Join the conversation @TheEvolveSec and slack.evolvesecurity.io

EVOLVE

Security Academy

Tommy McNeela, CISSP

How Denial of Service Attacks Work

Internet Access

Network: ???

Password: ???

EVOLVE Security Academy

Join the conversation @TheEvolveSec and slack.evolvesecurity.io

Tommy McNeela, CISSP

How Denial of Service Attacks Work

Welcome

Join the conversation!@TheEvolveSec and slack.evolvesecurity.io

Disclaimer

Don’t try to hack into other companies or other people’s personal accounts.

It is illegal and you will be arrested.

Use your own lab.

Following Along

- Download and install Oracle VirtualBox (https://www.virtualbox.org/wiki/Downloads)
- Download the two virtual appliances below, and import them into VirtualBox:
  - https://drive.google.com/open?id=0B2Vs-EwZxkS1dHVXeVFFZkxaM3M (DoS target)
  - https://drive.google.com/open?id=0B2Vs-EwZxkS1SWJkcjl5d0tTWGM (DoS attacker)

- Work together with your neighbors and collaborate

What is a DoS attack?

- A denial of service attack is any attack intended to disrupt the availability of a resource to legitimate users.

Real-world DoS mitigation

Why are we talking about DoS? It is the easiest and most common network attack used today.

Real-world DoS mitigation

Why are we talking about DoS? It is the easiest and most common network attack used today.

I am a network security engineer for US Cellular, and we detect and mitigate an average of more than 2200 DDoS attacks per day on the customer data network.

What is a DDoS attack?

- A Distributed Denial of Service attack is a coordinated DoS attack that uses many different hosts or attack vectors simultaneously to carry out the attack against the target.

How does an attacker have so many hosts to use?

- Usually, the attack originates from a botnet.

How does an attacker have so many hosts to use?

- Usually, the attack originates from a botnet.
- A botnet is a group of many hosts that are under an attacker’s control, usually gained through compromise by infections from malware such as Mirai.

Basic networking concepts

- Transmission Control Protocol (TCP)

Basic networking concepts

- Transmission Control Protocol (TCP)
  - Connection-based

Basic networking concepts

- Transmission Control Protocol (TCP)
  - Connection-based
- User Datagram Protocol (UDP)

Basic networking concepts

- Transmission Control Protocol (TCP)
  - Connection-based
- User Datagram Protocol (UDP)
  - Connectionless

How does a TCP connection occur?

- TCP Handshake process

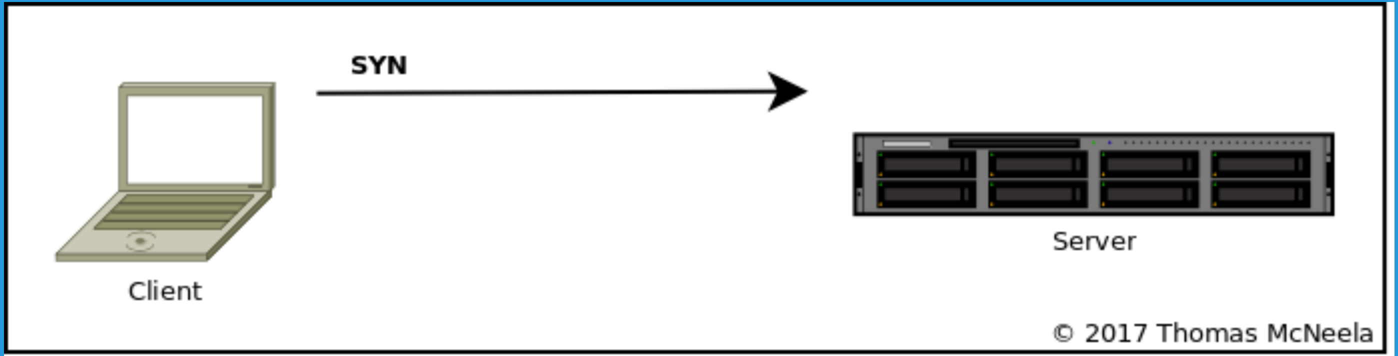
Join the conversation
@TheEvolveSec and
slack.evolvesecurity.io

TCP Handshake

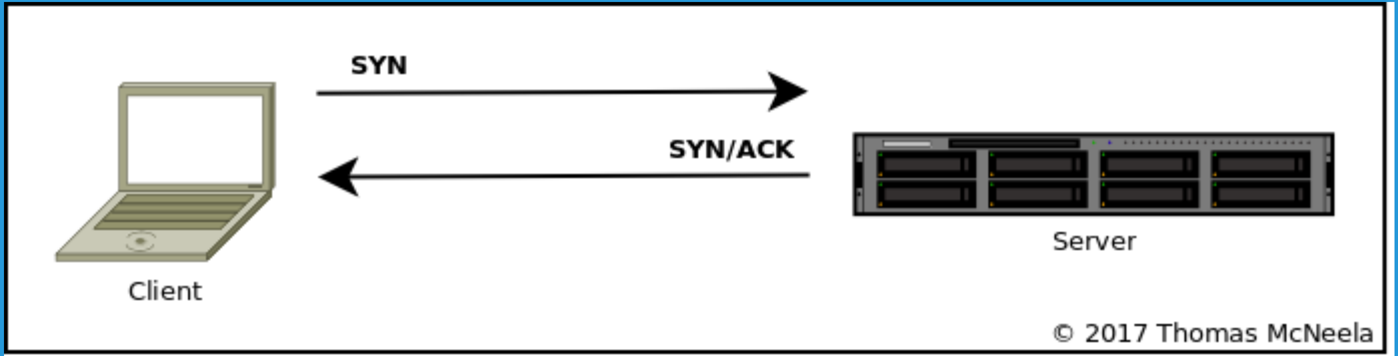
Client
Server
© 2017 Thomas McNeela

EVOLVE Security Academy

TCP Handshake (Step 1)

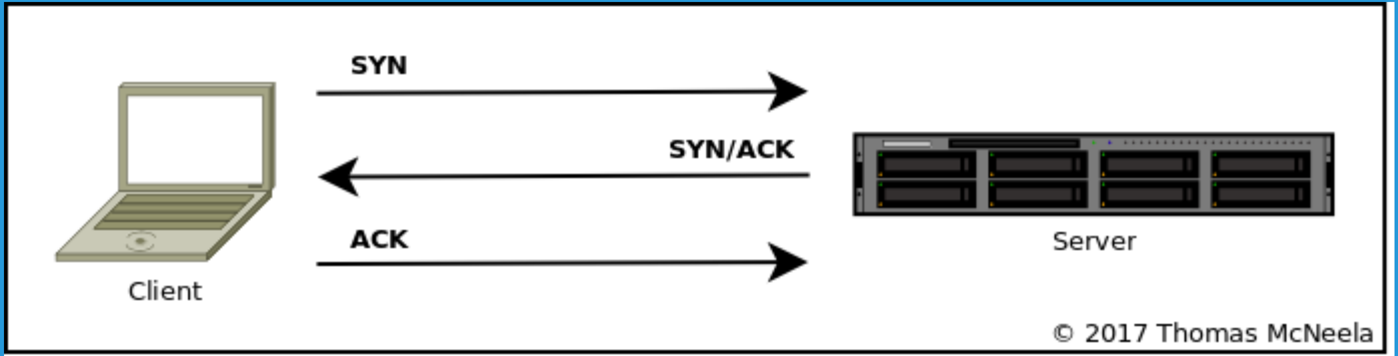


TCP Handshake (Step 2)



Join the conversation @TheEvolveSec and slack.evolvesecurity.io

TCP Handshake (Step 3)



Connection established!

