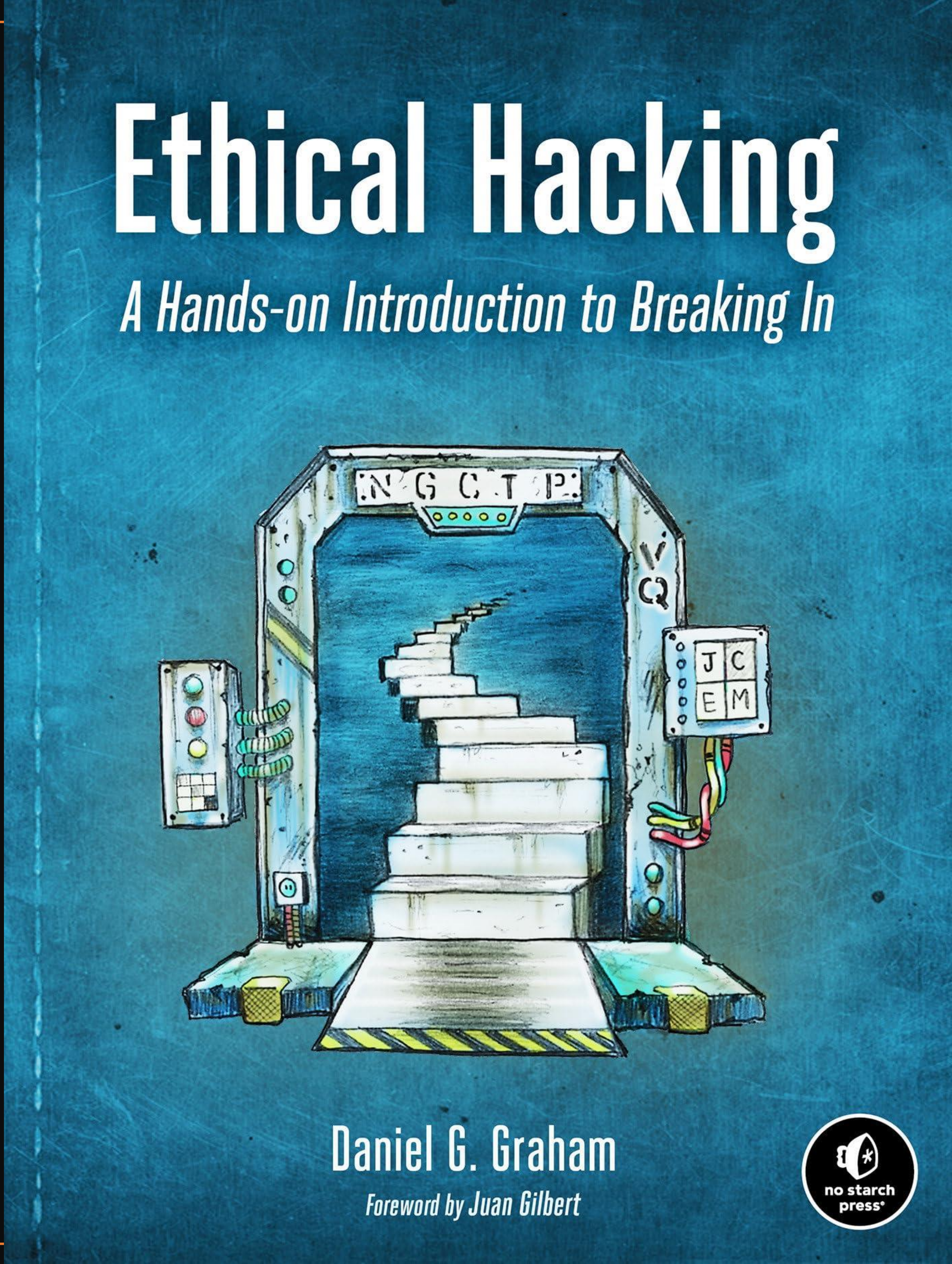
Chapter 14:

Pivoting and Privilege Escalation

Slides By:

Daniel Graham

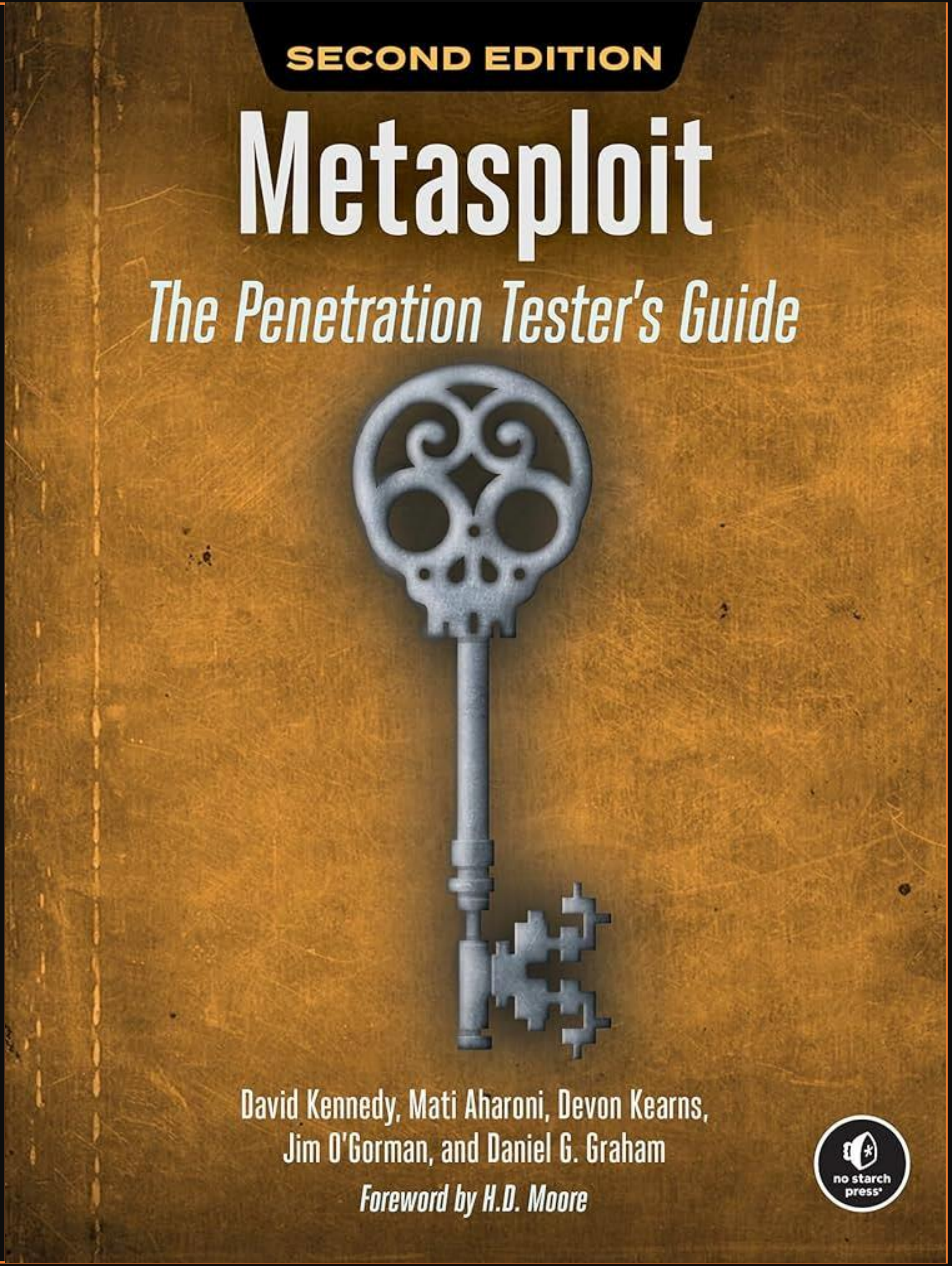


Chapter 15:

