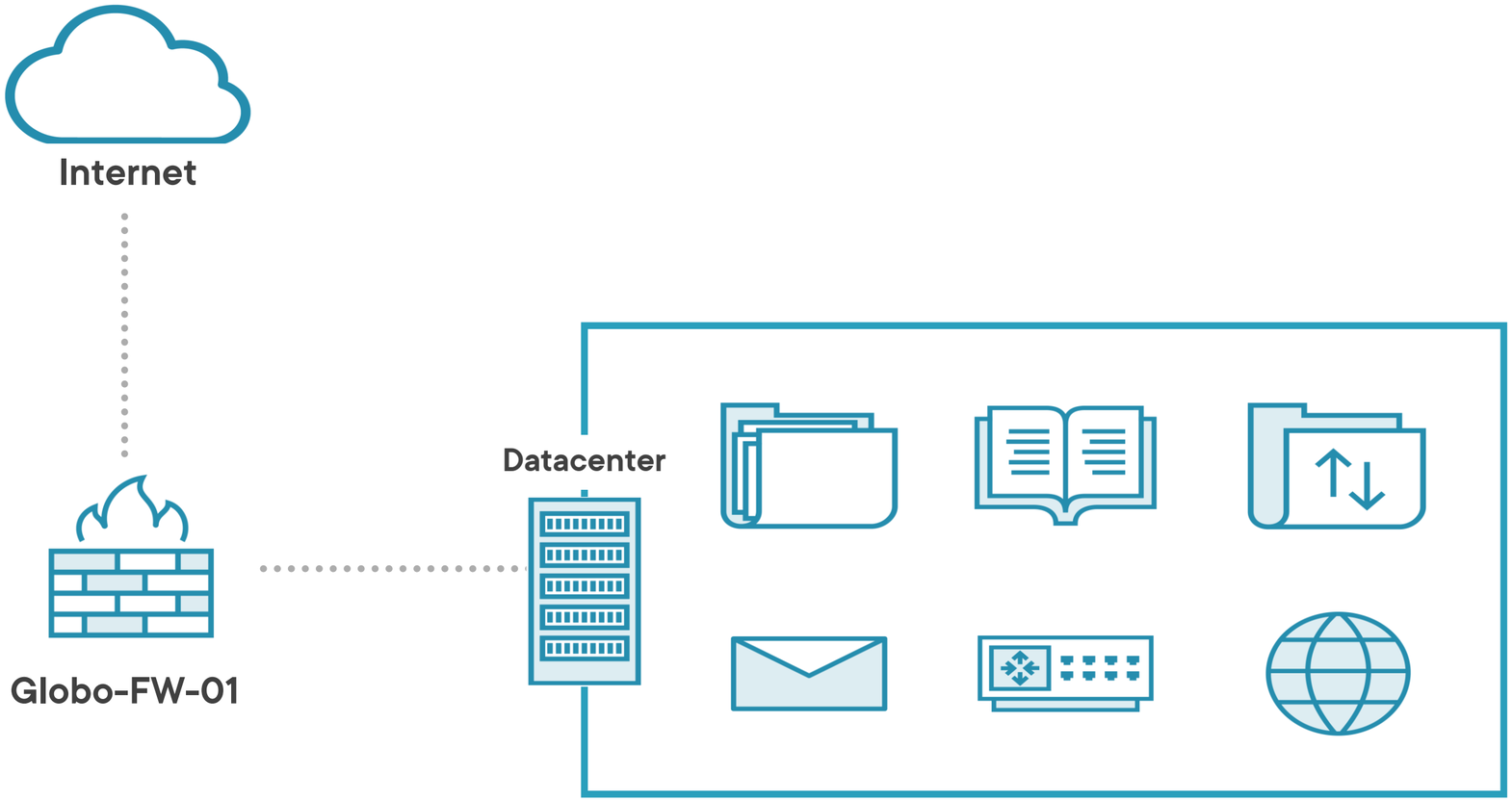
Course Overview

IDS, Firewalls and Honeypots

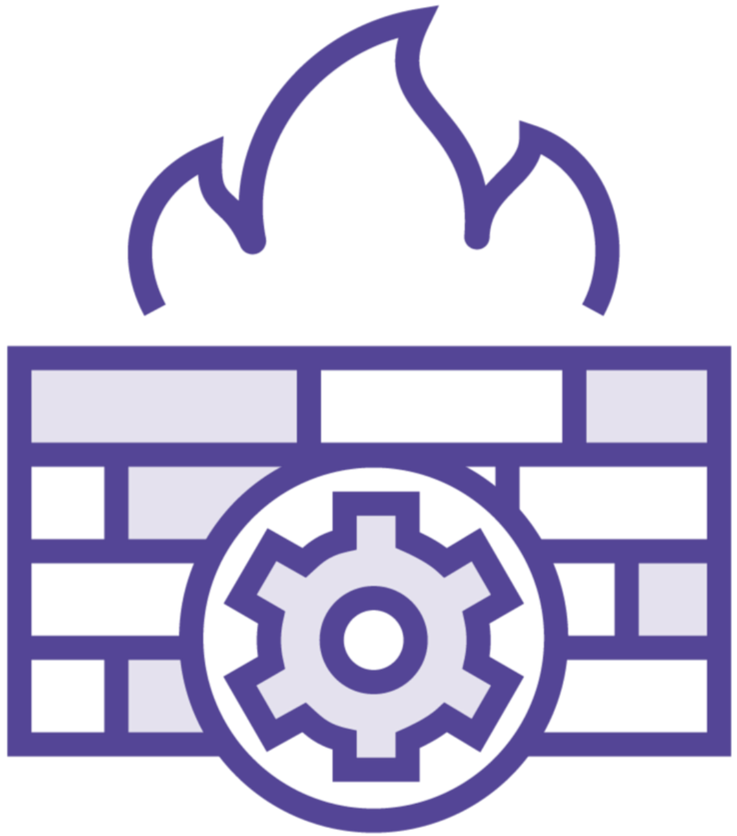
- Concepts & Solutions
  - IDS, IPS, Firewalls and Honeypots
- Tactics & Techniques
  - IDS/Firewall evading tools
  - Detecting honeypots
- ~~Countermeasures~~