EVOLVE Security Academy

IP Spoofing

- IP spoofing refers to modifying an IP packet header before sending it by replacing the source or destination IP address with a different address.

Common Network-Based DoS Attack Methods

Common Network-Based DoS Attack Methods

- Volume-based

Common Network-Based DoS Attack Methods

- Volume-based
  - –UDP flood

Common Network-Based DoS Attack Methods

- Volume-based
  - –UDP flood
  - –ICMP flood

Common Network-Based DoS Attack Methods

- Volume-based
  - UDP flood
  - ICMP flood
- Protocol/application-based

Common Network-Based DoS Attack Methods

- Volume-based
  - UDP flood
  - ICMP flood
- Protocol/application-based
  - SYN flood

Common Network-Based DoS Attack Methods

- Volume-based
  - UDP flood
  - ICMP flood
- Protocol/application-based
  - SYN flood
  - Connection flood

Common Network-Based DoS Attack Methods

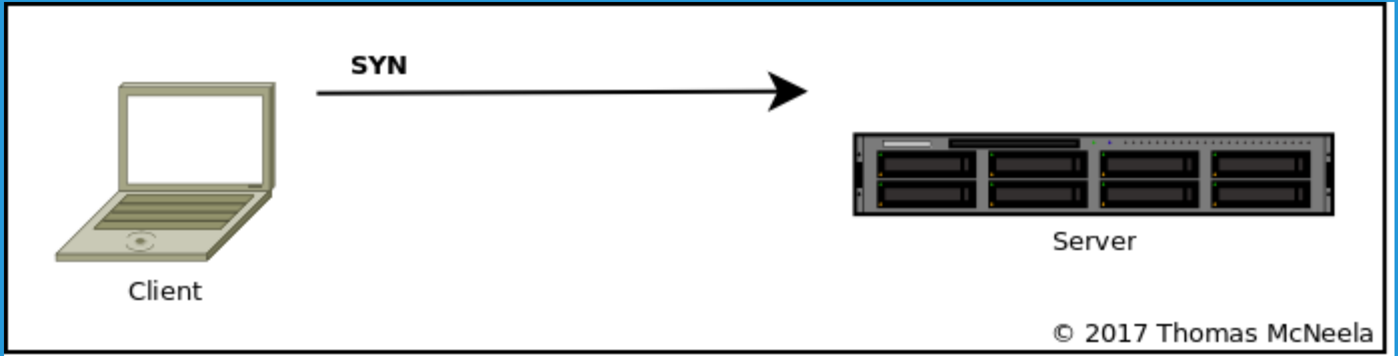
- Volume-based
  - UDP flood
  - ICMP flood
- Protocol/application-based
  - SYN flood
  - Connection flood
  - HTTP flood

Common Network-Based DoS Attack Methods

- Volume-based
  - –UDP flood
  - –ICMP flood
- Protocol/application-based
  - –SYN flood
  - –Connection flood
  - –HTTP flood
  - –Ping of Death