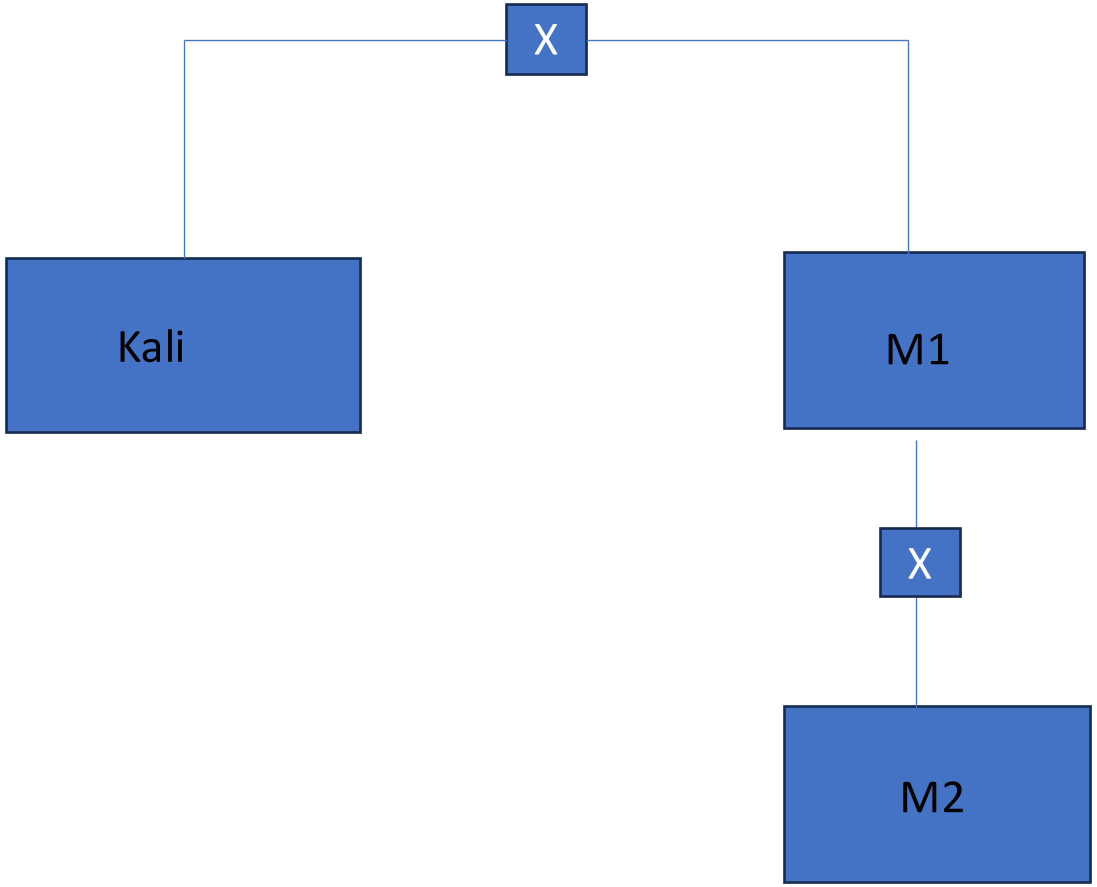
Simulated Pentest

Slides By:

Daniel Graham

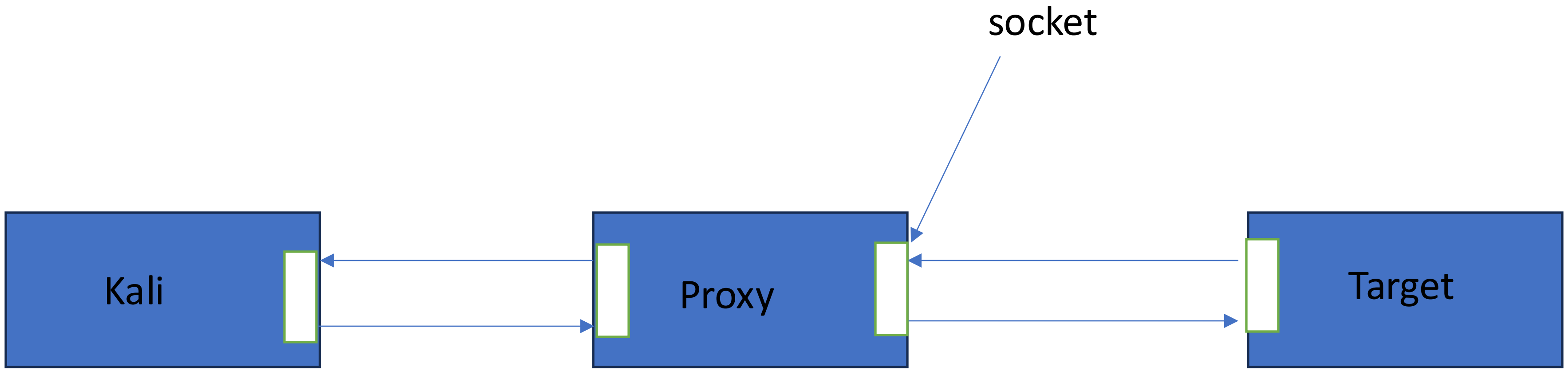

SECOND EDITION
Metasploit
The Penetration Tester's Guide
David Kennedy, Mati Aharoni, Devon Kearns,
Jim O'Gorman, and Daniel G. Graham
Foreword by H.D. Moore
no starch press

The setup.

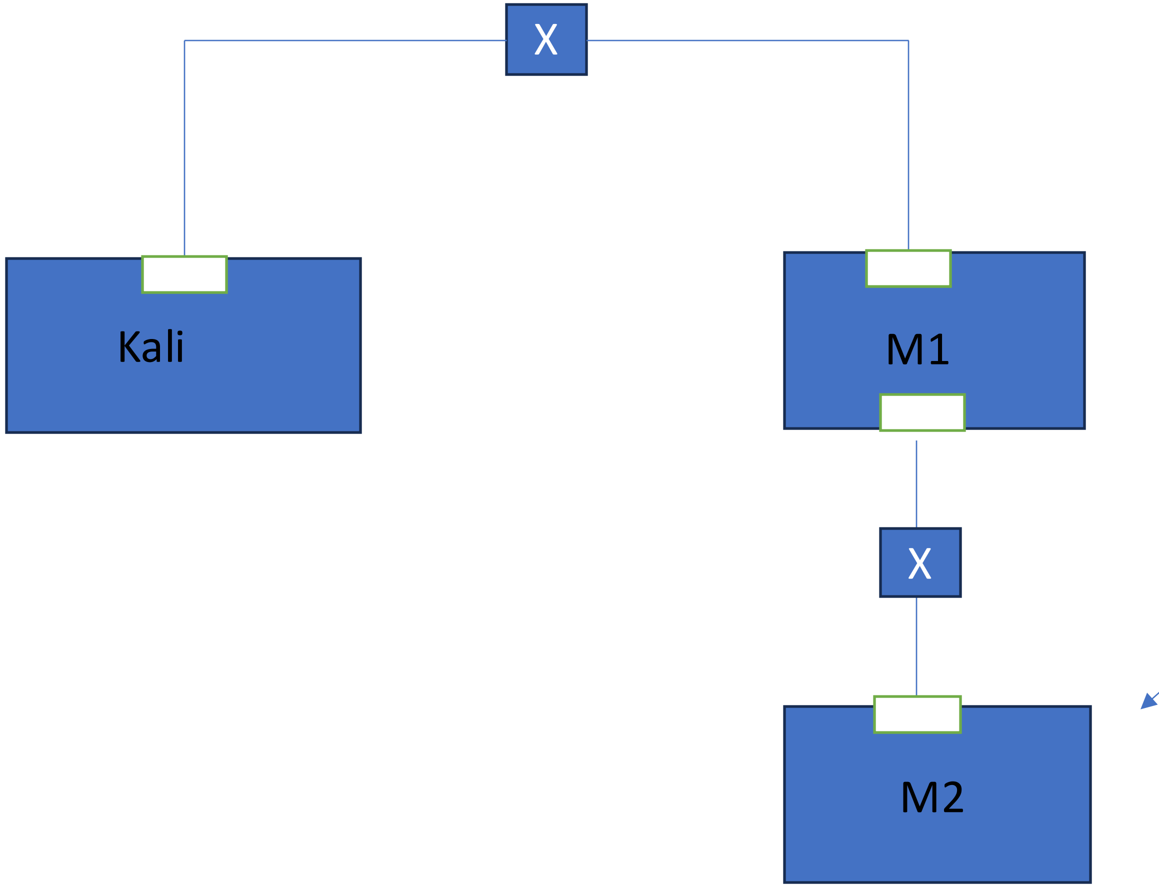


How could we attack this machine.

