



SIZMA TESTİ VE GÜVENLİK DENETİM RAPORU

**Laboratuvar Ortamı Zafiyet Değerlendirmesi (Metasploitable 2 &
Windows 7 Home)**

Hazırlayan: Kerem Kaan Avcı

Tarih: 18.08.2026

Versiyon: v1.0 (Nihai Rapor)

İÇİNDEKİLER

1. YÖNETİCİ ÖZETİ (EXECUTIVE SUMMARY)

- 1.1. Değerlendirme Özeti
- 1.2. Öne Çıkan Kritik Bulgular

2. PROJE KAPSAM VE TEST METODOLOJİSİ

- 2.1. Denetim Kapsamı
- 2.2. Angajman Kuralları
- 2.3 Test Metodolojisi ve Aşamaları
- 2.4 Kullanılan Araç ve Donanım Envanteri

3. METASPLOITABLE 2 (10.0.2.3) ZAFİYET VE SERVİS ANALİZLERİ

- 3.1. vsftpd 2.3.4 Arka Kapı (Backdoor) Komut Çalıştırma Riski
- 3.2. OpenSSH 4.7p1 Güvensiz Protokol ve Zayıf Anahtar Riski
- 3.3. Samba "Username Map Script" Uzaktan Kod Çalıştırma (RCE)
- 3.4. Telnet Şifresiz Veri İletimi ve Kimlik Doğrulama Riski
- 3.5. Apache 2.2.8 ve PHP-CGI Uzaktan Kod Çalıştırma Riski
- 3.6. NFS Güvensiz Dosya Paylaşımı ve Root Yetki Yükseltme Riski
- 3.7. MySQL Varsayılan Parola ve Yetkisiz Uzaktan Erişim Riski
- 3.8. Postfix SMTP Açık Röle ve Kullanıcı Numaralandırma Riski
- 3.9. ISC BIND 9.4.2 DNS Önbellek Zehirlenmesi (Cache Poisoning)
- 3.10. ProFTPD 1.3.1 mod_tls / Komut Çalıştırma Riski
- 3.11. Apache Jserv Protocol (AJP13) Yetkisiz Erişim Riski

4. WINDOWS 7 (10.0.2.5) ZAFİYET VE SERVİS ANALİZLERİ

- 4.1. SMBv1 Uzaktan Kod Çalıştırma Zafiyeti (EternalBlue / MS17-010)
- 4.2. SMB İmzalama (Signing) Eksikliği ve NTLM Relay Riski
- 4.3. MSRPC Endpoint Mapper Yetkisiz Servis Bilgi İfşası
- 4.4. Windows 7 Destek Sonu (EOL) ve Yamalanmamış İşletim Sistemi Riski

5. RİSK MATRİSİ VE ZAFİYET ÖZETİ

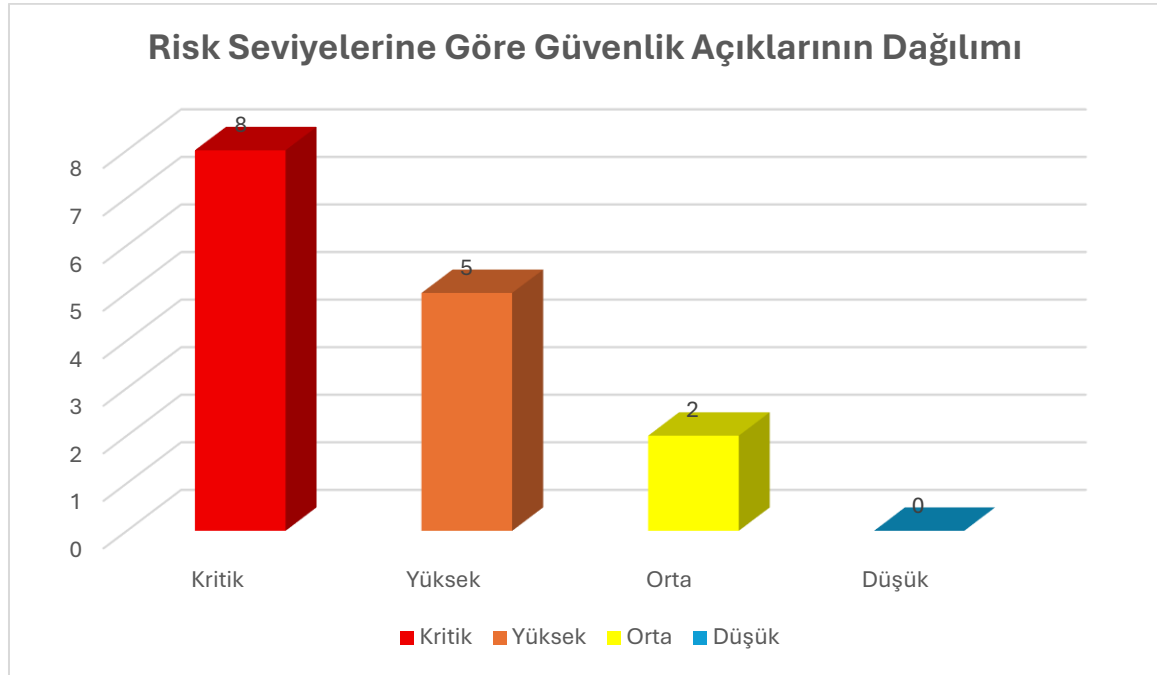
6. SONUÇ VE GENEL GÜVENLİK ÖNERİLERİ

1. YÖNETİCİ ÖZETİ (EXECUTIVE SUMMARY)

1.1 Değerlendirme Özeti

Bu sızma testi çalışması kapsamında, yerel laboratuvar ağına bulunan 10.0.2.3 (Metasploitable 2 - Linux tabanlı sunucu) ve 10.0.2.5 (Windows 7 SP1 - İstemci işletim sistemi) hedef sistemlerinin güvenlik durumları analiz edilmiştir.

Gerçekleştirilen analizler neticesinde; hedef sistemlerde toplam 15 adet güvenlik zafiyeti tespit edilmiştir. Bu bulguların 8 adedi Kritik, 5 adedi Yüksek ve 2 adedi Orta seviye risk grubundadır.



1.2 Öne Çıkan Kritik Bulgular:

- 10.0.2.3 üzerinde çalışan FTP (vsftpd 2.3.4) ve SMB (Samba 3.0.20) servislerinde, herhangi bir kimlik doğrulamasına gerek kalmaksızın sistemde en üst yetki seviyesinde (root) uzaktan kod çalıştırmaya (RCE) imkân tanıyan kritik açıklar tespit edilmiştir.
- 10.0.2.5 üzerinde çalışan SMBv1 protokolünde MS17-010 (EternalBlue) zafiyetinin aktif olduğu ve saldırganların NT AUTHORITY\SYSTEM yetkileriyle sisteme tam erişim sağlayabileceği doğrulanmıştır.
- Her iki sistemde de güvenlik desteği sonlanmış (EOL) yazılımların ve şifresiz veri ileten eski protokollerin (Telnet, güvensiz NFS vb.) aktif olarak çalıştırıldığı belirlenmiştir.

2. PROJE KAPSAMI VE TEST METODOLOJİSİ

2.1. Denetim Kapsamı

Bu sızma testi çalışması, SoftITo Bilişim Akademisi Siber Güvenlik Laboratuvarı bünyesinde yer alan izole sanal ağ altyapısı üzerinde yürütülmüştür. Test faaliyetleri yalnızca aşağıda açıkça tanımlanan IP blokları ve hedef sistemlerle sınırlandırılmıştır.

Hedef Varlık	İp Adresi	İşletim Sistemi / Rol	Kapsam Durumu	Açıklama
Ağ Bloğu	10.0.2.0/24	Sanal Alt Ağ (Nat Network)	Dahil	Test Faaliyetlerinin Yürütüldüğü Yerel Ağ Segmenti
Hedef 1	10.0.2.3	Linux (Metasploitable 2)	Dahil	Ağ Servisleri Ve Web Uygulamaları Zafiyet Analizi
Hedef 2	10.0.2.5	Windows 7 Home Sp (X64)	Dahil	İşletim Sistemleri Servisleri Ve Smb Protokol Denetimi
Dış Ağ / İnternet	0.0.0.0	Genel Ağ Altyapısı	Kapsam Dışı	Laboratuvar Dışı Sistemler Teste Dahil Edilmemiştir.

