

T.C.
SAKARYA ÜNİVERSİTESİ
BİLGİSAYAR VE BİLİŞİM BİLİMLERİ FAKÜLTESİ

BSM 471 AĞ GÜVENLİĞİ

PROJE/TASARIM RAPORU

PfSense Güvenlik Duvarı Tespit ve İzleme

B201210098 – İlknur KAYA
ilknur.kaya3@ogr.sakarya.edu.tr
B201210090 – Nurgül SERİN
nurgul.serin@ogr.sakarya.edu.tr

Bölüm : **BİLGİSAYAR MÜHENDİSLİĞİ**
Danışman : **Dr.Öğr.Üyesi MUSA BALTA**

2023-2024 Güz Dönemi

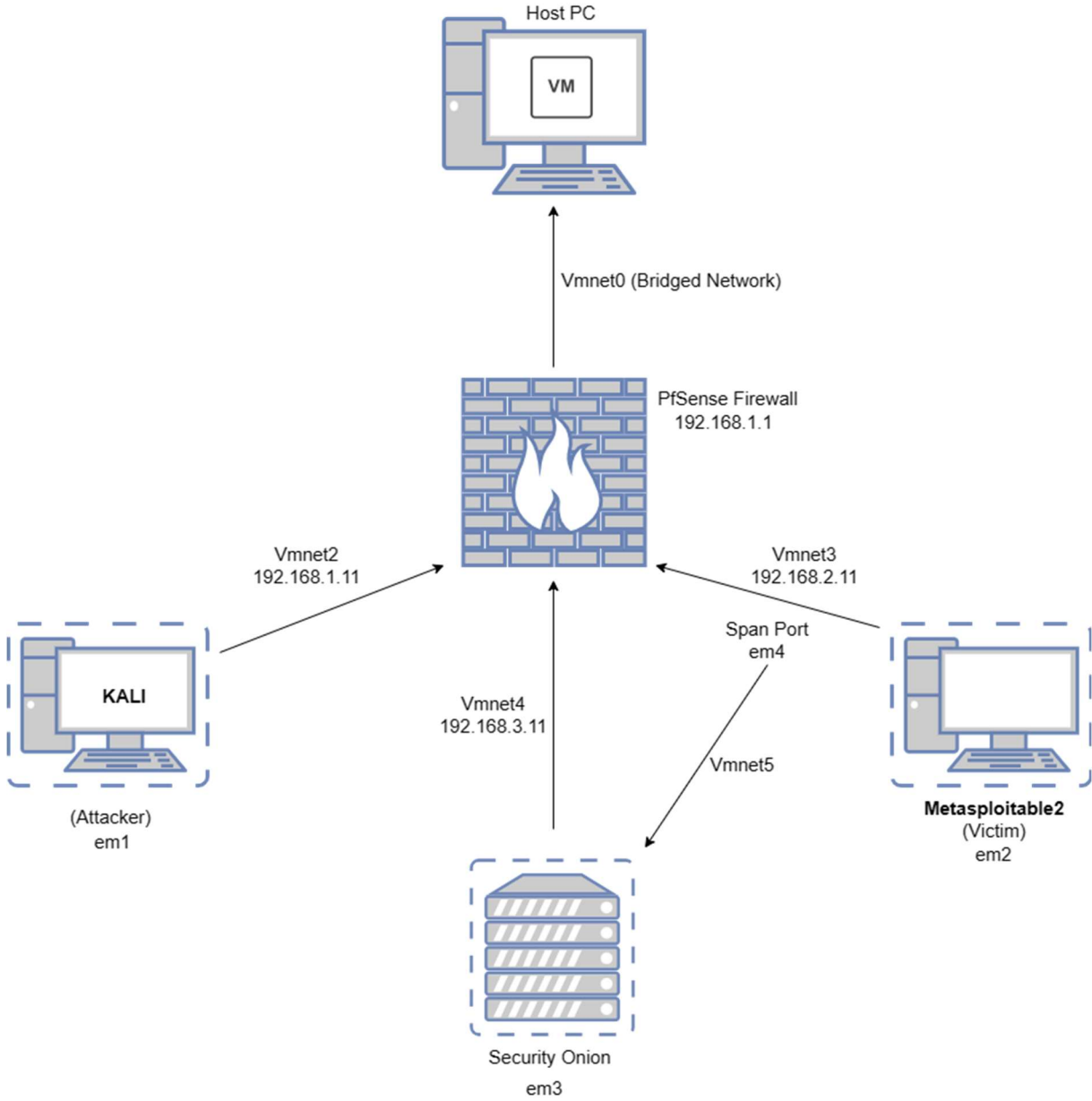
ÖZET

Anahtar kelimeler: PfSense, Kali, Metasploitable2, Security Onion, Ağ Topolojisi

Güvenlik duvarı bir ağın içine/dışına yönelik ya da ağın içindeki internet trafiğini denetleyip kısıtlamaya yarayan bir ağ güvenlik sistemidir. Böylece ağ üzerindeki tehditleri ya da güvenli bağlantıları ayırır ve güvenli olanlara izin verir. Bu proje için kullanılan güvenlik duvarı teknolojisi olan PfSense; FreeBSD tabanlı, ücretsiz, düşük sistem gereksinimlerine sahip, açık kaynak kodlara sahip olduğu için geliştirilmeye açıktır. Saldırgan Kali ve kurban Metasploitable2 arasındaki saldırı senaryolarını ve bunların engellenmesini VMware aracılığı ile kurulacak olan sanal makineler arası ağlar üzerinden gerçekleştirilecektir. Bu ağ içerisinde yer alan Security Onion ağ güvenliği izleme ve log kayıt yönetimini sağlayan Ubuntu tabanlı bir teknolojidir. Yapılacak olan saldırıları kurban ağı üzerinden izlenmesine olanak sağlayacaktır. Böylece mini siber güvenlik laboratuvarının oluşturulması amaçlanmıştır.

BÖLÜM 1. GİRİŞ

Projeye başlamadan önce kurulacak ağ topolojisi oluşturulmuştur. Daha sonrasında sırasıyla PfSense, Security Onion, Kali Linux ve Metasploitable2 kurulup yapılandırılması yapılmıştır. Projenin topolojisi aşağıdaki gibidir.

