Abusing Network Protocols

ithilgore

sock-raw.org

Why bother with Network Protocols?

Why not just code another 0day for your common web server out there?

"There is no saving the Internet.
There is postponing the inevitable
for a little longer."

"In short, we've got your passwords, your communication, and control over your computer."

Google™
talk
BETA

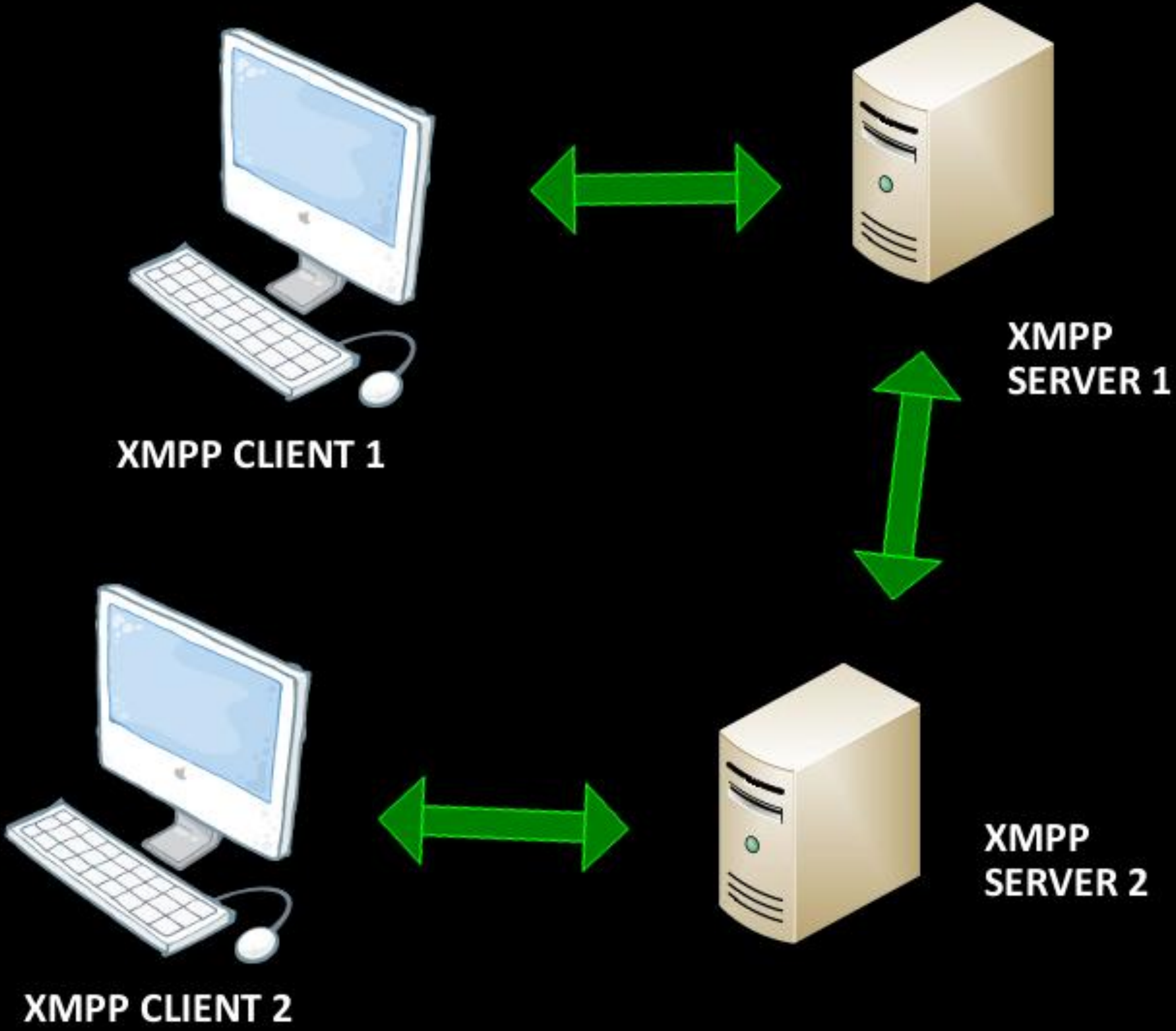
facebook®

CISCO™

XMPP™

XMPP

- XML as base format
- Instant Messaging / Middleware
- Decentralized Arch - Direct Federation Model
- Messages: “fire-and-forget” transport
- Presence: publish-subscribe mechanism
- IQ (Info/Query): control, error reporting etc



XMPP CLIENT 1

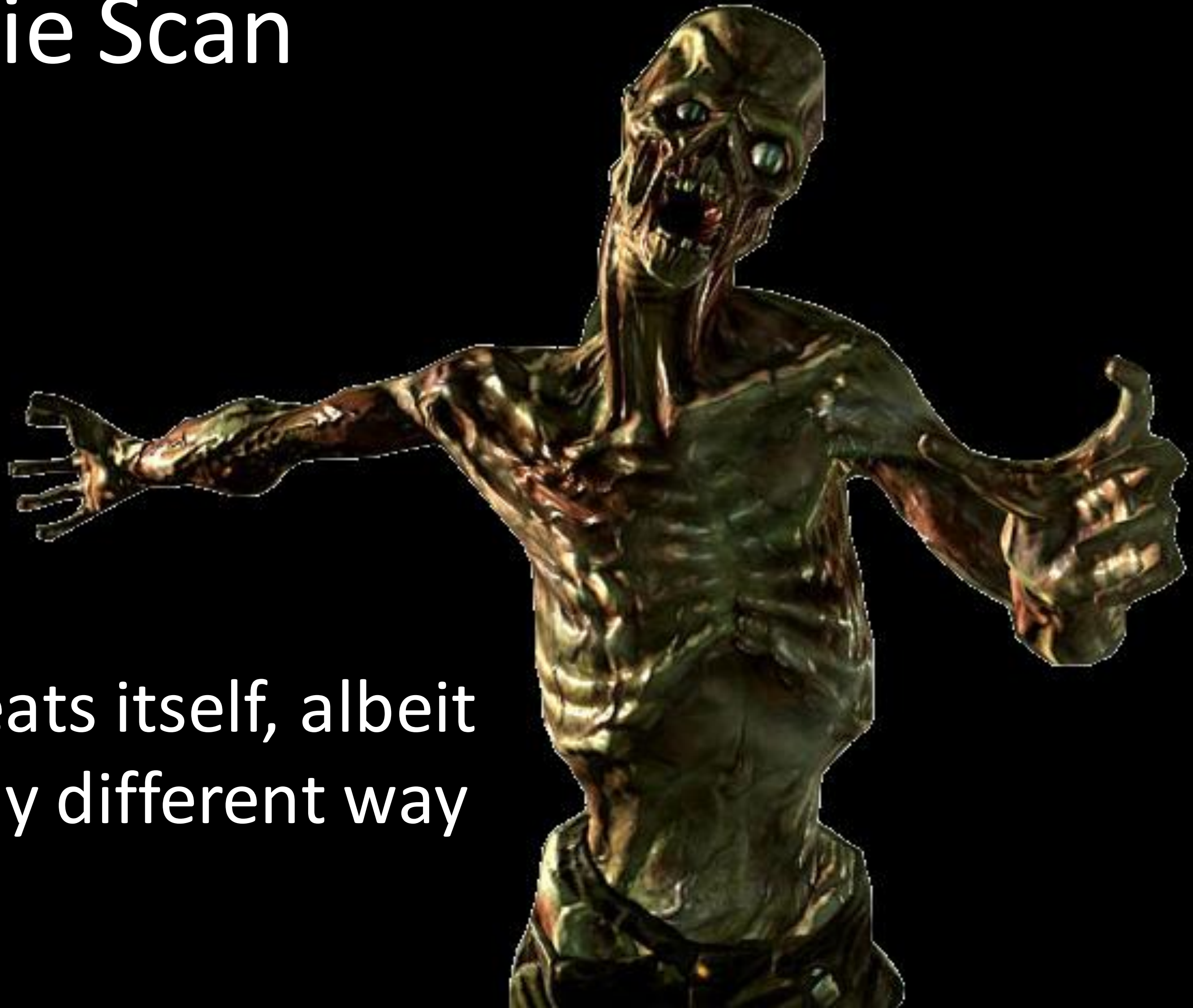
XMPP
SERVER 1

XMPP CLIENT 2

XMPP
SERVER 2

A long time ago in this galaxy…

Zombie Scan

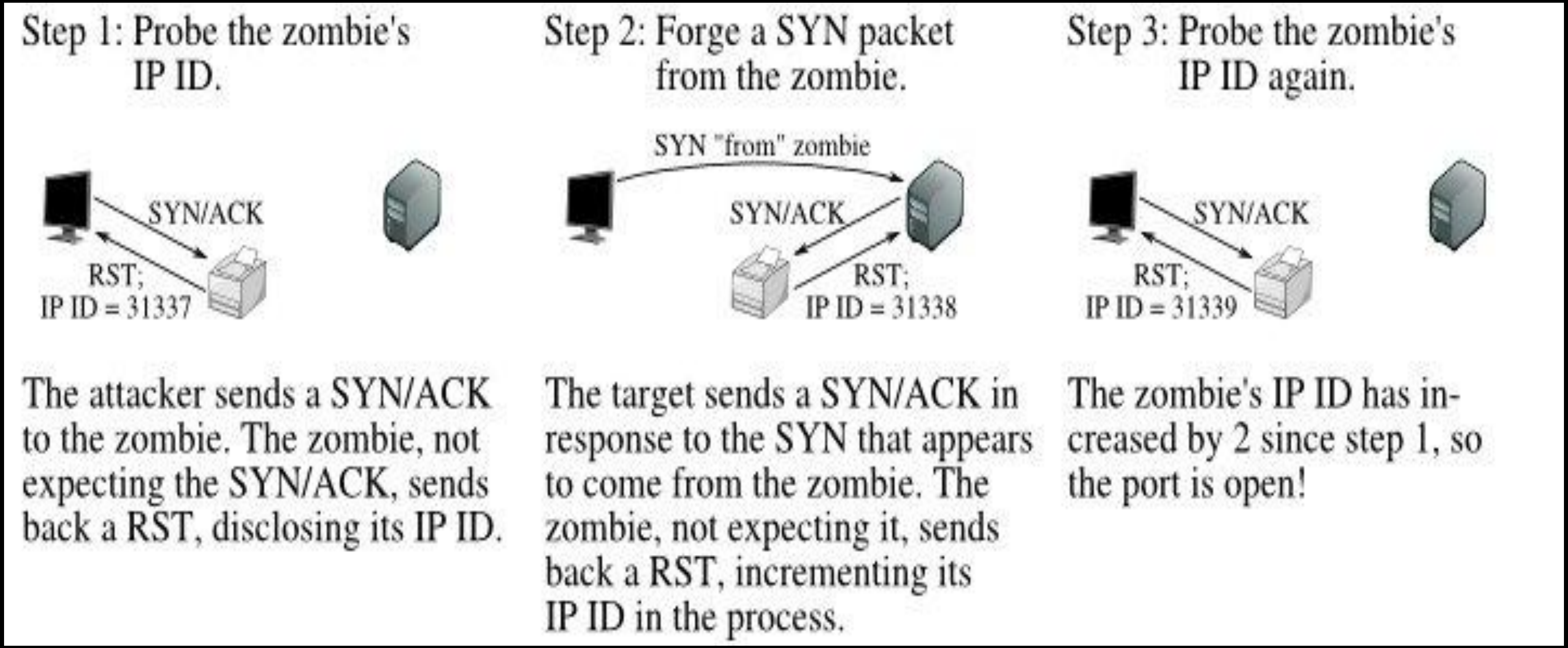


History repeats itself, albeit in a slightly different way

TCP facts

- Send SYN probe:
  Port Closed -> RST
  Port Open -> SYN/ACK
- Unsolicited SYN/ACK -> RST
- Unsolicited RST -> ignore

Zombie Scan – Open port



Step 1: Probe the zombie's IP ID.