IDS, Firewalls, and Honeypot Concepts

Firewalls



Firewalls 101

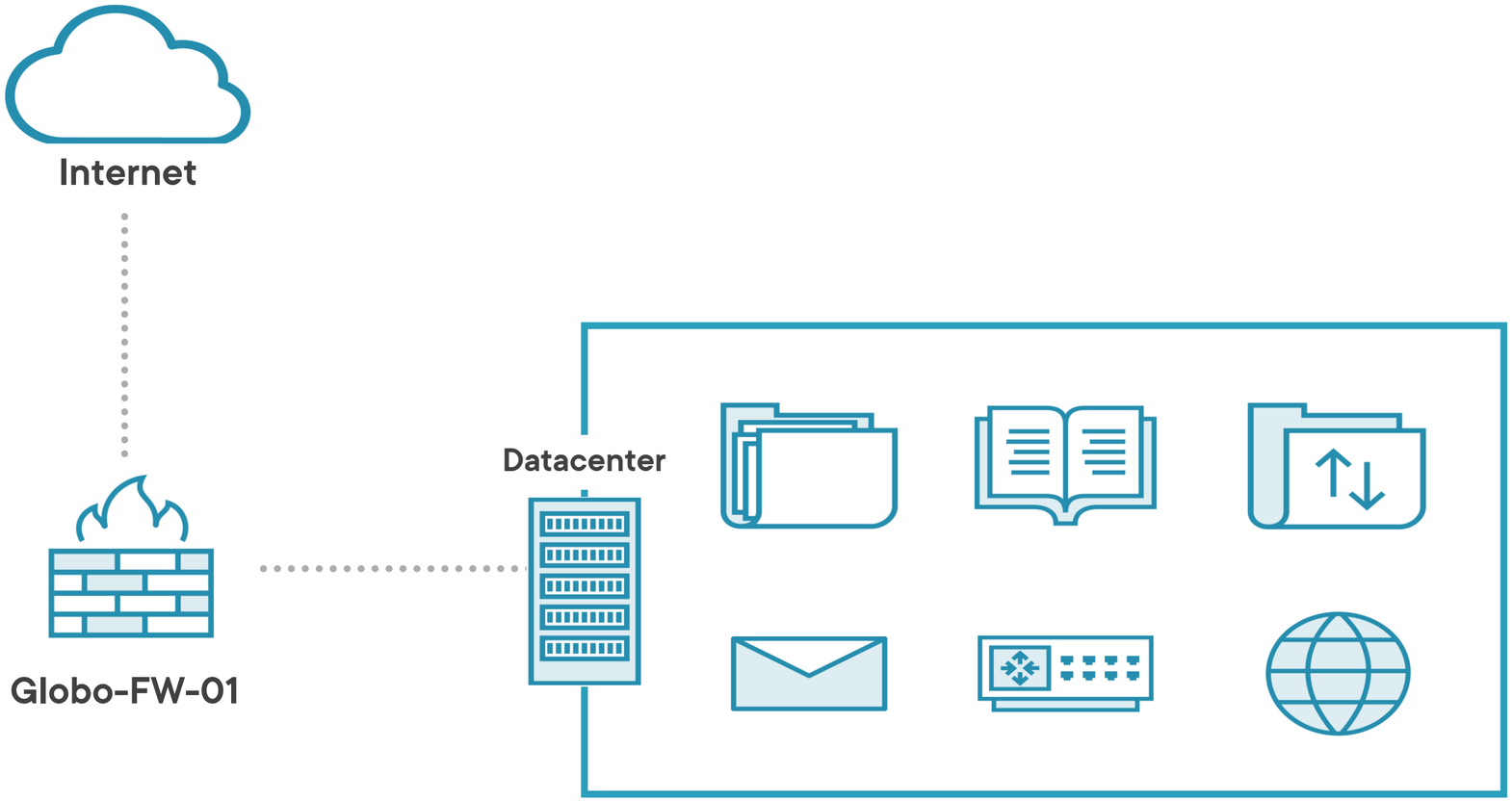


It's an appliance within a network used to protect internal resources from external access