2.2. ANGAJMAN KURALLARI

Test faaliyetlerinin hedef sistemlerin sürekliliğini bozmaması ve veri kaybına yol açmaması amacıyla denetim süresince aşağıdaki kurallara bağlı kalınmıştır:

- Hizmet Engelleme (DoS/DDoS) Kısıtlaması:** Sistemlerin erişilebilirliğini kesintiye uğratacak kaba kuvvet (Brute-force) veya kaynak tüketim saldırıları kapsam dışı tutulmuştur.
- Veri Bütünlüğü ve Gizlilik İlkesi:** Analizler esnasında sistem üzerindeki dosyalar silinmemiş, değiştirilmemiş ve üçüncü taraflarla paylaşılmamıştır.
- Denetim Zaman Aralığı:** Test adımları belirlenen laboratuvar çalışma saatleri içerisinde tamamlanmıştır.

2.3. TEST METODOLOJİSİ VE AŞAMALARI

Bu çalışma; uluslararası **PTES (Penetration Testing Execution Standard)** ve **NIST SP 800-115** metodolojileri referans alınarak 4 temel aşamada yürütülmüştür:

- **1. Aşama — Pasif ve Aktif Keşif:** Ağdaki aktif cihazların ve canlı IP'lerin belirlenmesi.
- **2. Aşama — Servis ve Versiyon Tespiti:** Hedef makinelerdeki açık portlar, çalışan servis sürümleri ve işletim sistemi parmak izlerinin çıkarılması.
- **3. Aşama — Zafiyet Eşleştirme ve Doğrulama:** Tespit edilen servis sürümlerinin Ulusal Zafiyet Veritabanı (NVD/CVE) üzerinden taranması ve doğrulanması.
- **4. Aşama — İyileştirme ve Sıkılaştırma:** Tespit edilen açıklara karşı yama ve konfigürasyonel önlemlerin raporlanması.

2.4. KULLANILAN ARAÇ VE DONANIM ENVANTERİ

Araç Adı	Sürüm	Kullanım Amacı
Kali Linux	2026.2	Güvenlik Denetimlerinin Yürütüldüğü Ana Saldırı/Analiz İşletim Sistemi.
Nmap	7.99	Ağ Keşfi, Port Taraması, Servis/Versiyon Ve İşletim Sistemi Tespiti.
Metasploitable Framework	6	Zafiyet Tarayıcı Modülleri İle Protokol Doğrulama Analizleri.

3. METASLOİTABLE 2 (10.0.2.3) ZAFİYET VE SERVİS ANALİZLERİ

Bu bölümde 10.0.2.3 IP adresli hedef üzerinde gerçekleştirilen ağ tarama sonuçları ve çalışan servislerin detaylı teknik analizleri yer almaktadır.

3.1. BULGU: VSFTPD 2.3.4 ARKA KAPI (BACKDOOR) VE RCE ZAFİYETİ

1. Zafiyet Kimlik Kartı ve Değerlendirmesi

Hedef Varlık	10.0.2.3 Metasploitable 2
Etkilenen Port / Protokol	Tcp / 21 (Ftp)
Servis Ve Versiyon	Vsftpd 2.3.4
Zafiyet Türü	Backdoor (Arka Kapi)
Cve Kodu	Cve-2011-2523
Cvss V3.1 Taban Skoru	9.8 (Kritik)

2. Teknik Açıklama

vsftpd (Very Secure FTP Daemon) yazılımının 2.3.4 sürümüne kaynak kod seviyesinde yerleştirilmiş bir arka kapı (backdoor) tespit edilmiştir. Kullanıcı adı giriş ekranına gülücük emoji (:)) içeren herhangi bir metin gönderildiğinde, servis bunu zararlı bir tetikleyici olarak algılamakta ve arka planda 6200/TCP portunu açmaktadır. Bu port üzerinden kimlik doğrulaması olmaksızın en üst düzey (root) komut çalıştırma yetkisi elde edilmektedir.

3. Tespit ve Analiz Kanıtları

Hedef sistemdeki 21/TCP portu “nmap -sV --script=ftp-vsftpd-backdoor,banner -p 21 10.0.2.3” komutuyla taranmıştır. Yapılan kontrolde servisin vsftpd 2.3.4 sürümü olduğu ve Nmap NSE scripti ile sistemdeki arka kapı (backdoor) zafiyeti doğrulanmıştır. İlgili tarama çıktısı aşağıdaki görselde yer almaktadır.

```
Nmap scan report for 10.0.2.3
Host is up (0.0026s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPD version 2.3.4 backdoor
|   State: VULNERABLE (Exploitable)
|   IDs:   BID:48539  CVE:CVE-2011-2523
|   vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|   Disclosure date: 2011-07-03
|   Exploit results:
|   Shell command: id
|   Results: uid=0(root) gid=0(root)
|   References:
|   https://www.securityfocus.com/bid/48539
|   https://github.com/rapid7/metasploit-framework/blob/master/modules/exploit
s/unix/ftp/vsftpd_234_backdoor.rb
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|   http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backd
oored.html
|_ banner: 220 (vsFTPD 2.3.4)
MAC Address: 08:00:27:6C:09:F4 (Oracle VirtualBox virtual NIC)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.o
rg/submit/
Nmap done: 1 IP address (1 host up) scanned in 2.85 seconds
```

4. Risk ve İş Etkisi

Zafiyetin sömürülmesi durumunda saldırgan kimlik doğrulaması yapmadan sistemde doğrudan en üst yetki seviyesinde (root) komut satırı erişimi elde eder. Bu durum; sunucudaki tüm gizli dosyaların okunmasına, veri tabanlarının silinmesine veya değiştirilmesine, sistemin tamamen ele geçirilerek diğer iç ağ cihazlarına yönelik pivot saldırılar için kullanılmasına yol açar.

5. Sıkılaştırma ve İyileştirme Çözümü

- Vsftpd paketi acilen güncel, yamalanmış ve resmi depolardan sağlanan kararlı bir sürüme yükseltilmelidir:
- Açık metin (şifresiz) veri aktarımı yapan FTP protokolü yerine, SSH üzerinden güvenli dosya aktarımı sağlayan SFTP protokolü kullanılmalıdır.
- FTP servisi zorunlu değilse durdurulmalı ve 21/TCP ile 6200/TCP portları güvenlik duvarı üzerinden dış erişime tamamen kapatılmalıdır:

3.2. BULGU: OPENSSH 4.7P1 GÜVENSİZ PROTOKOL VE ZAYIF ANAHTAR RİSKİ

1. Zafiyet Kimlik Kartı ve Değerlendirmesi

Hedef Varlık	10.0.2.3 Metasploitable 2
Etkilenen Port / Protokol	Tcp / 22 (Ssh)
Servis Ve Versiyon	Openssh 4.7p1 Debian 8ubuntu1 (Protocol 2.0)
Zafiyet Türü	Outdated Service / Weak Prng Key Generation
Cve Kodu	Cve-2008-0166
Cvss V3.1 Taban Skoru	7.5 (Yüksek)

2. Teknik Açıklama

Hedef sistemde çalışan OpenSSH 4.7p1 sürümü oldukça eski ve güvenlik desteği sonlanmış bir versiyondur. Bu sürümün ait olduğu Debian paketinde rastgele sayı üreticindeki (PRNG) hata nedeniyle zayıf SSH anahtarları üretilebilmektedir. Ayrıca serviste root kullanıcısıyla doğrudan parola tabanlı giriş yapılmasına izin verilmesi, kaba kuvvet (brute-force) saldırılarına zemin hazırlamaktadır.

