# Reconnaissance

sost@fabletech.com

Fabletech.com

1-2-2010

# Disclaimer

- In this course you will learn to attack systems which is illegal, so do not do this outside the lab.
- This course main purpose is to teach you how the attacker works in order to protect you self.
- Danish law "straffeloven §263 a" states that gaining access to a non public system is illegal... so don't

# YOU

- Show interest. We do not do it for the money
- Be active. If you don't get it ask again. If you believe we are wrong say so.
- We try to make the exercises as real as possible, which makes it easy to cheat. So don't.
- We have made this course for you. So if you have any ideas that could make this course better send us a mail. Don't wait until the end of the course. Let's us know.

# Yet another security course.... why

# Course overview

- Reconnaissance
- Web exploiation
- Reversing
- Shellcode
- Stack overflow
- Heap overflow
- Static analysis and fuzzing

# Reconnaissance

- This lesson is not only about how pentesters work, but also how hackers work.
- Penetrations testing (pen testing in short) are often divided into to categories. Blackbox and Whitebox testing. Blackbox testing is done without prior knowledge of the infrastructure. Whitebox testing is done with prior knowledge.

# What are we trying to find

- More info etc. Mail addresses news groups entries.
- Unpatched systems
- System that is not configured properly
- Applications with known bugs
- Weak system. This includes people

# Strategy

- Our overall goal is of course to gain access
- Leave as little footprints as possible
- Systematic iterative process. Even over time!

# My approach

- Onion like model
- The outer layers leave smaller footprints
- Each layer is iterative
- Peal the onion if necessary

# Obstacles

- Firewalls
- IDS
- Firewall topology
- Honey pots

# The basics IPv4

# TCP

# UDP

# ICMP

# Firewall

A firewall is a part of a computer system or network that is designed to block unauthorized access while permitting authorized communications.

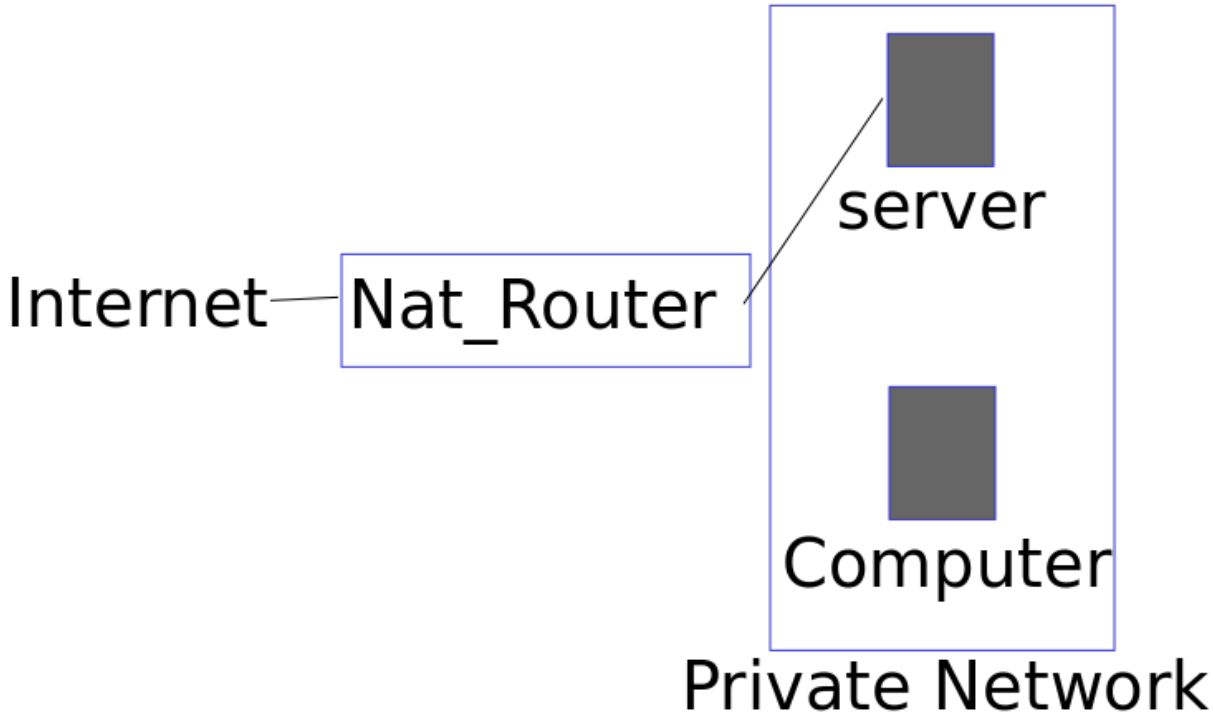
# Firewall types

- Packet firewall(stateless and statefull)
- Circuit-level gateway
- Proxy servers
- Application gateway