Join the conversation @TheEvolveSec and slack.evolvesecurity.io

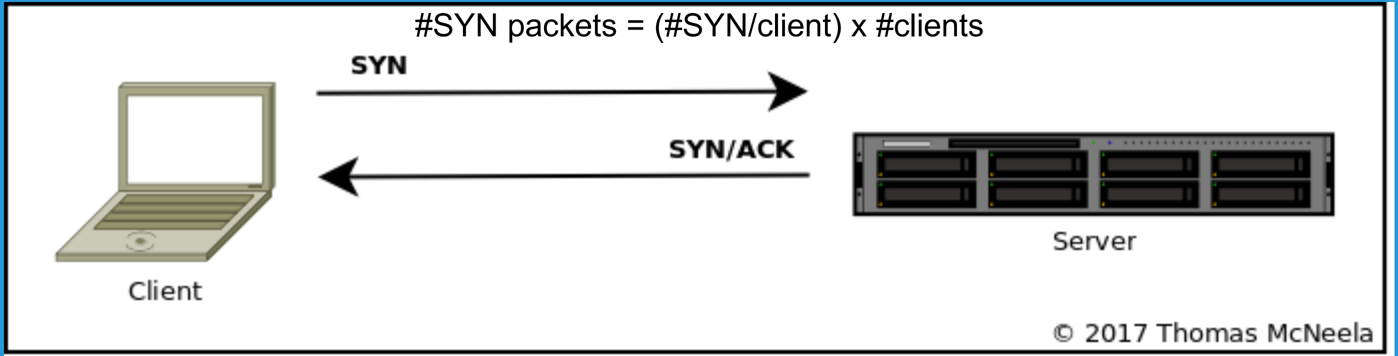
SYN Flood



EVOLVE Security Academy

Join the conversation
@TheEvolveSec and
slack.evolvesecurity.io

SYN Flood

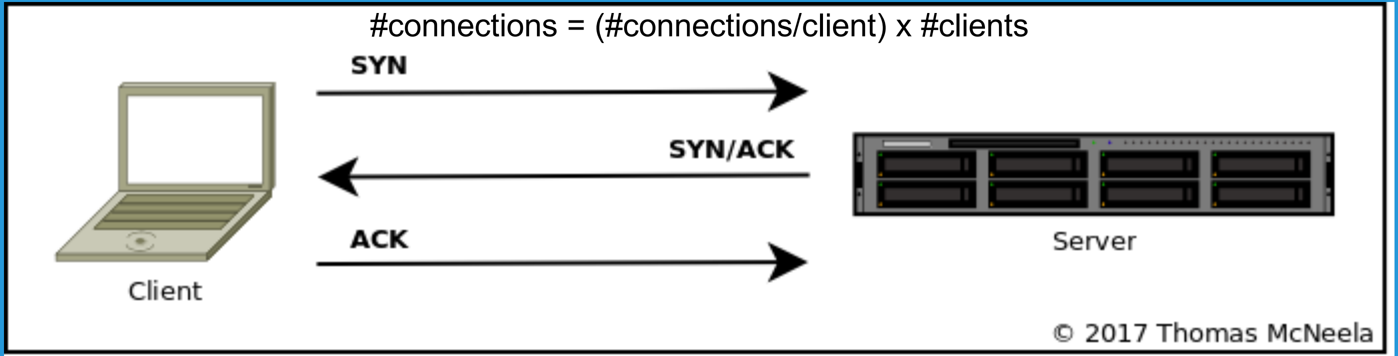

#SYN packets = (#SYN/client) x #clients

No ACK response sent

EVOLVE Security Academy

Connection Flood

Join the conversation @TheEvolveSec and slack.evolvesecurity.io



No data sent by client after TCP connection is established

EVOLVE Security Academy

HTTP Flood

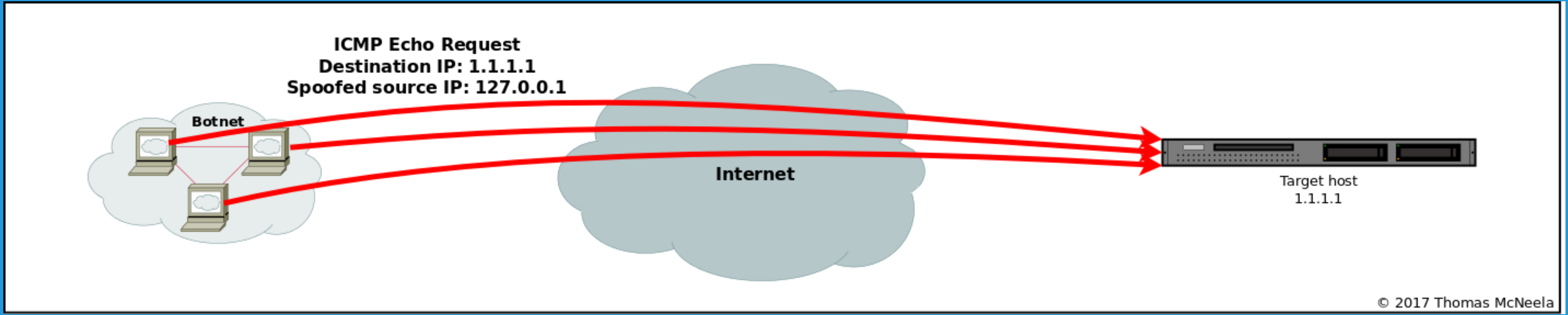
- After a TCP connection is made over port 80 (HTTP) or 443 (HTTPS), the attacking machine attempts to hold the connection open as long as possible and use as many resources as possible, reducing available resources to legitimate requests

Ping of Death

- Source IP is spoofed to be the IP address of the target machine, or the local loopback address.

Join the conversation
@TheEvolveSec and
slack.evolvesecurity.io

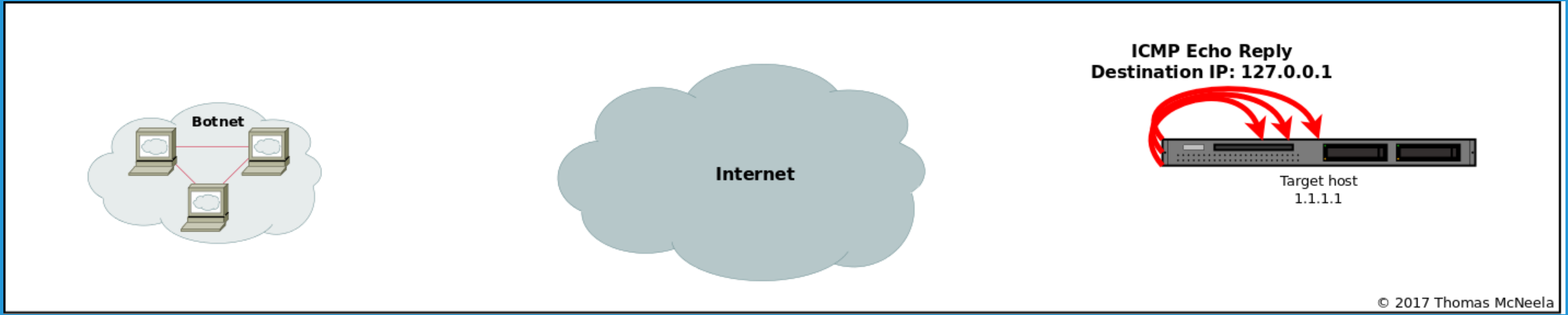
Ping of Death



EVOLVE
Security Academy

Join the conversation
@TheEvolveSec and
slack.evolvesecurity.io

Ping of Death



EVOLVE
Security Academy

Common Network-Based DoS Attack Methods (continued)

- Reflected and amplified

Common Network-Based DoS Attack Methods (continued)

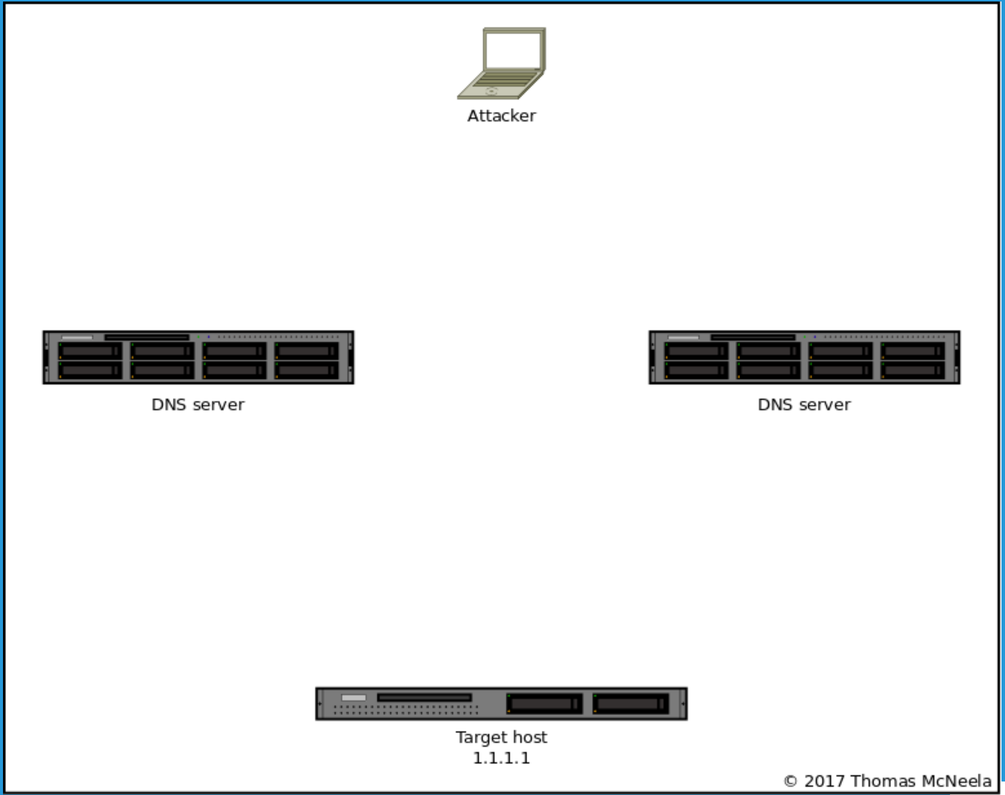
- Reflected and amplified
  - DNS amplification