The attacker sends a SYN/ACK to the zombie. The zombie, not expecting the SYN/ACK, sends back a RST, disclosing its IP ID.

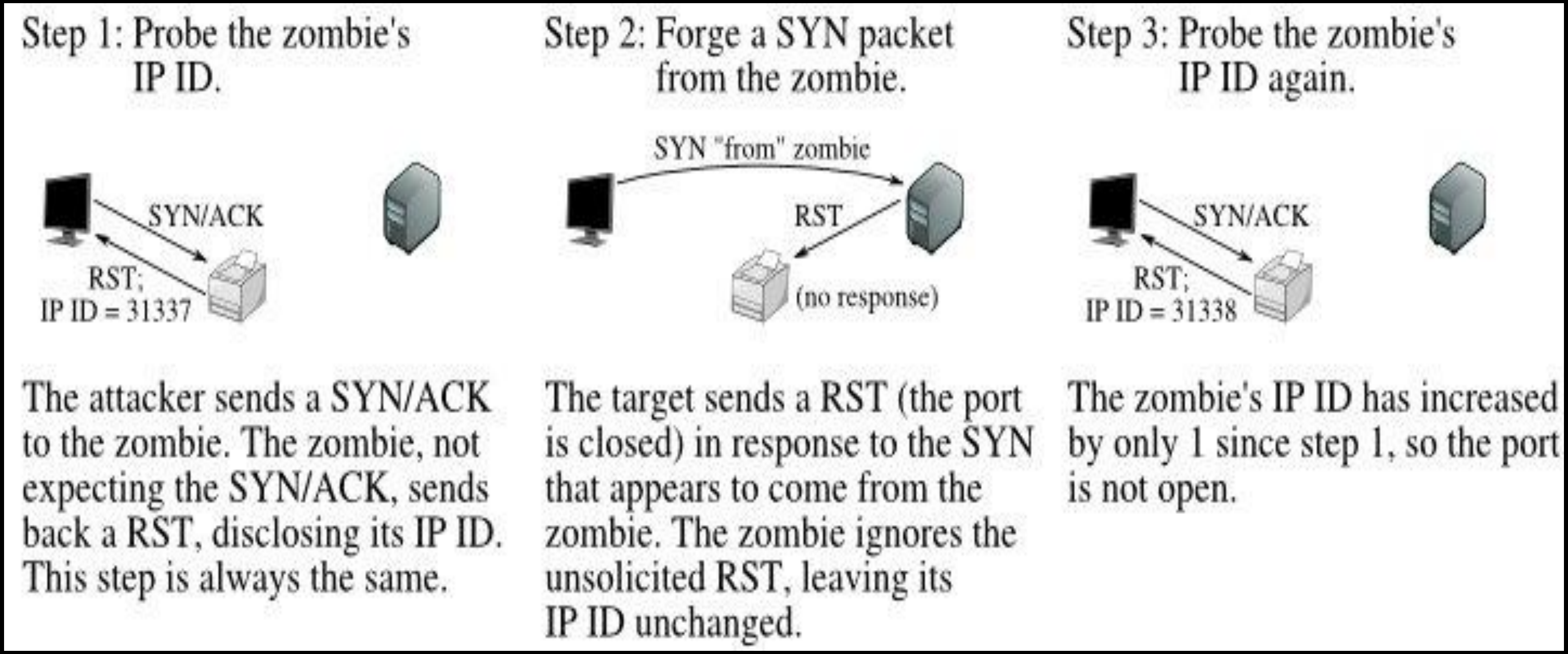
Step 2: Forge a SYN packet from the zombie.

The target sends a SYN/ACK in response to the SYN that appears to come from the zombie. The zombie, not expecting it, sends back a RST, incrementing its IP ID in the process.

Step 3: Probe the zombie's IP ID again.

The zombie's IP ID has increased by 2 since step 1, so the port is open!

Zombie Scan – Closed port



Step 1: Probe the zombie's IP ID.

The attacker sends a SYN/ACK to the zombie. The zombie, not expecting the SYN/ACK, sends back a RST, disclosing its IP ID. This step is always the same.

Step 2: Forge a SYN packet from the zombie.

The target sends a RST (the port is closed) in response to the SYN that appears to come from the zombie. The zombie ignores the unsolicited RST, leaving its IP ID unchanged.

Step 3: Probe the zombie's IP ID again.

The zombie's IP ID has increased by only 1 since step 1, so the port is not open.

XMPP File Transfer

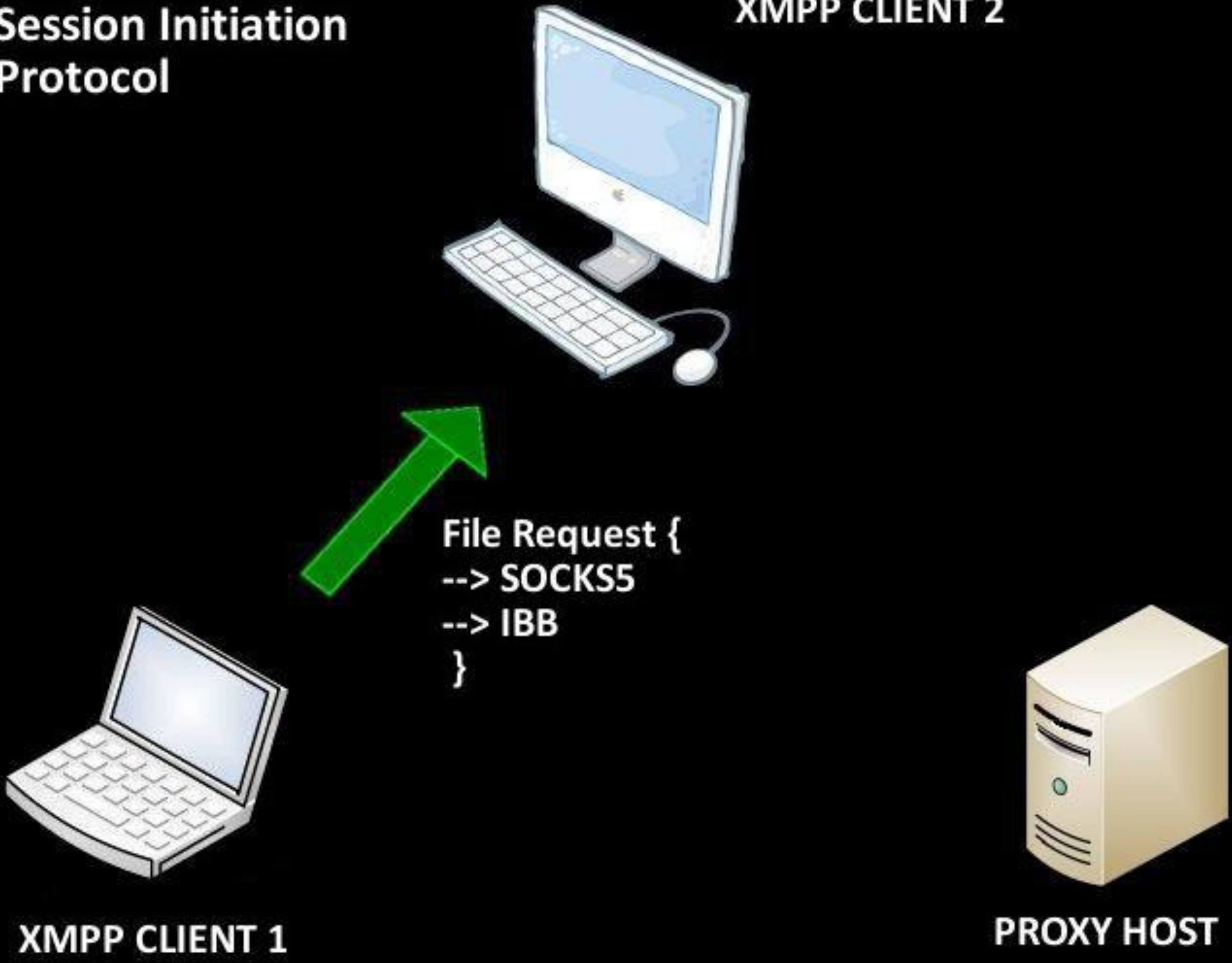
Session Initiation Protocol

- In-Band Bytestreams (IBB)
- SOCKS5 Bytestreams

JINGLE

- XMPP as signaling channel
- Data -> Out-of-band channel
- Jingle namespace (modern)
- IBB, SOCKS5, ICE-UDP, RAW-UDP