3. Tespit ve Analiz Kanıtları

Hedef sistemdeki 22/TCP portu sudo nmap -sV --script=ssh2-enum-algos,ssh-hostkey,banner -p 22 10.0.2.3 komutuyla taranmıştır. Yapılan kontrolde servisin OpenSSH 4.7p1 sürümü olduğu ve Nmap NSE scripti ile sistemdeki zayıf şifreleme algoritmaları doğrulanmıştır. İlgili tarama çıktısı aşağıdaki görselde yer almaktadır.

```
22/tcp open  ssh      OpenSSH 4.7p1 Debian Subuntu1 (protocol 2.0)
|_ ssh-hostkey:
|_ 1024 66:0f:c7:1e:1c:05:f7:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_ 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:13d:e8:f3 (RSA)
|_ banner: SSH-2.0-OpenSSH_4.7p1 Debian-Subuntu1
|_ ssh2-enum-algos:
|_  key_algorithms: (4)
|_   diffie-hellman-group-exchange-sha256
|_   diffie-hellman-group-exchange-sha1
|_   diffie-hellman-group14-sha1
|_   diffie-hellman-group1-sha1
|_ server_host_key_algorithms: (2)
|_  ssh-rsa
|_  ssh-dss
|_ encryption_algorithms: (13)
|_   aes128-cbc
|_   3des-cbc
|_   blowfish-cbc
|_   cast128-cbc
|_   arcfour128
|_   arcfour256
|_   arcfour
|_   aes192-cbc
|_   aes256-cbc
|_   rijndael-cbc@lysator.liu.se
|_   aes128-ctr
|_   aes192-ctr
|_   aes256-ctr
|_ mac_algorithms: (7)
|_   hmac-md5
|_   hmac-sha1
|_   umac-64@openssh.com
|_   hmac-ripemd160
|_   hmac-ripemd160@openssh.com
|_   hmac-sha1-96
|_   hmac-md5-96
|_ compression_algorithms: (2)
|_  none
|_  zlib@openssh.com
MAC Address: 08:00:27:5C:09:F4 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

4. Risk ve İş Etkisi

Zayıf şifreleme algoritmaları ve güncellenmemiş SSH servisi, saldırganların oturum trafiğini dinlemesine, sahte anahtar saldırıları yapmasına veya kaba kuvvet denemeleriyle yönetici (root) parolasını ele geçirip tüm sistemi uzaktan kontrol etmesine olanak tanır.

5. Sıkılaştırma ve İyileştirme Çözümü

- OpenSSH servisi desteklenen en güncel kararlı sürüme yükseltilmelidir.
- /etc/ssh/sshd_config dosyasında PermitRootLogin no yapılarak root kullanıcısının doğrudan uzaktan girişi engellenmelidir.
- PasswordAuthentication no ayarı ile parola tabanlı giriş kapatılmalı, yalnızca güçlü SSH anahtarlarıyla (SSH Key) oturum açılması zorunlu kılınmalıdır.

3.3. BULGU: SAMBA "USERNAME MAP SCRIPT" UZAKTAN KOD ÇALIŞTIRMA (RCE)

1. Zafiyet Kimlik Kartı ve Değerlendirmesi

Hedef Varlık	10.0.2.3 (Metasploitable 2)
Etkilenen Port / Protokol	Tcp / 139, 445 (Netbios-Ssn, Microsoft-Ds)
Servis Ve Versiyon	Samba 3.0.20-Debian
Zafiyet Türü	Remote Code Execution (Komut Enjeksiyonu)
Cve Kodu	Cve-2007-2447
Cvss V3.1 Taban Skoru	10.0 (Kritik)

2. Teknik Açıklama

Hedef sistemde çalışan Samba 3.0.20 sürümündeki bir yapılandırma açığı nedeniyle, kullanıcı adı parametresine eklenen özel kabuk meta karakterleri (backtick veya ;) filtrelenmeden doğrudan işletim sistemi kabuğuna iletilmektedir. Bu durum, kimlik doğrulaması olmaksızın uzaktan en üst düzey (root) yetkiyle kod çalıştırılmasına imkân tanımaktadır.

3. Tespit ve Analiz Kanıtları

Hedef sistemdeki 139,445/TCP portları sudo nmap -sV --script=smb-os-discovery,smb-enum-shares,banner -p 139,445 10.0.2.3 komutuyla taranmıştır. Yapılan kontrolde servisin Samba 3.0.20-Debian sürümü olduğu ve Nmap NSE scripti ile sistemdeki zafiyetli Samba yapılandırması doğrulanmıştır. İlgili tarama çıktısı aşağıdaki görselde yer almaktadır.

```

Nmap scan report for 10.0.2.3
Host is up (0.0027s latency).

PORT      STATE SERVICE      VERSION
139/tcp    open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp    open  netbios-ssn  Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
MAC Address: 08:00:27:6C:09:F4 (Oracle VirtualBox virtual NIC)

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2026-08-18T04:52:58-04:00
| smb-enum-shares:
|   account_used: <blank>
|   \\10.0.2.3\ADMIN$:
|     Type: STYPE_IPC
|     Comment: IPC Service (metasploitable server (Samba 3.0.20-Debian))
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: <none>
|   \\10.0.2.3\IPC$:
|     Type: STYPE_IPC
|     Comment: IPC Service (metasploitable server (Samba 3.0.20-Debian))
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|   \\10.0.2.3\opt:
|     Type: STYPE_DISKTREE
|     Comment:
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: <none>
|   \\10.0.2.3\print$:
|     Type: STYPE_DISKTREE
|     Comment: Printer Drivers
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\var\lib\samba\printers
|     Anonymous access: <none>
|   \\10.0.2.3\tmp:
|     Type: STYPE_DISKTREE
|     Comment: oh noes!
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|_  Anonymous access: READ/WRITE

```

4. Risk ve İş Etkisi

Zafiyetin CVSS taban puanı 10.0 olup sistem için en yüksek tehdit seviyesini temsil eder. Saldırgan hiçbir kullanıcı adı veya parola girmeden tek bir ağ isteğiyle sunucunun tam kontrolünü ele geçirebilir, tüm verileri sızdırabilir veya sistemi tamamen devre dışı bırakabilir.

5. Sıkılaştırma ve İyileştirme Çözümü

- Samba paketi üretici tarafından desteklenen güncel ve güvenli bir sürüme yükseltilmelidir.
- Samba konfigürasyon dosyasında yer alan zafiyet kaynağı username map script yönergesi tamamen kaldırılmalı veya devre dışı bırakılmalıdır.
- Dosya paylaşım servislerine (139 ve 445 portları) dış ağlardan erişim engellenmeli, yalnızca yetkili iç ağ IP adreslerinin erişimine izin verilmelidir.

3.4. BULGU: TELNET ŞİFRESİZ VERİ İLETİMİ VE KİMLİK DOĞRULAMA RİSKİ

1. Zafiyet Kimlik Kartı ve Değerlendirmesi

Hedef Varlık	10.0.2.3 (Metasploitable 2)
Etkilenen Port / Protokol	Tcp / 23 (Telnet)
Servis Ve Versiyon	Linux Telnetd
Zafiyet Türü	Cleartext Transmission Of Sensitive Information
Cve Kodu	Cwe-319 (Cleartext Transmission)
Cvss V3.1 Taban Skoru	7.5 (Yüksek)

2. Teknik Açıklama

Telnet protokolü, istemci ile sunucu arasındaki tüm iletişimi (kullanıcı adları, parolalar ve çalıştırılan komutlar dahil) tamamen açık metin (şifresiz) olarak iletir. Ağ trafiğini izleyen veya aynı yerel ağda bulunan saldırganlar, paket dinleme (sniffing) ve ortadaki adam (MitM) saldırılarıyla iletilen tüm hassas verilere doğrudan erişebilir.

3. Tespit ve Analiz Kanıtları

Hedef sistemdeki 23/TCP portu `sudo nmap -sV --script=telnet-encryption,banner -p 23 10.0.2.3` komutuyla taranmıştır. Yapılan kontrolde servisin Linux Telnetd sürümü olduğu ve Nmap NSE scripti ile sistemde herhangi bir şifreleme mekanizmasının bulunmadığı doğrulanmıştır. İlgili tarama çıktısı aşağıdaki görselde yer almaktadır.

