Reconnaissance

sost@fabletech.com

Fabletech.com

2011

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/pentesting
- Web exploitation
- Reversing
- Shellcode
- Stack overflow
- Heap overflow
- Static analysis and fuzzing

How do I pass this course?

There will be 7 assignments and one final assignment. You will need to pass 5 out of the 7 assignments in order to hand in the final assignment. In short pass 5 of the weekly assignments and the final . . . that is it.

Reconnaissance

- This lesson is not only about how pentesters work, but also how hackers work.
- Gaining access to systems normally consist of several steps. I normally divide this into reconnaissance and pentesting.
- 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!

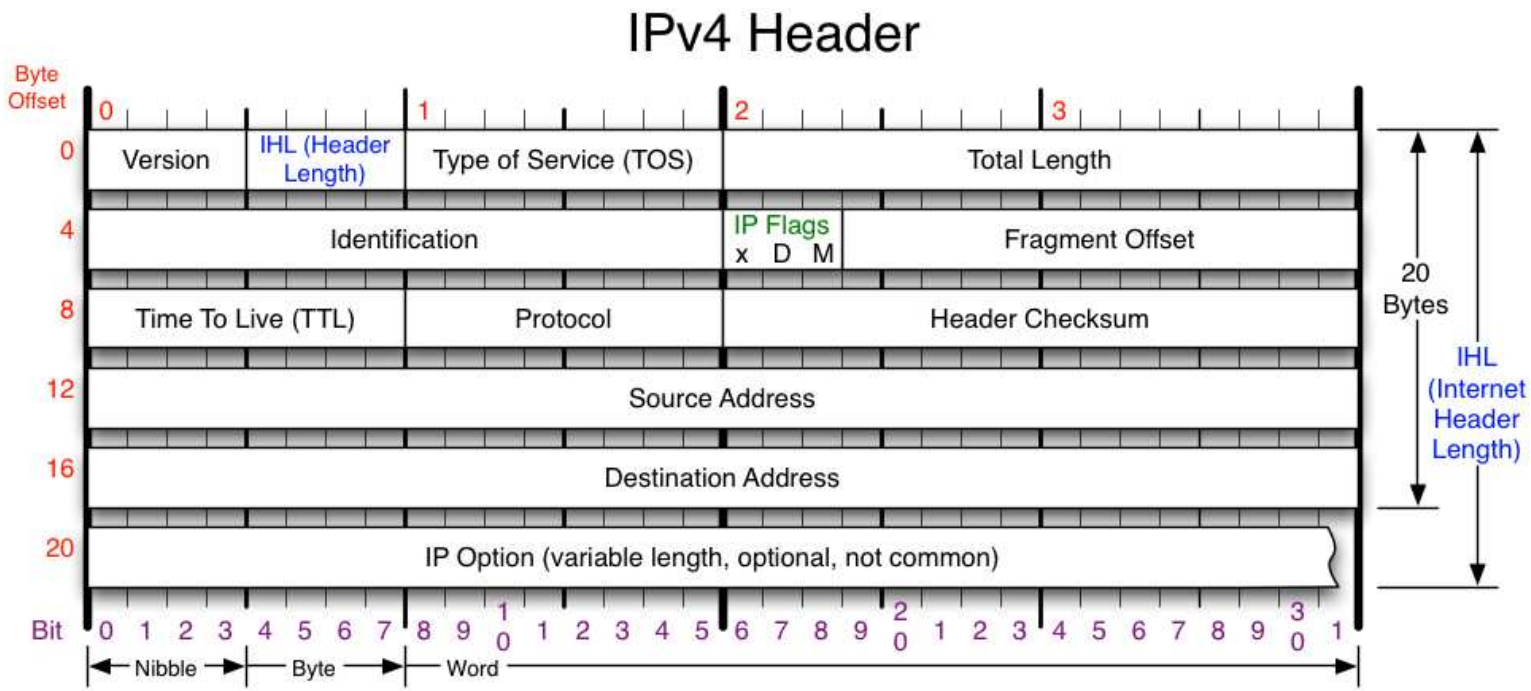
My approach

- 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



Version

Version of IP Protocol. 4 and 6 are valid. This diagram represents version 4 structure only.

Header Length

Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.

Protocol

IP Protocol ID. Including (but not limited to):

1 ICMP	17 UDP	57 SKIP
2 IGMP	47 GRE	88 EIGRP
6 TCP	50 ESP	89 OSPF
9 IGRP	51 AH	115 L2TP

Total Length

Total length of IP datagram, or IP fragment if fragmented. Measured in Bytes.

Fragment Offset

Fragment offset from start of IP datagram. Measured in 8 byte (2 words, 64 bits) increments. If IP datagram is fragmented, fragment size (Total Length) must be a multiple of 8 bytes.

Header Checksum

Checksum of entire IP header

IP Flags

x D M

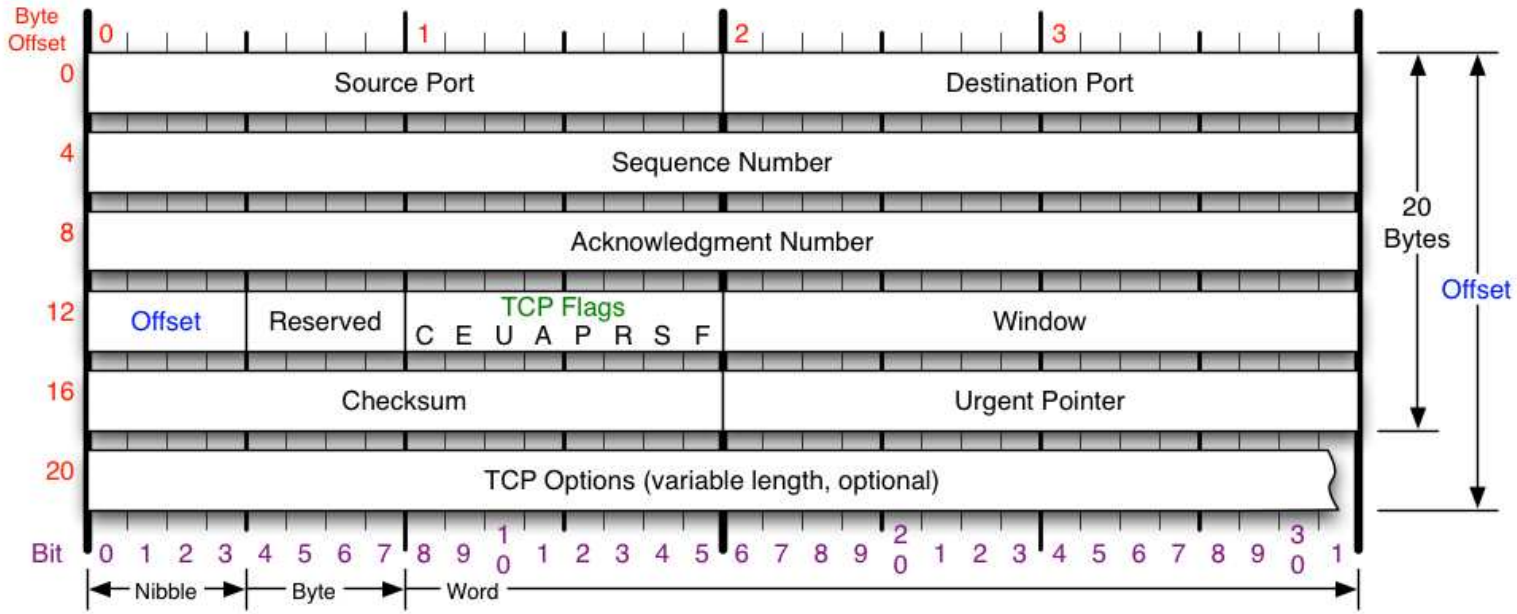
x 0x80 reserved (evil bit)
D 0x40 Do Not Fragment
M 0x20 More Fragments follow

RFC 791

Please refer to RFC 791 for the complete Internet Protocol (IP) Specification.