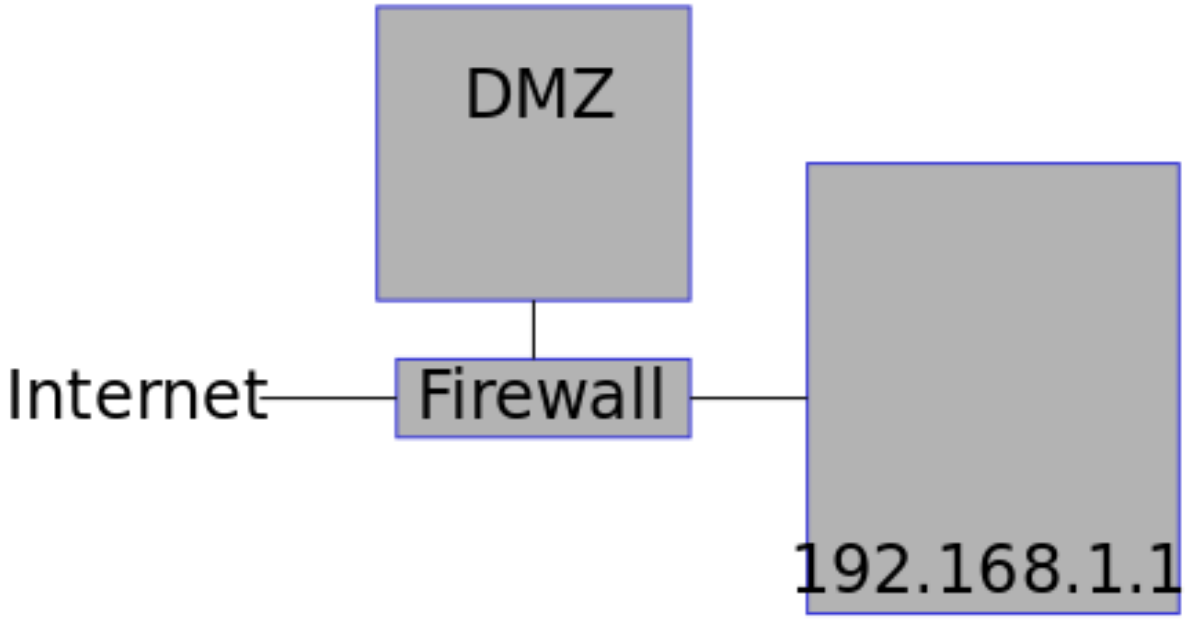
# IDS

- HIDS (host based) or NIDS (network based)
- Passive or Reactive
- Signature based or Statistical based