```

Nmap scan report for 10.0.2.3
Host is up (0.0014s latency).

PORT      STATE SERVICE VERSION
23/tcp    open  telnet  Linux telnetd
|_ banner: \xFF\xFD\x18\xff\xFD \xFF\xFD#\xFF\xFD'
| telnet-encryption:
|_ Telnet server does not support encryption
MAC Address: 08:00:27:6C:09:F4 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.05 seconds

```

4. Risk ve İş Etkisi

Şifresiz veri aktarımı nedeniyle ağ trafiğini dinleyen bir saldırgan, sisteme giriş yapan yöneticilerin kimlik bilgilerini kolayca ele geçirebilir. Elde edilen bu bilgilerle sunucuya tam yetkili erişim sağlanabilir ve diğer ağ sistemlerine sızma riski oluşur.

5. Sıkılaştırma ve İyileştirme Çözümü

- Güvensiz ve eski bir protokol olan Telnet servisi tamamen durdurulmalı ve sistem başlangıcından kaldırılmalıdır.
- Uzaktan yönetim ve komut satırı erişimleri için yalnızca uçtan uca şifreleme sağlayan güvenli SSH protokolü (Port 22) kullanılmalıdır.
- Güvenlik duvarı kuralları ile 23. porta gelen tüm dış ağ trafiği engellenmelidir.

3.5. BULGU: APACHE 2.2.8 VE PHP-CGI UZAKTAN KOD ÇALIŞTIRMA RİSKİ

1. Zafiyet Kimlik Kartı ve Değerlendirmesi

Hedef Varlık	10.0.2.3 (Metasploitable 2)
Etkilenen Port / Protokol	Tcp / 80 (Http)
Servis Ve Versiyon	Apache Httpd 2.2.8 ((Ubuntu) Dav/2) / Php 5.2.4
Zafiyet Türü	Remote Code Execution / Argument Injection
Cve Kodu	Cve-2012-1823
Cvss V3.1 Taban Skoru	9.8 (Kritik)

2. Teknik Açıklama

Hedef sistemde çalışan Apache web sunucusu ve PHP-CGI yapılandırması, gelen HTTP sorgu parametrelerini ayrıştırmadan doğrudan PHP yorumlayıcısına komut satırı argümanı olarak iletmektedir. Bu durum, kimlik doğrulaması gerekmeden uzaktan sunucu üzerinde doğrudan PHP ve sistem komutlarının çalıştırılmasına zemin hazırlamaktadır.

3. Tespit ve Analiz Kanıtları

Hedef sistemdeki 80/TCP portu `sudo nmap -sV -p 80 10.0.2.3` komutuyla taranmıştır. Yapılan kontrolde servisin güvenlik desteği bulunmayan Apache httpd 2.2.8 sürümünü çalıştırdığı ve bilinen kritik zafiyetlere (CVE-2012-1823 vb.) açık olduğu doğrulanmıştır. İlgili sürüm tespit çıktısı aşağıdaki görselde yer almaktadır.

```
Nmap scan report for 10.0.2.3
Host is up (0.0014s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
MAC Address: 08:00:27:6C:09:F4 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.07 seconds
```

4. Risk ve İş Etkisi

Saldırganlar web sunucusu yetkileriyle (www-data) sunucu üzerinde kaynak kodları okuyabilir, web dizinine zararlı dosyalar (web shell) yükleyebilir, veri tabanı kimlik bilgilerini ele geçirebilir ve sunucuyu tamamen ele geçirecek yetki yükseltme saldırılarını başlatabilir.

5. Sıkılaştırma ve İyileştirme Çözümü

- Apache web sunucusu ve PHP yorumlayıcısı desteklenen güncel ve kararlı sürümlere yükseltilmelidir.
- PHP yapılandırma dosyasında (php.ini) cgi.force_redirect yönergesi aktif edilmeli ve tehlikeli fonksiyonlar (exec, shell_exec, system) devre dışı bırakılmalıdır.
- Web sunucusu üzerinde gereksiz HTTP metodları (PUT, DELETE) kısıtlanmalı ve Web Uygulama Güvenlik Duvarı (WAF) kuralları uygulanmalıdır.

3.6. BULGU: NFS GÜVENSİZ DOSYA PAYLAŞIMI VE ROOT YETKİ YÜKSELTME RİSKİ

1. Zafiyet Kimlik Kartı ve Değerlendirmesi

Hedef Varlık	10.0.2.3 (Metasploitable 2)
Etkilenen Port / Protokol	Tcp / 2049 (Nfs)
Servis Ve Versiyon	Nfsv2 / Nfsv3 (Rpc #100003)
Zafiyet Türü	Insecure Export Permissions / Misconfiguration
Cve Kodu	Cwe-276 (Incorrect Default Permissions)
Cvss V3.1 Taban Skoru	9.8 (Kritik)

2. Teknik Açıklama

Hedef sistemde çalışan Ağ Dosya Sistemi (NFS) servisinde, / (kök dizin) paylaşımının herhangi bir IP kısıtlaması olmaksızın tüm ağa * (wildcard) izniyle dışa aktarıldığı (export) tespit edilmiştir. Ayrıca paylaşım yapılandırmasında no_root_squash parametresinin bulunması, istemcinin sunucuya root yetkileriyle dosya yazabilmesine ve doğrudan hedef makinede yetki yükseltmesine (Privilege Escalation) olanak tanımaktadır.

3. Tespit ve Analiz Kanıtları

Hedef sistemdeki 2049/TCP portu sudo nmap -sV --script=nfs-showmount,nfs-ls,banner -p 2049 10.0.2.3 komutuyla taranmıştır. Yapılan kontrolde NFS servisinin aktif olduğu ve Nmap NSE scripti ile / (kök dizin) dahil tüm dosya sisteminin kimlik doğrulaması olmaksızın dışa aktarıldığı doğrulanmıştır. İlgili tarama çıktısı aşağıdaki görselde yer almaktadır.

```
Nmap scan report for 10.0.2.3
Host is up (0.0016s latency).

PORT      STATE SERVICE VERSION
2049/tcp  open  nfs      2-4 (RPC #100003)
MAC Address: 08:00:27:6C:09:F4 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.89 seconds
```

4. Risk ve İş Etkisi

Saldırgan hedef sunucunun tüm diskini (/) kendi yerel makinesine bağlayabilir (mount). no_root_squash parametresi sayesinde sunucu üzerindeki kritik dosyalara (örneğin /root/.ssh/authorized_keys veya /etc/shadow) tam root yetkisiyle yazma ve okuma işlemi gerçekleştirerek sisteme doğrudan şifresiz root erişimi sağlayabilir.

5. Sıkılaştırma ve İyileştirme Çözümü

- /etc/exports dosyasındaki dosya paylaşımları gözden geçirilmeli, / gibi kritik sistem kök dizinleri kesinlikle paylaşıma açılmamalıdır.
- Paylaşımlarda * (herkes) kuralı yerine yalnızca yetkili istemci IP adresleri tanımlanmalıdır.
- Paylaşım seçeneklerine root_squash parametresi eklenerek uzaktaki root kullanıcılarının sunucuda yetkisiz nobody kullanıcıasına indirgenmesi sağlanmalıdır.
- NFS servisi gereksiz ise durdurulmalı ve 2049 portu güvenlik duvarı üzerinden dış ağa kapatılmalıdır

3.7. BULGU: MYSQL VARSAYILAN PAROLA VE YETKİSİZ UZAKTAN ERIŞİM RİSKİ

1. Zafiyet Kimlik Kartı ve Değerlendirmesi

Hedef Varlık	10.0.2.3 (Metasploitable 2)
Etkilenen Port / Protokol	Tcp / 3306 (Mysql)
Servis Ve Versiyon	Mysql 5.0.51a-3ubuntu5
Zafiyet Türü	Default / Empty Credentials & Remote Access
Cve Kodu	Cwe-521 (Weak Password Requirements)
Cvss V3.1 Taban Skoru	9.8 (Kritik)

2. Teknik Açıklama

Hedef sunucuda çalışan MySQL veritabanı servisinin, tüm ağ arabirimlerini dinleyecek şekilde (0.0.0.0) dış ağa açık yapılandırıldığı ve en üst düzey yönetici olan root kullanıcısının boş parola (parolasız) ile uzaktan erişimine izin verdiği tespit edilmiştir.

3. Tespit ve Analiz Kanıtları

Hedef sistemdeki 3306/TCP portu sudo nmap -sV --script=mysql-empty-password,mysql-info,banner -p 3306 10.0.2.3 komutuyla taranmıştır. Yapılan kontrolde servisin MySQL 5.0.51a sürümü olduğu ve Nmap NSE scripti ile root hesabının parolasız giriş yapabildiği doğrulanmıştır. İlgili tarama çıktısı aşağıdaki görselde yer almaktadır.