TCP

TCP Header



TCP Flags

C E U A P R S F

Congestion Window

C 0x80 Reduced (CWR)
E 0x40 ECN Echo (ECE)
U 0x20 Urgent
A 0x10 Ack
P 0x08 Push
R 0x04 Reset
S 0x02 Syn
F 0x01 Fin

Congestion Notification

ECN (Explicit Congestion Notification). See RFC 3168 for full details, valid states below.

Packet State	DSB	ECN bits
Syn	0 0	1 1
Syn-Ack	0 0	0 1
Ack	0 1	0 0
No Congestion	0 1	0 0
No Congestion	1 0	0 0
Congestion	1 1	0 0
Receiver Response	1 1	0 1
Sender Response	1 1	1 1

TCP Options

0 End of Options List
1 No Operation (NOP, Pad)
2 Maximum segment size
3 Window Scale
4 Selective ACK ok
8 Timestamp

Checksum

Checksum of entire TCP segment and pseudo header (parts of IP header)

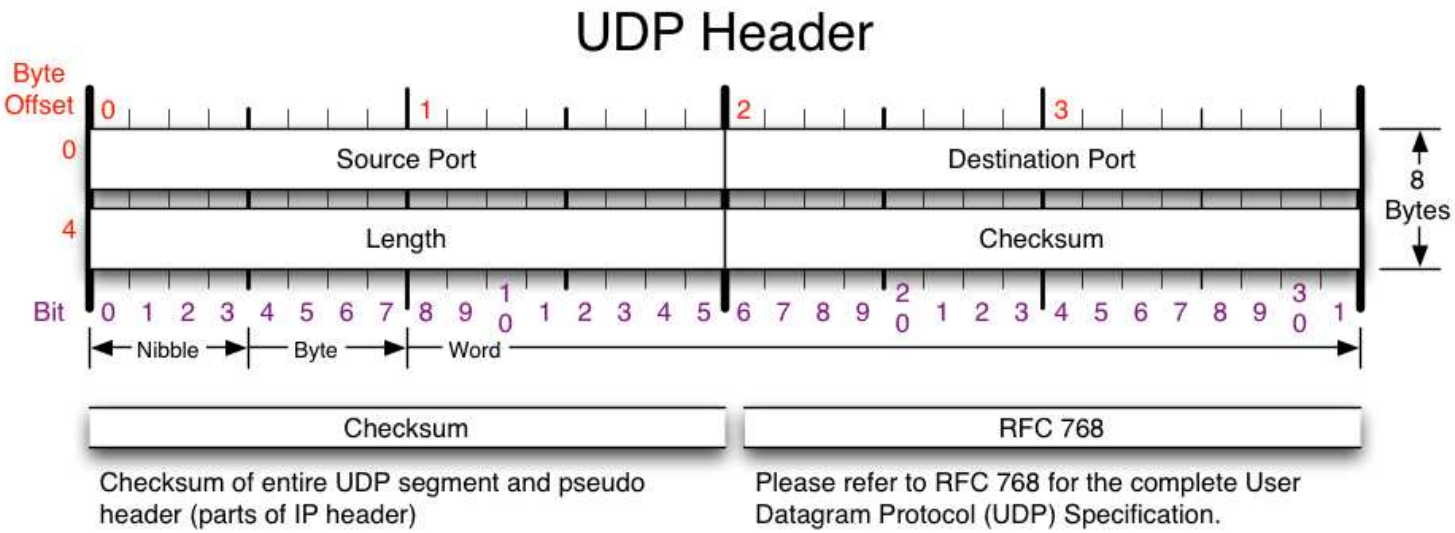
Offset

Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.

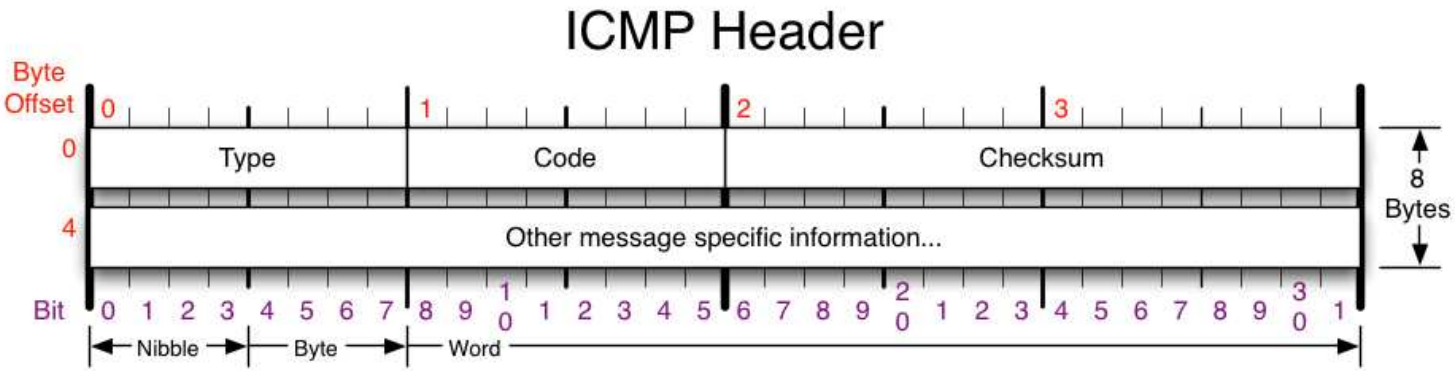
RFC 793

Please refer to RFC 793 for the complete Transmission Control Protocol (TCP) Specification.

UDP


UDP Header
Byte Offset
0
4
Bit
0 1 2 3
Source Port
Destination Port
Length
Checksum
8 Bytes
0 1 2 3 4 5 6 7 8 9 10 1 2 3 4 5 6 7 8 9 20 1 2 3 4 5 6 7 8 9 30 1
Nibble
Byte
Word
Checksum
RFC 768
Checksum of entire UDP segment and pseudo header (parts of IP header)
Please refer to RFC 768 for the complete User Datagram Protocol (UDP) Specification.
Copyright 2008 - Matt Baxter - mjb@fatpipe.org - www.fatpipe.org/~mjb/Drawings/

ICMP



ICMP Message Types

Type	Code/Name
0	Echo Reply
3	Destination Unreachable
	0 Net Unreachable
	1 Host Unreachable
	2 Protocol Unreachable
	3 Port Unreachable
	4 Fragmentation required, and DF set
	5 Source Route Failed
	6 Destination Network Unknown
	7 Destination Host Unknown
	8 Source Host Isolated
	9 Network Administratively Prohibited
	10 Host Administratively Prohibited
	11 Network Unreachable for TOS
3	Destination Unreachable (continued)
	12 Host Unreachable for TOS
	13 Communication Administratively Prohibited
4	Source Quench
5	Redirect
	0 Redirect Datagram for the Network
	1 Redirect Datagram for the Host
	2 Redirect Datagram for the TOS & Network
	3 Redirect Datagram for the TOS & Host
8	Echo
9	Router Advertisement
10	Router Selection
11	Time Exceded
	0 TTL Exceeded
	1 Fragment Reassembly Time Exceeded
12	Parameter Problem
	0 Pointer Problem
	1 Missing a Required Operand
	2 Bad Length
13	Timestamp
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply
30	Traceroute

Checksum

Checksum of ICMP header

RFC 792

Please refer to RFC 792 for the Internet Control Message protocol (ICMP) specification.