Session Initiation Protocol



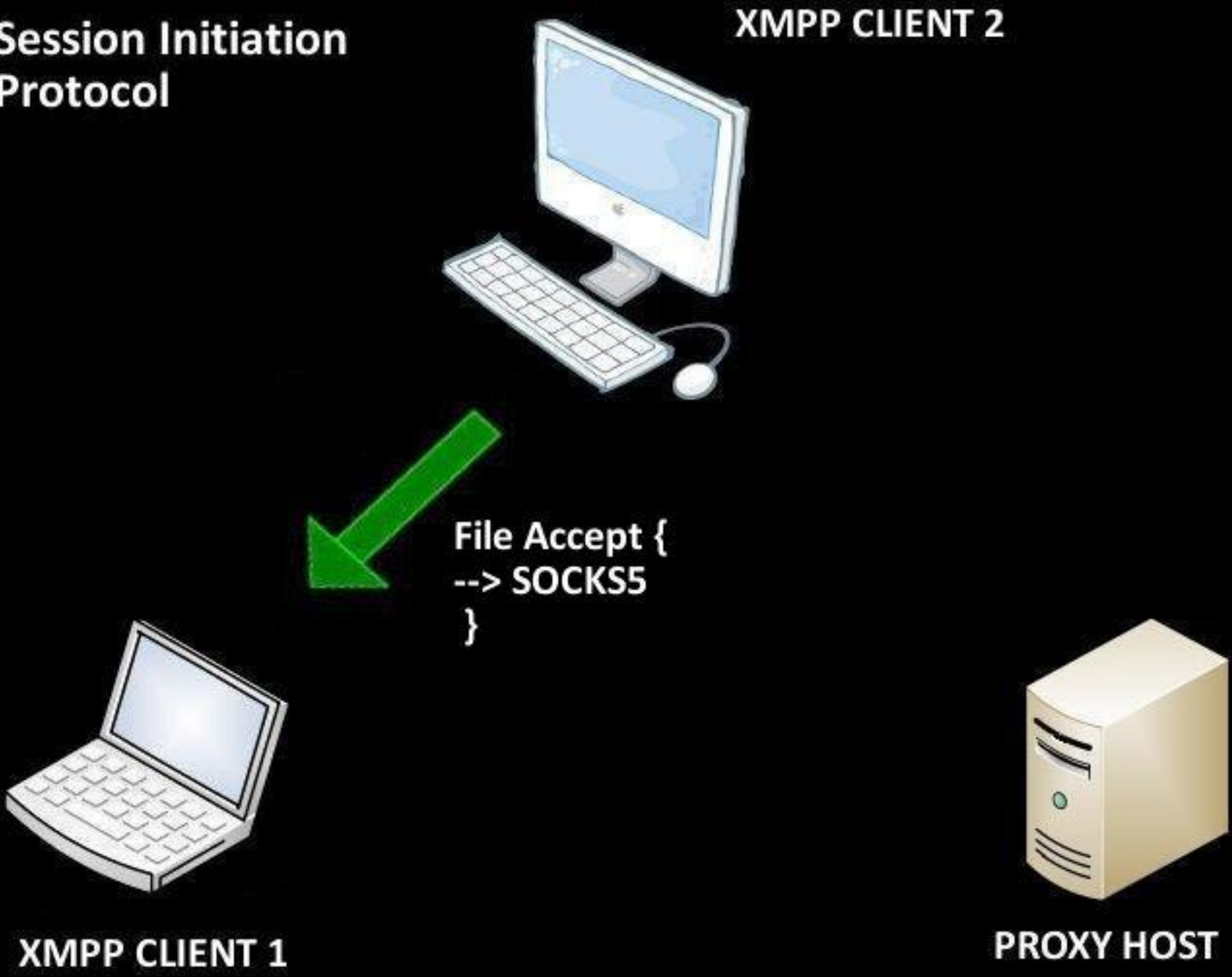
XMPP CLIENT 2

File Request {
--> SOCKS5
--> IBB
}

XMPP CLIENT 1

PROXY HOST

Session Initiation Protocol



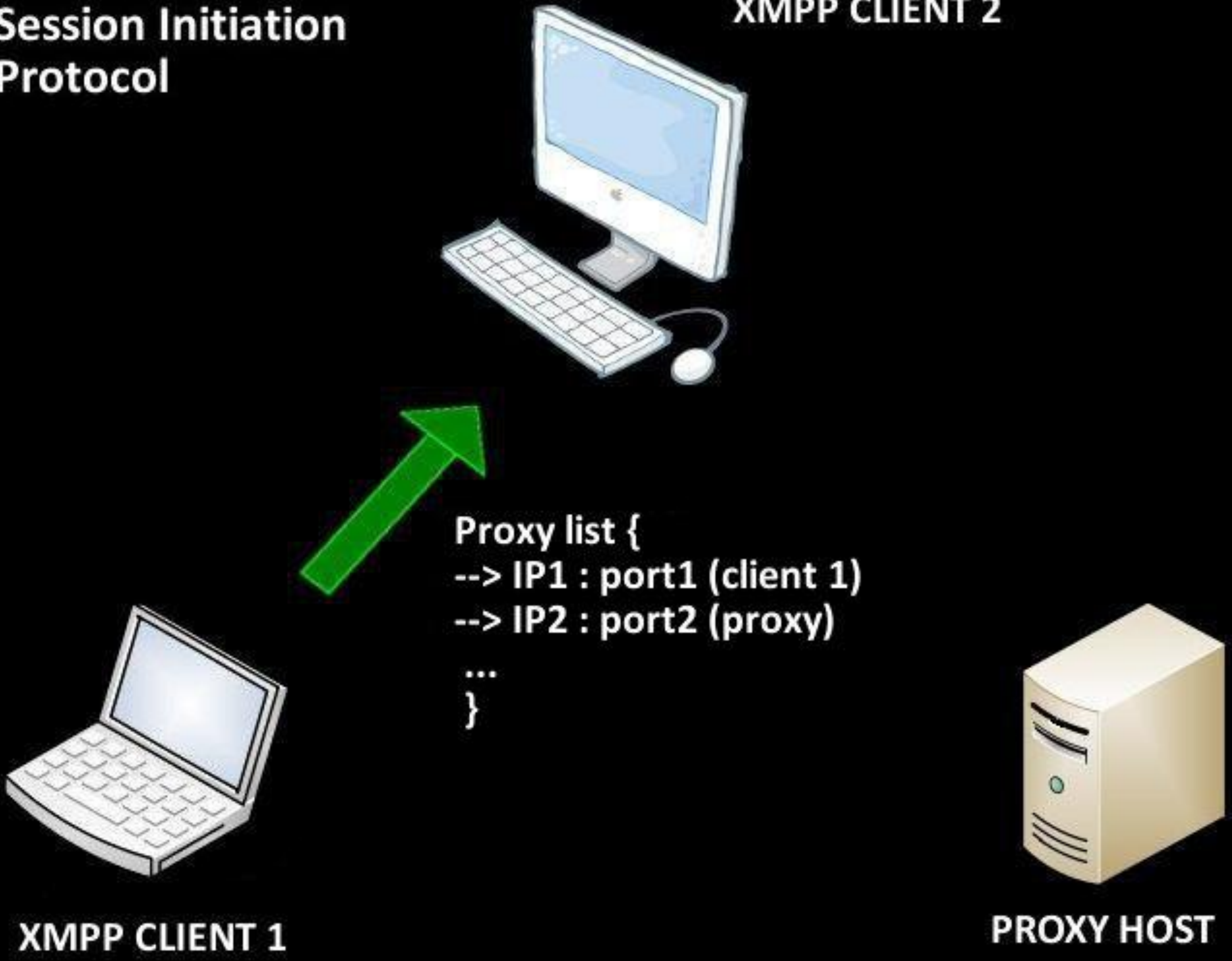
XMPP CLIENT 2

File Accept {
--> SOCKS5
}

XMPP CLIENT 1

PROXY HOST

Session Initiation Protocol



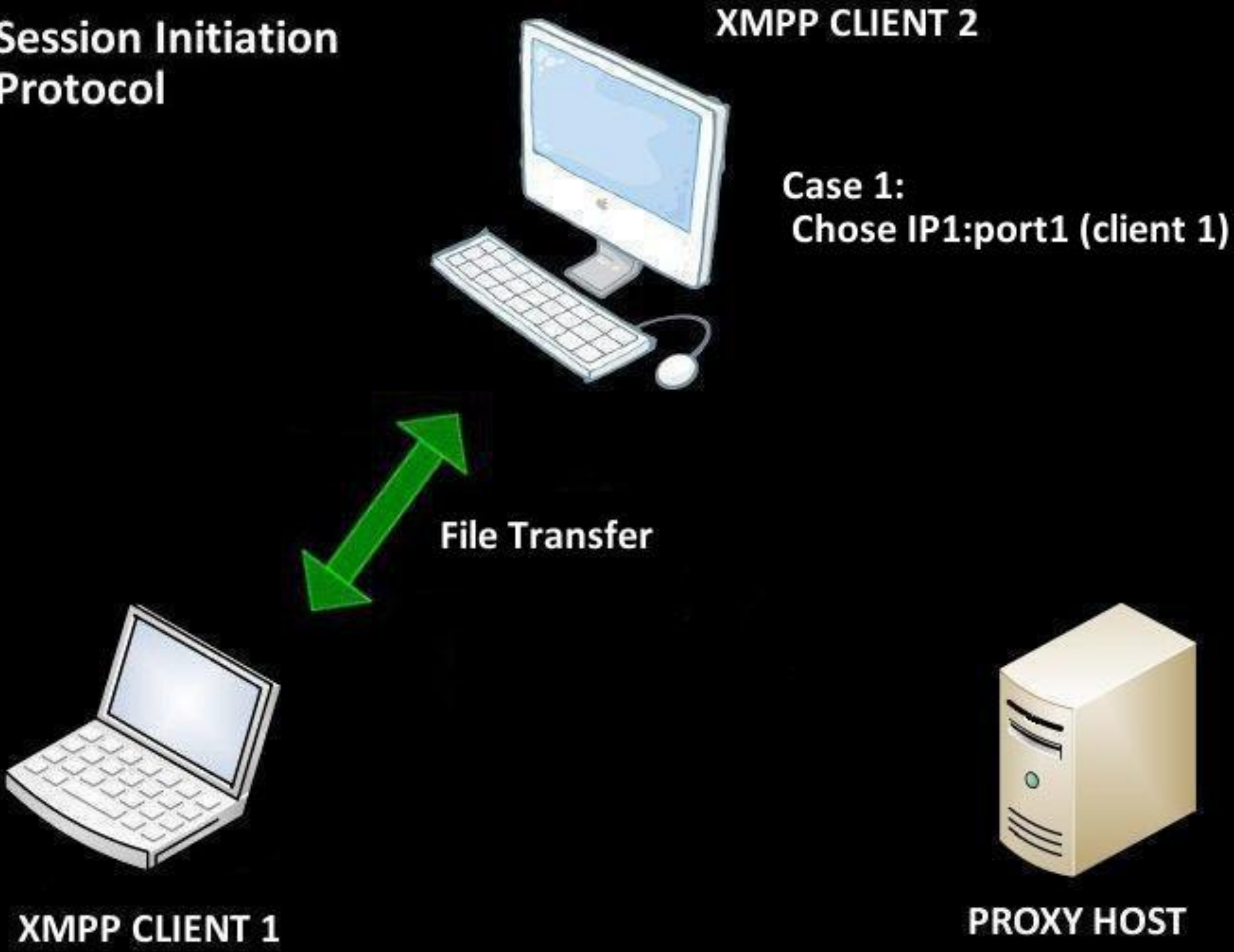
XMPP CLIENT 2

Proxy list {
--> IP1 : port1 (client 1)
--> IP2 : port2 (proxy)
...
}

XMPP CLIENT 1

PROXY HOST

Session Initiation Protocol



XMPP CLIENT 2

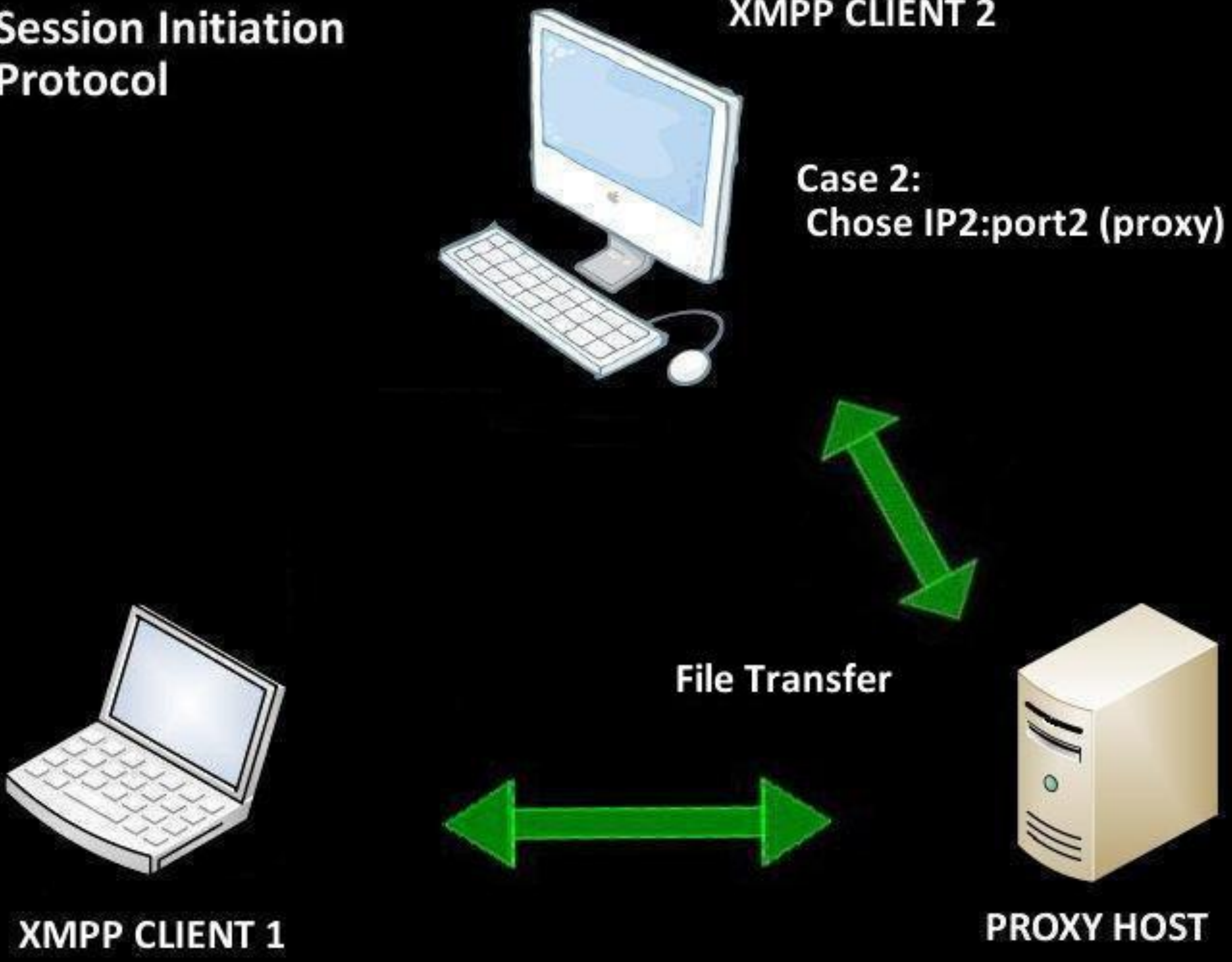
Case 1:
Chose IP1:port1 (client 1)

