Project Subject

Vulnerability and Metasploitable

Full Name

Haydar Can Kotanoglu

Project Duration

Bitis Tarihi: 08/06/2025

1. Hedef Sistemlerdeki Güvenlik Açıklarının Tespiti ve Analizi

1.1. Projenin Amacı

Bu projenin temel amacı, belirlenen hedef sistemlerdeki (Metasploitable ve Windows Host) internete açık servislerindeki güvenlik açıklarını tespit etmektir. Sağlanan veriler ışığında, bu sistemlerin çalışan servisleri ve potansiyel zafiyetleri ayrıntılı olarak analiz edilmiştir.

1.2. Bilgi Toplama ve Keşif

Siber güvenlik değerlendirmesinin temelini, hedef sistemler hakkında detaylı bilgi toplama ve keşif süreci oluşturur. Bu süreç, IP adresi ve ağ bilgilerinin belirlenmesi, servis tespiti, işletim sistemi tespiti ve güvenlik açığı taramasını içerir. Nmap ve Nessus gibi araçlar kullanılarak sistemler kapsamlı bir şekilde incelenmiştir.

1.3. Zafiyet Analizi ve Raporlama

Bu bölümde, sağlanan Nessus çıktıları ve sistem komutları kullanılarak hedef sistemlerdeki güvenlik açıkları ve sistem yapılandırmaları detaylı bir şekilde analiz edilmiştir. Proje, mevcut zafiyet tarama verilerini analiz etme ve raporlama becerilerini sergilemeyi amaçlamaktadır.

---

2. Bilgi Toplama ve Keşif Adımları

Bir siber güvenlik değerlendirmesinin temelini, hedef sistemler hakkında detaylı bilgi toplama ve keşif süreci oluşturur. Bu süreç, genellikle aşağıdaki adımları içerir:

- **IP Adresi ve Ağ Bilgilerinin Belirlenmesi:** Hedef sistemlerin ağdaki konumları (IP adresleri) ve temel ağ yapılandırmaları tespit edilir.
- **Servis Tespiti (Port Tarama):** Hedef IP adresleri üzerinde çalışan ağ servisleri (HTTP, FTP, SSH, DNS vb.) ve bu servislerin kullandığı port numaraları belirlenir. Bu amaçla Nmap gibi port tarama araçları kullanılır. Nmap, `-sV` parametresi ile servis versiyonlarını, `-sC` ile varsayılan güvenlik açığı ve bilgi toplama scriptlerini çalıştırabilir ve `-p-` ile tüm TCP/UDP portlarını tarayabilir.
- **İşletim Sistemi Tespiti:** Hedef sistemlerde çalışan işletim sistemleri ve versiyonları, çeşitli ağ parmak izi teknikleri ve araçları (Nmap OS detection, Nessus vb.) ile tahmin edilmeye çalışılır.
- **Güvenlik Açığı Taraması:** Keşfedilen servisler ve sistemler üzerinde bilinen güvenlik açıklarını tespit etmek amacıyla Nessus gibi otomatik zafiyet tarama araçları kullanılır. Bu araçlar, geniş bir zafiyet veritabanına karşı hedefleri test eder ve potansiyel riskleri raporlar. Bu proje, sağlanan Nessus tarama çıktıları ve sistem komut çıktıları üzerinden doğrudan zafiyet analizi ve durum tespiti üzerine odaklanmaktadır.

---

3. Metasploitable Host (10.10.1.2) Analizi

IP adresi 10.10.1.2 olan Metasploitable sanal makinesi, üzerinde çeşitli güvenlik açıkları barındıran bir test sistemidir.

3.1. Kullanılan Araçlar ve Bilgi Kaynakları

- **Nessus Professional:**
  - **Nessus Server Bilgileri:** URL / IP Adresi: `https://10.10.1.6:8834`, Kullanıcı Adı: sysadm
  - **Nessus Versiyonu:** 10.8.4 (Plugin Feed: 202506020928)
  - **Tarama Adları:** "Grad1" (Metasploitable Host için), "Windows No Credential Scan" (Windows Host için)
  - **Tarama Politikaları:** "Advanced Scan" ve "Basic Network Scan"
- **Linux Komut Satırı Araçları (Metasploitable Host - 10.10.1.2 üzerinde):** `uname -a`, `uptime`, `df -h`, `sudo dmidecode`, `cat /etc/passwd`, `cat /etc/shadow`. (Nessus tarafından sağlanan çıktılarda netstat benzeri komutların da kullanıldığı anlaşılmaktadır.)
- **Nmap (Network Mapper):**
  - **Komut (Metasploitable Host):** `nmap -sV -sS 10.10.1.2 -p-`
  - **Kullanım Amacı:** Kapsamlı port taraması ve servis versiyon tespiti.