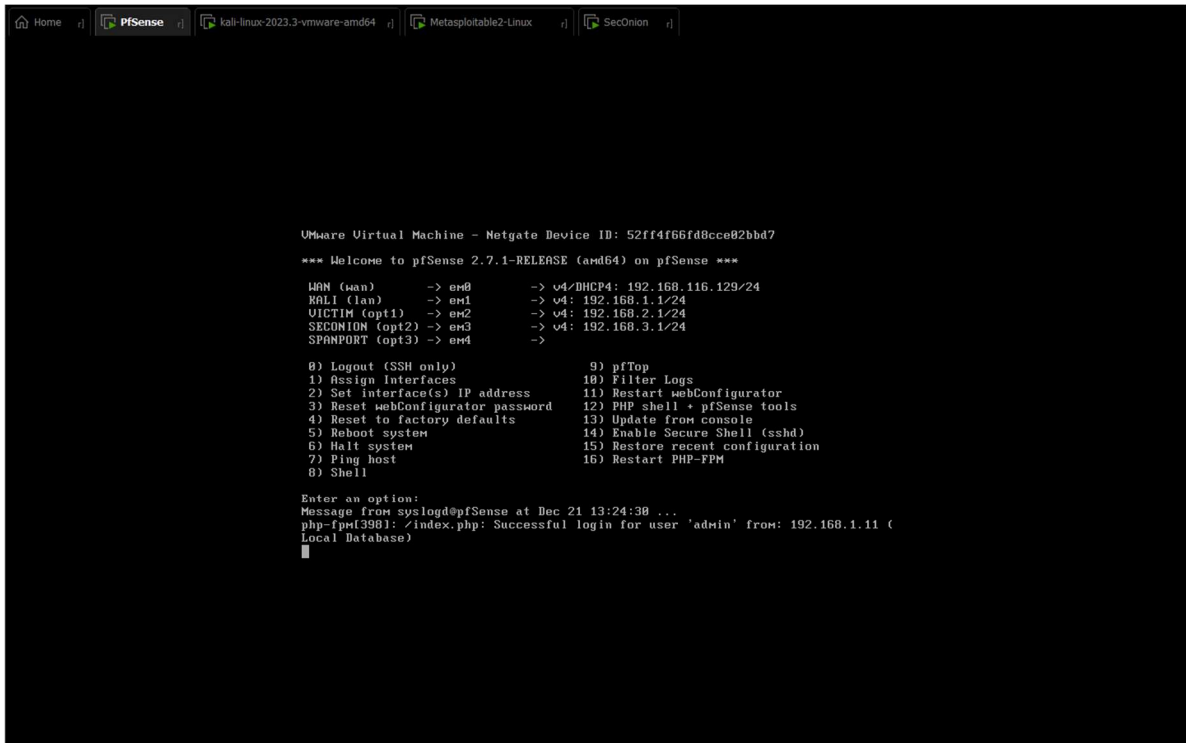


Güvenlik duvarı ağ topolojisi

BÖLÜM 2. KURULUM VE YAPILANDIRMA

2.1 PfSense

Öncelikle PfSense kurulumu için VMware network ayarlarından vmnet0 ı bridged ayarladık. Böylelikle ana bilgisayarın internetine köprü olacak ağ bağlantısı oluşturduk. Kurulumda 5 adet vmnet tanımladık. Arayüzlerimiz olan em0, em1, em2, em3 ve em4 ü sırasıyla oluşturduk. Oluşturulan arayüzlere IP ataması yaptık. Kali ve Metasploitable için DHCP yapılandırmasını açtık ve adres aralıklarını ayarladık. (örn: 192.168.1.11 – 192.168.1.200) Tek bi porta atama yapılmadı. Bu port Security Onion için olan SpanPort'tur. Kurban makinenin ağını takip eden port budur.



```

VMware Virtual Machine - Netgate Device ID: 52ff4f66fd8cce82bbd7
*** Welcome to pfSense 2.7.1-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.116.129/24
KALI (lan)     -> em1      -> v4: 192.168.1.1/24
VICTIM (opt1)  -> em2      -> v4: 192.168.2.1/24
SECURITYONION (opt2) -> em3      -> v4: 192.168.3.1/24
SPANPORT (opt3) -> em4      ->

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults    13) Update from console
5) Reboot system               14) Enable Secure Shell (ssh)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option:
Message from syslogd@pfSense at Dec 21 13:24:38 ...
php-fpm[398]: /index.php: Successful login for user 'admin' from: 192.168.1.11 (
Local Database)

```

PfSense Arayüzü

2.2 Security Onion

Bu projede en zorlayıcı yer Security Onion kurulumu oldu. Kaynak olarak çok fazla 2.3 versiyonları olmasına rağmen yeni versiyonları da ana bilgisayar için fazla büyük bir yapıydı. 6 Nisanda desteği kapatılacak olan 2.3.280 versiyonunu kullandık. Kurulum aşamasında bir adet NAT bağlantısı, vmnet4 ve vmnet5 kullandık. Kurulumda Evaluation modunda kurduk. Bu mod test amacıyla hızlı bir kurulum için tasarlanmış olmakla üretim kullanımı için tasarlanmamıştır. Projemiz için bu kadarı yeterli olacaktır.