Firewall

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

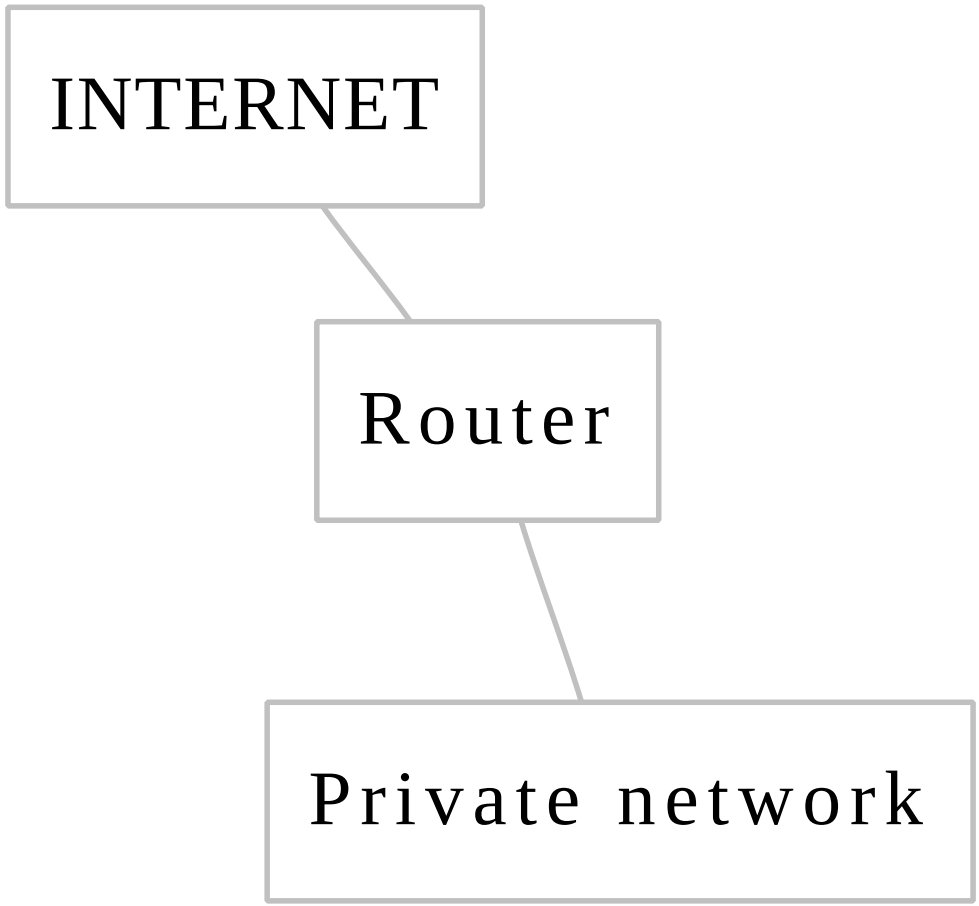
Firewall types

- Packet filtering(stateless and statefull)
- Circuit-level gateways
- Application gateways

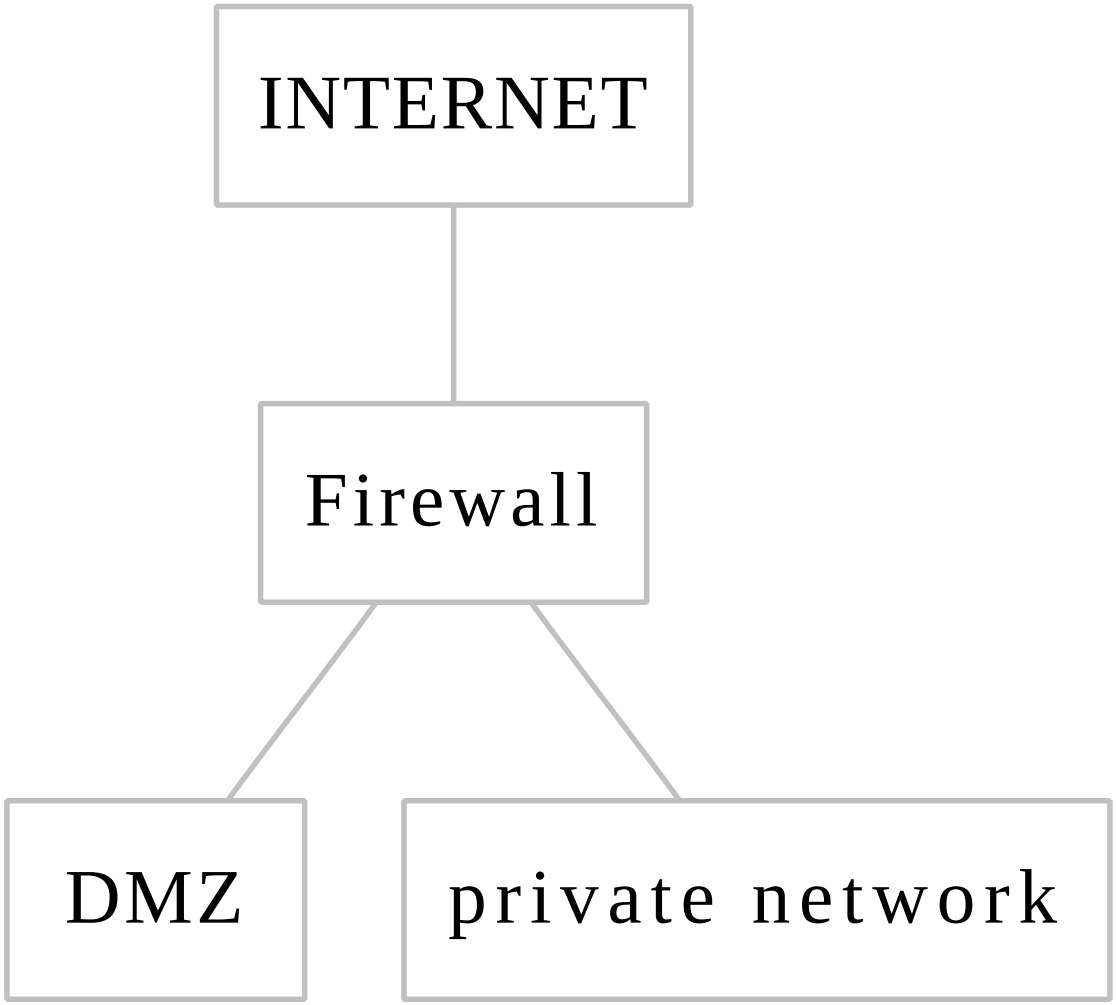
IDS

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

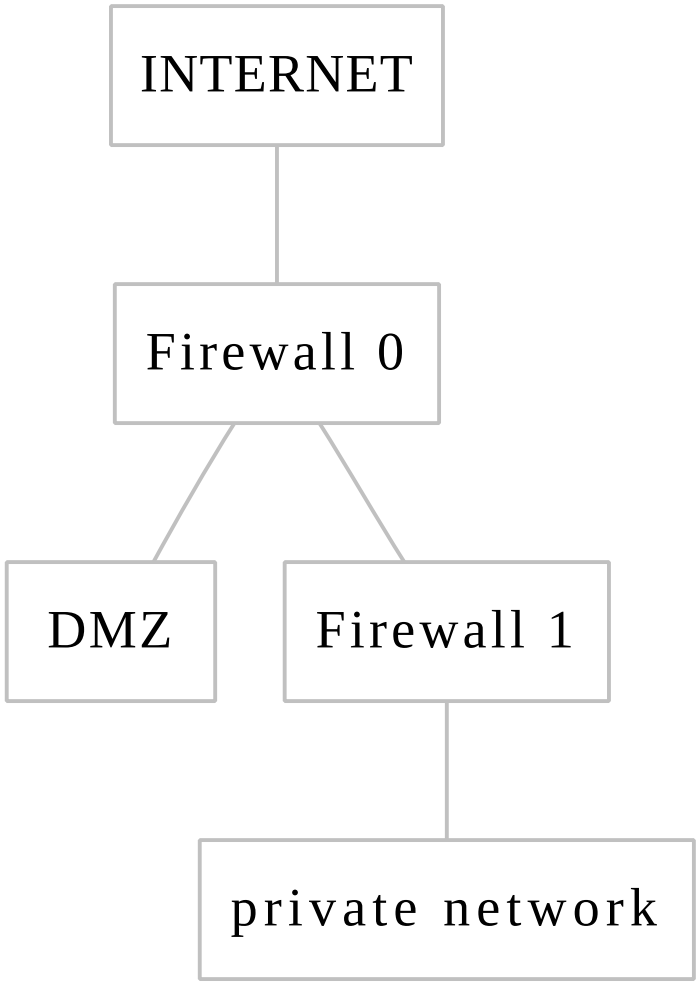
Firewall topology. Nat



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

What would be the strategy for attacking 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)
- tcptracepath (tcp)