What is a proxy



The setup.



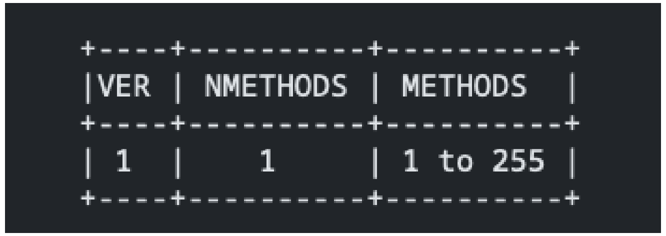
How could we attack this machine.

Python implementation of a proxy

```
import socket

HOST = '127.0.0.1'  # Proxy listens on localhost
PORT = 8888         # Proxy port

def start_proxy():
    server = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    server.bind((HOST, PORT))
    server.listen(5)
    print(f"[*] Proxy running on {HOST}:{PORT}")

    while True:
        client_socket, addr = server.accept()
        print(f"[*] Connection from {addr}")
        request = client_socket.recv(4096)

        # Forward request to external server
        with socket.socket(socket.AF_INET, socket.SOCK_STREAM) as proxy_socket:
            proxy_socket.connect((”<kali-ip>", 8080))  # Forwarding all requests to <kali-ip>
            proxy_socket.sendall(request)
            response = proxy_socket.recv(4096)

        # Send response back to client
        client_socket.sendall(response)
        client_socket.close()

if __name__ == "__main__":
    start_proxy()
```

Socks5 Proxy

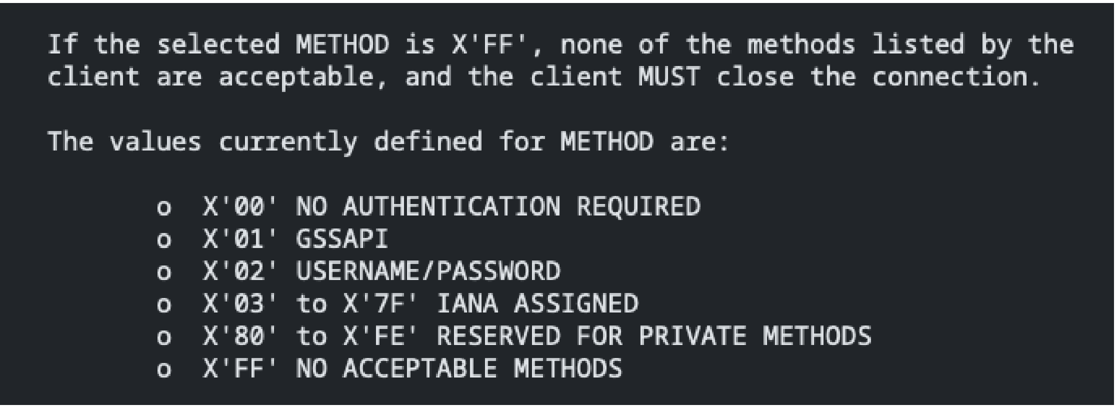
Socks5 extends Socks4 to support IPV6 and UDP



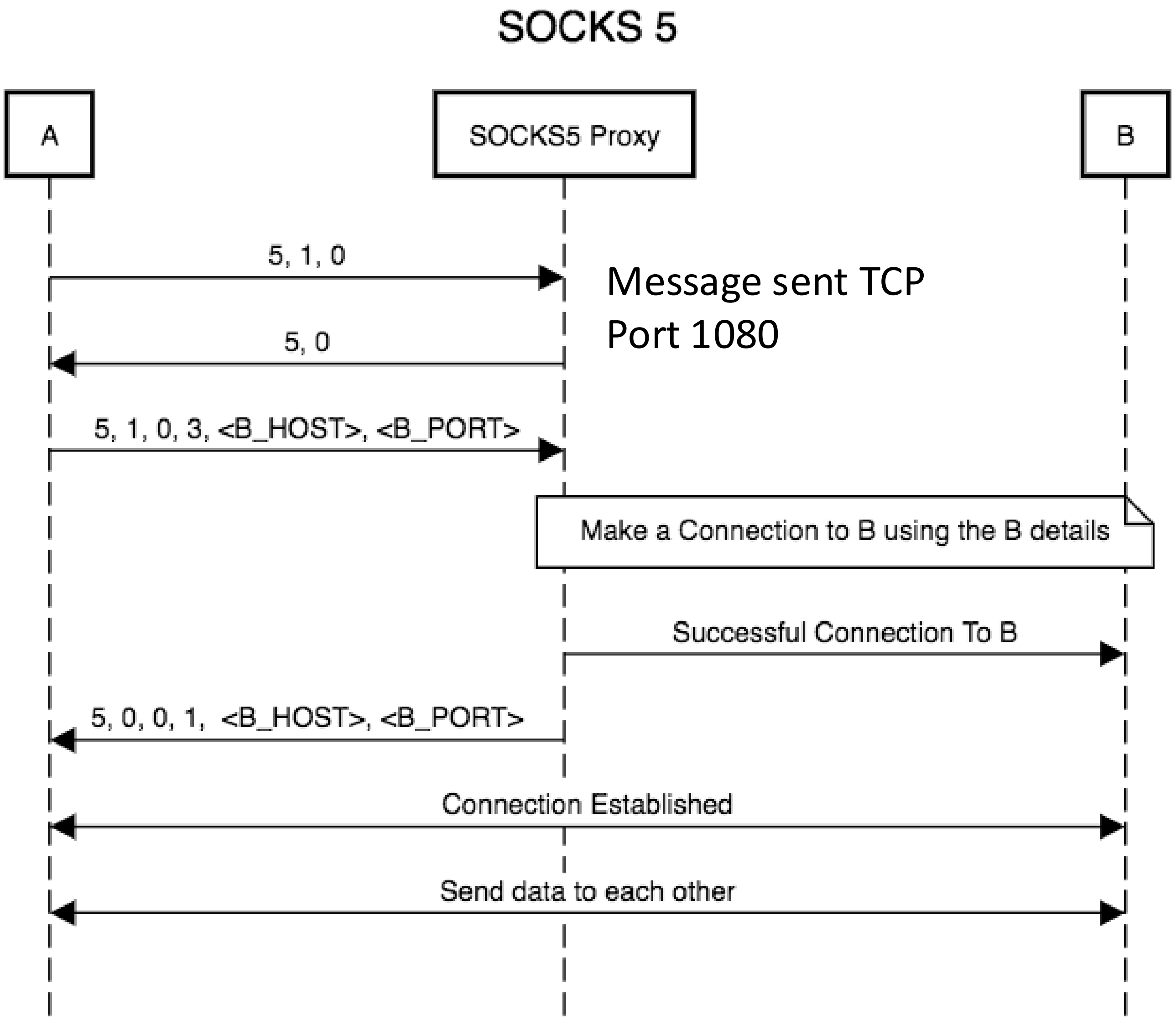
```
+----+----------+----------+
|VER | NMETHODS | METHODS  |
+----+----------+----------+
| 1  |    1     | 1 to 255 |
+----+----------+----------+
```

VER field is set to X'05' for this version of the protocol.