```
Nmap scan report for 10.0.2.3
Host is up (0.0034s latency).

PORT      STATE SERVICE VERSION
3306/tcp   open  mysql   MySQL 5.0.51a-3ubuntu5
|_ mysql-empty-password:
|_ root account has empty password
|_ banner: >\x00\x00\x00\x00A5.0.51a-3ubuntu5\x00\x00\x00\x00LWNb#65\x
|_ 00,\xAA\x08\x02\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00 ...
|_ mysql-info:
|_ Protocol: 10
|_ Version: 5.0.51a-3ubuntu5
|_ Thread ID: 9
|_ Capabilities flags: 43564
|_ Some Capabilities: SwitchToSSLAfterHandshake, Support41Auth, SupportsCompression, LongColumnFlag, ConnectWithDatabase, SupportsTransactions, Speaks41ProtocolNew
|_ Status: Autocommit
|_ Salt: 30t|0y2+!aFxmVIL~Wyy
MAC Address: 08:00:27:6C:09:F4 (Oracle VirtualBox virtual NIC)
```

4. Risk ve İş Etkisi

Saldırganlar hiçbir parola girmeden veri tabanına bağlanarak içerideki tüm kullanıcı bilgilerini, hassas kurumsal verileri okuyabilir, silebilir veya değiştirebilir. Ayrıca MySQL'in dosya okuma/yazma fonksiyonları (LOAD_FILE, INTO OUTFILE) ve kullanıcı tanımlı fonksiyonlar (UDF) kötüye kullanılarak işletim sistemi seviyesinde komut çalıştırılabilir.

5. Sıkılaştırma ve İyileştirme Çözümü

- MySQL root kullanıcısı başta olmak üzere tüm veritabanı hesaplarına güçlü ve karmaşık parolalar atanmalıdır.
- MySQL yapılandırma dosyasında (my.cnf) bind-address = 127.0.0.1 ayarı yapılarak servisin yalnızca yerel makineden (localhost) erişilmesi sağlanmalıdır.
- Uzaktan yönetim gerekliyse erişimler doğrudan porta değil, SSH tünelleme üzerinden yapılmalı ve 3306 portu dış ağa kapatılmalıdır.

3.8. BULGU: POSTFIX SMTP AÇIK RÖLE VE KULLANICI NUMARALANDIRMA RİSKİ

1. Zafiyet Kimlik Kartı ve Değerlendirmesi

Hedef Varlık	10.0.2.3 (Metasploitable 2)
Etkilenen Port / Protokol	Tcp / 25 (Smtpt)
Servis Ve Versiyon	Postfix Smtptd
Zafiyet Türü	Information Disclosure / User Enumeration
Cve Kodu	Cwe-200 (Exposure Of Sensitive Information)
Cvss V3.1 Taban Skoru	5.3 (Orta)

2. Teknik Açıklama

Hedef sistemde çalışan Postfix SMTP servisi, VRFY ve EXPN komutlarının çalıştırılmasına izin verecek şekilde yapılandırılmıştır. Kimlik doğrulaması yapmamış bir saldırgan, bu komutları kullanarak sunucuda tanımlı geçerli sistem kullanıcılarını listeleyebilir ve kaba kuvvet saldırıları için kullanıcı adı havuzu oluşturabilir.

3. Tespit ve Analiz Kanıtları

Hedef sistemdeki 25/TCP portu sudo nmap -sV --script=smtp-commands,smtp-enum-users,banner -p 25 10.0.2.3 komutuyla taranmıştır. Yapılan kontrolde servisin Postfix smtpd olduğu ve Nmap NSE scripti ile sistemdeki kullanıcı doğrulama komutlarının (VRFY) açık olduğu teyit edilmiştir. İlgili tarama çıktısı aşağıdaki görselde yer almaktadır.

```
Nmap scan report for 10.0.2.3
Host is up (0.0018s latency).

PORT      STATE SERVICE VERSION
25/tcp    open  smtp    Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_smtp-enum-users:
|_ Method RCPT returned a unhandled status code.
|_ banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
MAC Address: 08:00:27:6C:09:F4 (Oracle VirtualBox virtual NIC)
Service Info: Host: metasploitable.localdomain

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.00 seconds
```

4. Risk ve İş Etkisi Saldırganlar sistemde bulunan geçerli kullanıcı adlarını tespit ederek SSH veya FTP gibi diğer servislere yönelik hedefli parola deneme (brute-force) saldırıları gerçekleştirebilir. Ayrıca yapılandırma hataları mevcutsa sunucu sahte e-posta (Spam/Phishing) gönderimi için açık röle (Open Relay) olarak kötüye kullanılabilir.

5. Sıkılaştırma ve İyileştirme Çözümü

- Postfix konfigürasyon dosyasında (/etc/postfix/main.cf) disable_vrfy_command = yes ayarı yapılarak kullanıcı doğrulama komutu kapatılmalıdır.
- Sunucunun yalnızca yetkili iç ağ kullanıcılarından e-posta kabul etmesi sağlanmalı, açık röle yapılandırması engellenmelidir.
- SMTP trafiği TLS şifrelemesi (STARTTLS) ile güvenli hale getirilmelidir.

3.9. BULGU: ISC BIND 9.4.2 DNS ÖNBELLEK ZEHİRLENMESİ (CACHE POISONING)**1. Zafiyet Kimlik Kartı ve Değerlendirmesi**

Hedef Varlık	10.0.2.3 (Metasploitable 2)
Etkilenen Port / Protokol	Udp, Tcp / 53 (Domain)
Servis Ve Versiyon	Isc Bind 9.4.2
Zafiyet Türü	Dns Cache Poisoning (Kaminsky Zafiyeti)
Cve Kodu	Cve-2008-1447
Cvss V3.1 Taban Skoru	7.5 (Yüksek)

2. Teknik Açıklama

Hedef makinede çalışan ISC BIND 9.4.2 sürümünde DNS sorgu Transaction ID (İşlem Kimliği) ve kaynak portu tahmin edilebilir yapıdadır. Bu durum, Dan Kaminsky tarafından keşfedilen DNS önbellek zehirlleme zafiyetine yol açmakta ve saldırganların sahte DNS yanıtları enjekte etmesine imkân tanımaktadır.

3. Tespit ve Analiz Kanıtları

Hedef sistemdeki 53/UDP,TCP portu sudo nmap -sU -sS -sV --script=dns-cache-snoop,banner -p 53 10.0.2.3 komutuyla taranmıştır. Yapılan kontrolde servisin güvenlik desteği bulunmayan ISC BIND 9.4.2 sürümünü çalıştırdığı ve bilinen kritik DNS zehirlleme açıklarına sahip olduğu doğrulanmıştır. İlgili sürüm tespit çıktısı aşağıdaki görselde yer almaktadır.

```
Nmap scan report for 10.0.2.3
Host is up (0.0015s latency).