File Transfer

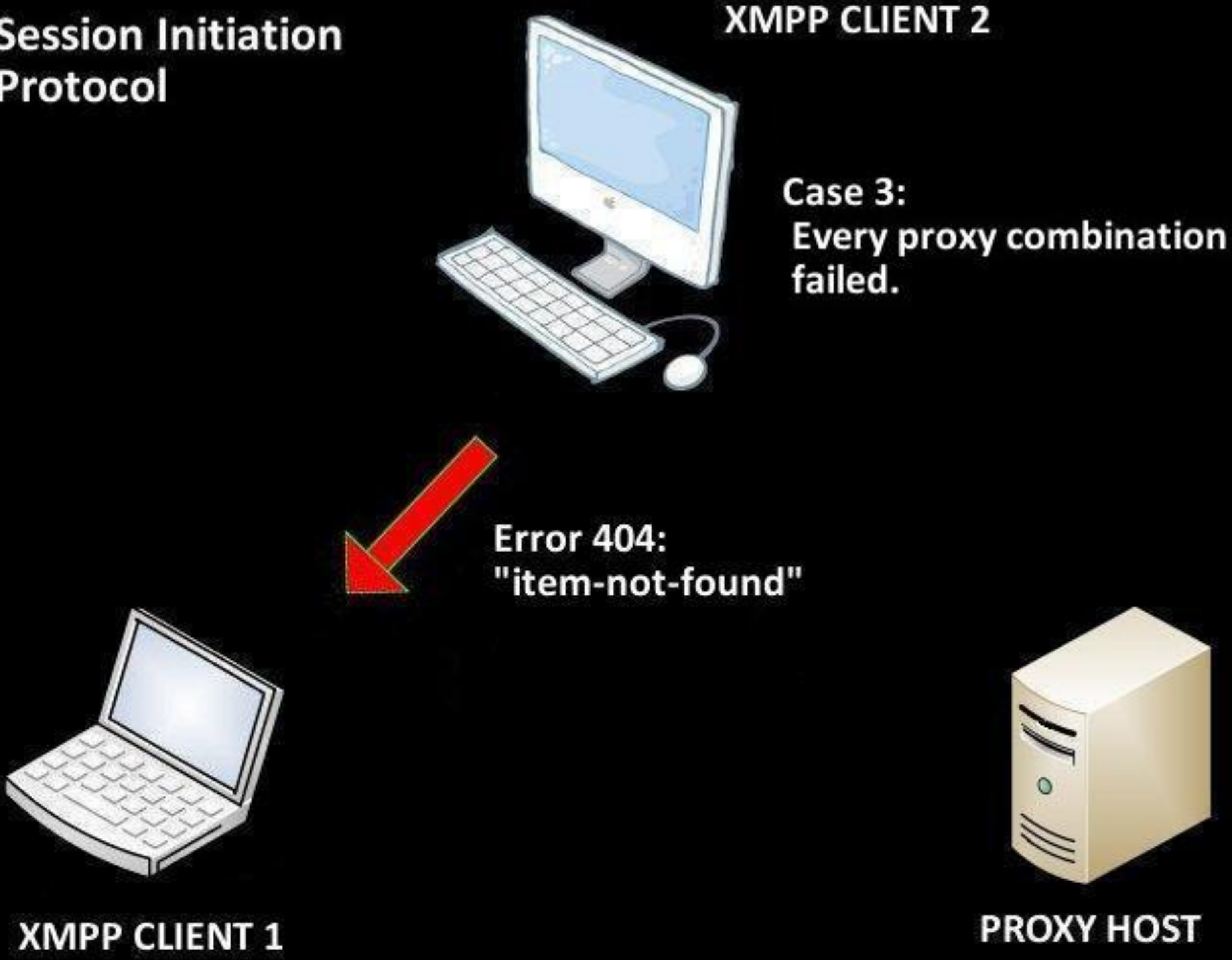
XMPP CLIENT 1

PROXY HOST

Session Initiation Protocol



Session Initiation Protocol



XMPP CLIENT 2

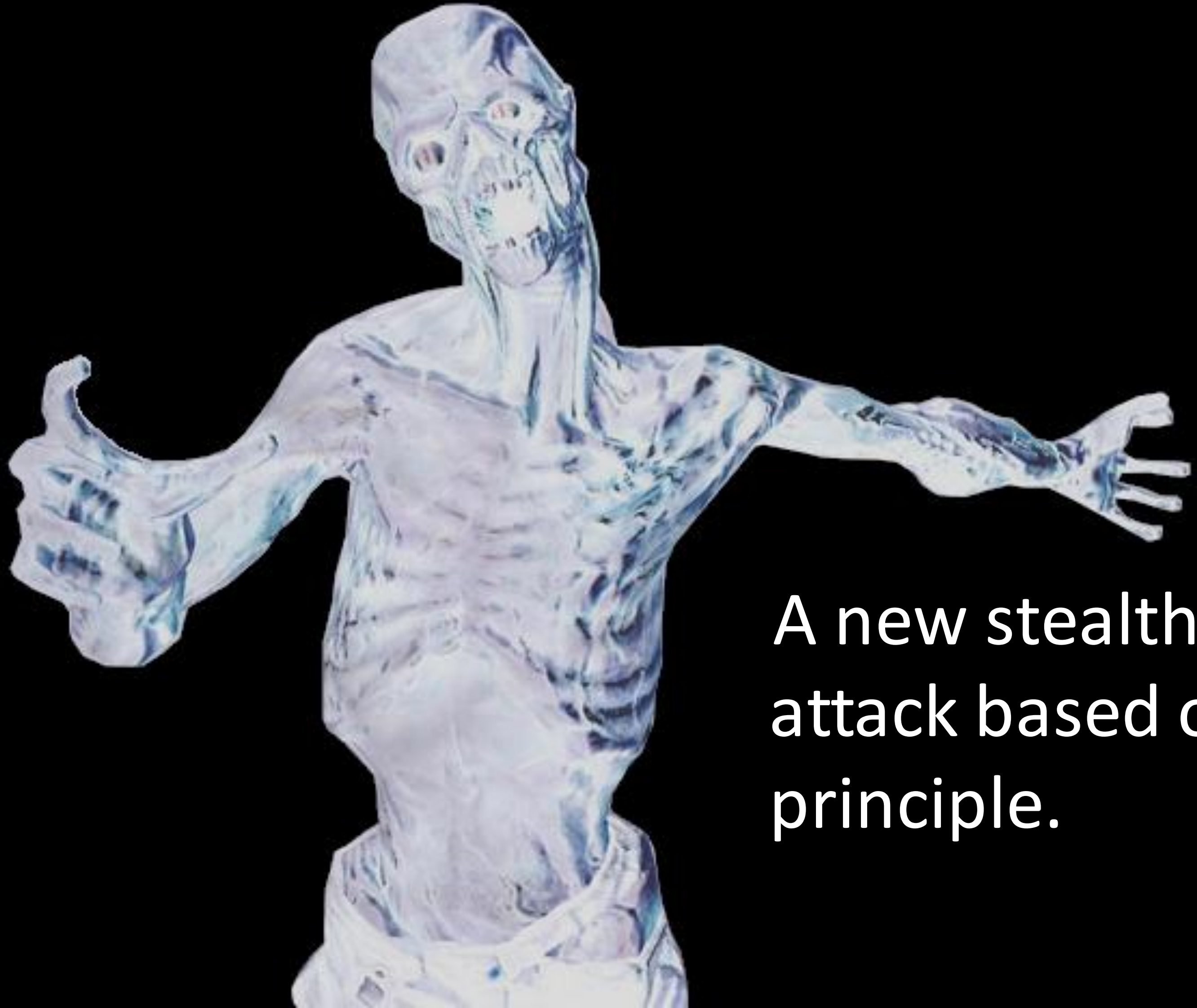
Case 3:
Every proxy combination failed.

Error 404:
"item-not-found"

XMPP CLIENT 1

PROXY HOST

Zombie Proxy Attack



A new stealthy portscanning attack based on the “zombie” principle.

It’s all about timing.

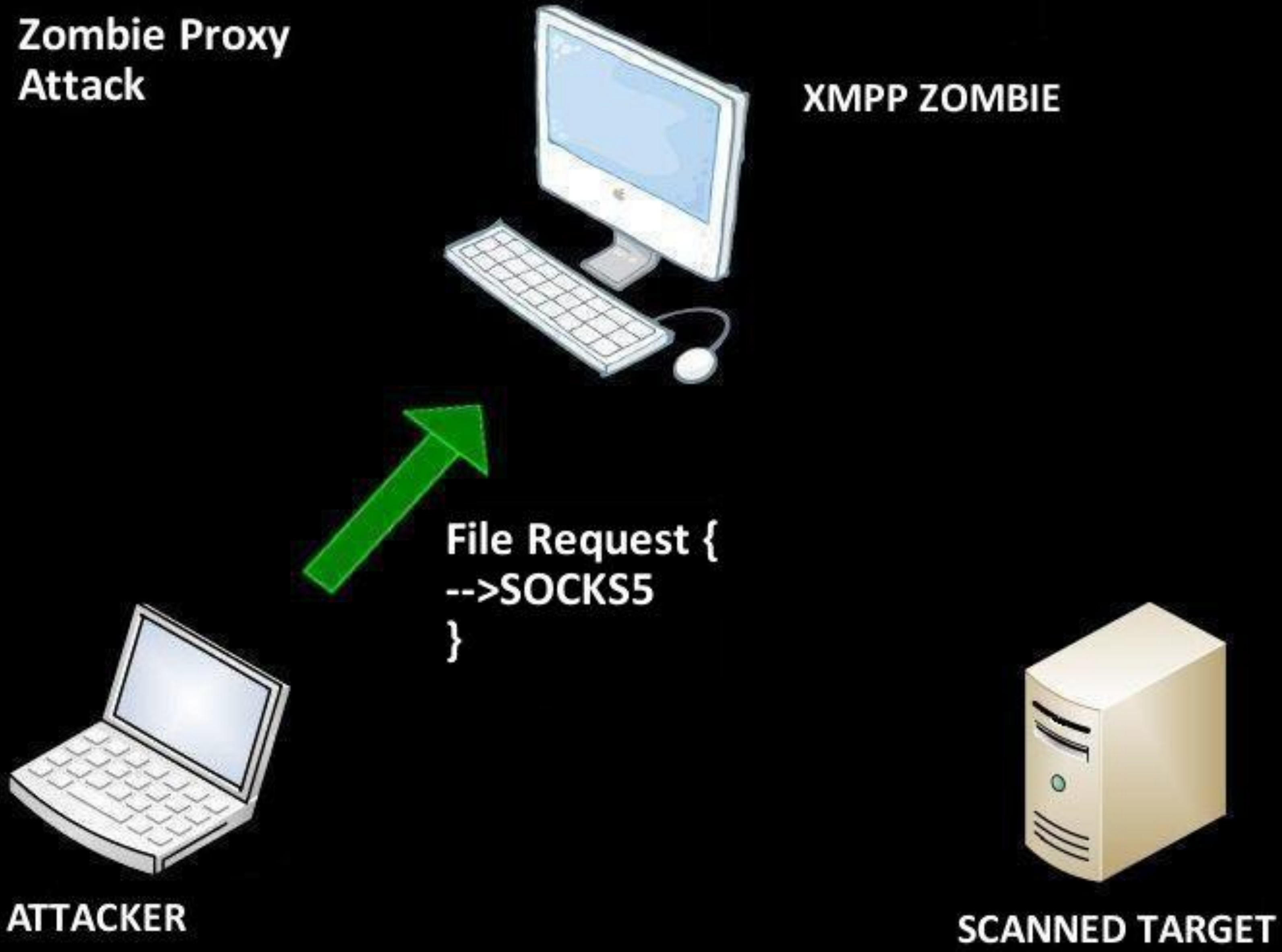
Technique’s principle

The “item-not-found” error message’s time delay differs depending on whether the proxy port is open or filtered.