NMETHODS: Number of the Methods



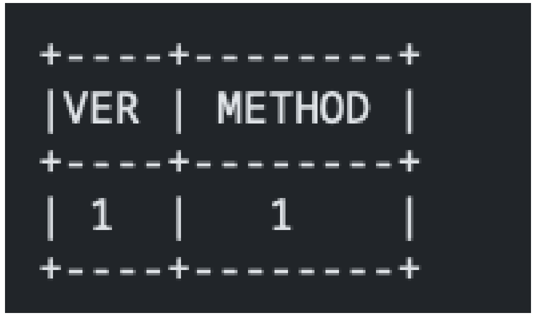
```
If the selected METHOD is X'FF', none of the methods listed by the
client are acceptable, and the client MUST close the connection.

The values currently defined for METHOD are:

       o  X'00' NO AUTHENTICATION REQUIRED
       o  X'01' GSSAPI
       o  X'02' USERNAME/PASSWORD
       o  X'03' to X'7F' IANA ASSIGNED
       o  X'80' to X'FE' RESERVED FOR PRIVATE METHODS
       o  X'FF' NO ACCEPTABLE METHODS
```


SOCKS 5
A
SOCKS5 Proxy
B
5, 1, 0
5, 0
5, 1, 0, 3, <B_HOST>, <B_PORT>
Make a Connection to B using the B details
Successful Connection To B
5, 0, 0, 1, <B_HOST>, <B_PORT>
Connection Established
Send data to each other

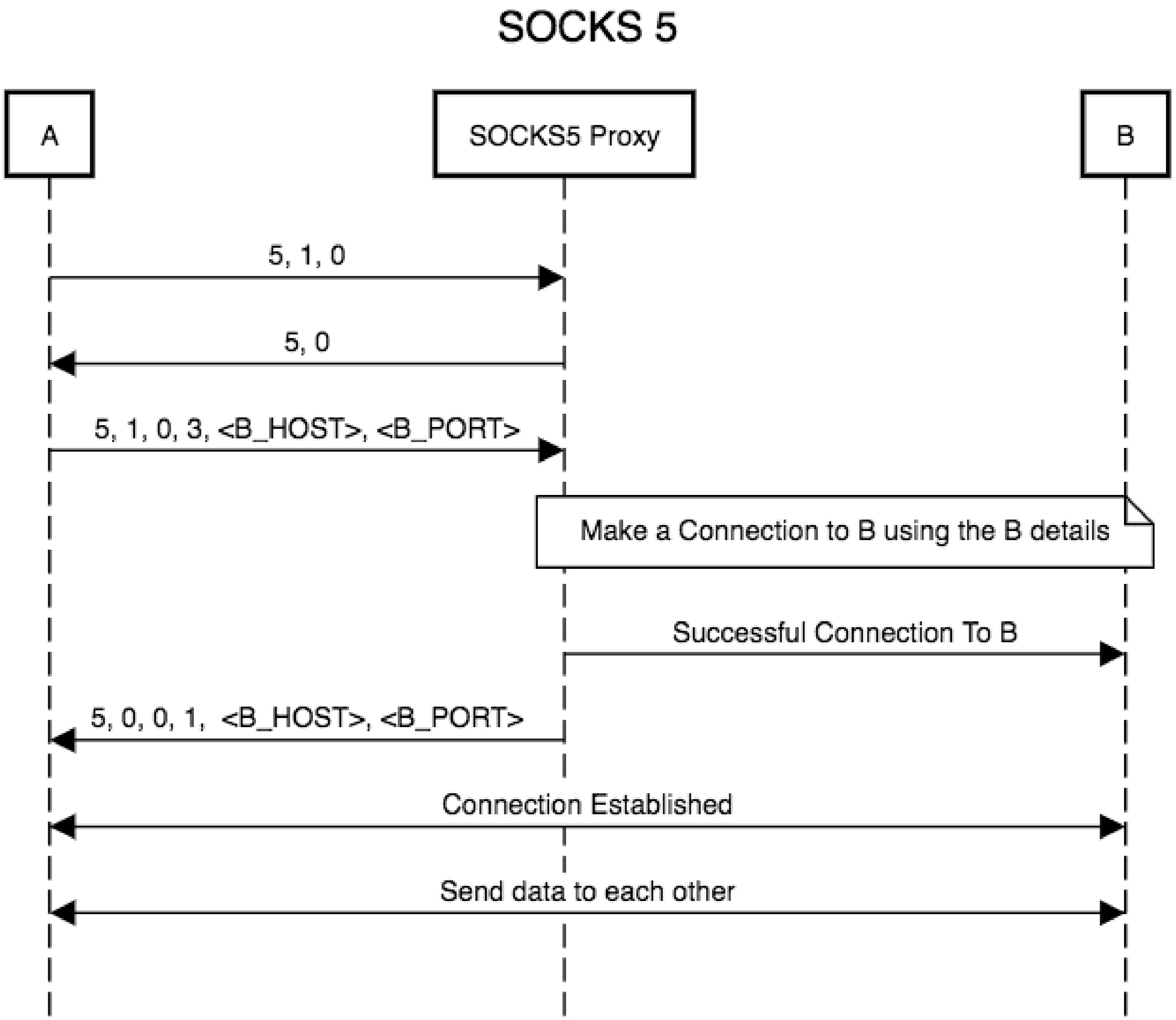
Message sent TCP
Port 1080

Ref: https://medium.com/@nimit95/socks-5-a-proxy-protocol-b741d3bec66c

Socks5 Proxy

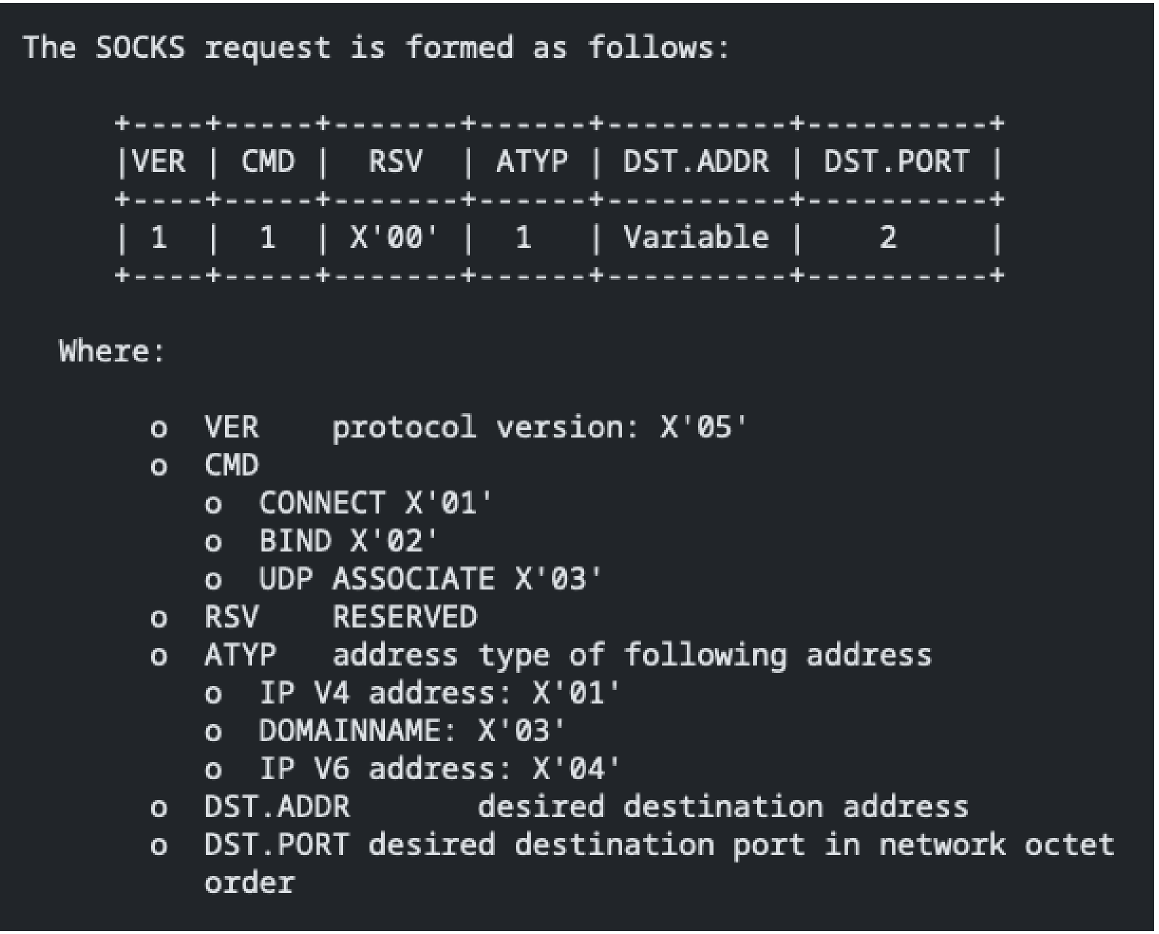


```
+----+--------+
|VER | METHOD |
+----+--------+
| 1  |   1    |
+----+--------+
```

