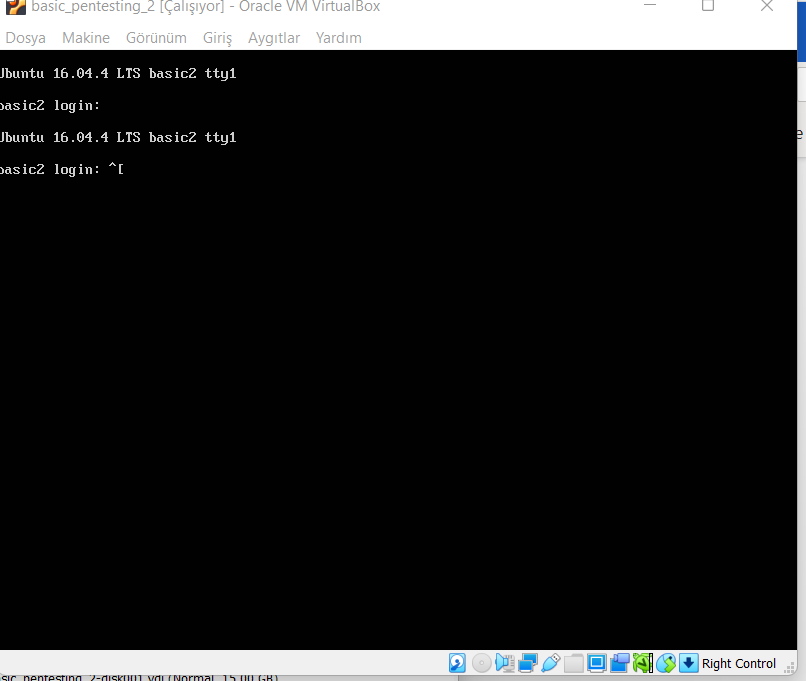
# Basic Pentesting: Walkthrough 2| Vulnhub

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

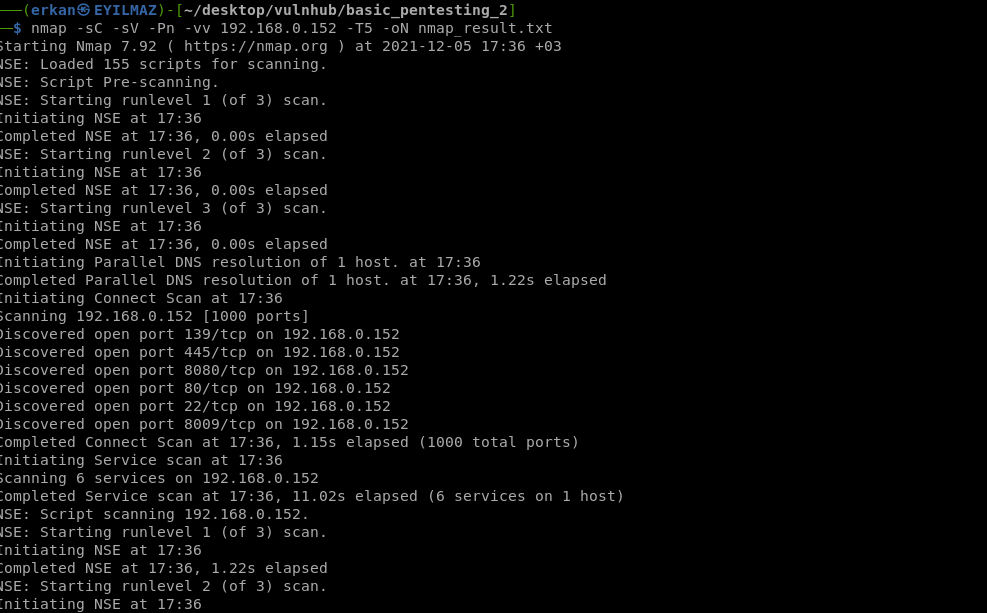
-sV parametresi versiyon taraması yapmasını