Attack steps

1. Send file request. Advertise SOCKS5 only.
2. If receiver accepts, send proxy list filled with target's IP address and one of its ports.
3. If you get the error message in < 1-5 seconds, port is open.
4. If you get error message in > 10 seconds, port is filtered.
5. Goto 1 until all hosts/ports scanned.

Zombie Proxy Attack



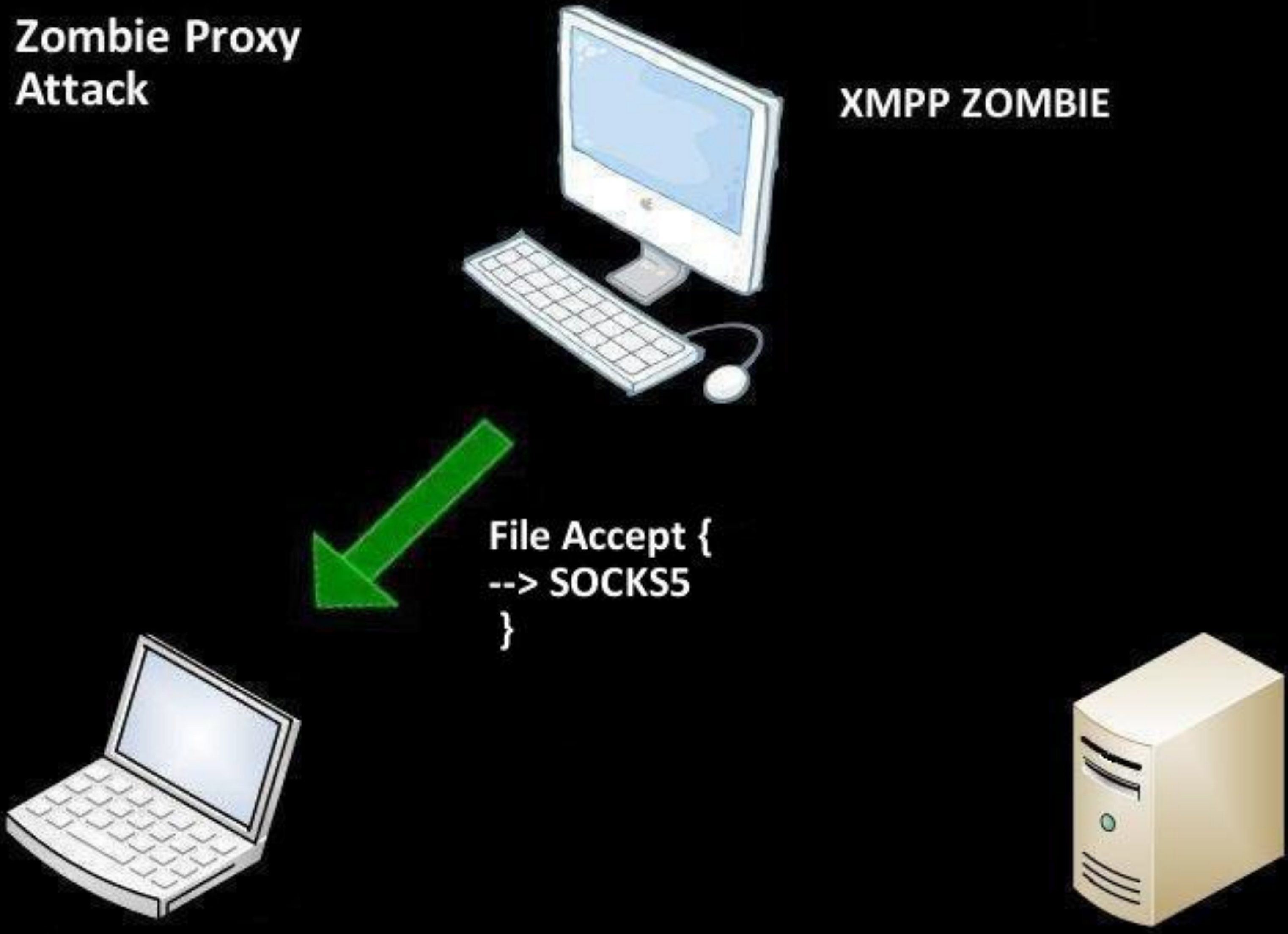
XMPP ZOMBIE

File Request {
-->SOCKS5
}

ATTACKER