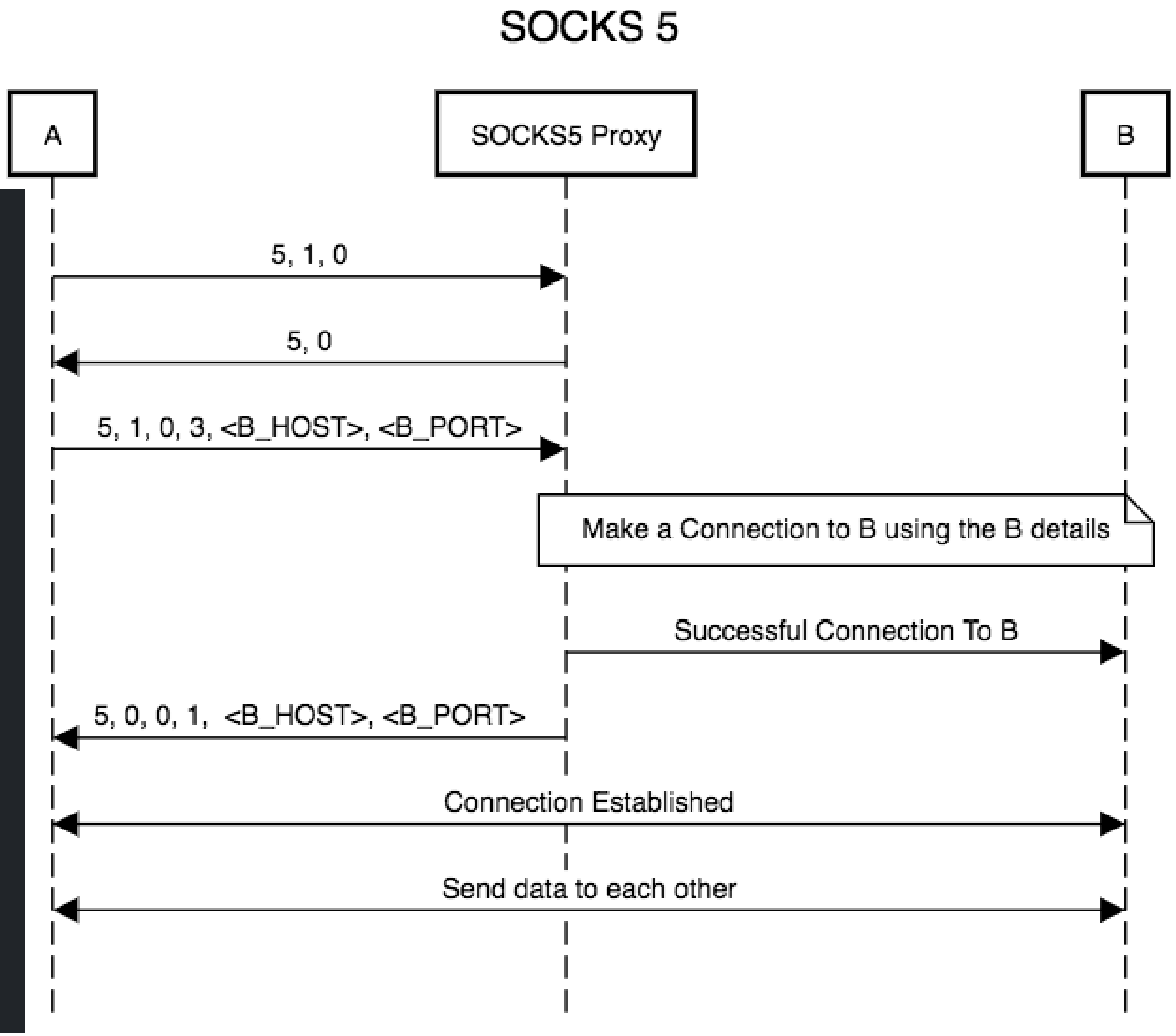

SOCKS 5
A
SOCKS5 Proxy
B
5, 1, 0
5, 0
5, 1, 0, 3, <B_HOST>, <B_PORT>
Make a Connection to B using the B details
Successful Connection To B
5, 0, 0, 1, <B_HOST>, <B_PORT>
Connection Established
Send data to each other

Ref: https://medium.com/@nimit95/socks-5-a-proxy-protocol-b741d3bec66c

Socks5 Proxy

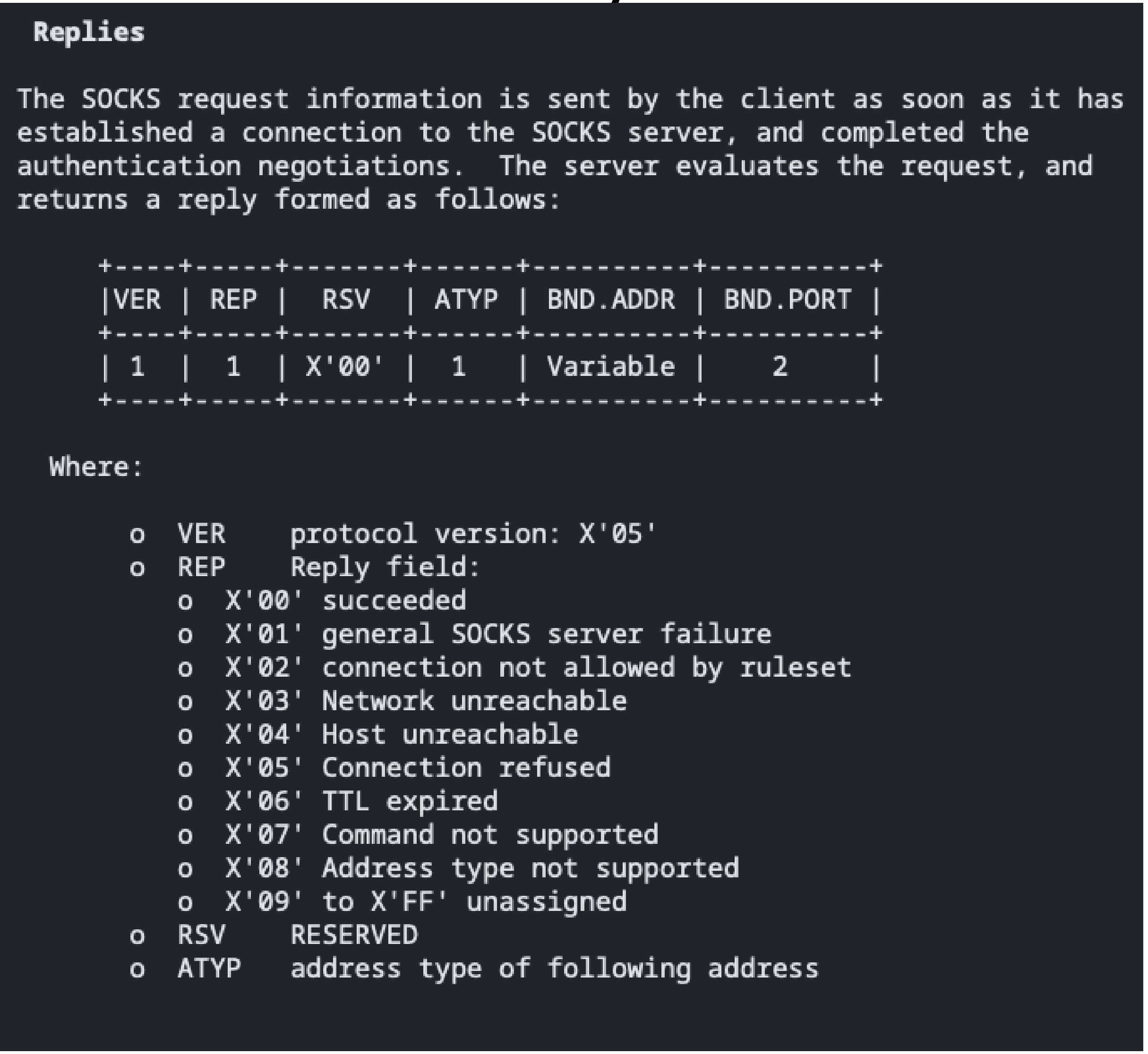


```
The SOCKS request is formed as follows:

     +----+-----+-------+------+----------+----------+
     |VER | CMD |  RSV  | ATYP | DST.ADDR | DST.PORT |
     +----+-----+-------+------+----------+----------+
     | 1  |  1  | X'00' |  1   | Variable |    2     |
     +----+-----+-------+------+----------+----------+

  Where:

       o  VER    protocol version: X'05'
       o  CMD
          o  CONNECT X'01'
          o  BIND X'02'
          o  UDP ASSOCIATE X'03'
       o  RSV    RESERVED
       o  ATYP   address type of following address
          o  IP V4 address: X'01'
          o  DOMAINNAME: X'03'
          o  IP V6 address: X'04'
       o  DST.ADDR       desired destination address
       o  DST.PORT desired destination port in network octet
          order
```