tracepath/traceroute

```
> tracepath ask.diku.dk/22
 ...
 8:  adm3-27.net.ku.dk (130.225.204.5)
 9:  life3-25.net.ku.dk (192.38.110.150)
10:  hco3-22.net.ku.dk (192.38.110.217)
11:  hco2-25.net.ku.dk (130.225.204.90)
12:  diku.net.ku.dk (130.225.204.106)
13:  192.38.110.242 (192.38.110.242)
14:  no reply
```

tcptracepath

```
>  tcptraceroute ask.diku.dk 22
...
 8  adm3-27.net.ku.dk (130.225.204.5)
 9  life3-25.net.ku.dk (192.38.110.150)
10  hco3-22.net.ku.dk (192.38.110.217)
11  hco2-25.net.ku.dk (130.225.204.90)
12  diku.net.ku.dk (130.225.204.106)
13  192.38.110.242
14  ask.diku.dk (130.225.96.225) [open]
```

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, 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

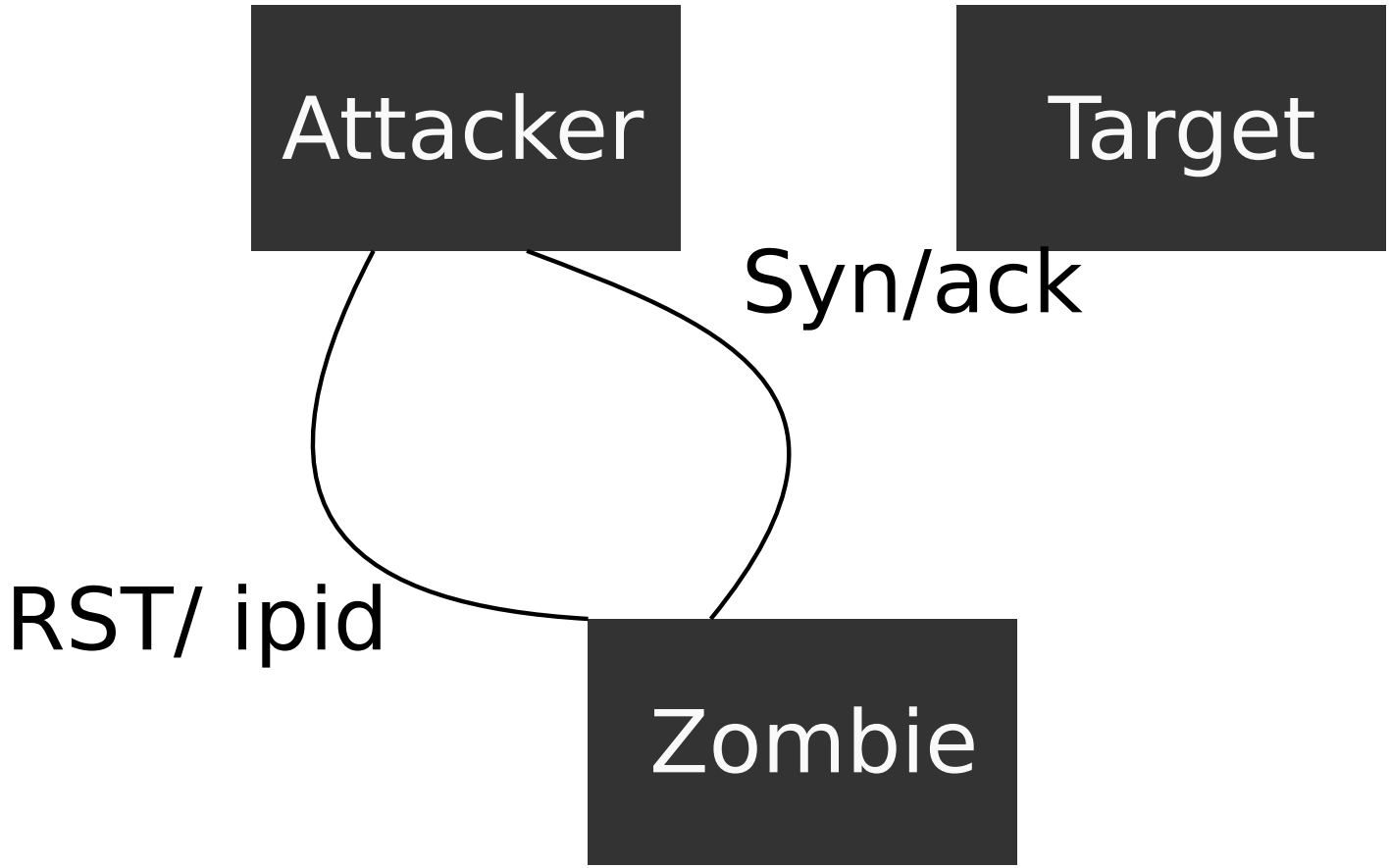
Nmap discovery

- Ping sweeping nmap -sP target (used to find alive host in a range arp and tcp)
- SYN scan nmap -PS (syn)
- ACK scan nmap -PA (ack)
- UDP scan nmap -PU (srcport 49152)
- SCTP scan nmap -PY (not really used)
- ICMP Echo nmap -PE
- ICMP timestamp nmap -PP (rfc 792)
- ICMP netmask nmap -PM (rfc 950)
- NO ping -PN (skip discovery)
- ARP ping -PR