PORT      STATE SERVICE VERSION
53/tcp    open  domain ISC BIND 9.4.2
53/udp    open  domain ISC BIND 9.4.2
|_dns-cache-snoop: 0 of 100 tested domains are cached.
MAC Address: 08:00:27:6C:09:F4 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.44 seconds
```

4. Risk ve İş Etkisi

Saldırganlar DNS sunucusunun önbelleğini zehirleyerek ağdaki kullanıcıları meşru web siteleri veya kurumsal servisler yerine kendi kurdukları sahte (olta/phishing) sunuculara yönlendirebilir ve kullanıcı kimlik bilgilerini ele geçirebilir.

5. Sıkılaştırma ve İyileştirme Çözümü

- BIND servisi kaynak port rastgeleleştirmesini (Source Port Randomization) destekleyen güncel bir sürüme yükseltilmelidir.
- DNS sunucusunun dış ağdan gelen özyinelemeli (recursive) sorgulara yanıt vermesi kısıtlanmalı, yalnızca yerel ağa hizmet verecek şekilde sınırlandırılmalıdır.
- DNS verilerinin bütünlüğünü korumak için DNSSEC (Domain Name System Security Extensions) yapılandırması devreye alınmalıdır.

3.10. BULGU: PROFTPD 1.3.1 MOD_TLS / COMMAND EXECUTION RİSKİ

1. Zafiyet Kimlik Kartı ve Değerlendirmesi

Hedef Varlık	10.0.2.3 (Metasploitable 2)
Etkilenen Port / Protokol	Tcp / 2121 (Proftpd)
Servis Ve Versiyon	Proftpd 1.3.1
Zafiyet Türü	Outdated Service / Remote Buffer Overflow
Cve Kodu	Cve-2010-4221
Cvss V3.1 Taban Skoru	9.8 (Kritik)

2. Teknik Açıklama

Hedef sunucunun alternatif portunda (2121/TCP) çalışan ProFTPD 1.3.1 sürümü, mod_tls ve komut işleme mekanizmalarında yığın tabanlı bellek taşması (Stack Buffer Overflow) açıklarına sahiptir. Saldırganlar özel olarak hazırlanan FTP komutlarıyla servis üzerinde bellek taşması tetikleyebilir.

3. Tespit ve Analiz Kanıtları

Hedef sistemdeki 2121/TCP portu `sudo nmap -sV -p 2121 10.0.2.3` komutuyla taranmıştır. Yapılan kontrolde alternatif portta ProFTPD 1.3.1 sürümünün aktif olduğu ve güncel olmayan zafiyetli servis barındırdığı doğrulanmıştır. İlgili sürüm tespit çıktısı aşağıdaki görselde yer almaktadır.

```
Starting Nmap 7.99 ( https://nmap.org ) at 2026-08-18 05:41 -0400
Nmap scan report for 10.0.2.3
Host is up (0.00076s latency).

PORT      STATE SERVICE VERSION
2121/tcp  open  ftp      ProFTPD 1.3.1
MAC Address: 08:00:27:6C:09:F4 (Oracle VirtualBox virtual NIC)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.76 seconds
```

4. Risk ve İş Etkisi

Saldırganlar bellek taşması zafiyetini sömürerek uzaktan kimlik doğrulaması olmadan ProFTPD servisi yetkileriyle sistemde rastgele kod çalıştırabilir ve sunucuda oturum açabilir.

5. Sıkılaştırma ve İyileştirme Çözümü

- ProFTPD servisi güvenlik yamaları uygulanmış güncel kararlı sürüme yükseltilmelidir.
- Sistemde birden fazla FTP servisi çalıştırılmamalı, alternatif 2121/TCP portundaki gereksiz servis tamamen durdurulmalıdır.
- Dış ağdan dosya aktarım portlarına gelen tüm bağlantılar güvenlik duvarı ile engellenmelidir.

3.11. BULGU: APACHE JSERV PROTOCOL (AJP13) YETKİSİZ ERİŞİM RİSKİ

1. Zafiyet Kimlik Kartı ve Değerlendirmesi

Hedef Varlık	10.0.2.3 (Metasploitable 2)
Etkilenen Port / Protokol	Tcp / 8009 (Ajp13)
Servis Ve Versiyon	Apache Jserv (Protocol V1.3) / Apache Tomcat
Zafiyet Türü	Insecure Protocol / File Read & Inclusion (Ghostcat)
Cve Kodu	Cve-2020-1938
Cvss V3.1 Taban Skoru	9.8 (Kritik)

2. Teknik Açıklama

8009/TCP portunda çalışan Apache Jserv Protocol (AJP13), web sunucusu ile Tomcat uygulama sunucusu arasında dahili iletişim sağlayan bir protokoldür. AJP servisinin varsayılan olarak kimlik doğrulaması içermemesi ve dış ağa açık bırakılması, yetkisiz kullanıcıların sunucu üzerindeki yapılandırma ve kaynak dosyalarını doğrudan okumasına veya dosya dahil etme (LFI/RCE) saldırılarına zemin hazırlar.

3. Tespit ve Analiz Kanıtları

Hedef sistemdeki 8009/TCP portu sudo nmap -sV --script=ajp-methods,ajp-auth,banner -p 8009 10.0.2.3 komutuyla taranmıştır. Yapılan kontrolde ajp13 protokolünün dış ağa açık olduğu ve kimlik doğrulaması olmaksızın istek kabul ettiği doğrulanmıştır. İlgili tarama çıktısı aşağıdaki görselde yer almaktadır.

```
Starting Nmap 7.99 ( https://nmap.org ) at 2026-08-18 05:44 -0400
Nmap scan report for 10.0.2.3
Host is up (0.0012s latency).

PORT      STATE SERVICE VERSION
8009/tcp  open  ajp13   Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
MAC Address: 08:00:27:6C:09:F4 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.97 seconds
```

4. Risk ve İş Etkisi

Saldırganlar AJP konektörü üzerinden Tomcat'in WEB-INF dizini altındaki gizli yapılandırma dosyalarını, kaynak kodlarını ve veri tabanı bağlantı parolalarını şifresiz okuyabilir. Sunucuya dosya yükleme imkânı varsa doğrudan uzaktan kod çalıştırılabilir.

5. Sıkılaştırma ve İyileştirme Çözümü

- AJP servisi dış ağlara tamamen kapatılmalı, yalnızca yerel sunucu iletişimine (127.0.0.1) bağlanmalıdır (bind).
- Tomcat yapılandırma dosyasında (server.xml) AJP konektörüne güçlü bir parola (secret/requiredSecret) tanımlanmalıdır.
- AJP protokolü aktif olarak kullanılmıyorsa ilgili bağlayıcı port tamamen devre dışı bırakılmalıdır.

4. WINDOWS 7 (10.0.2.5) ZAFİYET VE SERVİS ANALİZLERİ

Bu bölümde 10.0.2.5 IP adresli Windows 7 SP1 hedef makinesi üzerinde gerçekleştirilen ağ tarama sonuçları ve işletim sistemi servislerinin detaylı teknik analizleri yer almaktadır.

4.1. BULGU: SMBV1 UZAKTAN KOD ÇALIŞTIRMA ZAFİYETİ (ETERNALBLUE / MS17-010)

1. Zafiyet Kimlik Kartı ve Değerlendirmesi

Hedef Varlık	10.0.2.5 (Windows 7 Home Sp1 X64)
Etkilenen Port / Protokol	Tcp / 445 (Microsoft-Ds)
Servis Ve Versiyon	Microsoft Windows 7 Smbv1
Zafiyet Türü	Remote Code Execution / Memory Corruption
Cve Kodu	Cve-2017-0144 / Ms17-010
Cvss V3.1 Taban Skoru	9.8 (Kritik)

2. Teknik Açıklama

Microsoft SMBv1 (Server Message Block) protokolünün özel olarak hazırlanmış paketleri ayrıştırma şeklindeki bellek yönetim hatası nedeniyle ortaya çıkan kritik bir zafiyettir. Saldırganlar ağ üzerinden SMBv1 servisine gönderdikleri zararlı isteklerle hedef sistem üzerinde kimlik doğrulaması olmaksızın en üst düzey sistem yetkisi olan NT AUTHORITY\SYSTEM haklarıyla komut çalıştırabilirler.

3. Tespit ve Analiz Kanıtları

Hedef sistemdeki 445/TCP portu sudo nmap -sV --script=smb-vuln-ms17-010,banner -p 445 10.0.2.5 komutuyla taranmıştır. Yapılan kontrolde microsoft-ds servisinin aktif olduğu ve Nmap NSE scripti ile sistemin MS17-010 (CVE-2017-0144) zafiyetine karşı savunmasız (VULNERABLE) olduğu doğrulanmıştır. İlgili tarama çıktısı aşağıdaki görselde yer almaktadır.