Common Network-Based DoS Attack Methods (continued)

- Reflected and amplified
  - –DNS amplification
  - –Smurf

DNS Amplification

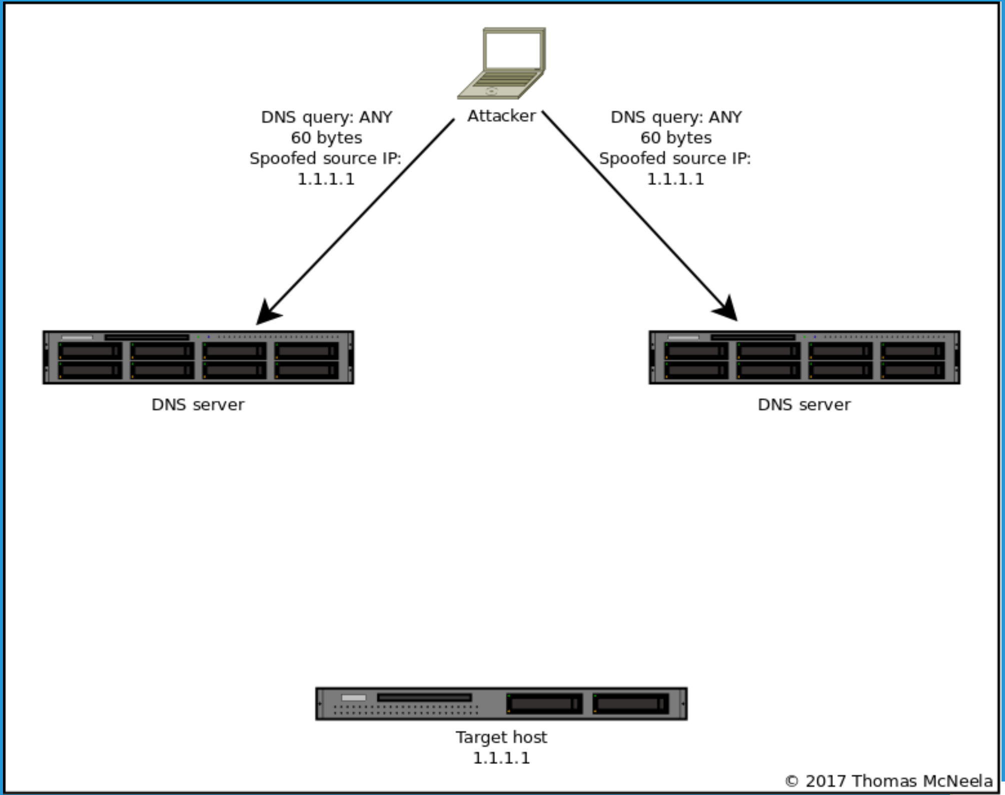
Join the conversation @TheEvolveSec and slack.evolvesecurity.io



EVOLVE Security Academy

DNS Amplification

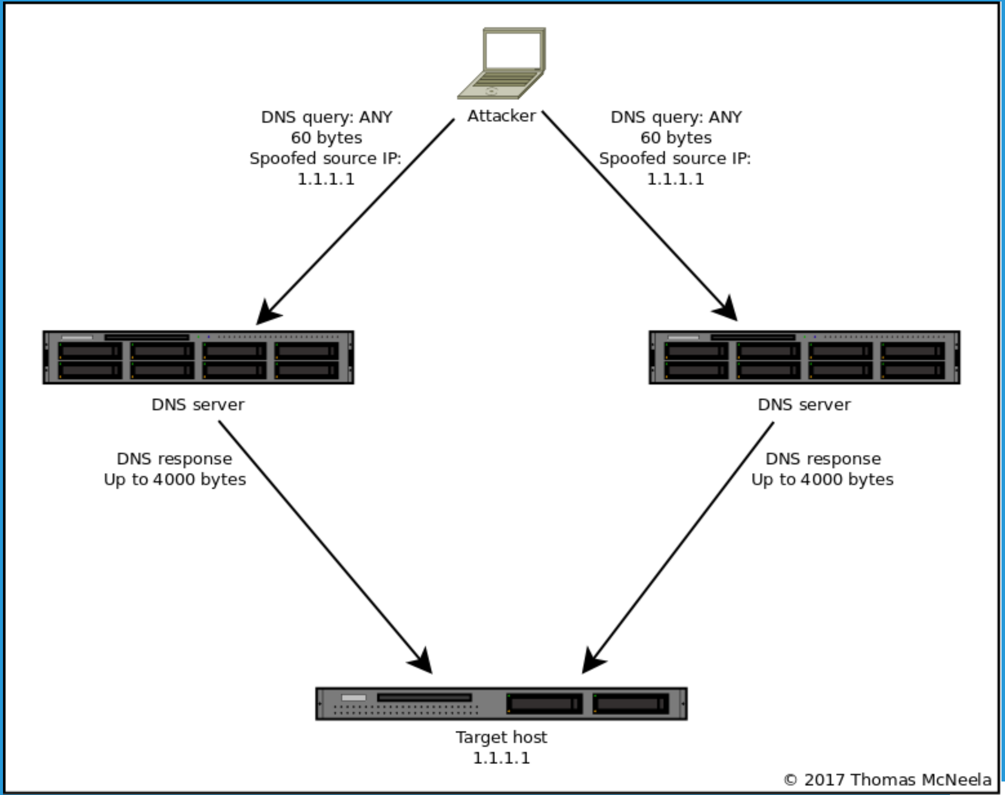
Join the conversation @TheEvolveSec and slack.evolvesecurity.io