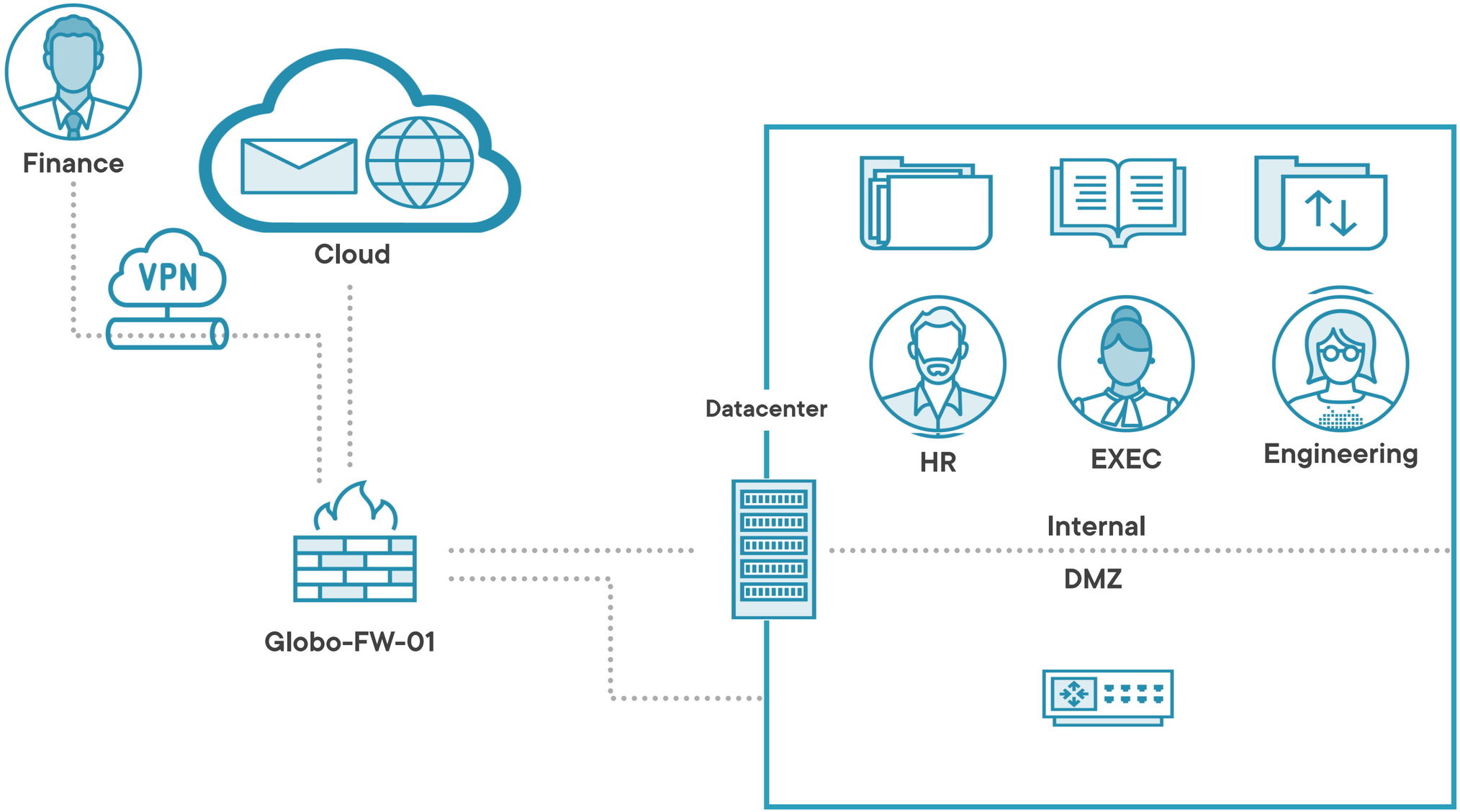
Used to monitor traffic and either *allows* or *denies* traffic based on predefined rules

Most firewalls are multi-homed, one interface connected to the internal network, another to the external

Firewalls



Firewalls



Firewall Terms

Bastion hosts

Moderates traffic

Hardened to withstand attacks

DMZ

Screened subnet firewall

Secure servers accessible from Internet

Access Control Lists

Packet filtering rules allowing or denying traffic

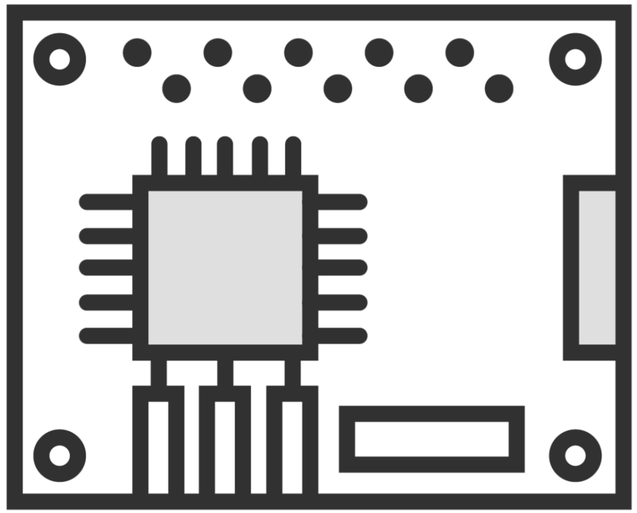
Stateful Packet Inspection

Examines packets headers, destination, protocol, dest. port, flags

Network Address/Port Translation (NAPT)

Multiple internal IPs mapped to single public IP

Types of Firewalls



Circuit level gateway

Application layer firewall

Web Application Firewall (WAF)

Intrusion Detection/Prevention Systems

Detects intrusions and can send alerts and/or blocks the attack

Filters inbound *and* outbound streams of traffic looking for malicious behavior

Malicious behavior detection is based on configured rules/signatures

Compares packets against known patterns or anomalies

Can be host-based or network-based

Search... Rule Doc Search

Documents Downloads Products Community Talos Res

Protect your network with the world's most powerful Open Source detection software.