-pN parametresi makine kapalı bile görünse taramaya devam etmesini

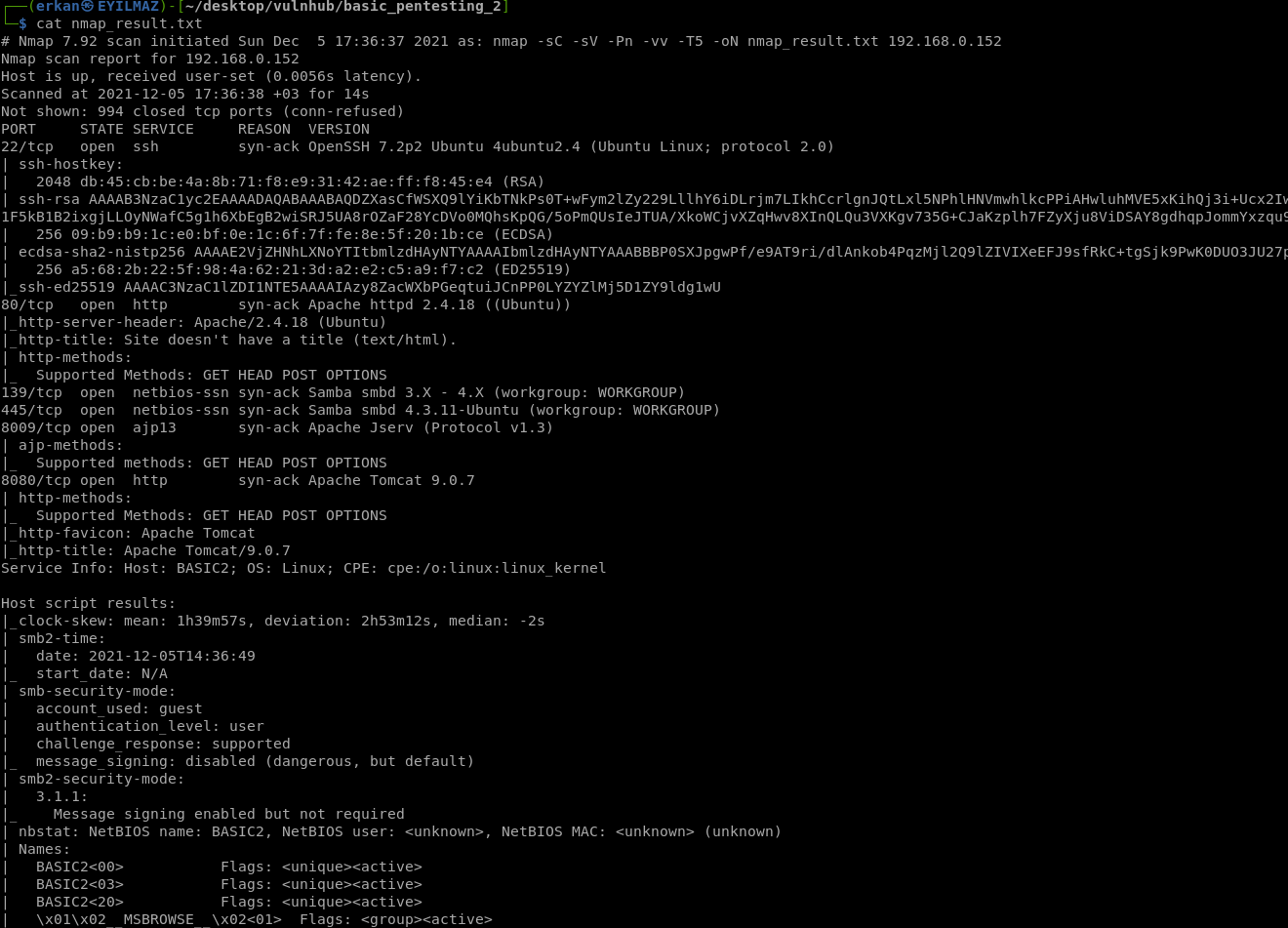
-vv parametresi olabildiğince işlem yapılırken bize bilgi vermesini