SCANNED TARGET

Zombie Proxy Attack



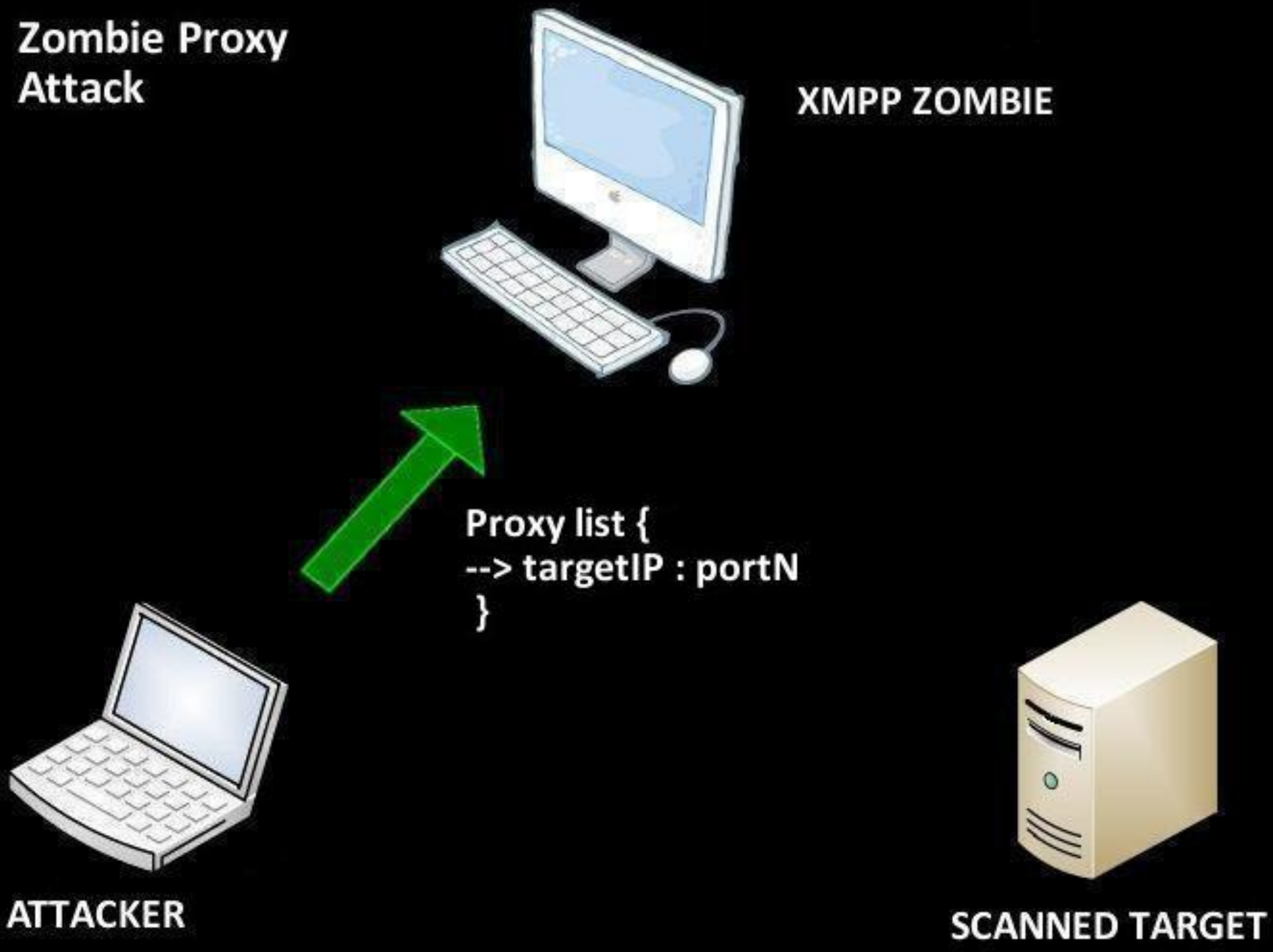
XMPP ZOMBIE

File Accept {
--> SOCKS5
}

ATTACKER

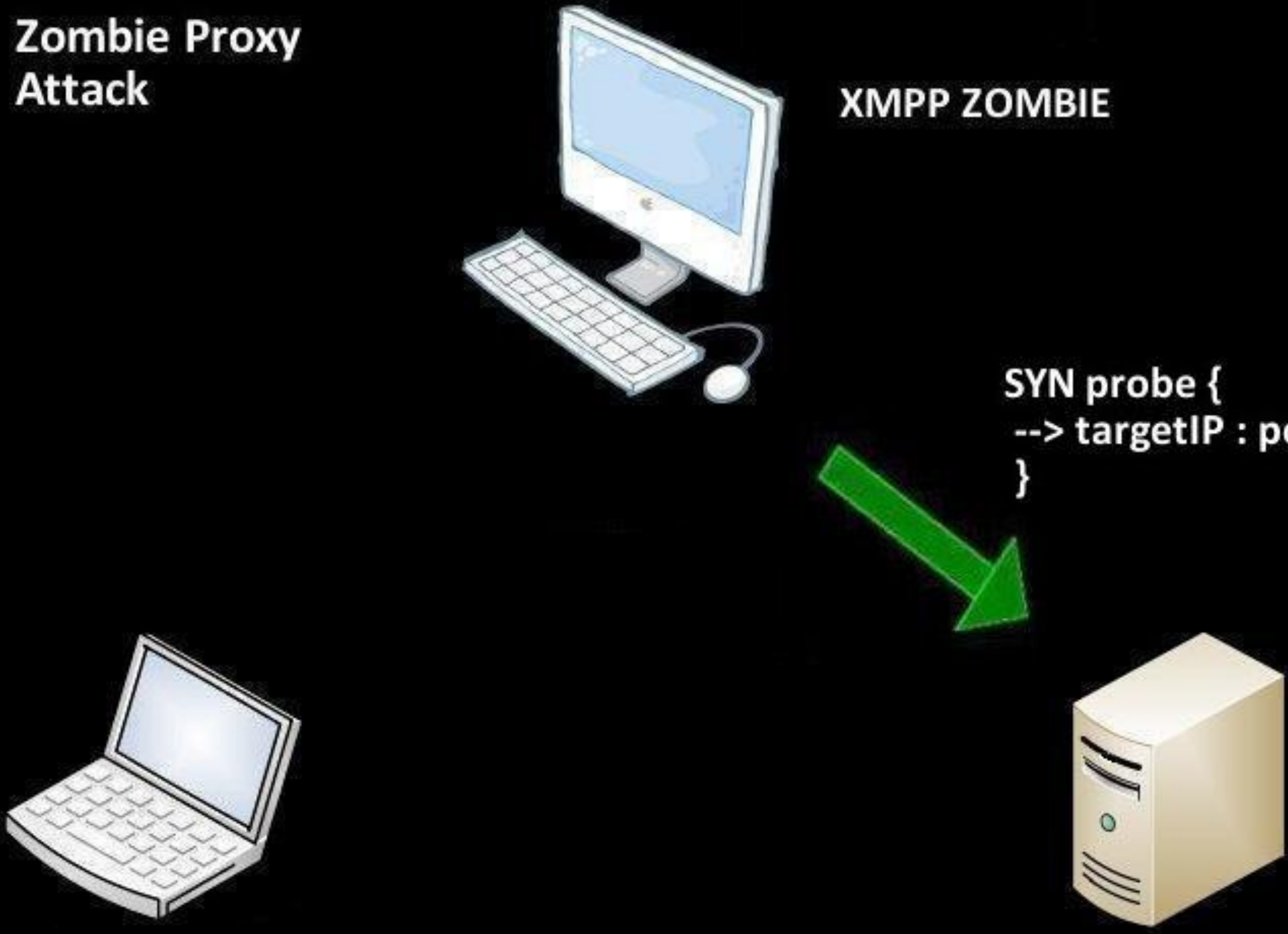
SCANNED TARGET

Zombie Proxy Attack



```
Proxy list {
--> targetIP : portN
 }
```

Zombie Proxy Attack



XMPP ZOMBIE

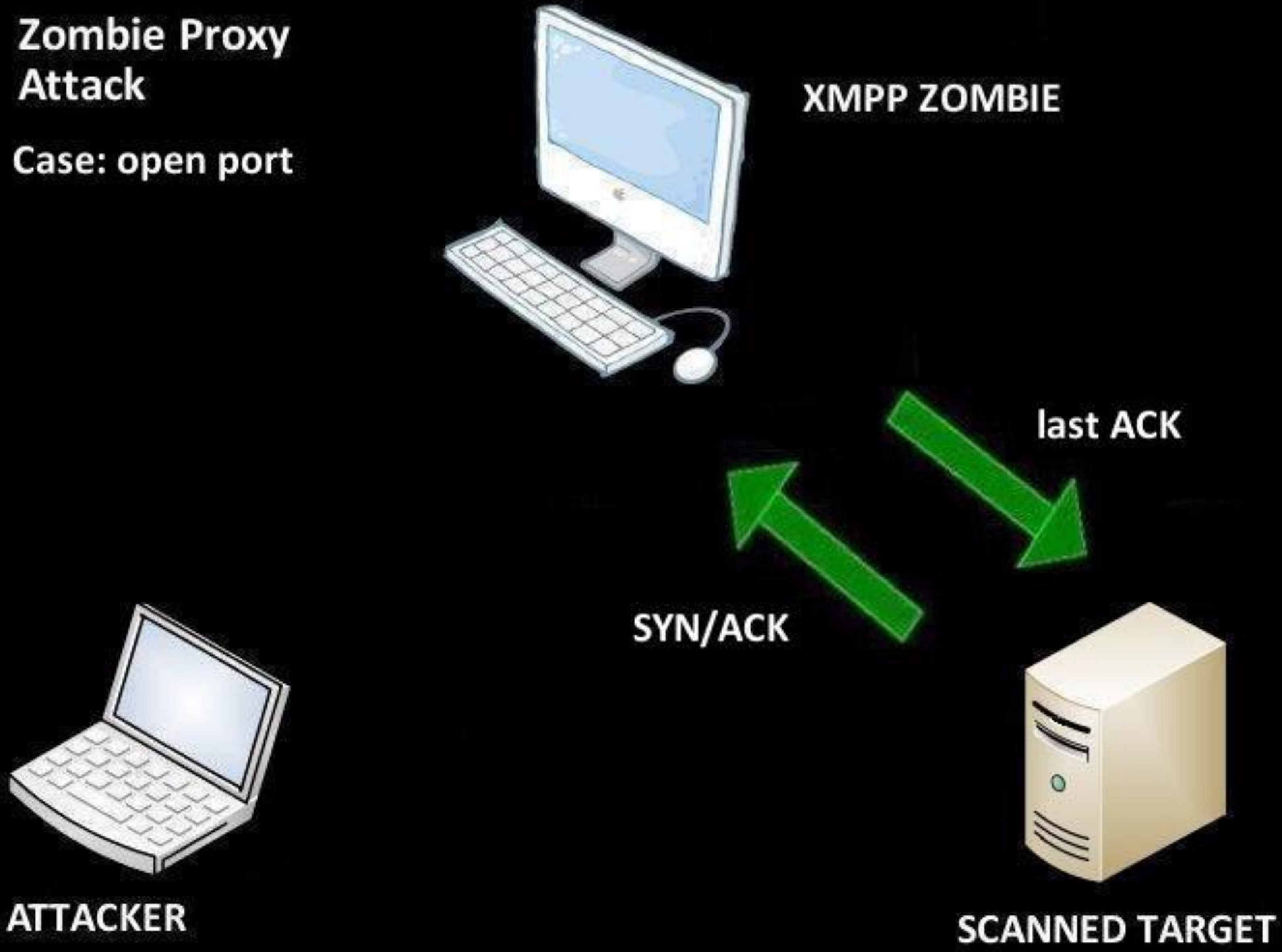
SYN probe {
 --> targetIP : portN
}

ATTACKER

SCANNED TARGET

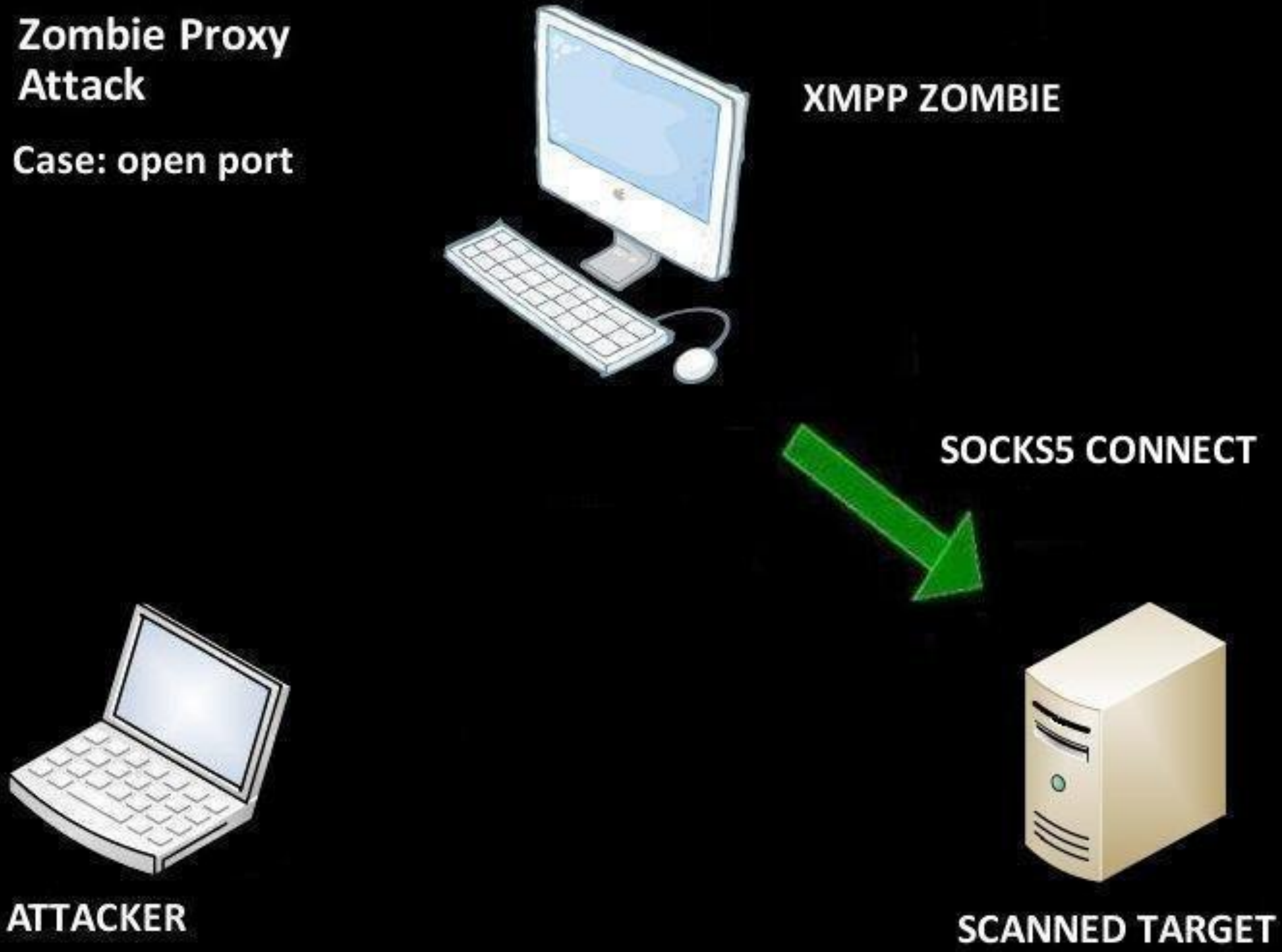