EVOLVE Security Academy

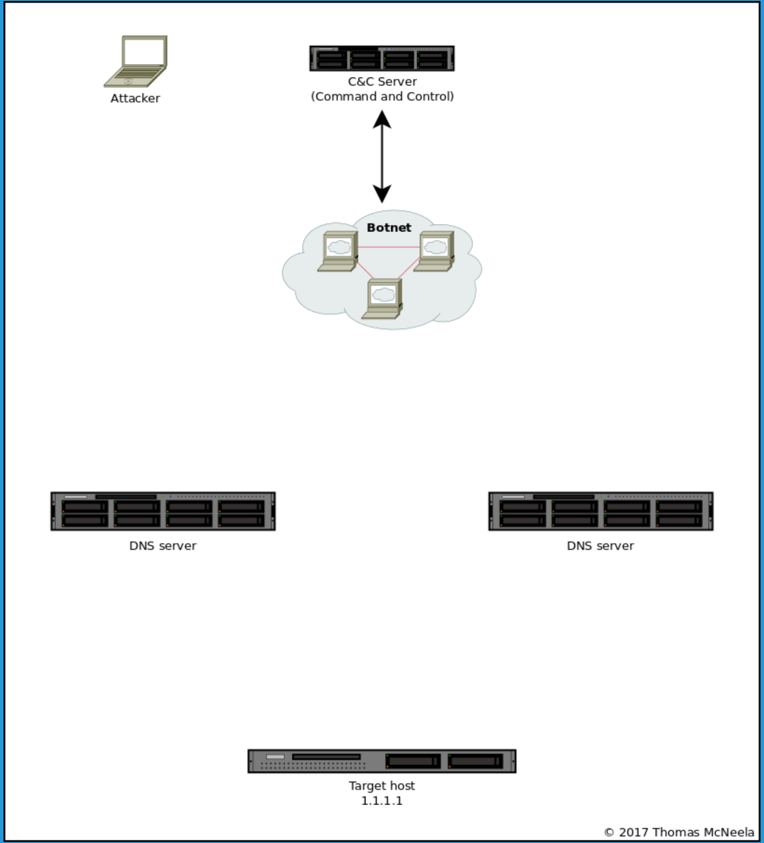
DNS Amplification

Join the conversation
@TheEvolveSec and
slack.evolvesecurity.io



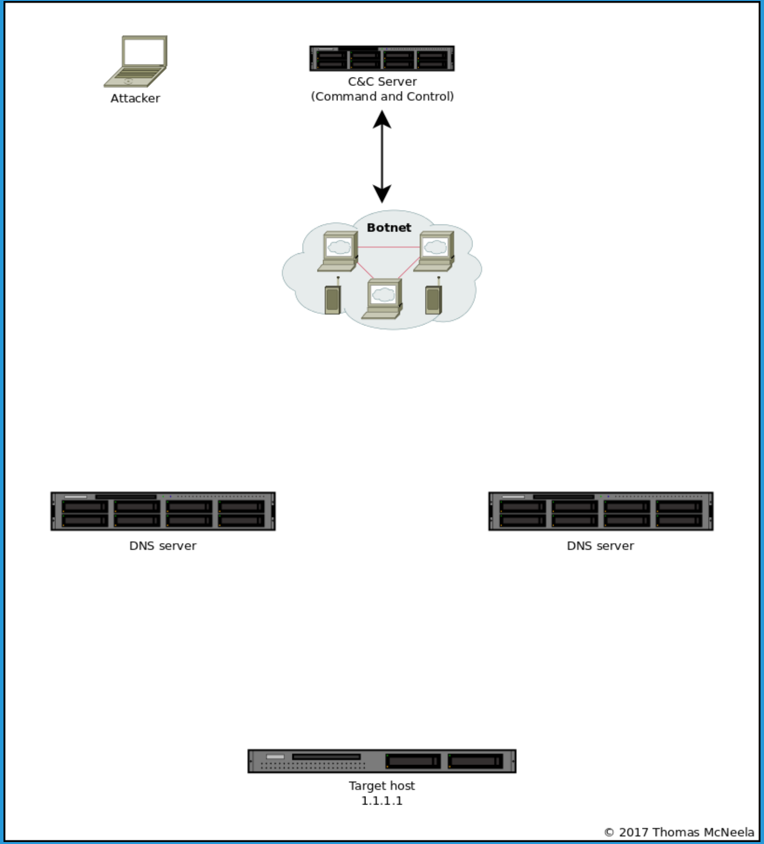
EVOLVE
Security Academy

DNS Amplification with Botnet



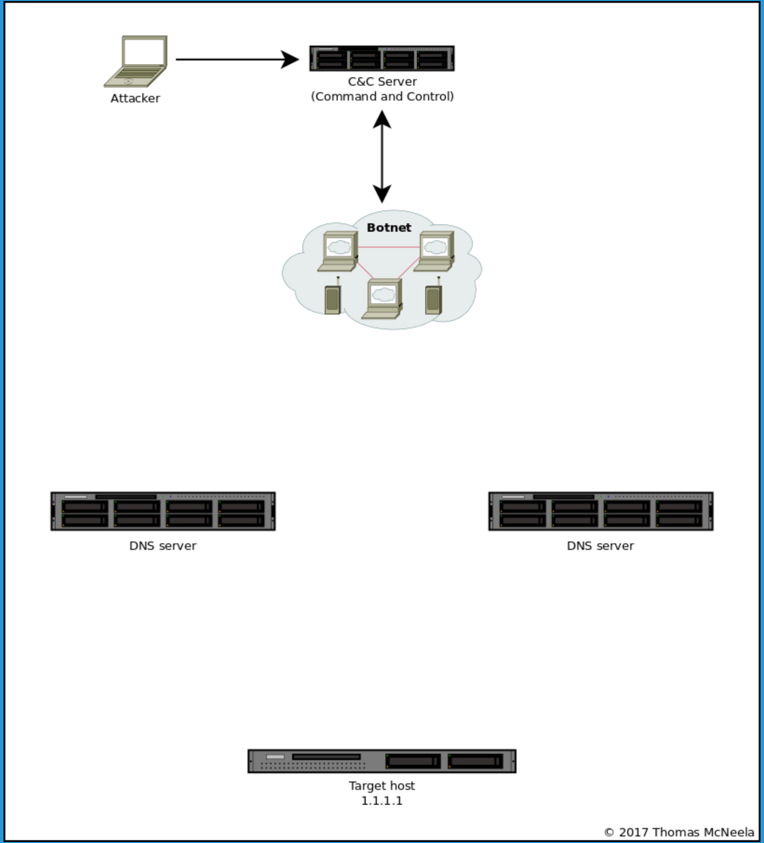
EVOLVE Security Academy