-T5 parametresi olabildiğince hızlı bir şekilde tarama yapmasını

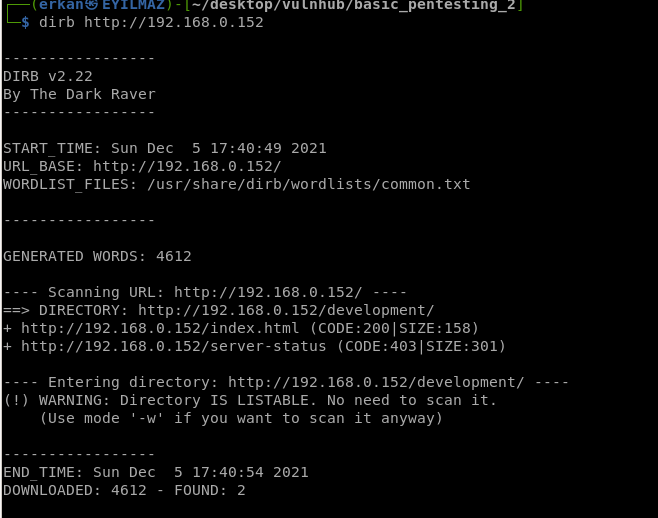
-oN parametresi ise çıktıyı normal formatta nmap\_result.txt’ye yazmasını sağlıyor.



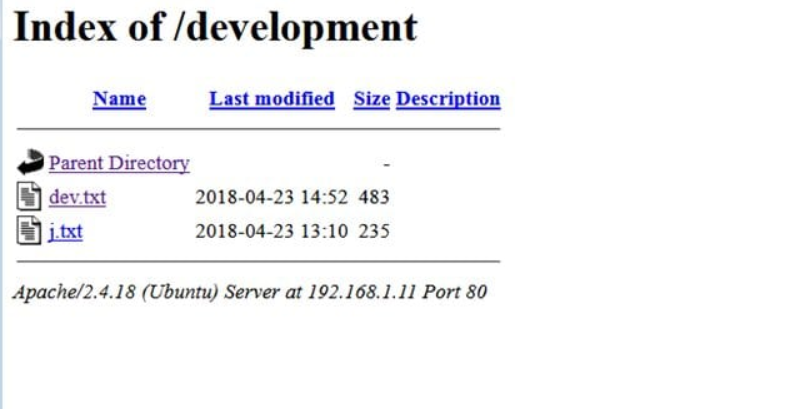
Çıktı dosyası aşağıdaki gibidir.



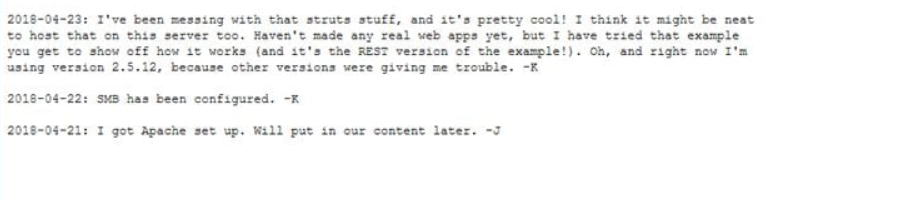
Burada bir web server açık olduğunu görünce web serverdaki directoryleri dirb kullanarak bulmaya çalışıyorum .



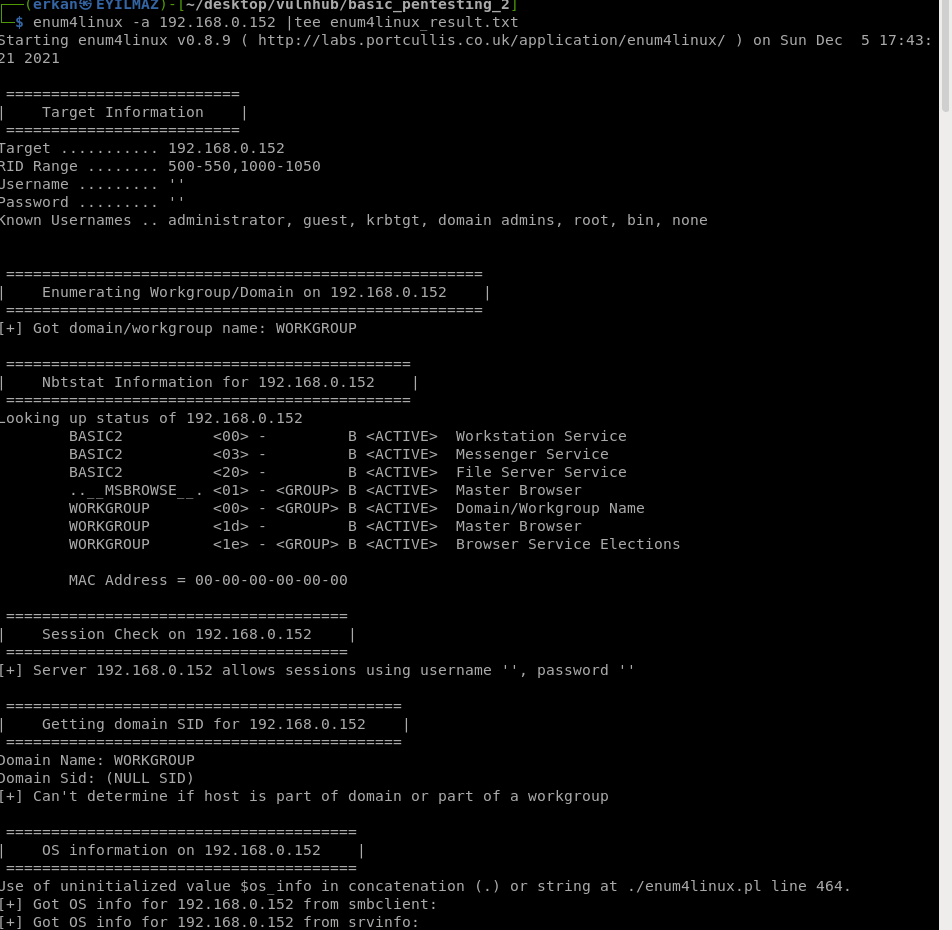
Burada teker teker bu adreslere gidip bilgi topluyorum.