2.3 Kali Linux

Kali makinemiz bizim hem saldırgan makinemiz hem de PfSense ve Security Onion için ağ arayüzlerini kullanacağımız makinemiz olacaktır. Bu yüzden kurulumda bir NAT ve vmnet2 tanımlanmıştır. NAT üzerinden gelen adresi Kali masaüstünden web erişimine izin vermek için Security Onion içinde Analyst rolü kısmına giriyoruz. 192.168.1.1 ile PfSense web arayüzünden güvenlik duvarı ayarlarımızı gerçekleştiriyoruz. Arayüzler kısmında LAN -> Kali, OPT1 -> Victim, OPT2 -> SecOnion ve OPT3 -> SpanPort olarak değiştiriyoruz. SpanPort arayüzünü etkin hale getiriyoruz. Böylece kurban ağını izleyecek olan Victim arayüzü ile SpanPort arasında köprü oluşturuyoruz. WAN üzerinden gelen bütün trafiğe izin veriyoruz ve ilk yapılandırmamızı bitiriyoruz.

2.4 Metasploitable

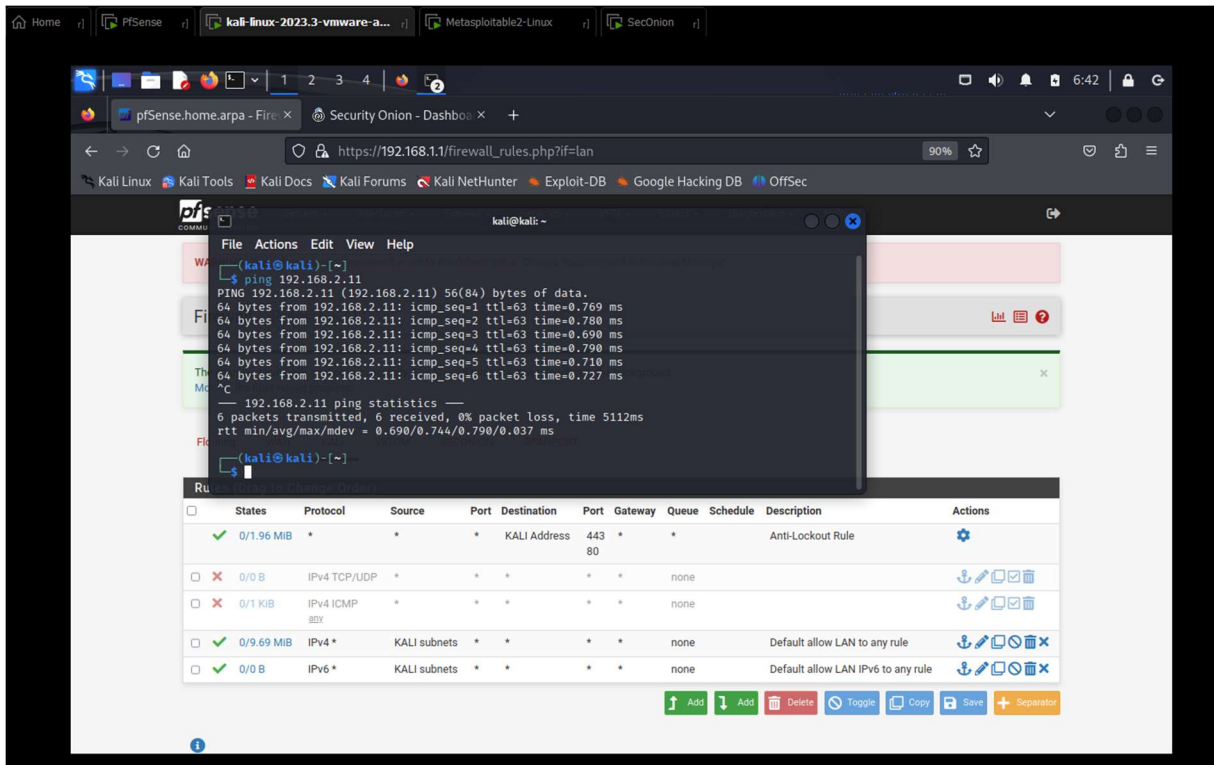
Bu kısımda kurban bilgisayar olduğu için yapacağımız herhangi bir özel değişiklik bulunmuyor. Sanal makinemizi kuruyoruz ve açıyoruz. Ifconfig ile adres kontrolü yapıyoruz ve 192.168.2.11 ile vmnet3'ü yakalıyoruz.