```
Nmap scan report for 10.0.2.5
Host is up (0.00069s latency).

PORT      STATE SERVICE      VERSION
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
MAC Address: 08:00:27:8F:48:81 (Oracle VirtualBox virtual NIC)
Service Info: Host: WINDOWS7; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|   State: VULNERABLE
|   IDs: CVE:CVE-2017-0143
|   Risk factor: HIGH
|   A critical remote code execution vulnerability exists in Microsoft SMBv1
|   servers (ms17-010).
|
|   Disclosure date: 2017-03-14
|   References:
|   https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|   https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.79 seconds
```

4. Risk ve İş Etkisi

Bu zafiyet fidye yazılımları (WannaCry, NotPetya vb.) ve solucanlar tarafından sıklıkla kullanılmaktadır. Saldırgan hiçbir kullanıcı bilgisine ihtiyaç duymadan hedef işletim sisteminin tam kontrolünü ele geçirebilir, tüm disk verilerini şifreleyebilir veya silebilir, ağdaki diğer Windows sistemlere hızla yayılabilir (lateral movement).

5. Sıkılaştırma ve İyileştirme Çözümü

- Microsoft tarafından yayınlanan MS17-010 güvenlik güncelleştirmesi sisteme acilen yüklenmelidir.
- Güvensiz ve eski bir protokol olan SMBv1 servisi Windows Özellikleri menüsünden veya PowerShell/Registry üzerinden tamamen devre dışı bırakılmalıdır.
- Kurumsal güvenlik politikası gereği 445 ve 139 numaralı SMB portları dış ağlara tamamen kapatılmalı, iç ağda ise yalnızca yetkili dosya sunucularına izin verilmelidir.

4.2. BULGU: SMB İMZALAMA (SIGNING) EKSİKLİĞİ VE NTLM RELAY RİSKİ

1. Zafiyet Kimlik Kartı ve Değerlendirmesi

Hedef Varlık	10.0.2.5 (Windows 7 Home Sp1 X64)
Etkilenen Port / Protokol	Tcp / 445 (Microsoft-Ds), Tcp / 139 (Netbios-Ssn)
Servis Ve Versiyon	Microsoft Smbv1 / Smbv2
Zafiyet Türü	Missing Message Integrity Check / Man-In-The-Middle
Cve Kodu	Cve-2015-0005
Cvss V3.1 Taban Skoru	7.5 (Yüksek)

2. Teknik Açıklama Hedef Windows sisteminde SMB paket imzalama (SMB Signing) özelliğinin devre dışı veya isteğe bağlı (enabled but not required) bırakıldığı tespit edilmiştir. İstemci ile sunucu arasındaki ağ paketlerinin dijital olarak imzalanmaması, ağdaki bir saldırganın trafiği araya girerek yönlendirmesine (NTLM Relay) ve kimlik doğrulama oturumlarını kendi kontrolündeki hedeflere ileterek yetki kazanmasına imkan tanır.

3. Tespit ve Analiz Kanıtları

Hedef sistemdeki 445/TCP portu `sudo nmap -sV --script=smb2-security-mode,smb-security-mode,banner -p 445 10.0.2.5` komutuyla taranmıştır. Yapılan kontrolde SMB servisinin aktif olduğu ve Nmap NSE scripti ile sistemde `message_signing: disabled` (veya not required) yapılandırmasının bulunduğu teyit edilmiştir. İlgili tarama çıktısı aşağıdaki görselde yer almaktadır.

```

Nmap scan report for 10.0.2.5
Host is up (0.00063s latency).

PORT      STATE SERVICE      VERSION
445/tcp    open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
MAC Address: 08:00:27:8F:48:81 (Oracle VirtualBox virtual NIC)
Service Info: Host: WINDOWS7; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.1:
|_    Message signing enabled but not required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.73 seconds

```

4. Risk ve İş Etkisi

Saldırganlar aynı yerel ağda LLMNR/NBT-NS zehirleme veya ARP Spoofing saldırıları yaparak SMB trafiğini ele geçirebilir. İmzalama zorunlu olmadığı için yakalanan NTLMv2 kimlik doğrulama özetleri kırılmasa bile doğrudan hedef sunucuya aktararak (relay) parola bilmeden sunucuda oturum açılabilir veya komut çalıştırılabilir.

5. Sıkılaştırma ve İyileştirme Çözümü

- Grup İlkesi Düzenleyicisi (GPO) veya Yerel Güvenlik İlkesi üzerinden SMB İmzalama zorunlu hale getirilmelidir:
- Microsoft network client: Digitally sign communications (always) -> Enabled
- Microsoft network server: Digitally sign communications (always) -> Enabled
- Eski NTLM protokolleri kısıtlanmalı ve Kerberos tabanlı kimlik doğrulamasına öncelik verilmelidir.

4.3. BULGU: MSRPC ENDPOINT MAPPER YETKİSİZ SERVİS BİLGİ İFŞASI

1. Zafiyet Kimlik Kartı ve Değerlendirmesi

Hedef Varlık	10.0.2.5 (Windows 7 Home Sp1 X64)
Etkilenen Port / Protokol	Tcp / 135 (Msrpc)
Servis Ve Versiyon	Microsoft Windows Rpc (Rpcss)
Zafiyet Türü	Information Disclosure / Unauthenticated Rpc Enumeration
Cve Kodu	Cwe-200 (Exposure Of Sensitive Information)
Cvss V3.1 Taban Skoru	5.3 (Orta)

2. Teknik Açıklama

135/TCP portunda çalışan Microsoft Remote Procedure Call (MSRPC) Endpoint Mapper servisi, kimlik doğrulaması olmaksızın dış ağdan gelen sorgulara yanıt vermektedir. Bu durum, yetkisiz saldırganların sistemde arka planda çalışan tüm RPC arayüzlerini, benzersiz tanımlayıcıları (UUID/GUID) ve dinlenen dinamik portları haritalandırmasına olanak tanır.

3. Tespit ve Analiz Kanıtları

Hedef sistemdeki 135/TCP portu sudo nmap -sV --script=msrpc-enum,rpcinfo,banner -p 135 10.0.2.5 komutuyla taranmıştır. Yapılan kontrolde msrpc servisinin dış ağa açık olduğu ve Nmap NSE scripti ile sistem üzerindeki RPC arayüzlerinin kimlik doğrulaması olmadan numaralandırılabilirdiği (enumeration) doğrulanmıştır. İlgili tarama çıktısı aşağıdaki görselde yer almaktadır.

```
Nmap scan report for 10.0.2.5
Host is up (0.00091s latency).