DNS Amplification with Botnet



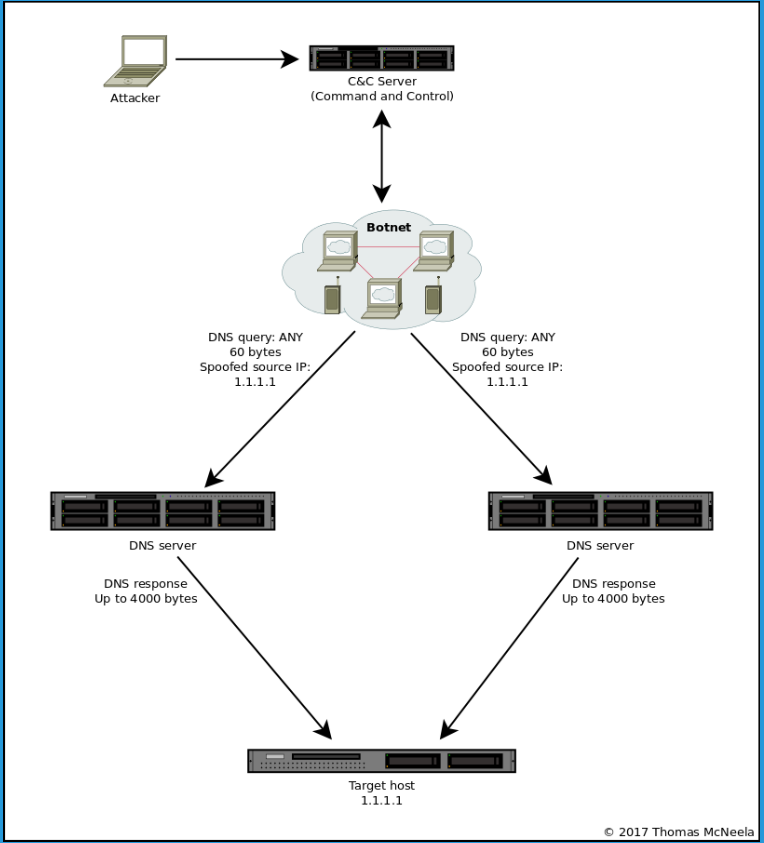
EVOLVE Security Academy

DNS Amplification with Botnet



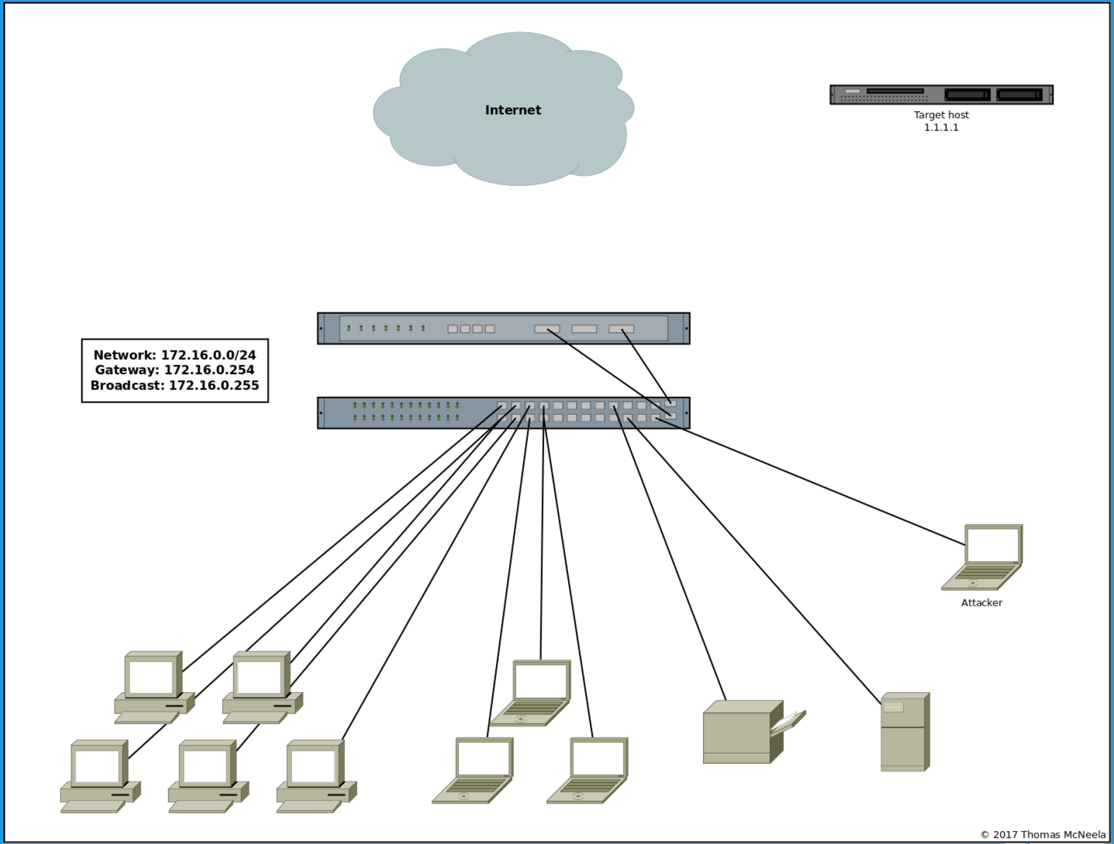
EVOLVE Security Academy

DNS Amplification with Botnet



Smurf

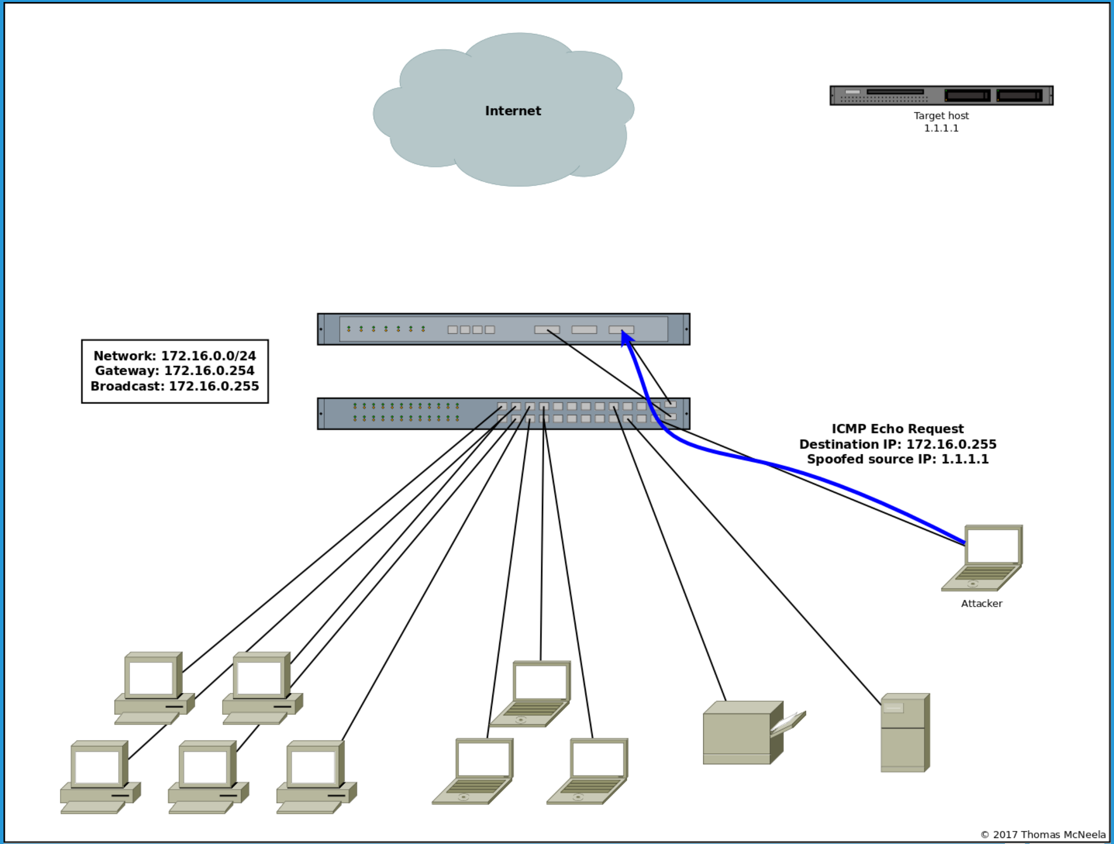
Join the conversation @TheEvolveSec and slack.evolvesecurity.io