BÖLÜM 3. Saldırılar, Önlemler ve Çıktılar

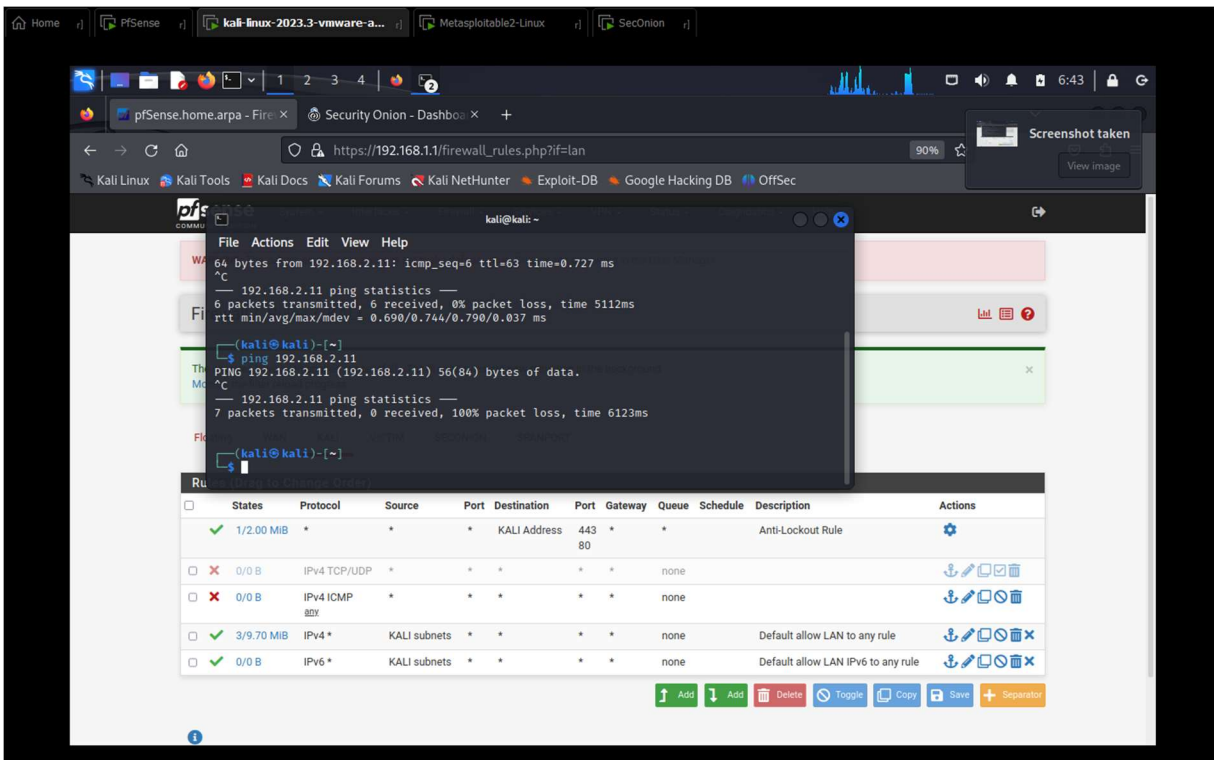
3.1 Ping ile Bağlantı Kontrolü

Ping, ICMP protokolü temelinde çalışan bir test komutudur. İletim hattının kontrolü için kullanılan ping paketleri ağ üzerinde bulunan aktif cihazların ulaşılabilir olup olmadığının tespitinde kullanılır. Hedef IP adresine ping komutu verildiğinde karşı tarafa ECHO_REQUEST istek paketi gönderilir. İstek kendine ulaşan hedef IP adresi kaynak noktasına ECHO_REPLY cevap paketini yollar. İki mesaj arasındaki süreye gecikme süresi denir.