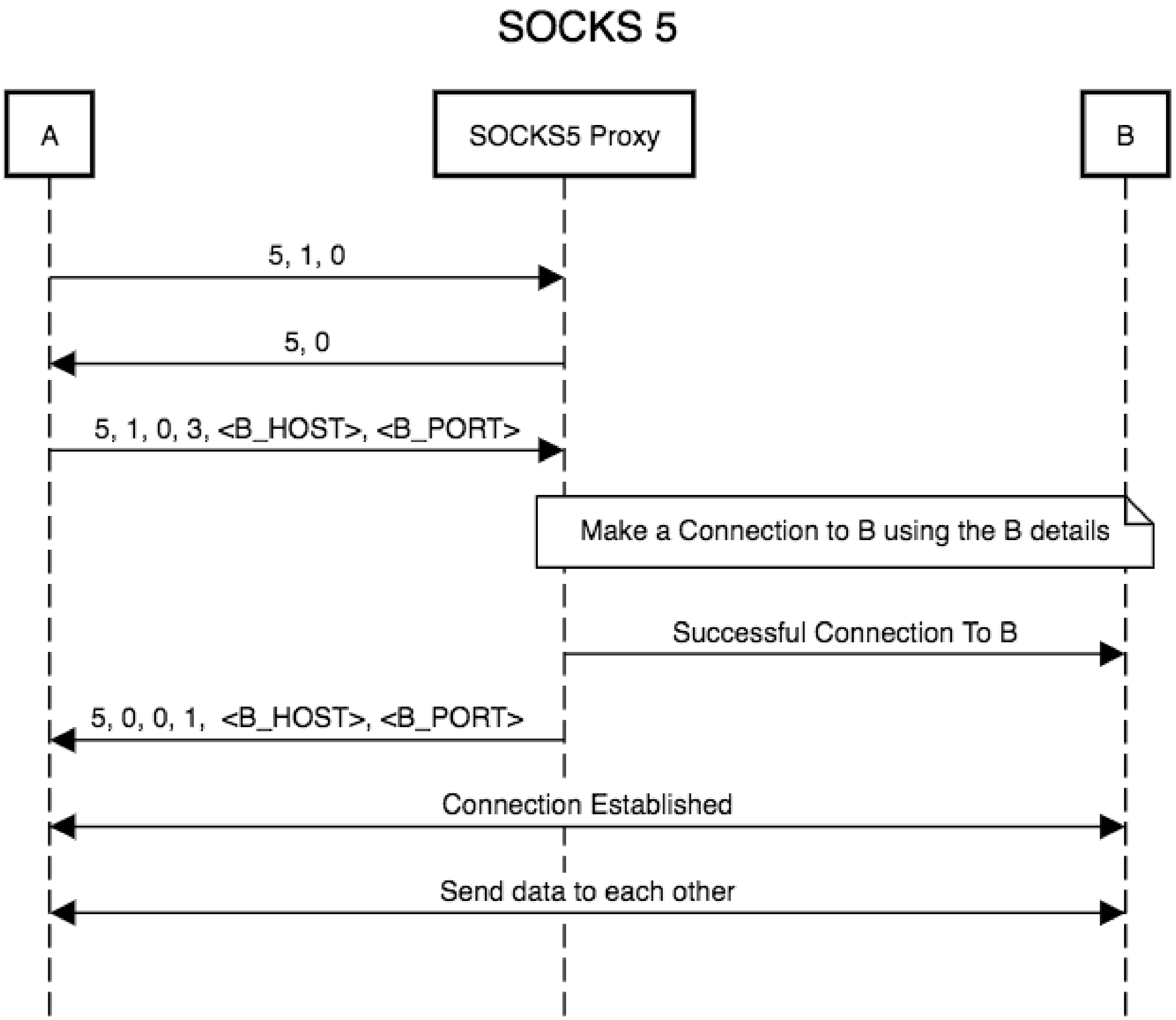

SOCKS 5
A
SOCKS5 Proxy
B
5, 1, 0
5, 0
5, 1, 0, 3, <B_HOST>, <B_PORT>
Make a Connection to B using the B details
Successful Connection To B
5, 0, 0, 1, <B_HOST>, <B_PORT>
Connection Established
Send data to each other

Ref: https://medium.com/@nimit95/socks-5-a-proxy-protocol-b741d3bec66c

Socks5 Proxy



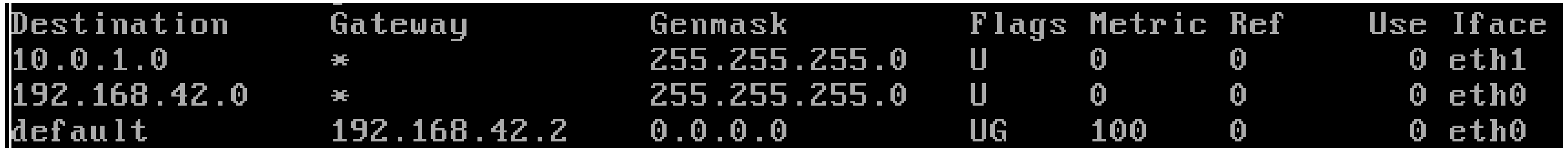
```
Replies

The SOCKS request information is sent by the client as soon as it has
established a connection to the SOCKS server, and completed the
authentication negotiations.  The server evaluates the request, and
returns a reply formed as follows:

     +----+-----+-------+------+----------+----------+
     |VER | REP |  RSV  | ATYP | BND.ADDR | BND.PORT |
     +----+-----+-------+------+----------+----------+
     | 1  |  1  | X'00' |  1   | Variable |    2     |
     +----+-----+-------+------+----------+----------+

  Where:

       o  VER    protocol version: X'05'
       o  REP    Reply field:
          o  X'00' succeeded
          o  X'01' general SOCKS server failure
          o  X'02' connection not allowed by ruleset
          o  X'03' Network unreachable
          o  X'04' Host unreachable
          o  X'05' Connection refused
          o  X'06' TTL expired
          o  X'07' Command not supported
          o  X'08' Address type not supported
          o  X'09' to X'FF' unassigned
       o  RSV    RESERVED
       o  ATYP   address type of following address
```