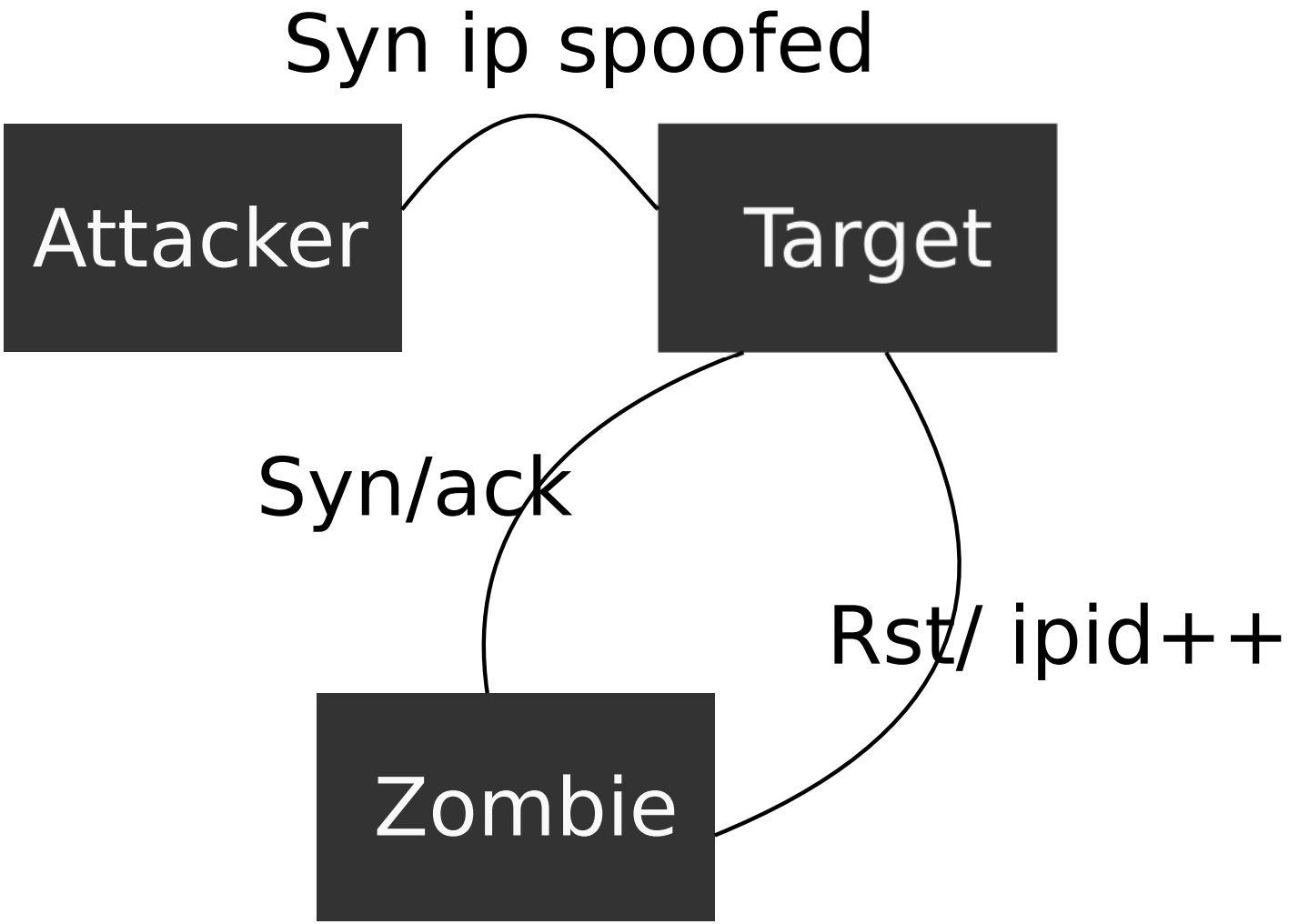
nmap scan types

- TCP sync scan nmap -sS (open: syn,syn/ack and closed: syn,rst/ack)
- TCP connect scan nmap -sT (syn,syn/ack,ack)
- UDP scan nmap -sU
- TCP NULL scan nmap -sN (Does not set any bits TCP header flag is 0)
- TCP FIN scan nmap -sF (FIN)
- Xmas scan nmap -sX (FIN, PSH, URG flags)
- TCP ack scan -sA (ack scan WTF!! open and closed return rst)
- TCP Window scan -sW (Same as ack but open ports have positive window size)
- TCP Maimon (fin/ack) scan -sM (drop pkt if open)
- Idle scan (lets go)