Bu bağlamda kontrol için saldırgan Kali makinemiz üzerinden 192.168.2.11 IP adresine ping atılıp cevap alınmaktadır. Bağlantımızın yapıldığını anlamış bulunmaktayız. Güvenlik önlemi için ICMP izinlerini kapatırsak ping atamayacak konuma gelmemiz öngörülmüş ve gerçekleşmiştir.



ICMP bloklama kapalıyken hedef makineye ping atımı



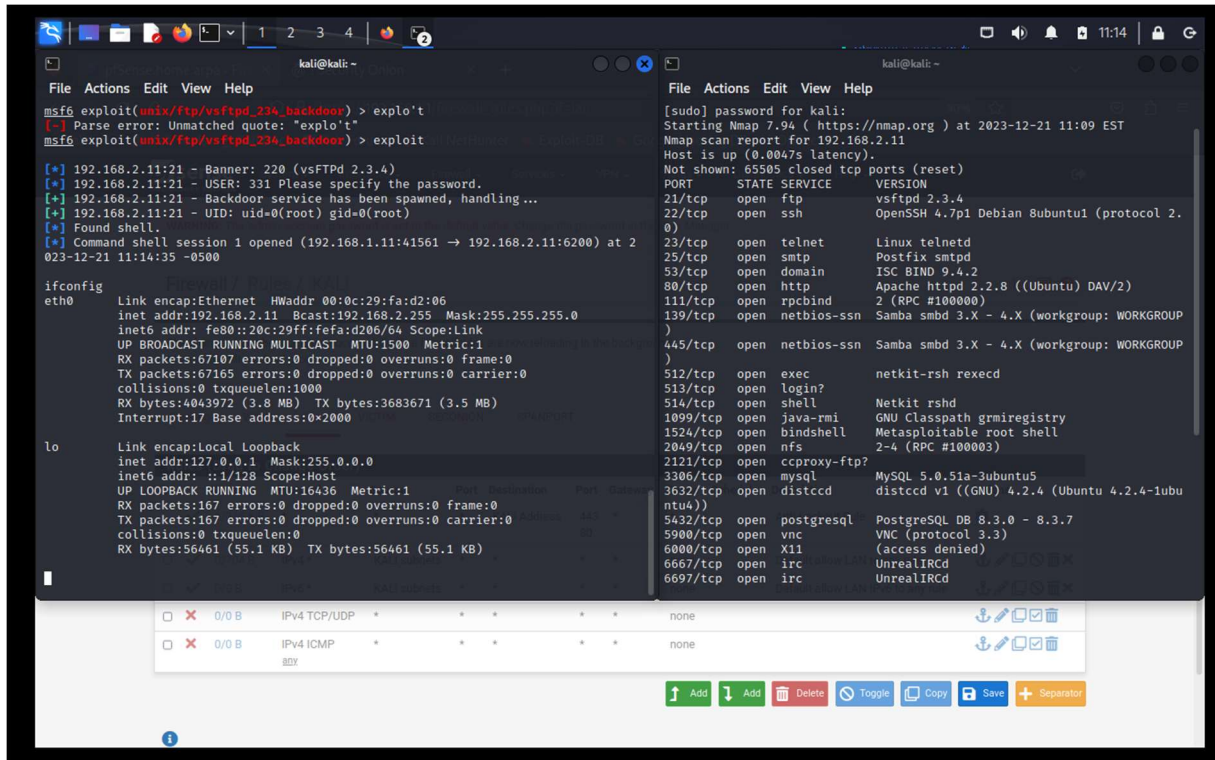
ICMP bloklama açıkken hedef makineye ping atımı