Get Started

Download Rules

Documents

Snort 3.0 is he

Upgrade to experien new features and imp

Upgrade Now

Snort 3 is available!

Visit Snort.org/snort3 for more information.

DOWNLOAD SNORT

SNORT WEBSITE

SNORT BLOG

SNORT RULE DOCUMENTATION

Snort

Snort is an open-source intrusion prevention system offered by Cis
is capable of real-time traffic analysis and packet logging on IP net
It can perform protocol analysis, content searching/matching, and
be used to detect a variety of attacks and probes, such as buffer
overflows, stealth port scans, CGI attacks, SMB probes, OS fingerp
attempts, and much more.

Snort can be used as a packet sniffer like tcpdump, a packet logge
(useful for network traffic debugging, etc), network file logging dev
(capturing files in realtime from network traffic), or as a full blown
network intrusion prevention system. The mission for Snort is to d
the most effective and comprehensive real-time network defense
solutions on the planet.

Talos authors the official Snort Subscriber Rule Set.

IRC:

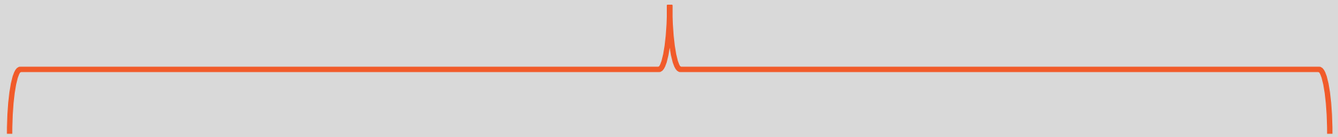
Service: irc.freenode.net
Channel: #snort

```
# The include files commented below have been disabled
# because they are not available in the stock Debian
# rules. If you install the Sourcefire VRT please make
# sure you re-enable them again:

#include $RULE_PATH/app-detect.rules
include $RULE_PATH/attack-responses.rules
include $RULE_PATH/backdoor.rules
include $RULE_PATH/bad-traffic.rules
#include $RULE_PATH/blacklist.rules
#include $RULE_PATH/botnet-cnc.rules
include $RULE_PATH/browser-chrome.rules
#include $RULE_PATH/browser-firefox.rules
#include $RULE_PATH/browser-ie.rules
#include $RULE_PATH/browser-other.rules
#include $RULE_PATH/browser-plugins.rules
#include $RULE_PATH/browser-webkit.rules
include $RULE_PATH/chat.rules
#include $RULE_PATH/content-replace.rules
include $RULE_PATH/ddos.rules
include $RULE_PATH/dns.rules
include $RULE_PATH/dos.rules
include $RULE_PATH/experimental.rules
#include $RULE_PATH/exploit-kit.rules
include $RULE_PATH/exploit.rules
#include $RULE_PATH/file-executable.rules
#include $RULE_PATH/file-flash.rules
#include $RULE_PATH/file-identify.rules
#include $RULE_PATH/file-image.rules
#include $RULE_PATH/file-multimedia.rules
#include $RULE_PATH/file-office.rules
#include $RULE_PATH/file-other.rules
#include $RULE_PATH/file-pdf.rules
include $RULE_PATH/finger.rules
include $RULE_PATH/ftp.rules
include $RULE_PATH/icmp-info.rules
include $RULE_PATH/icmp.rules
include $RULE_PATH/imap.rules
#include $RULE_PATH/indicator-compromise.rules
#include $RULE_PATH/indicator-obfuscation.rules
```

```
# Rules


alert icmp any any -> any any (msg:"Pinging like a boss! MJT...";sid:1000004;)
```