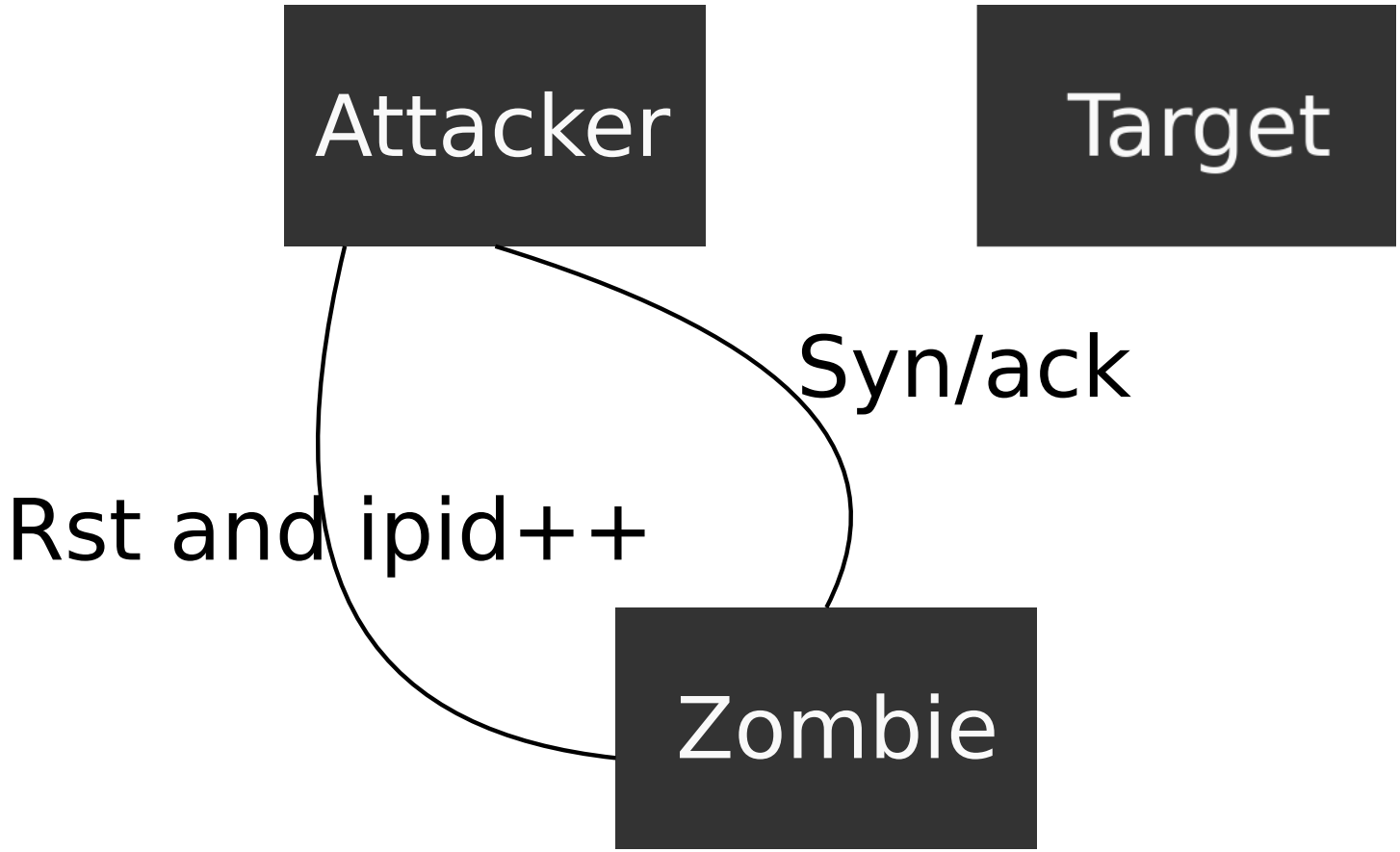
Idle scan/ port open



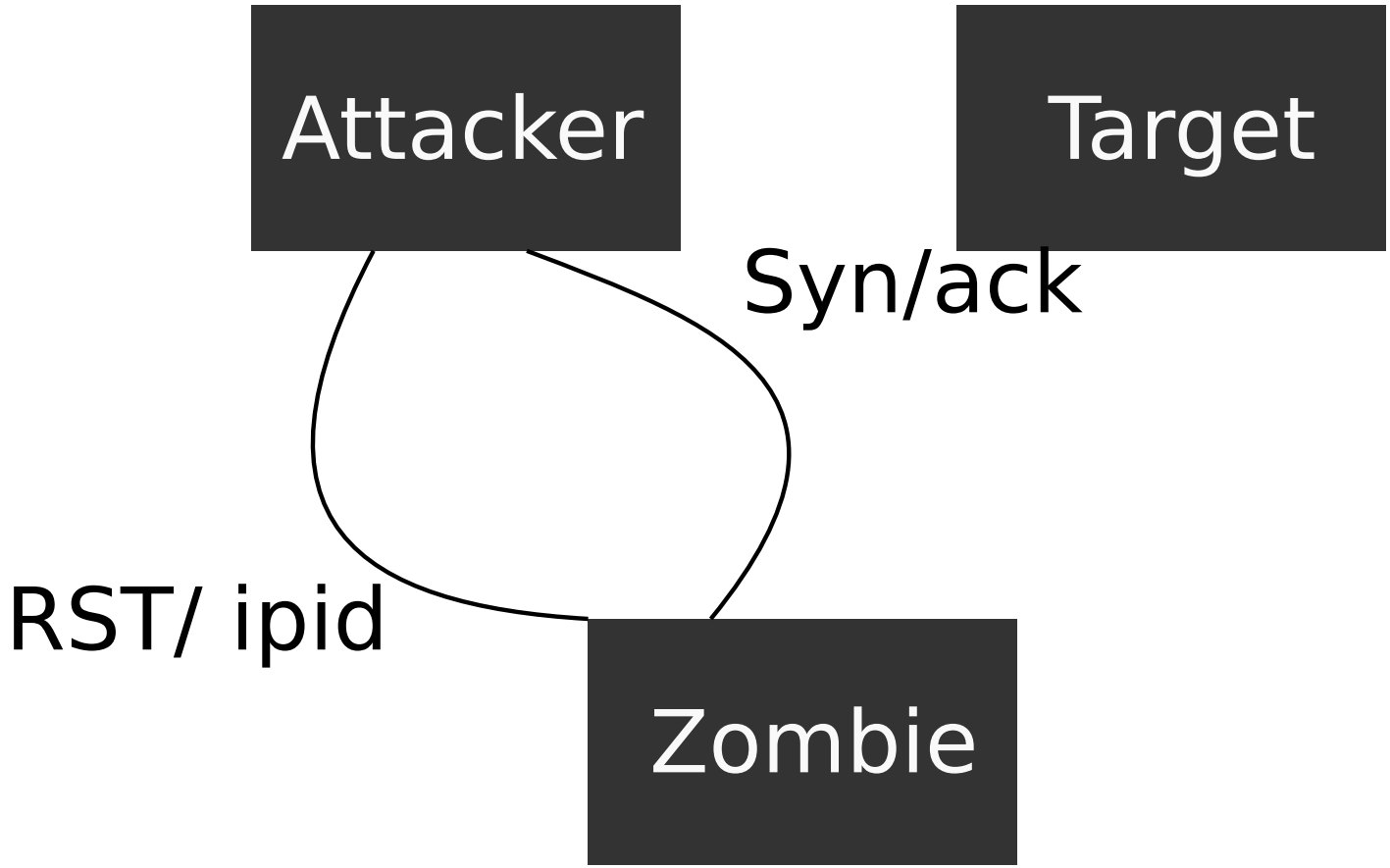
Idle scan/ port open



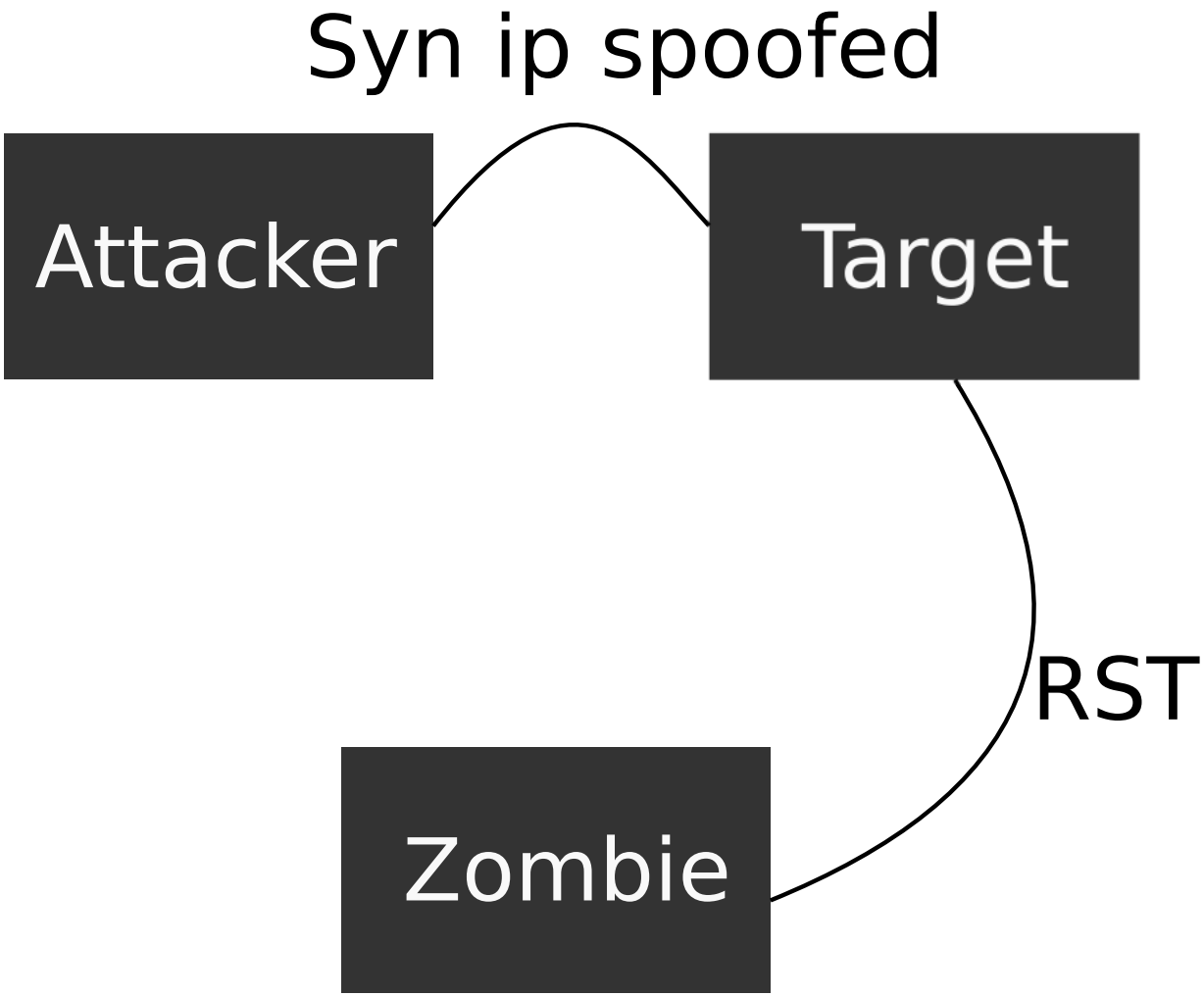
Idle scan/ port open



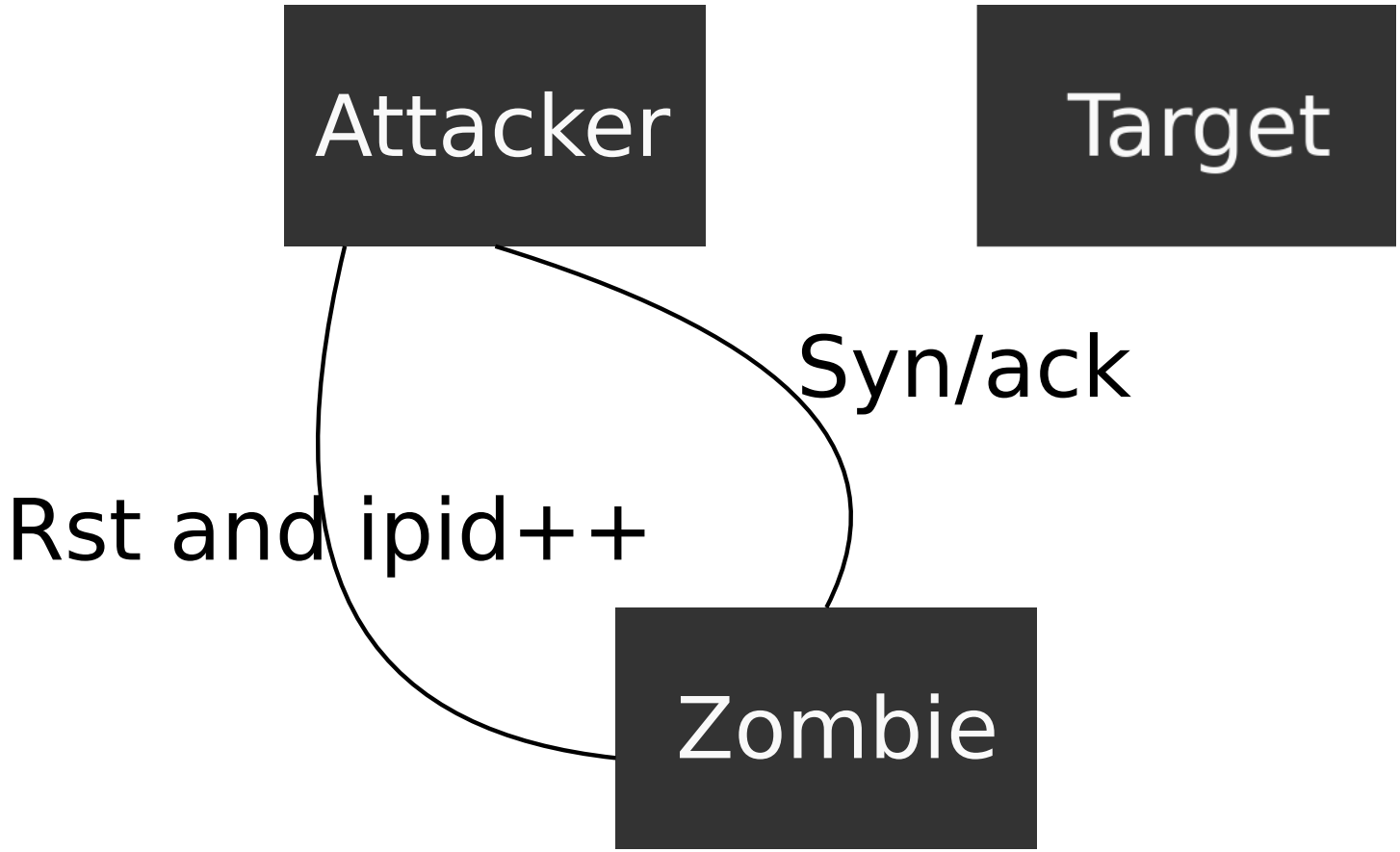
Idle scan/ port closed



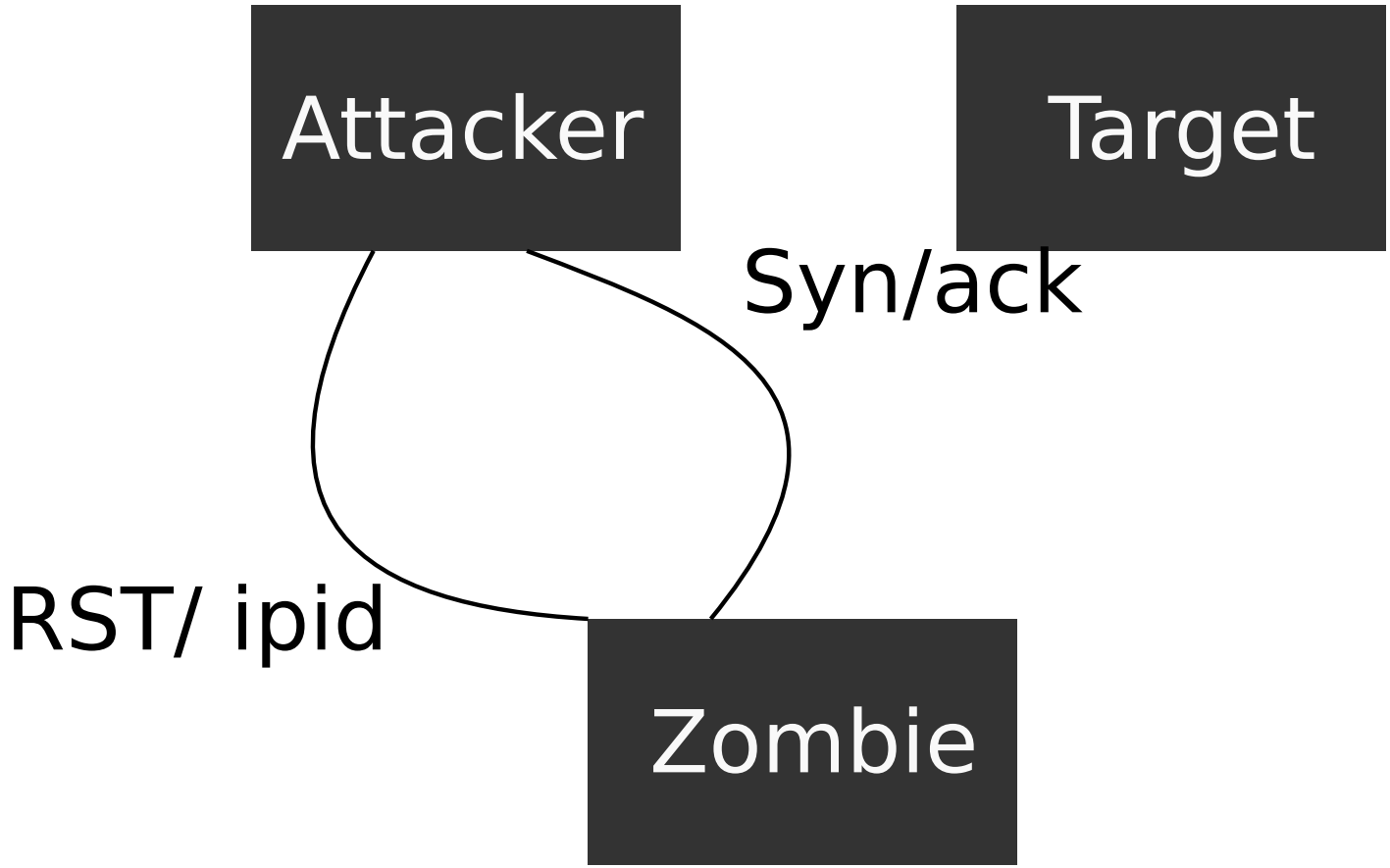
Idle scan/ port closed



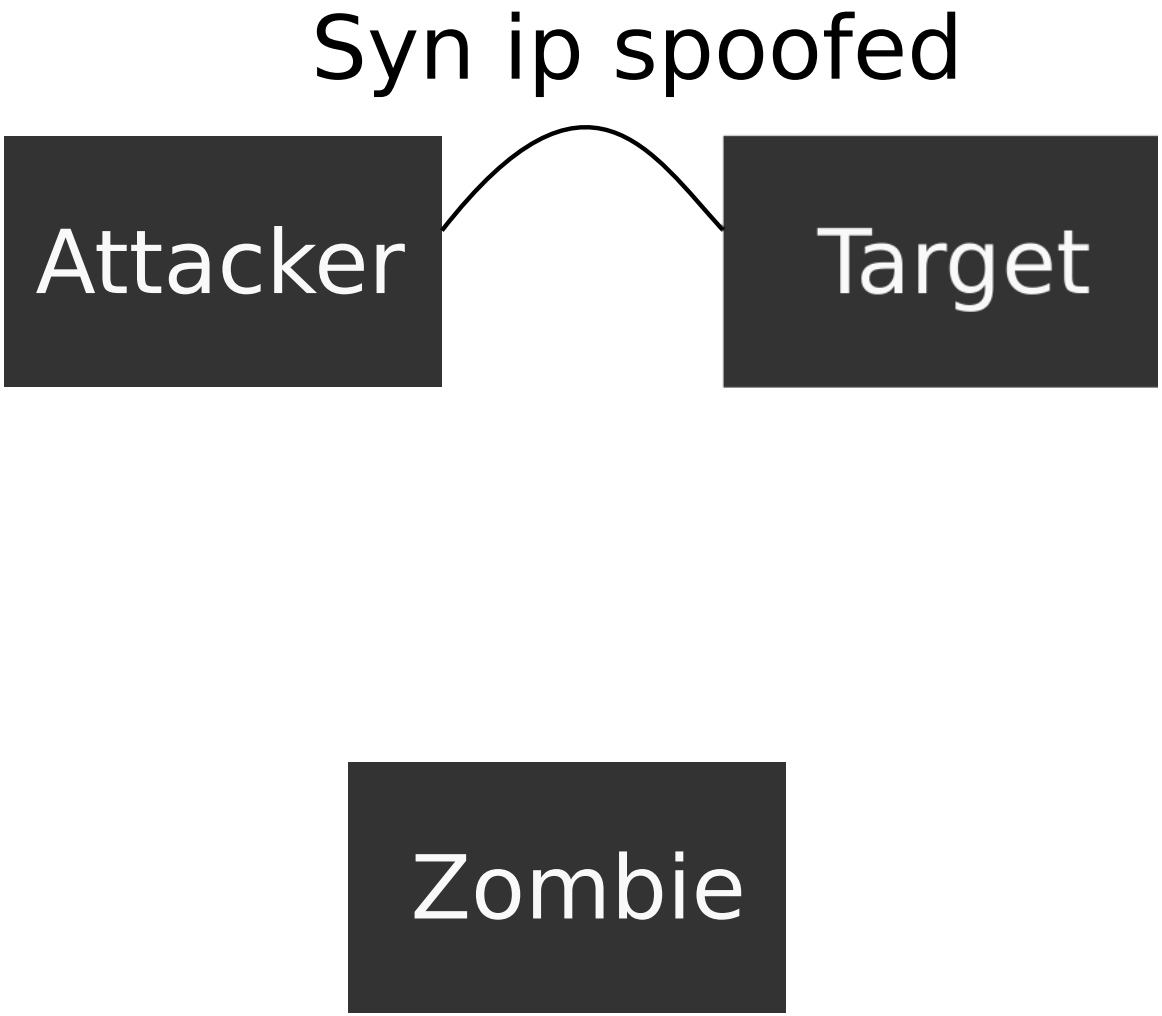
Idle scan/ port closed



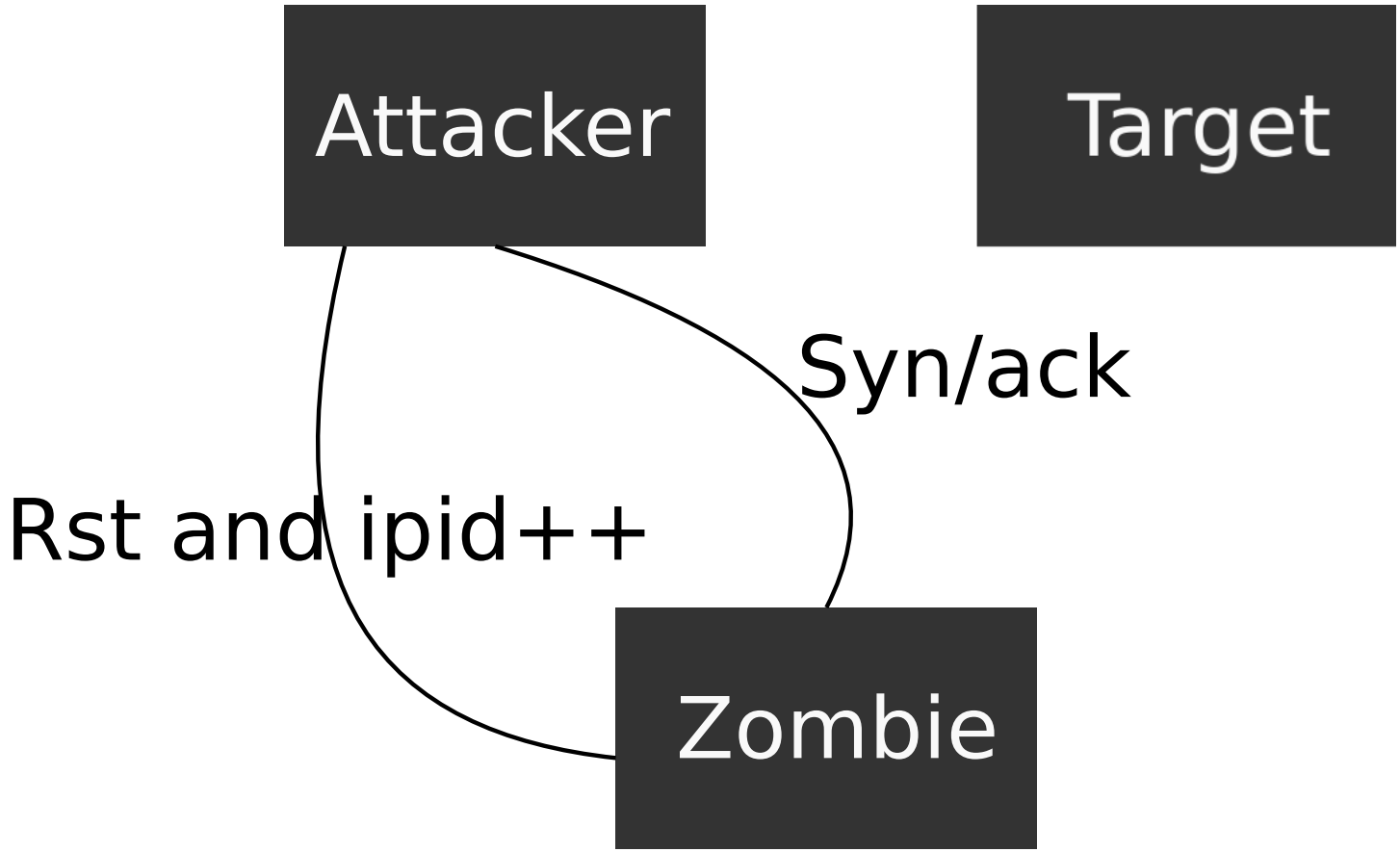
Idle scan/ port filtered



Idle scan/ port filtered



Idle scan/ port filtered



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

Example

```
> curl -i -s http://localhost/site1/ | grep ^Server
Server: Apache/2.2.14 (Ubuntu)
> curl -i -s http://localhost/site2/ | grep ^Server
Server: SimpleHTTP/0.6 Python/2.6.4
```

Pentesting/Tools

- Nessus (open source until 3.0)
- Metasploit (open source)
- Core Impact (not open source)
- Canvas (not open source)

DoS

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

Connection hijacking

- Arp poisoning
- RST hijacking
- Continued Hijacking

HBGary Federal

This week assignment

In this exercise you will pentest the network 192.168.56.*. You can access it through pcs.diku.dk. You goal is to locate the hidden service. You will know you have found the service when you get the answer "hidden service found...". Write a short essay one page MAX where you account for your findings.