3.2 Metasploit 21/FTP Port Exploit

FTP (File Transfer Protokol) bir dosya aktarım protokolüdür. Bir dosya FTP kullanılarak başka bir TCP/IP ağı üzerindeki kullanıcıya aktarılabilir. Aktarım gereksinimleri için iletim denetimi protokolünü (TCP) kullanır. ICMP kısıtlaması yaptığımızda ağ üzerinden diğer bilgisayara ulaşamamıştık. Bu durumda FTP de çalışmayabilir ama bu engellenmiş demek değildir. Bu yüzden ayrı olarak güvenlik duvarı kuralını test ettik.

Bu saldırı için öncelikle kurbanın IP si ile açık bağlantı noktalarını taramak için nmap kullandık (sudo nmap -T4 -sV -p- 192.168.2.11) . Bunun sonucunda ilk sırada çıkan vsftpd için msfconsole da arama yaptık. Arama sonucunda çıkan arka kapı zaafiyetini RHOSTS ayarını yaptıktan sonra exploit dedik. Böylece kurban bilgisayar erişimimizi sağlamış olduk. Ifconfig ile test ettiğimiz kurban bilgisayarın IP adresini gördük.

Bu saldırı TCP kullandığı için TCP/UDP engellemesi yapmak istedik. Bunun sonucunda ilk başta nmap ile portlarımızı görüyorken görememeye başladık. Yine de portu bildiğimiz için denemek için msfconsole da tekrar denedik ama exploit ile yine de kurban bilgisayara sızamadık.



TCP/UDP bloklama kapalyken sızma testi

The screenshot shows a Kali Linux terminal with two windows. The left window is Metasploit (msf6) and the right window is a terminal running Nmap.

Metasploit (msf6) Window:

```

msf6 > search vsftpd 2.3.4
Matching Modules
#  Name
-  -
0  exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VS
FTP v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit
/unix/ftp/vsftpd_234_backdoor

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.2.11
RHOSTS => 192.168.2.11
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[-] 192.168.2.11:21 - Exploit failed [unreachable]: Rex::ConnectionTimeout The co
nnection with (192.168.2.11:21) timed out.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[-] 192.168.2.11:21 - Exploit failed [unreachable]: Rex::ConnectionTimeout The co
nnection with (192.168.2.11:21) timed out.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >

```

Terminal Window:

```

(kali@kali)-[~]
$ sudo nmap -T4 -sV -p- 192.168.2.11
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-21 11:15 EST

(kali@kali)-[~]
$ sudo nmap -T4 -sV -p- 192.168.2.11
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-21 11:26 EST
Stats: 0:09:43 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stea
lth Scan
SYN Stealth Scan Timing: About 44.26% done; ETC: 11:48 (0:12:15 remaini
ng)
Nmap scan report for 192.168.2.11
Host is up (0.00080s latency).
All 65535 scanned ports on 192.168.2.11 are in ignored states.
Not shown: 65535 filtered tcp ports (no-response)

Service detection performed. Please report any incorrect results at htt
ps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1318.11 seconds

```

At the bottom of the terminal window, there is a table with network-related information:

Protocol	Port	State	Reason	Service	
0/0 B	IPV4 ICMP	*	*	*	none
0/0 B	IPV4 TCP/UDP	*	*	*	none

TCP/UDP bloklama açıkken sızma testi

The screenshot shows the Security Onion dashboard with a list of network events. The dashboard has a dark theme and a sidebar with the Security Onion logo.