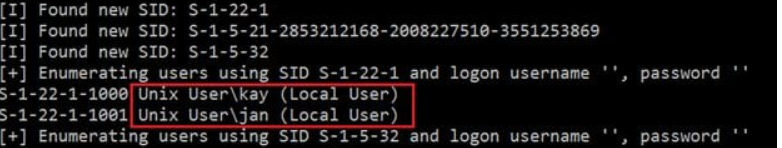
Burada da dev.txt dosyasının içeriğine bakıyorum.



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



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



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.



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

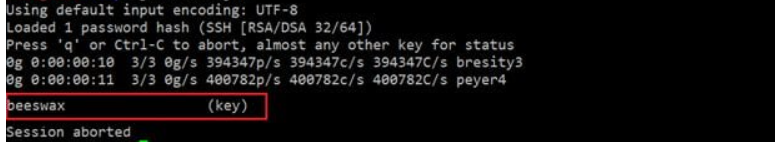
Olduğunu öğreniyorum .

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 .

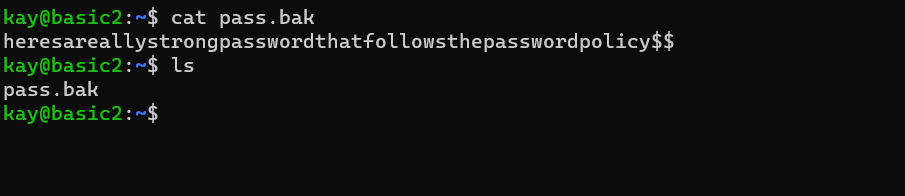
Sshtojohn ve john toolarını kullnarak kayın şifresini öğreniyoruz.



Ssh ile içeri girince cir dosyanın içinde

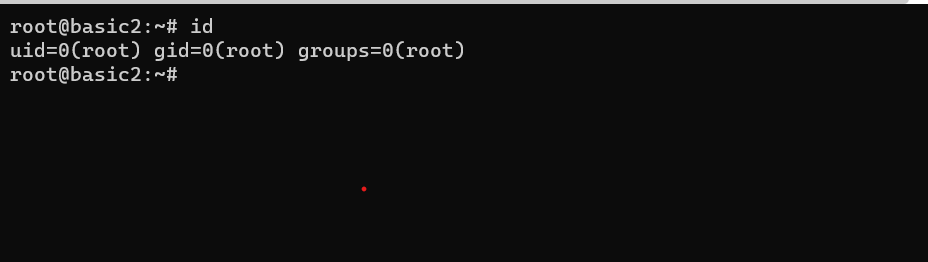
heresareallystrongpasswordthatfollowsthepasswordpolicy$$

Şifresini buluyoruz bu kayın şifresi



Sudo –i yapıyoruz ve root kullanıcısına geçiyoruz .

Id komutunu çalıştırıp kontrol ediyoruz.



Artık root’uz.

Okuduğunuz için teşşekürler.