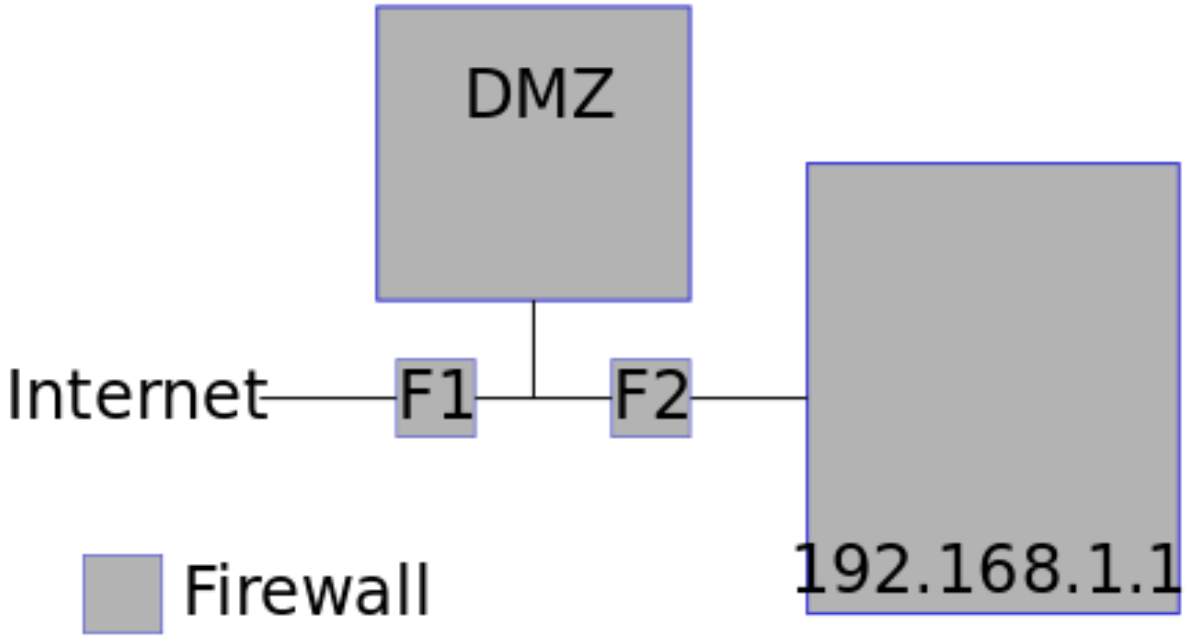
# Firewall topology. Nat



# Firewall topology. DMZ



# Firewall topology. More secure DMZ



# Honey pots

Vulnerable servers that are sitting targets for hackers. Their purpose is get hacked in order to gain knowledge of how the attacker works.

# Target

Fabletech.com

# Methods

- Search engine
- BGP
- DNS
- Whois
- Port scanning
- Banner grabbing

# Google for the win

The more information you collect the greater you chances are for success.

- Google Hacking (http://www.hackersforcharity.org/ghdb/)

# BGP Border gateway protocol

The core route on the internet is done by BGP. Each BGP router has an id number called autonomous systems (AS). The BGP service port is located on 179 tcp and udp. Unfortunately these are almost never accessible.

# traceroute

- traceroute (ping)
- tracepath (udp)
- tcptracpath (tcp)

# DNS udp(tcp) port 53

- dig diku.dk find the ip
- dig SOA diku.dk find start of authority
- dig -x ip find the domain name
- dig MX diku.dk find the ip of the mail servers
- dig AXFR diku.dk (don't try this it does not work )
- Records: A, AAAA, ANY, MX, SOA, LOC, TXT etc..

# Whois?

Whois will attempt to lookup internet resources such as Domain name, ips and AS numbers.

# Port scanning

There are many scanner tools out there and all of them works in different ways. It is vital to know your port scanner tool in order to get the results. NMAP is the one that we are going to use.

# nmap The portscanner

- default only scans 1660 ports
- ports can have 6 states. open, closed, filtered, unfiltered, open—filtered and closed—filtered.
- can detect the os type -O
- can scan ip ranges
- can traceroute
- can be scripted

# Nmap discovery

- Ping sweeping nmap -sP target (used to find alive host in a range)
- SYN scan nmap -PS
- ACK scan nmap -PA
- UDP scan nmap -PU
- SCTP scan nmap -PY
- ICMP Echo nmap -PE
- ICMP timestamp nmap -PP
- ICMP netmask nmap -PM
- NO ping -PN
- ARP ping -PR

# nmap scan types

- TCP sync scan nmap -sS
- TCP connect scan nmap -sT
- UDP scan nmap -sU
- TCP NULL scan nmap -sN (Does not set any bits TCP header flag is 0)
- TCP FIN scan nmap -sF
- Xmax scan nmap -sX (FIN, PSH, URG flags)
- TCP ack scan -sA
- TCP Window scan -sW (Same as ack but open ports have positive window size)
- TCP Maimon (fin/ack) scan -sM
- Idle scan

# Bannergrabbing

```
host$ telnet localhost 80
Trying ::1...
Connected to localhost.
Escape character is '^]'.
GET / HTML/1.1

HTTP/1.1 200 OK
Date: Sat, 23 Jan 2010 11:16:53 GMT
Server: Apache/2.2.12 (Ubuntu)
Last-Modified: Mon, 07 Dec 2009 14:45:41 GMT
Content-Length: 177
Vary: Accept-Encoding
Connection: close
Content-Type: text/html
```

# Reverse Proxy DEMO

# Tools

- Nessus
- Metasploit (demo)

# DoS

- Syn flooding
- Ping of Death
- Teardrop
- Ping Flooding
- Amplification Attacks
- Distributed DoS Flooding

# Connection hijacking

- Arp poisoning
- RST hijacking
- Continued Hijacking