Time	Source IP	Destination IP	Port	Protocol	Event Description
2023-12-21 11:26:12.980 -05:00	192.168.2.11	192.168.1.11	41561	GPL ATTACK_RESPONSE	id check returned i
2023-12-21 11:12:31.358 -05:00	192.168.1.11	192.168.2.11	111	GPL RPC portmap listing	TCP 111
2023-12-21 11:12:31.255 -05:00	192.168.1.11	192.168.2.11	111	GPL RPC portmap listing	TCP 111
2023-12-21 11:12:31.205 -05:00	192.168.1.11	192.168.2.11	80	ET SCAN Possible Nmap User-Agent	Observ
2023-12-21 11:12:31.205 -05:00	192.168.1.11	192.168.2.11	80	ET SCAN Nmap Scripting Engine User-Agen	
2023-12-21 11:12:31.203 -05:00	192.168.1.11	192.168.2.11	111	GPL RPC portmap listing	TCP 111
2023-12-21 11:12:31.154 -05:00	192.168.1.11	192.168.2.11	8180	ET SCAN Possible Nmap User-Agent	Observ
2023-12-21 11:12:31.154 -05:00	192.168.1.11	192.168.2.11	8180	ET SCAN Nmap Scripting Engine User-Agen	
2023-12-21 11:12:31.153 -05:00	192.168.1.11	192.168.2.11	80	ET SCAN Possible Nmap User-Agent	Observ
2023-12-21 11:12:31.153 -05:00	192.168.1.11	192.168.2.11	80	ET SCAN Nmap Scripting Engine User-Agen	
2023-12-21 11:12:31.104 -05:00	192.168.1.11	192.168.2.11	8180	ET SCAN Possible Nmap User-Agent	Observ

Version: 2.3.280 © 2023 Security Onion Solutions, LLC Terms and Conditions

Sızma Testi Security Onion Dashboard Çıktısı

elastic Find apps, content, and more.

Dashboard Security Onion - Alerts

Full screen Share Clone Reset Edit

event.dataset: alert

Last 24 hours

Low & Medium Severity High & Critical Severity

		@timestamp	source.ip	source.port	destination.ip	destination.port	log.offset	network.community_id	_type
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Dec 21, 2023 @ 11:26:12.980	192.168.2.11	6280	192.168.1.11	41561	721983538994374	1:uiJFcyLx15NpQoEgZ7W94v1JItc=	Hunt and optionally pivot to PCAP/Cases
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Dec 21, 2023 @ 11:17:51.778	-	-	-	-	-	-	Hunt and optionally pivot to PCAP/Cases
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Dec 21, 2023 @ 11:12:31.358	192.168.1.11	617	192.168.2.11	111	1056340293130719	1:v9/WjMTba14IVdazZyLVhdc++9I=	Hunt and optionally pivot to PCAP/Cases
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Dec 21, 2023 @ 11:12:31.255	192.168.1.11	617	192.168.2.11	111	1056340293130719	1:v9/WjMTba14IVdazZyLVhdc++9I=	Hunt and optionally pivot to PCAP/Cases
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Dec 21, 2023 @ 11:12:31.205	192.168.1.11	60558	192.168.2.11	80	1531494672585770	1:Zazskb4VnPgEEDBv066XWlR/tdg=	Hunt and optionally pivot to PCAP/Cases
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Dec 21, 2023 @ 11:12:31.205	192.168.1.11	60558	192.168.2.11	80	1531494672585770	1:Zazskb4VnPgEEDBv066XWlR/tdg=	Hunt and optionally pivot to PCAP/Cases
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Dec 21, 2023 @ 11:12:31.203	192.168.1.11	911	192.168.2.11	111	1017807994076591	1://AoUsS2SaA4QX//BWkxILs1HKCE=	Hunt and optionally pivot to PCAP/Cases

Sızma Testi Elastic (Kibana) Dashboard Çıktısı

BÖLÜM 4. KAYNAKÇA

1. <https://docs.securityunion.net/en/2.3/>
2. <https://docs.netgate.com/pfsense/en/latest/>
3. <https://medium.com/@brgil/ftp-backdoor-command-execution-9a95973c02a3>