3.2. Sistem Bilgileri (Yerel Komut Çıktılarından)

- **İşletim Sistemi:** Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux. Bu, Nessus OS Identification (Plugin ID 11936) çıktısıyla da desteklenmektedir ve sistemin Ubuntu 8.04 tabanlı olduğu anlaşılmaktadır.
- **Çalışma Süresi (Uptime):** 6:22 (sağlanan uptime komutu çıktısındaki değer).
- **Disk Kullanımı:** `/dev/mapper/metasploitable-root` dosya sistemi 7.0G boyutunda olup, 1.5G kullanılmış ve 5.2G boş alan mevcuttur (%22 kullanım). Diğer geçici dosya sistemleri (varrun, varlock, udev, devshm) de listelenmiştir.
- **Donanım Bilgileri (dmidecode):**
  - **BIOS:** SeaBIOS, Sürüm: rel-1.16.3-0-ga6ed6b701f0a-prebuilt.qemu.org, Yayın Tarihi: 04/01/2014.
  - **Sistem:** QEMU, Ürün Adı: Standard PC (i440FX + PIIX, 1996), Sürüm: pc-i440fx-9.0.
  - **İşlemci:** QEMU, 2000 MHz, 1 Çekirdek.
  - **Bellek:** 2048 MB RAM.
- **Kullanıcı Hesapları ve Parola Bilgileri (/etc/passwd ve /etc/shadow):**
  - Çok sayıda sistem ve kullanıcı hesabı bulunmaktadır. `root`, `msfadmin`, `postgres`, `user`, `service`, `sys`, `klog`, `yusuf` ve `mavci` gibi kullanıcıların parola hash'leri `/etc/shadow` dosyasında listelenmiştir. `msfadmin` kullanıcısının parolasının "msfadmin" olduğu Telnet banner'ından (Plugin ID 10281) ve genel bilinirliğinden anlaşılmaktadır. Diğer kullanıcıların parolaları da zayıf veya varsayılan olabilir. Nessus Plugin ID 83303 ("Unix/Linux - Local Users Information: Passwords Never Expire") çıktısına göre `root`, `sys`, `klog`, `msfadmin`, `postgres`, `user`, `service`, `yusuf`, `mavci` kullanıcılarının parolaları süresiz olarak ayarlanmıştır.

3.3. Ağ Servisleri ve Port Bilgileri (Nmap ve Nessus Çıktılarından)

Metasploitable host (10.10.1.2) üzerinde çalışan ve dışarıdan erişilebilen başlıca servisler ve portları şunlardır:

PORT	PROTOCOL	SERVICE	VERSION
21 - FTP	TCP - vsftpd 2.3.4,	FTP,	vsftpd 2.3.4,
22 - SSH	OpenSSH 4.7p1, L	SSH,	OpenSSH 4.7p1,
23 - Telnet	inux telnetd, Postfix	Telnet,	Linux telnetd,
25 - SMTP	smtpd,	SMTP,	Postfix smtpd,
53 - DNS	ISC BIND 9.4.2,	DNS,	ISC BIND 9.4.2,
80 - HTTP	Apache httpd 2.2.8,	HTTP,	Apache httpd 2.2.8,
111 - RPCbind	Samba smbd 3.X - 4.X,	RPCbind,	Samba smbd 3.X - 4.X,
139 - NetBIOS-SSN	Samba smbd 3.0.20-	NetBIOS-SSN,	Samba smbd 3.0.20-
445 - SMB	Debian,	SMB,	Debian,
512 - rsh	netkit-rsh rexecd,	rsh,	netkit-rsh rexecd,
513 - rlogin	xinetd	rlogin,	xinetd, GNU Classpath
514 - rexec	UDP - GNU Classpath	rexec,	grmiregistry,
1099 - Java RMI	grmiregistry,	Java RMI,	Metasploitable root
1524 - Bind Shell	Metasploitable root	Bind Shell,	shell, NFS Versions 2-
2049 - NFS	shell,	NFS,	4, ProFTPD 1.3.1,
2121 - FTP	NFS Versions 2-4,	MySQL,	MySQL 5.0.51a-
3306 - MySQL	ProFTPD 1.3.1,	distccd,	3ubuntu5,
3632 - distccd	MySQL 5.0.51a-	PostgreSQL,	distccd v1,
5432 - PostgreSQL	3ubuntu5,	VNC,	PostgreSQL DB 8.3.1,
5900 - VNC	distccd v1,	X11,	Xtightvnc, UnrealIRCd
6000 - X11	PostgreSQL DB 8.3.1,	IRC,	3.2.8.1,
6667 - IRC	Xtightvnc,	AJP13,	Apache JServ v1.3 /
6697 - AJP13	UnrealIRCd 3.2.8.1,	Apache Tomcat,	Apache-Coyote/1.1,
8009 - Apache Tomcat	Apache JServ v1.3 /	Ruby DRb	Apache
8180 - Apache Tomcat	Apache-Coyote/1.1,		Tomcat/Coyote JSP
8787 - Ruby DRb	Apache		engine 1.1,
	Tomcat/Coyote JSP		Ruby DRb RMI (Ruby
	engine 1.1,		1.8)
	Ruby DRb RMI (Ruby		
	1.8)		