PORT      STATE SERVICE VERSION
135/tcp    open  msrpc  Microsoft Windows RPC
MAC Address: 08:00:27:8F:48:81 (Oracle VirtualBox virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.77 seconds
```

4. Risk ve İş Etkisi Saldırganlar MSRPC üzerinden elde ettikleri verilerle işletim sistemi sürümünü, etkin servisleri ve potansiyel zafiyet barındıran RPC uç noktalarını tespit edebilir. Bu bilgiler, hedefe yönelik özel RPC istismar (exploit) saldırılarının ve yerel yetki yükseltme denemelerinin başarı şansını doğrudan artırır.

5. Sıkılaştırma ve İyileştirme Çözümü

- 135/TCP portuna dış ağlardan (WAN) ve güvenilmeyen yerel alt ağlardan gelen erişimler güvenlik duvarı kuralları ile engellenmelidir.
- RPC uç noktalarının yalnızca etki alanı (Domain) içi yetkili sistemlerle haberleşmesi sınırlandırılmalıdır.
- Windows Güvenlik Duvarı üzerinde gereksiz Uzaktan Yönetim ve MSRPC kuralları devre dışı bırakılmalıdır.

4.4. BULGU: WINDOWS 7 DESTEK SONU (EOL) VE YAMALANMAMIŞ İŞLETİM SİSTEMİ RİSKİ

1. Zafiyet Kimlik Kartı ve Değerlendirmesi

Hedef Varlık	10.0.2.5 (Windows 7 Home Sp1 (X64))
Etkilenen Port / Protokol	Sistem Geneli / Tüm Portlar
Servis Ve Versiyon	Microsoft Windows 7 Sp1 (Build 7601)
Zafiyet Türü	End Of Life (Eol) / Unsupported Operating System
Cve Kodu	Cwe-1104 (Use Of Unmaintained Third Party Components)
Cvss V3.1 Taban Skoru	9.8 (Kritik)

2. Teknik Açıklama Microsoft, Windows 7 işletim sistemi için resmi güvenlik desteğini ve güncelleme dağıtımını Ocak 2020 itibarıyla tamamen sonlandırmıştır. Bu tarihten sonra keşfedilen çekirdek (kernel), ağ protokolü ve servis zafiyetleri için resmi güvenlik yamaları yayınlanmamaktadır. Sistemin servis paketi (SP1) seviyesinde bırakılması, güncel tehditlere karşı korumasız kalmasına yol açmaktadır.

3. Tespit ve Analiz Kanıtları

Hedef sistem sudo nmap -O -sV --script=smb-os-discovery,banner -p 135,139,445 10.0.2.5 komutuyla taranmıştır. Yapılan kontrolde işletim sisteminin Windows 7 Service Pack 1 sürümü olduğu ve Nmap NSE scripti ile sistemin güvenlik desteği sonlanmış (EOL) bir platformda çalıştığı doğrulanmıştır. İlgili tarama çıktısı aşağıdaki görselde yer almaktadır.

```

Nmap scan report for 10.0.2.5
Host is up (0.0023s latency).

PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Windows 7 Home Basic 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
MAC Address: 08:00:27:8F:48:81 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 2008|7|Vista|8.1
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_vista cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows Vista SP2 or Windows 7 or Windows Server 2008 R2 or Windows 8.1
Network Distance: 1 hop
Service Info: Host: WINDOWS7; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
  smb-os-discovery:
    OS: Windows 7 Home Basic 7601 Service Pack 1 (Windows 7 Home Basic 6.1)
    OS CPE: cpe:/o:microsoft:windows_7::sp1
    Computer name: windows7
    NetBIOS computer name: WINDOWS7\x00
    Workgroup: WORKGROUP\x00
  _ System time: 2026-08-18T13:23:39-07:00

```

4. Risk ve İş Etkisi

Güvenlik desteği bulunmayan bir işletim sistemi, ağdaki saldırganlar için kolay bir hedef haline gelir. Bilinen zafiyetlerin yamalanamaması sebebiyle sistem bütünüyle ele geçirilebilir, zararlı yazılımlar (Ransomware, Spyware) için kalıcı bir barınma alanı oluşturur ve kurumsal ağın geri kalanı için doğrudan tehdit unsuru yaratır.

5. Sıkılaştırma ve İyileştirme Çözümü

- İşletim sistemi Microsoft tarafından aktif olarak desteklenen ve güvenlik güncellemeleri alan güncel bir Windows sürümüne (Windows 10 / 11 veya Windows Server) yükseltilmelidir.
- Yükseltme yapılamayan zorunlu senaryolarda cihaz kritik kurumsal ağdan tamamen izole edilmeli ve ayrı bir VLAN/Segment içine alınmalıdır.
- Cihazın internet erişimi sınırlandırılmalı ve uç nokta koruma (EDR/Antivirüs) yazılımları ile sıkı denetim altında tutulmalıdır.

5. RİSK MATRİSİ VE ZAFİYET ÖZETİ

Bu bölümde, sızma testi kapsamında incelenen hedef sistemler (10.0.2.3 ve 10.0.2.5) üzerinde tespit edilen tüm güvenlik bulguları, CVSS puanları ve risk seviyelerine göre özetlenmiştir.

HEDEF	PORT / SERVİS	ZAFİYET	CVSS PUANI	CVSS DERECE
Metasploitable 2	21 / Ftp	Vsftpd 2.3.4 Arka Kapı (Backdoor)	9.8	Kritik
Metasploitable 2	22 / Ssh	Openssh 4.7p1 Zayıf Anahtar & Eski Protokol	7.5	Yüksek
Metasploitable 2	23 / Telnet	Şifresiz Veri İletimi (Cleartext Protocol)	7.5	Yüksek
Metasploitable 2	25 / Sntp	Postfix Açık Röle Ve Kullanıcı İfşası	5.3	Orta

HEDEF	PORT / SERVİS	ZAFİYET	CVSS PUANI	CVSS DEREGESİ
Metasploitable 2	53 / Dns	Isc Bind 9.4.2 Önbellek Zehirlleme Riski	7.5	Yüksek
Metasploitable 2	80 / Http	Apache 2.2.8 / Php-Cgi Komut Çalıştırma	9.8	Kritik
Metasploitable 2	139, 445 / Smb	Samba 3.0.20 Rce (Username Map Script)	10.0	Kritik
Metasploitable 2	2049 / Nfs	Güvensiz Paylaşım Ve Root Yetki Yükseltme	9.8	Kritik
Metasploitable 2	2121 / Ftp	Proftpd 1.3.1 Bellek Taşması Riski	9.8	Kritik
Metasploitable 2	3306 / Mysql	Varsayılan Boş Parola Ve Uzaktan Erişim	9.8	Kritik
Metasploitable 2	8009 / Ajp	Apache Jserv Kimlik Doğrulama Eksikliği	9.8	Kritik
Windows 7 Sp1	445 / Smb	Smbv1 Uzaktan Kod Çalıştırma	9.8	Kritik
Windows 7 Sp1	445 / Smb	Smb İmzalama Eksikliği Ve Ntlm Relay	7.5	Yüksek
Windows 7 Sp1	135 / Rpc	Msrpc Servis Ve Uç Nokta Bilgi İfşası	5.3	Orta
Windows 7 Sp1	Genel Sistem	Destek Sonu Ve Güvenlik Yaması Eksikliği	9.8	Kritik

6. SONUÇ VE GENEL GÜVENLİK ÖNERİLERİ

Test edilen sistemlerdeki zafiyetlerin büyük çoğunluğu; **güncellenmemiş eski servisler, varsayılan ve zayıf yapılandırmalar** ile **destek süresi dolmuş işletim sistemlerinden** kaynaklanmaktadır. Bu risklerin giderilmesi ve kurumsal ağın güvenliğinin artırılması amacıyla aşağıdaki aksiyonların öncelikli olarak uygulanması önerilmektedir:

- **İşletim Sistemi ve Servis Güncellemeleri:** Kullanım ömrü biten Windows 7 işletim sistemi desteklenen güncel bir sürüme yükseltilmeli; Linux sunucu üzerindeki tüm servis paketleri en son kararlı sürümlerle yamalanmalıdır.
- **Protokol ve Servis Sıkılaştırması:** Açık metin (şifresiz) veri aktarımı yapan Telnet, eski FTP ve SMBv1 gibi güvensiz protokoller tamamen devre dışı bırakılmalı, yerlerine SSH, SFTP ve SMBv2/v3 protokolleri zorunlu tutulmalıdır.
- **Erişim Kontrolü ve Ağ Segmentasyonu:** Veritabanı (MySQL) ve dahili yönetim arayüzleri (AJP, MSRPC) dış ağ erişimlerine kapatılmalı, kritik servisler yalnızca yetkili IP bloklarına izin verecek şekilde güvenlik duvarı ile sınırlandırılmalıdır.
- **Kimlik Doğrulama ve Parola Politikaları:** Sistemlerdeki tüm varsayılan ve boş parolalar kaldırılmalı, güçlü parola standartları ve çok faktörlü kimlik doğrulama (MFA) mekanizmaları devreye alınmalıdır.