SOCKS 5
A
SOCKS5 Proxy
B
5, 1, 0
5, 0
5, 1, 0, 3, <B_HOST>, <B_PORT>
Make a Connection to B using the B details
Successful Connection To B
5, 0, 0, 1, <B_HOST>, <B_PORT>
Connection Established
Send data to each other

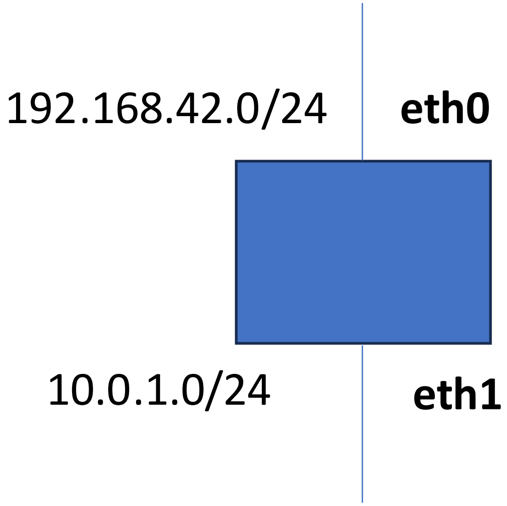
Ref: https://medium.com/@nimit95/socks-5-a-proxy-protocol-b741d3bec66c

Routes

1. **eth0** is connected to the internal network (192.168.42.0/24).
2. **eth1** is connected to an external network (10.0.1.0/24).
3. The device has a **default gateway on eth0 (192.168.1.1)** for internet access.



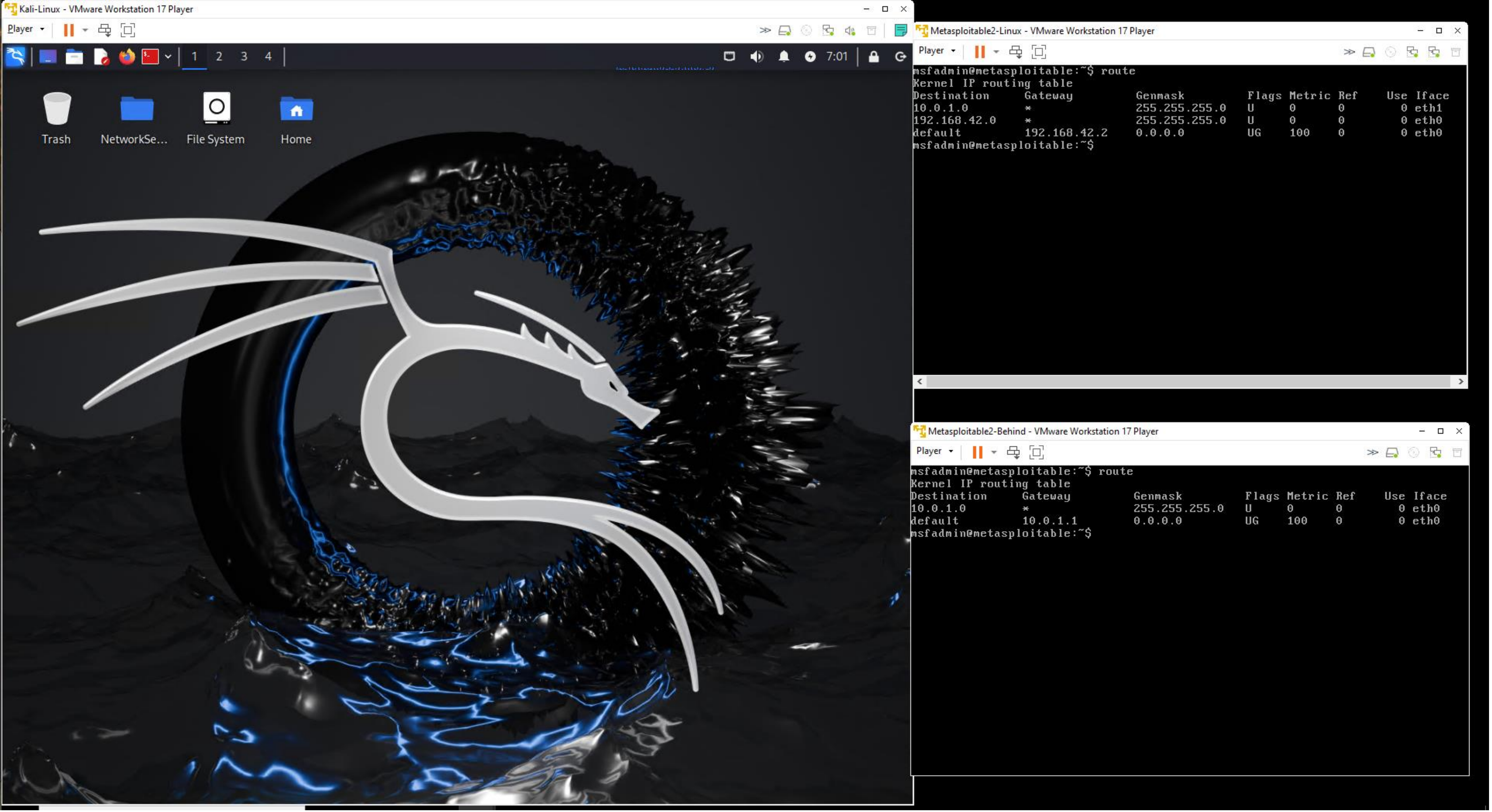
```
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.0.1.0        *               255.255.255.0   U     0      0        0 eth1
192.168.42.0    *               255.255.255.0   U     0      0        0 eth0
default         192.168.42.2    0.0.0.0         UG    100    0        0 eth0
```



* Means no gateway necessary

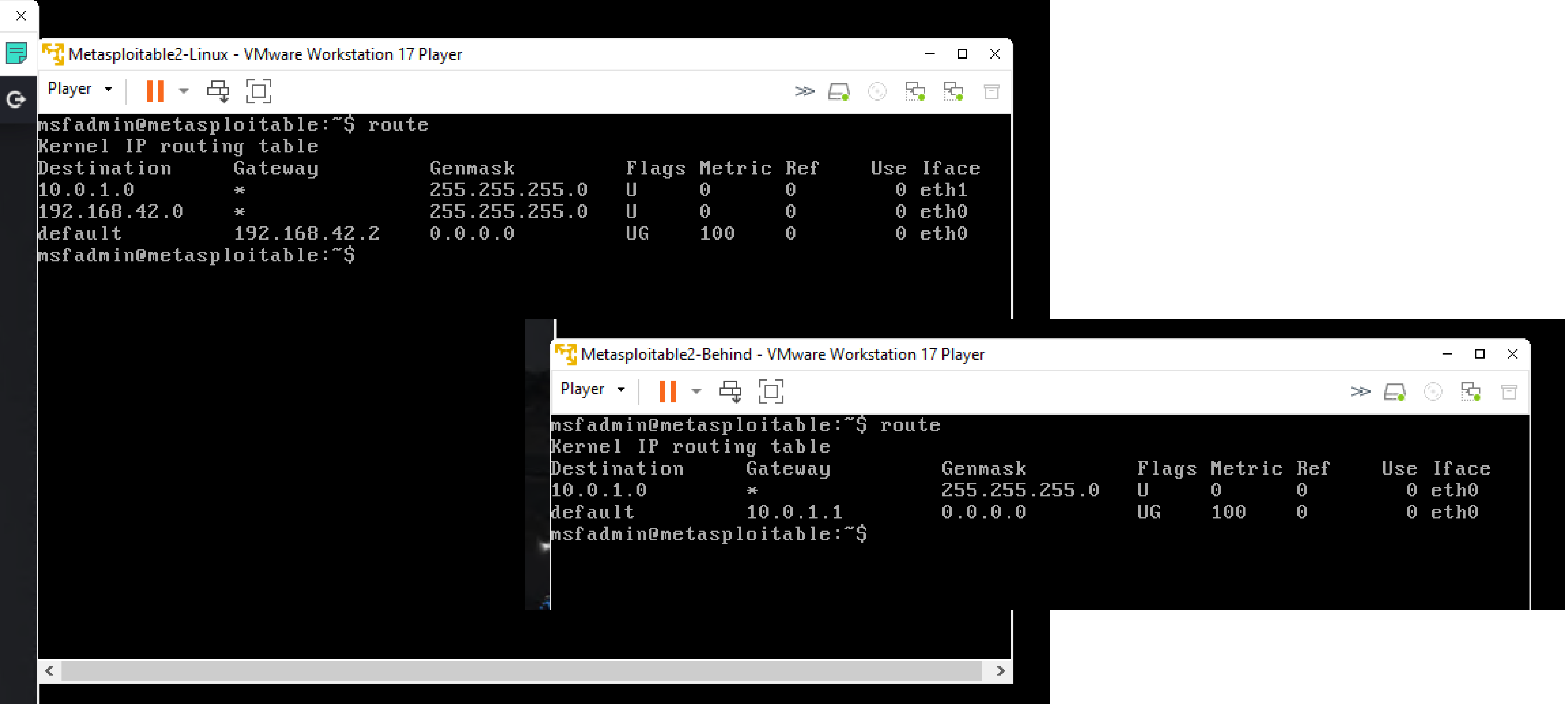
Flags: Indicate route properties.
- U (Up): The route is active.
- G (Gateway): The route goes through a gateway.
- H (Host): The destination is a single host.
- R (Reinstate): Used for dynamic routes.