Snort rules

Action->Protocol->Source Addr->Source Port->Direction->Dest. Addr->Dest. Port

Snort Console Log

```
 08/08-14:36:17.844276  [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.27 -> 192.168.0
.176
08/08-14:36:17.844276  [**] [1:1000004:0] Pinging like a boss! MJT... [**] [Priority: 0] {ICMP} 192.168.0.27 -> 192.168.0.176
08/08-14:36:17.844276  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.27 -> 192.168.0.176
08/08-14:36:17.844307  [**] [1:1000004:0] Pinging like a boss! MJT... [**] [Priority: 0] {ICMP} 192.168.0.176 -> 192.168.0.27
08/08-14:36:17.844307  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.176 -> 192.168.0.2
7
08/08-14:36:18.852029  [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.27 -> 192.168.0.
176
```

Honeypots

A decoy to lure attackers who are trying to access the network

Loaded with vulnerabilities to distract the attacker

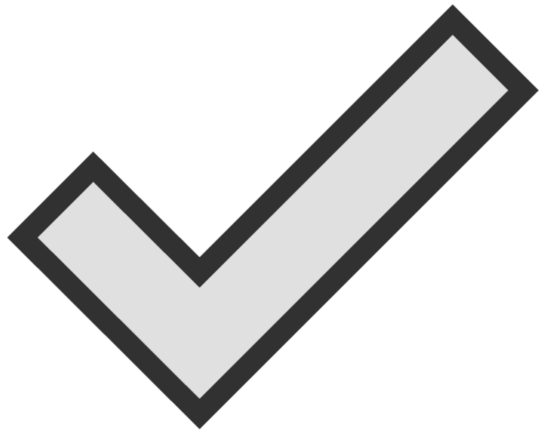
Any interaction is a sign of malicious activity

Types range from low to high interaction, research and production

Types of Honeypots

High-interaction

Medium-interaction



Low-interaction

Pure/production

PROJECT HONEY POT tm BETA

Welcome to Project Honey Pot | Login
Buy Swag
Refer a Friend
Terms of Use

Home | IP Data | Statistics | Services | Help | About

Welcome | Login | Create New Account

HELP STOP SPAMMERS BEFORE THEY EVEN GET YOUR ADDRESS!

SIGN UP FOR FREE

LOGIN

More about Project Honey Pot...

"Now a group of white hats is riding across the prairie to take a bite out of spam."
— Brian Livingston, Datamation

"By identifying illicit harvesters, Project Honey Pot opens up a new front in the war on spam."
— Ethan Preston, SecurityFocus

About Us
FAQ

Project Statistics

Trap Addresses Monitored
494,476,913

Trap Monitoring Capability
388,180,000,000

Spam Servers Identified
106,088,317

IPs Monitored
137,998,484

Harvesters Identified
891,540

Dictionary Attackers
28,378,278

Comment Spammers
1,304,500

Search Engines
2,176,250

Rule Breakers
37,248

NEW Bad Web Hosts NEW
1,343,101

https://projecthoneypot.org

Tactics and Techniques

Evading Firewalls/IDS

Use fragmented packets

- ***nmap -f 10.x.y.z***

Firewalking

- ***nmap --script=firewalk 10.x.y.z***

HTTP/ICMP tunneling

- Bypasses rules through obfuscation of traffic

DNS Tunneling

- Provides a TCP tunnel through DNS protocol

Banner Grabbing

- ***nmap -sV --script=banner 10.x.y.z***

Evading Firewalls/IDS

Denial of service

False positive generation

Libwhisker

Nessus

Countermeasures?

- Keep security appliances up to date
- Review ACLs and test

“E-voiding”/Tactics for Honeypots

Well configured honeypots are hard to detect

Target known IPs for valid machines

DO NOT **put any useful information on honeypots**

Place your honeypot outside your network, in a DMZ preferably

Honeypot Hunter

- Commercial scanner

Demo

Snort Live

Nmap evasion techniques

Learning Check

- **Network Address/Port Translation (NAT or NAPT)**
- **IDS/IPS**
- **Production or pure honeypot**
- **Stateful packet inspection**

Module Review

Key Learnings

Firewall, IDS, IPS and honeypot concepts

Tactics and Techniques

~~Countermeasures~~.Evasion

Up Next:
Domain Review