Zombie Proxy Attack

Case: open port



Zombie Proxy Attack

Case: open port



XMPP ZOMBIE

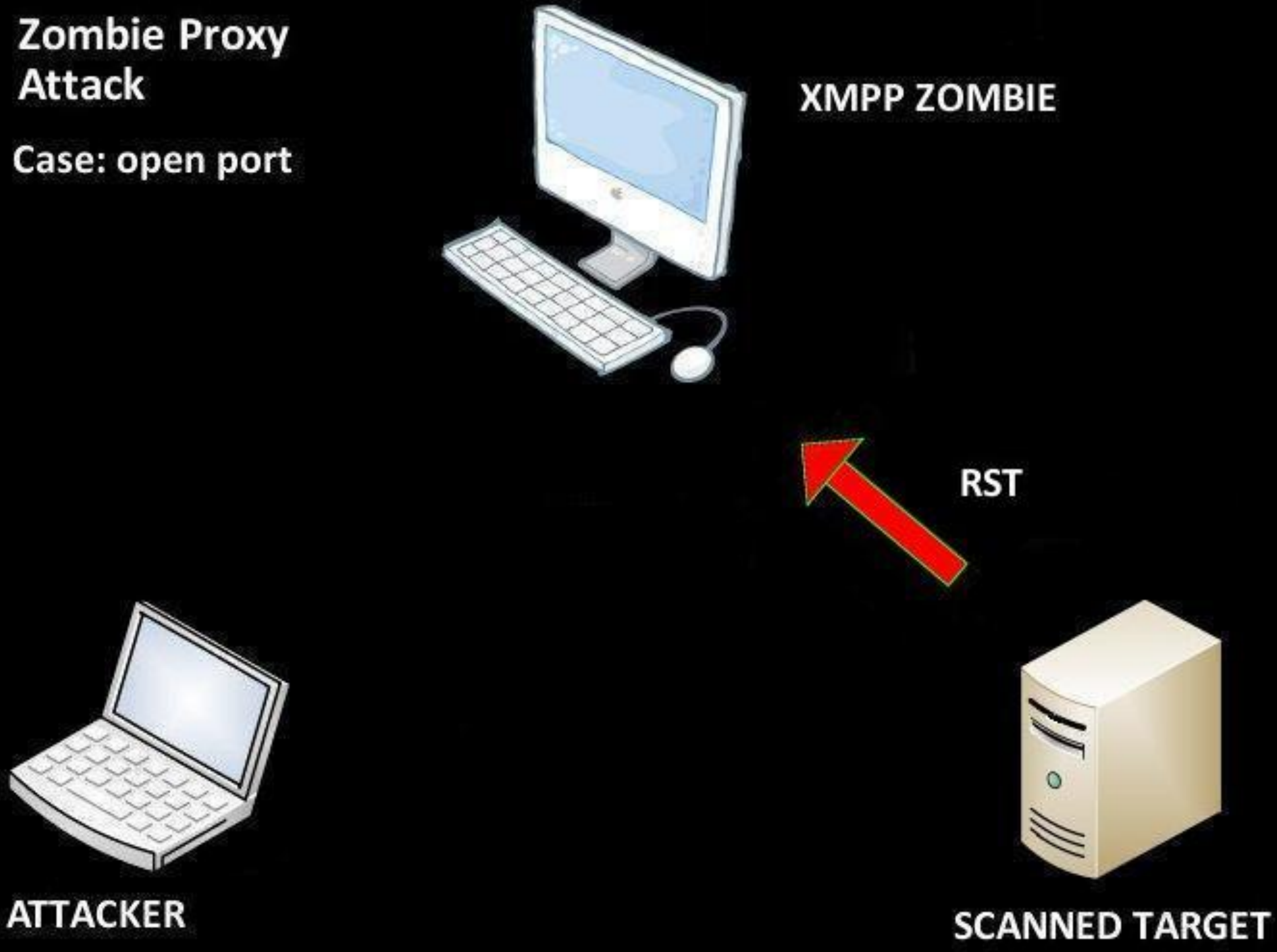
SOCKS5 CONNECT

ATTACKER

SCANNED TARGET

Zombie Proxy Attack

Case: open port



XMPP ZOMBIE

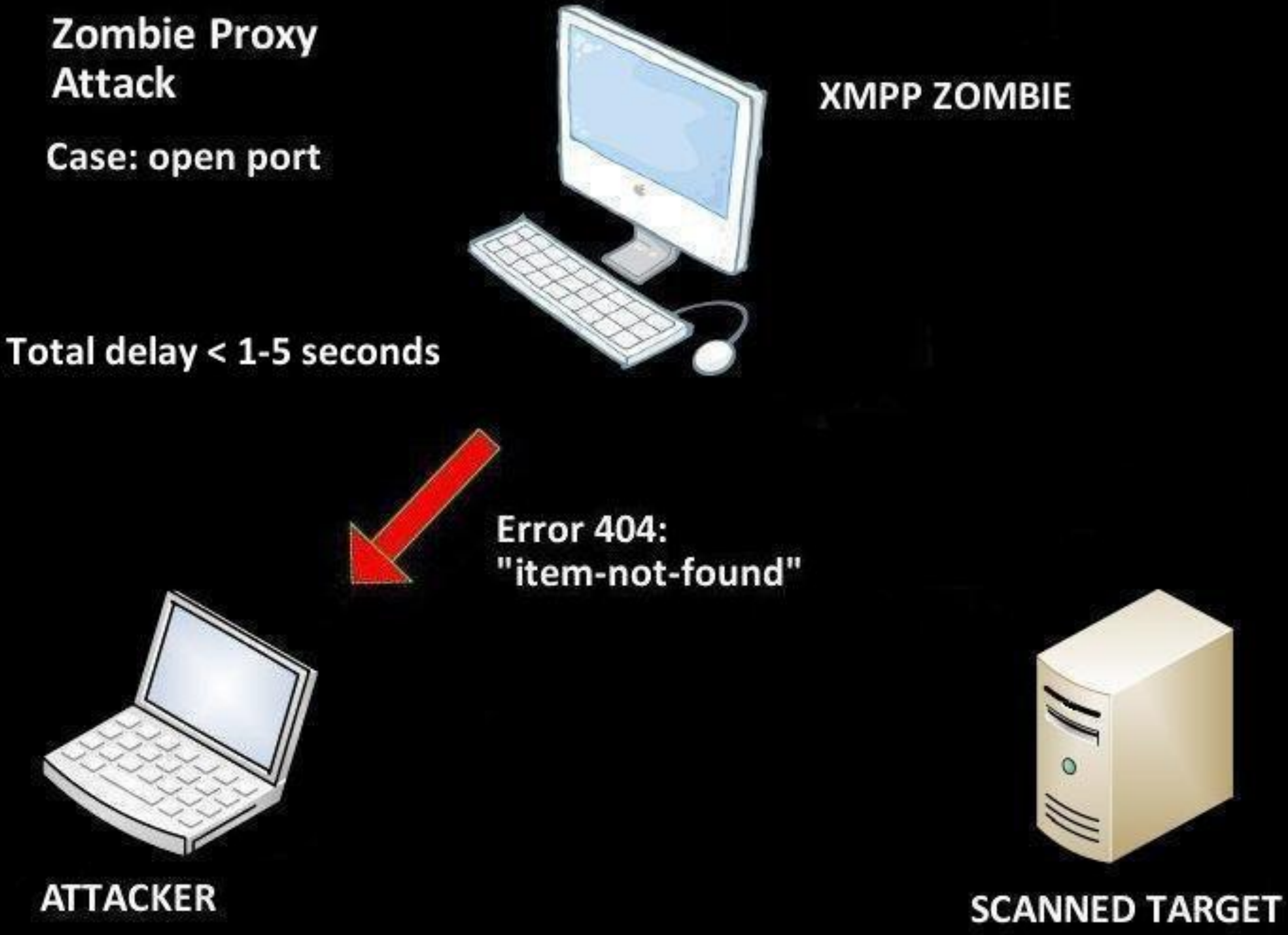
RST

ATTACKER

SCANNED TARGET

Zombie Proxy Attack

Case: open port



XMPP ZOMBIE

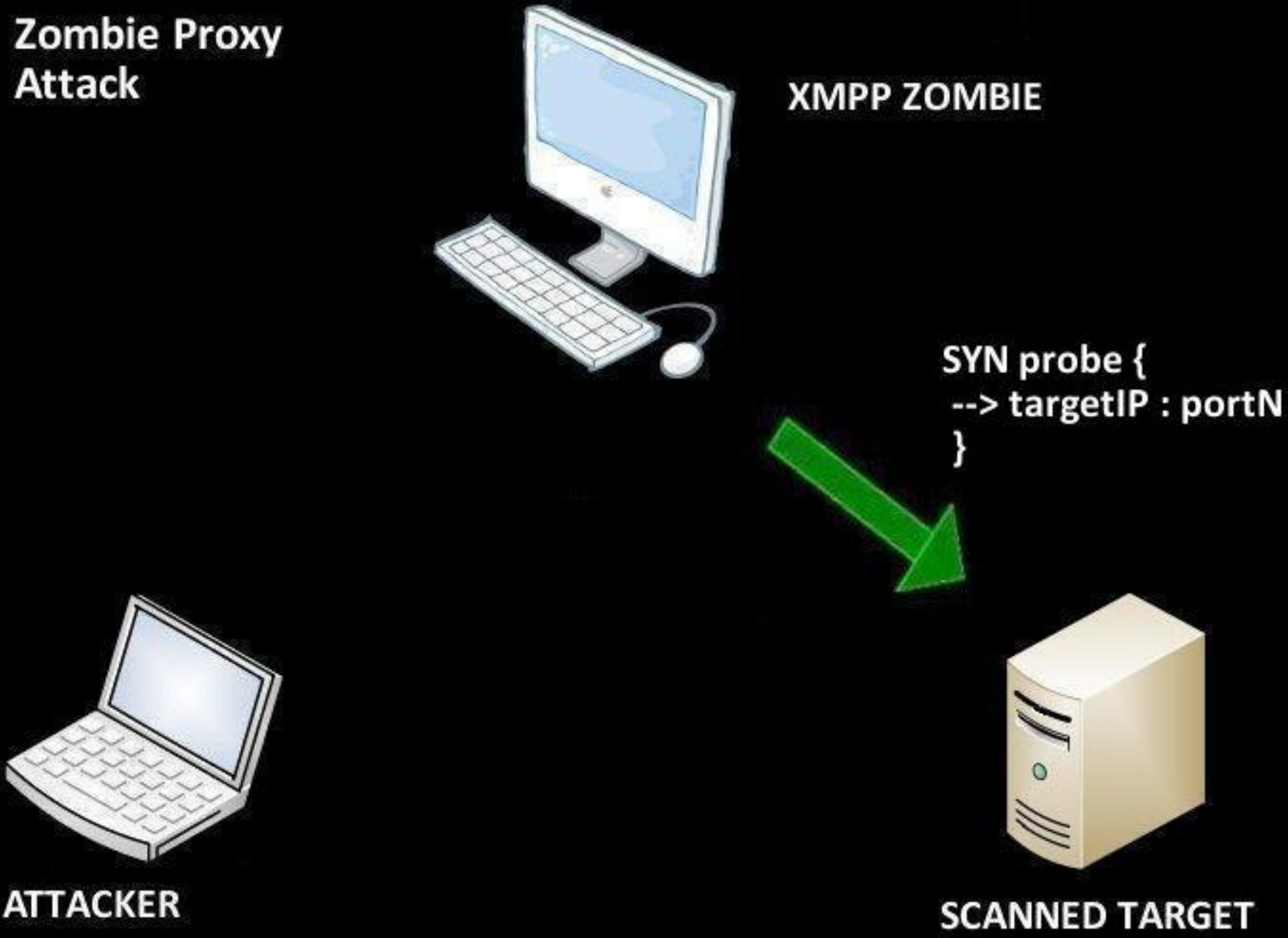
Total delay < 1-5 seconds

Error 404:
"item-not-found"