Metric: The cost of using this route (lower is preferred).
- Routes with lower metrics are chosen first.


Kali-Linux - VMware Workstation 17 Player
Player
1
2
3
4
7:01
Trash
NetworkSe...
File System
Home
Metasploitable2-Linux - VMware Workstation 17 Player
Player
Metasploitable2-Behind - VMware Workstation 17 Player
Player

```
msfadmin@metasploitable:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.0.1.0        *               255.255.255.0   U     0      0        0 eth1
192.168.42.0    *               255.255.255.0   U     0      0        0 eth0
default         192.168.42.2    0.0.0.0         UG    100    0        0 eth0
msfadmin@metasploitable:~$
```

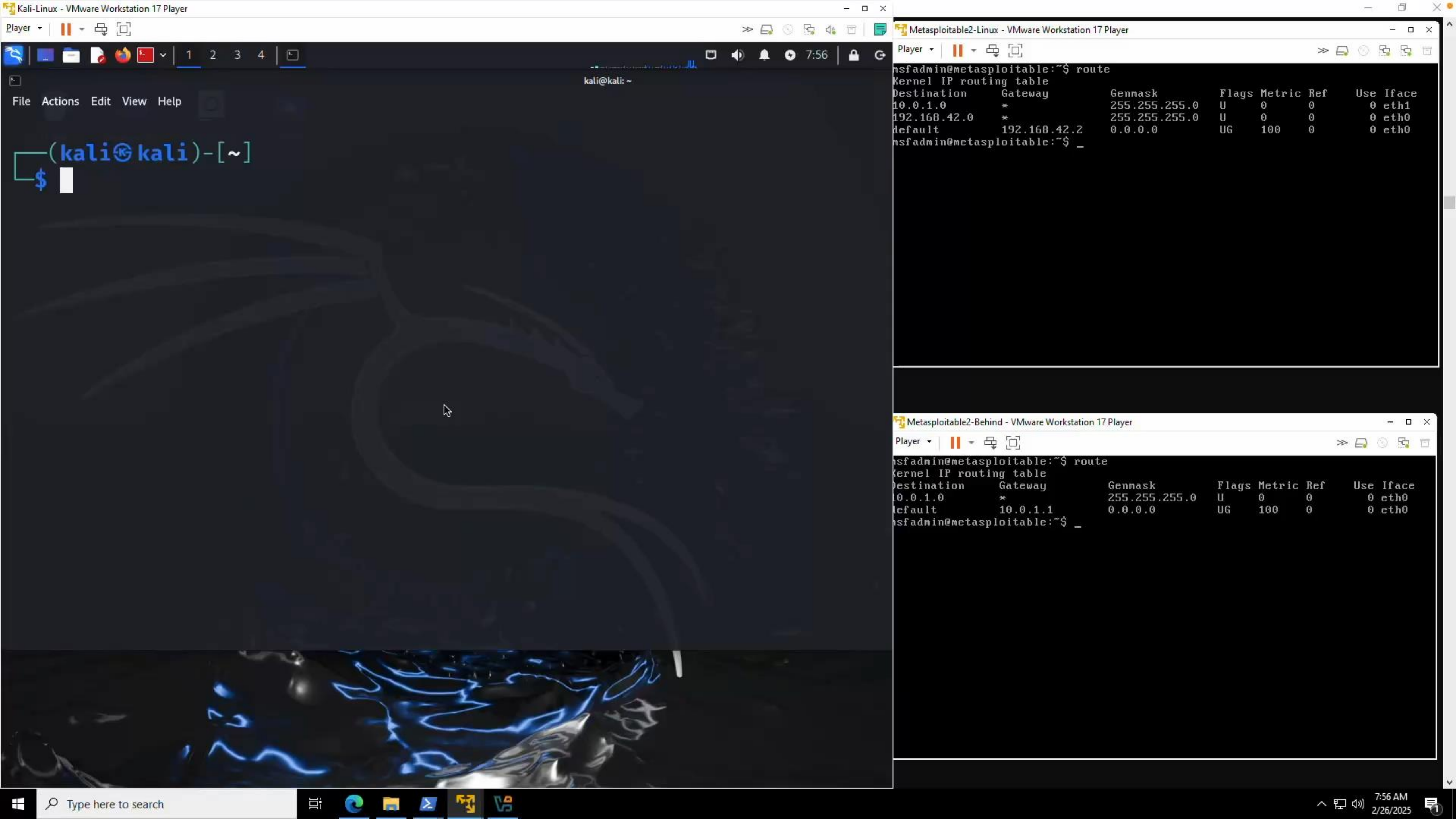
```
msfadmin@metasploitable:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.0.1.0        *               255.255.255.0   U     0      0        0 eth0
default         10.0.1.1        0.0.0.0         UG    100    0        0 eth0
msfadmin@metasploitable:~$
```


Metasploitable2-Linux - VMware Workstation 17 Player
Player

```
msfadmin@metasploitable:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.0.1.0        *               255.255.255.0   U     0      0        0 eth1
192.168.42.0    *               255.255.255.0   U     0      0        0 eth0
default         192.168.42.2    0.0.0.0         UG    100    0        0 eth0
msfadmin@metasploitable:~$
```

Metasploitable2-Behind - VMware Workstation 17 Player
Player

```
msfadmin@metasploitable:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.0.1.0        *               255.255.255.0   U     0      0        0 eth0
default         10.0.1.1        0.0.0.0         UG    100    0        0 eth0
msfadmin@metasploitable:~$
```


Kali-Linux - VMware Workstation 17 Player
Player
1
2
3
4
7:56
kali@kali: ~
File
Actions
Edit
View
Help
Metasploitable2-Linux - VMware Workstation 17 Player
Player
Metasploitable2-Behind - VMware Workstation 17 Player
Player
Type here to search
7:56 AM
2/26/2025

```
┌──(kali㉿kali)-[~]
└─$ 
```

```
msfadmin@metasploitable:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.0.1.0        *               255.255.255.0   U     0      0        0 eth1
192.168.42.0    *               255.255.255.0   U     0      0        0 eth0
default         192.168.42.2    0.0.0.0         UG    100    0        0 eth0
msfadmin@metasploitable:~$ _
```

```
msfadmin@metasploitable:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.0.1.0        *               255.255.255.0   U     0      0        0 eth0
default         10.0.1.1        0.0.0.0         UG    100    0        0 eth0
msfadmin@metasploitable:~$ _
```

But want if we want to use tools like NMAP to scan the target machine

Proxy chains

- Draw the idea.