EVOLVE Security Academy

Smurf

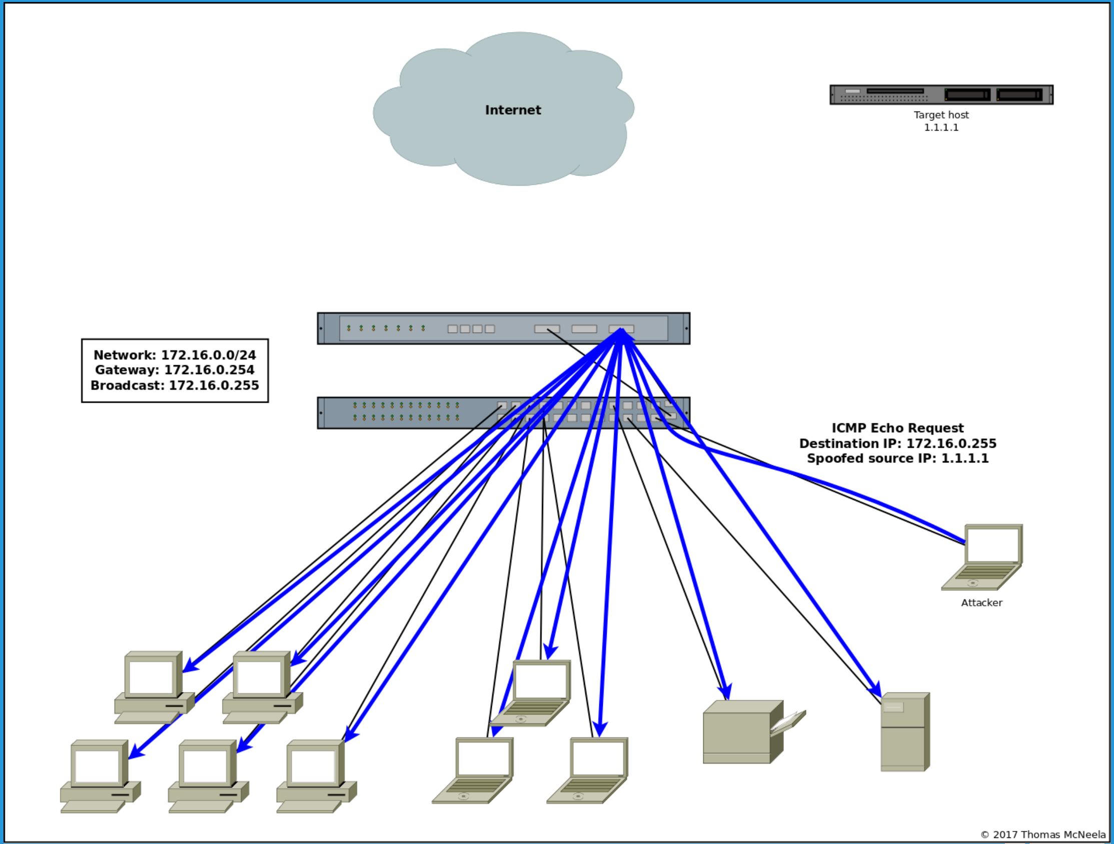
Join the conversation @TheEvolveSec and slack.evolvesecurity.io



EVOLVE Security Academy

Smurf

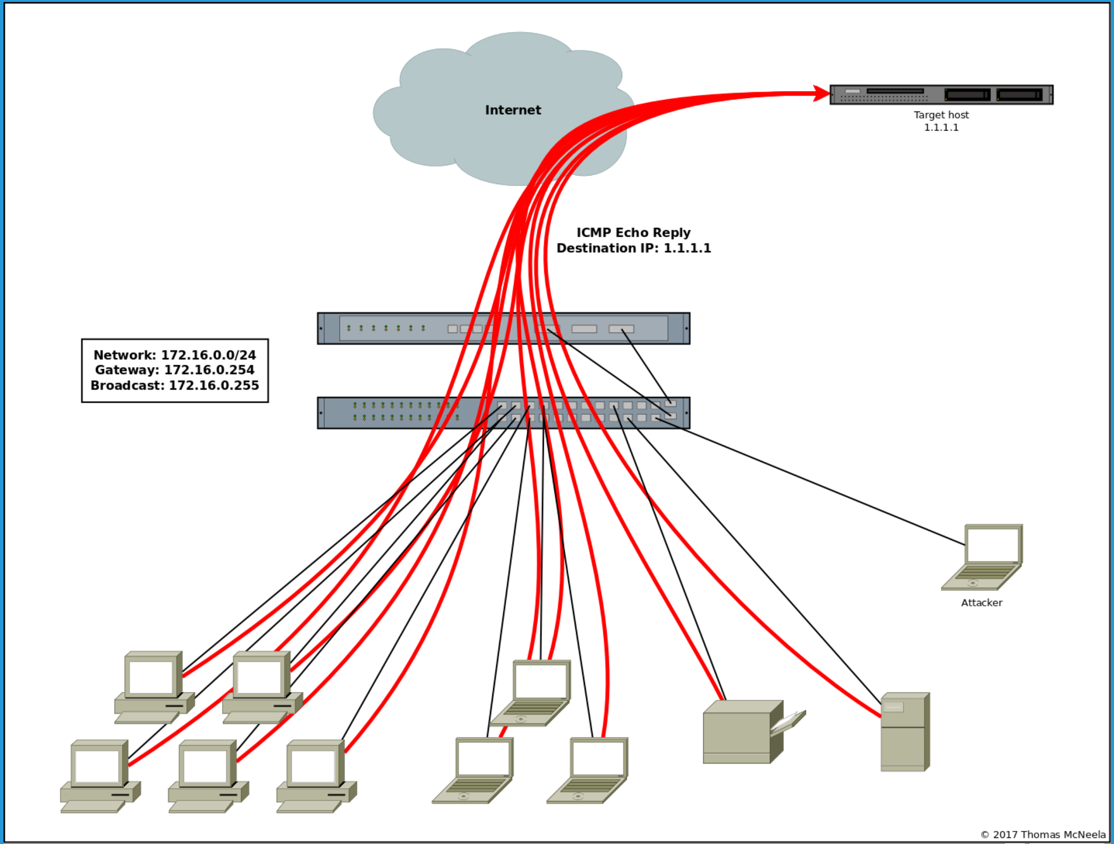
Join the conversation @TheEvolveSec and slack.evolvesecurity.io