ATTACKER

SCANNED TARGET

Zombie Proxy Attack



XMPP ZOMBIE

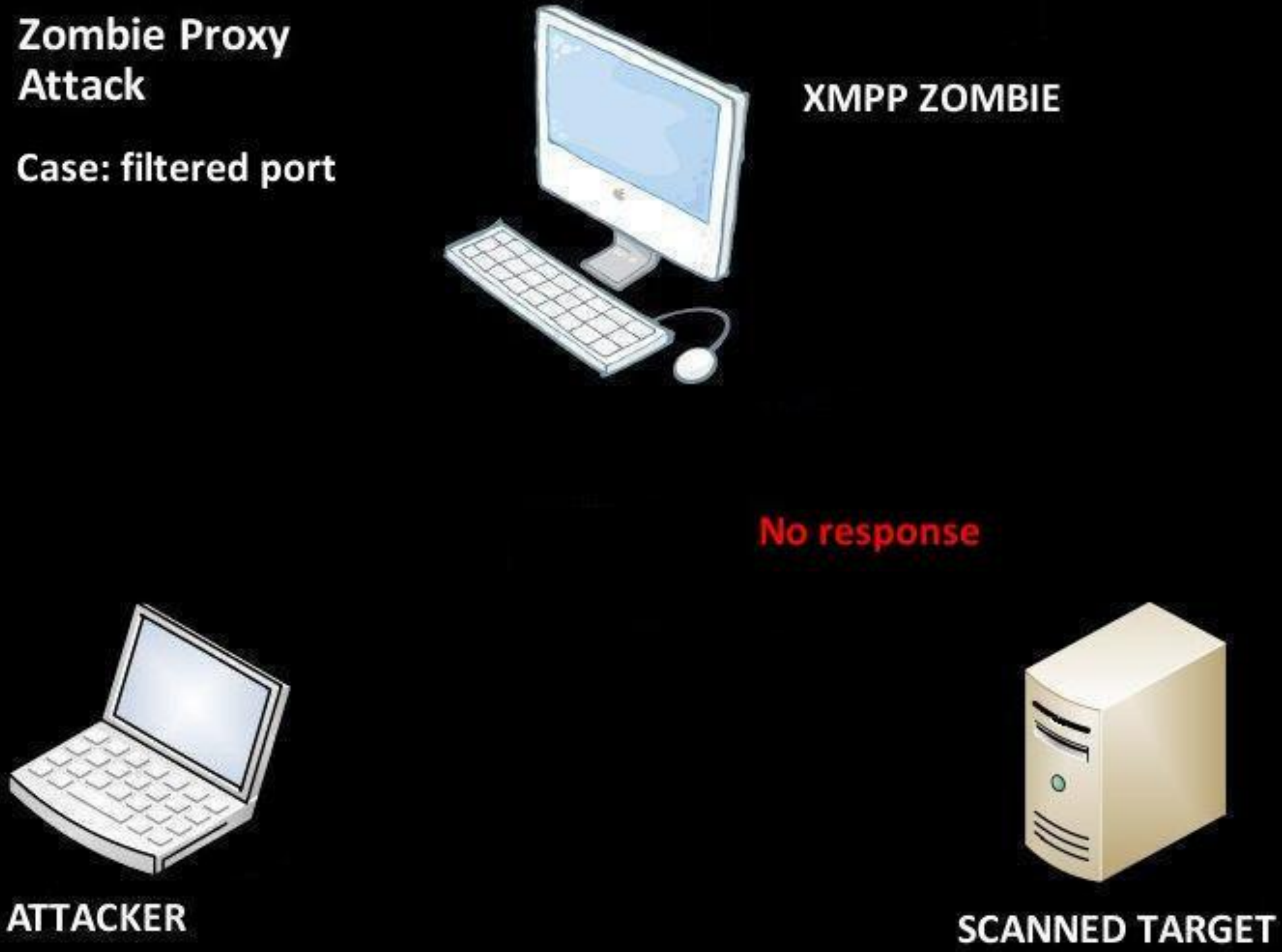
SYN probe {
 --> targetIP : portN
}

ATTACKER

SCANNED TARGET

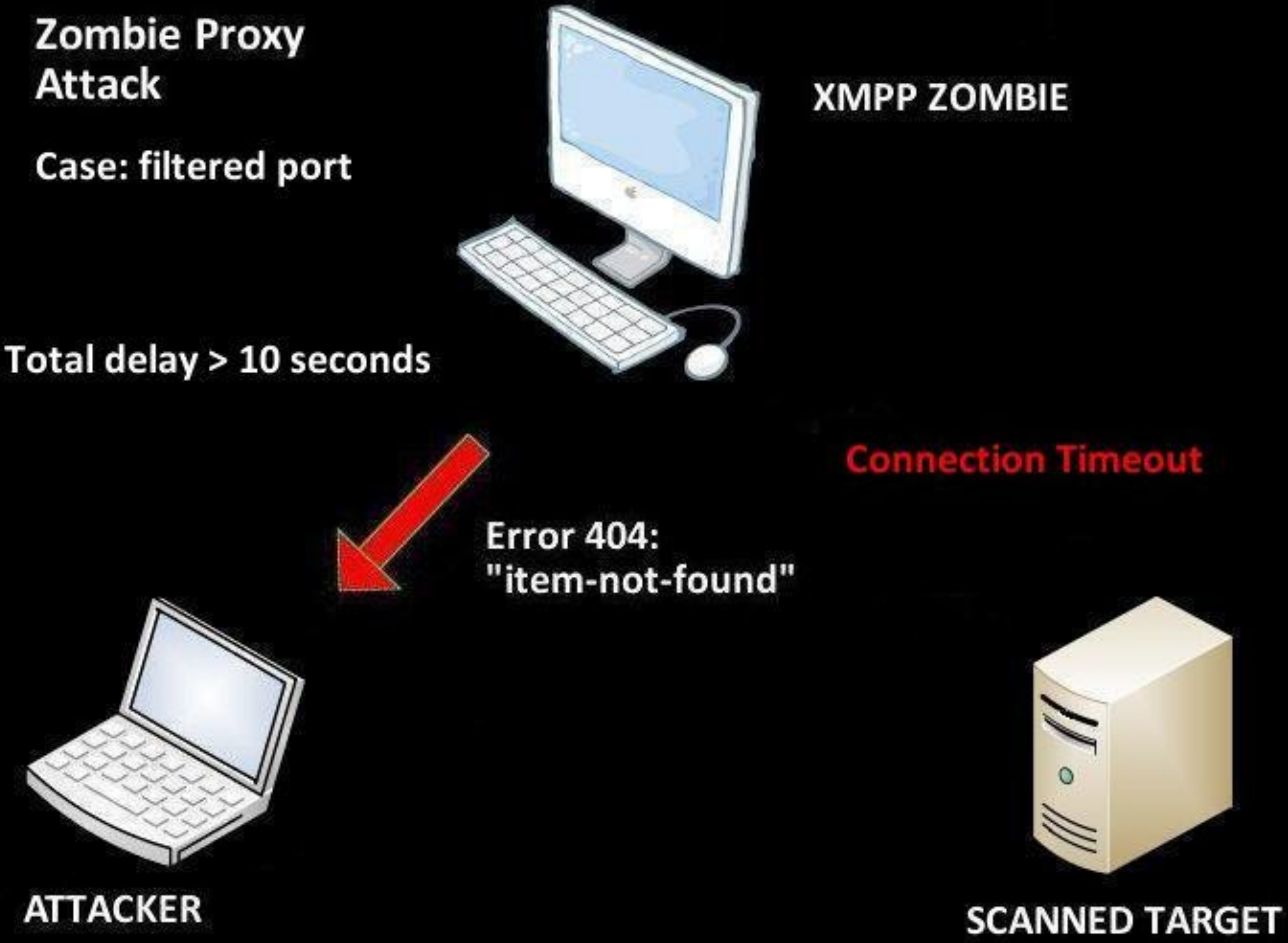
Zombie Proxy Attack

Case: filtered port



Zombie Proxy Attack

Case: filtered port



XMPP ZOMBIE

Total delay > 10 seconds

Connection Timeout

Error 404:
"item-not-found"

ATTACKER

SCANNED TARGET

Post-mortem

- delay1 (open port) < delay2 (filtered port)
- Can’t accurately scan protocols with pipelining (e.g. HTTP 1.1). delay1 = delay2 because server ignores SOCKS5 probe and waits for more requests
- delay3 (closed port) < delay1

Attack Automation

File auto-accept feature

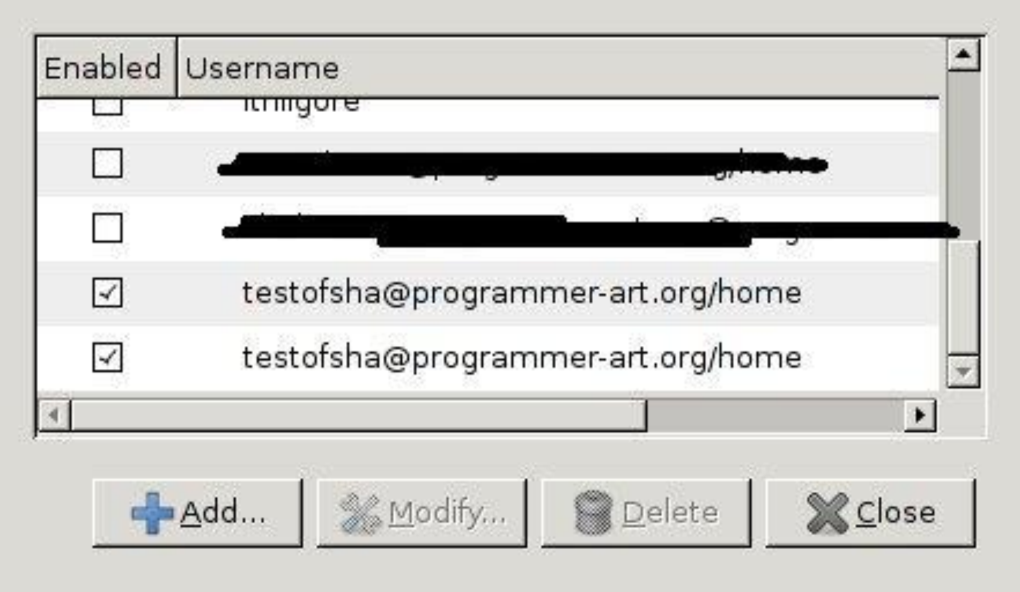
+ Social Engineering

= automation

default plugin

+ iChax

SE made easy



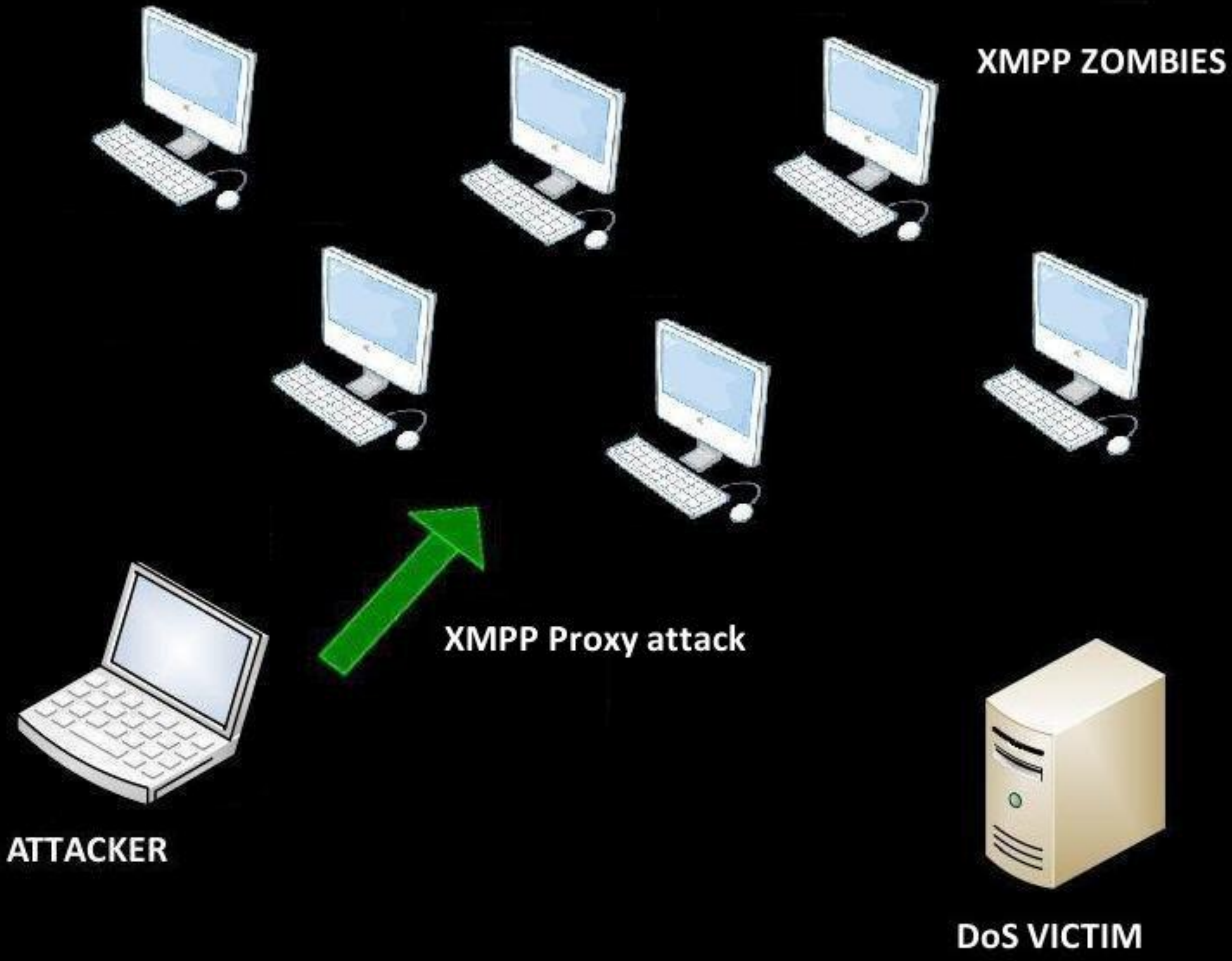
Enabled	Username
□	ithilgore
□	[redacted]
□	[redacted]
☑	testofsha@programmer-art.org/home
☑	testofsha@programmer-art.org/home

Internationalization

JIDs:

full Unicode range

DoS Attacks revised



XMPP ZOMBIES

XMPP Proxy attack

ATTACKER

DoS VICTIM

XMPP Zombie DoS attack

- Stealth: IP never revealed to victim
- Unlimited host/port specification per file request
- Potence: connections sequential, many zombies needed

TCP Persist Timer Attack

- Originally described in a Phrack #66 article.
- Exploits inherent feature of TCP (Persist Timer).
- Generic, stateless and much prolonged DoS attack performed by the Nkiller2 PoC tool.
- Asynchronous network I/O for maximum speed and few resources.
- Single host can easily stall a web server.

DNSSEC DoS Attack

- Strong cryptography = too much data
- Djb’s work showed 3900% amplification: so a request of 100 bytes yields response of 3900 bytes.
- DNS source addresses still easily spoofed.

Questions?