EVOLVE Security Academy

Smurf

Join the conversation @TheEvolveSec and slack.evolvesecurity.io



Lab 1

- In this lab, we will attempt several types of DoS attacks against a web server.
- We will monitor traffic on the server and observe the effects of the attack in real time.

Following Along

- Download and install Oracle VirtualBox (https://www.virtualbox.org/wiki/Downloads)
- Download the two virtual appliances below, and import them into VirtualBox:
  - https://drive.google.com/open?id=0B2Vs-EwZxkS1dHVXeVFFZkxaM3M (DoS target)
  - https://drive.google.com/open?id=0B2Vs-EwZxkS1SWJkcjl5d0tTWGM (DoS attacker)

- Work together with your neighbors and collaborate

Lab 1

Join the conversation
@TheEvolveSec and
slack.evolvesecurity.io

1. Launch VirtualBox
2. If you don't already have one set up, create a host-only network adapter (File -> Preferences -> Network -> Host-only Networks -> + -> OK).
3. Start both virtual machines.
4. Log into both virtual machines.
    a. Username: foobar
    b. Password: abc123

EVOLVE
Security Academy

Lab 1

5. On the target machine, issue the command:
   ifconfig
   a. In the output, note the IP address on the second line after “inet addr:” -- this is the IP address of the target machine.
6. Open a web browser on your local machine, and navigate to the IP address of the target machine.

Lab 1

7. On the target VM, issue the command: sudo tcptrack -fi enp0s3
8. Let's start with a UDP flood attack. On the attacker VM, issue the command: udp_flood.sh <target_vm_ip> 20
9. Observe any activity on the target VM, and try refreshing your browser.
10. Stop the attack with the command: udp_flood.sh STOP

Lab 1

Join the conversation
@TheEvolveSec and
slack.evolvesecurity.io

11. Let’s try a SYN flood attack. On the attacker VM, issue the command: syn_flood.sh <target_vm_ip> 20
12. Observe any activity on the target VM, and try refreshing your browser.
13. Stop the attack with the command: syn_flood.sh STOP

EVOLVE
Security Academy

Lab 1

Join the conversation @TheEvolveSec and slack.evolvesecurity.io

14. Let’s try a TCP connection flood attack. On the attacker VM, issue the command: conn_flood.sh <target_vm_ip> 50
15. Observe any activity on the target VM, and try refreshing your browser.
16. Stop the attack with the command: conn_flood.sh STOP

Lab 2

- In this lab, we will attempt to mitigate the DoS attacks we performed in lab one. We will be using the Linux local firewall application iptables.
- Again, we will monitor traffic on the server and observe the effects of the attack in real time.

Lab 2

Join the conversation
@TheEvolveSec and
slack.evolvesecurity.io

1. On the target VM, press the q key.
2. Issue the command: cat bin/iptables.save
3. These are the actual firewall rules we are going to implement. Let’s go over some of the most significant ones.

EVOLVE
Security Academy

Lab 2

```
-A PREROUTING -m conntrack --ctstate INVALID -j DROP
-A PREROUTING -p tcp -m tcp ! --tcp-flags FIN,SYN,RST,ACK SYN -m conntrack --ctstate NEW -j DROP
-A PREROUTING -p tcp -m tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG NONE -j DROP
-A PREROUTING -p tcp -m tcp --tcp-flags FIN,SYN FIN,SYN -j DROP
-A PREROUTING -p tcp -m tcp --tcp-flags SYN,RST SYN,RST -j DROP
-A PREROUTING -p tcp -m tcp --tcp-flags FIN,SYN FIN,SYN -j DROP
-A PREROUTING -p tcp -m tcp --tcp-flags FIN,RST FIN,RST -j DROP
-A PREROUTING -p tcp -m tcp --tcp-flags FIN,ACK FIN -j DROP
-A PREROUTING -p tcp -m tcp --tcp-flags ACK,URG URG -j DROP
-A PREROUTING -p tcp -m tcp --tcp-flags FIN,ACK FIN -j DROP
-A PREROUTING -p tcp -m tcp --tcp-flags PSH,ACK PSH -j DROP
-A PREROUTING -p tcp -m tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG FIN,SYN,RST,PSH,ACK,URG -j DROP
-A PREROUTING -p tcp -m tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG NONE -j DROP
-A PREROUTING -p tcp -m tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG FIN,PSH,URG -j DROP
-A PREROUTING -p tcp -m tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG FIN,SYN,PSH,URG -j DROP
-A PREROUTING -p tcp -m tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG FIN,SYN,RST,ACK,URG -j DROP
```

Lab 2

```
-A INPUT -p tcp -m connlimit --connlimit-above 4 --connlimit-mask 32 --connlimit-saddr -j REJECT --reject-with tcp-reset
```

Lab 2

Join the conversation
@TheEvolveSec and
slack.evolvesecurity.io

```
-A INPUT -p tcp -m conntrack --ctstate NEW -m limit --limit 5/sec --limit-burst 3 -j ACCEPT

-A INPUT -p tcp -m conntrack --ctstate NEW -j DROP
```

EVOLVE
Security Academy

Lab 2

Join the conversation
@TheEvolveSec and
slack.evolvesecurity.io

4. Implement the firewall rules with the command: sudo iptables-restore bin/iptables.save
5. Resume monitoring the TCP traffic with the command: sudo tcptrack -fi enp0s3

EVOLVE
Security Academy

Lab 2

6. Since the only attack that actually succeeded in lab 1 was the TCP connection flood, let's try it again. On the attacker VM, issue the command: conn_flood.sh <target_vm_ip> 50
7. Observe any activity on the target VM, and try refreshing your browser.
8. Stop the attack with the command: conn_flood.sh STOP

Join the conversation
@TheEvolveSec and
slack.evolvesecurity.io

Thank you.

Q&A

EVOLVE
Security Academy

Contact

- Paul Petefish
  - Paul@EvolveAcademy.io
- Andrew Hamilton
  - Andrew@EvolveAcademy.io

www.EvolveAcademy.io