3.4. Kritik Seviye Zafiyetler (Nessus Çıktılarından)

- **Plugin ID 20007: SSL Version 2 and 3 Protocol Detection (Port 25/SMTP, 5432/PostgreSQL)**
  - **Açıklama:** SMTP (Postfix) ve PostgreSQL servisleri, güvensiz SSLv2 ve SSLv3 protokollerini desteklemektedir.
  - **Risk Faktörü:** Kritik.
  - **Öneri:** Bu protokoller devre dışı bırakılmalı, TLS 1.2+ kullanılmalıdır.
- **Plugin ID 32314: Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (Port 22/SSH)**
  - **Açıklama:** OpenSSH sunucusunun anahtarları zayıf rastgele sayı üretimi nedeniyle tahmin edilebilirdir.
  - **CVE:** CVE-2008-0166.
  - **Risk Faktörü:** Kritik.
  - **Öneri:** SSH anahtarları güvenli bir şekilde yeniden üretilmeli, ilgili OpenSSL ve OpenSSH paketleri derhal güncellenmelidir.
- **Plugin ID 51988: Bind Shell Backdoor Detection (Port 1524/TCP)**
  - **Açıklama:** 1524 numaralı portta kimlik doğrulaması gerektirmeyen bir root komut satırı (shell) dinlemektedir. Nessus, `id` komutunu çalıştırarak `uid=0(root)` çıktısını almıştır. Bu, sisteme tam yetkili erişim sağlayan kritik bir arka kapıdır.
  - **Risk Faktörü:** Kritik.
  - **Öneri:** Bu arka kapı derhal kapatılmalı, sistemin nasıl ele geçirildiği detaylıca araştırılmalı ve güvenlik ihlali doğrulanırsa sistem yeniden kurulmalıdır.
- **Plugin ID 77823: Bash Remote Code Execution (Shellshock) (Port 22/SSH üzerinden tespit)**
  - **Açıklama:** Sistemdeki Bash versiyonu, "Shellshock" (CVE-2014-6271) olarak bilinen ve ortam değişkenleri üzerinden uzaktan kod çalıştırmaya olanak tanıyan kritik bir komut enjeksiyonu zafiyetine sahiptir. Nessus, `TERM` ortam değişkenini manipüle ederek `/usr/bin/id` komutunu çalıştırmış ve `uid=0(root)` çıktısını elde etmiştir.
  - **CVE:** CVE-2014-6271.
  - **Risk Faktörü:** Kritik.
  - **Öneri:** Bash versiyonu acilen güncellenmelidir.
- **Plugin ID 134862: Apache Tomcat AJP Connector Request Injection (Ghostcat) (Port 8009/AJP)**
  - **Açıklama:** Apache Tomcat 5.5 (Apache-Coyote/1.1) üzerinde çalışan AJP konnektörü, "Ghostcat" (CVE-2020-1938, CVE-2020-1745) olarak bilinen, dosya okuma/içerme ve potansiyel uzaktan kod çalıştırma (RCE) zafiyetine sahiptir. Nessus, `/WEB-INF/web.xml` dosyasını okuyabildiğini doğrulamıştır.
  - **CVE:** CVE-2020-1938, CVE-2020-1745.
  - **Risk Faktörü:** Kritik.
  - **Öneri:** AJP konnektör yapılandırması güncellenerek yetkilendirme zorunlu kılınmalı veya Tomcat sunucusu acilen desteklenen ve güvenli bir versiyona yükseltilmelidir.

3.5. Yüksek Seviye Zafiyetler (Nessus Çıktılarından)

- **Plugin ID 10205: rlogin Service Detection (Port 513/TCP)**
  - **Açıklama:** rlogin servisi çalışmaktadır. Bu servis şifresiz iletişim kurar ve zayıf kimlik doğrulama mekanizmalarına sahiptir.
  - **CVE:** CVE-1999-0651.
  - **Risk Faktörü:** Yüksek.
  - **Öneri:** Servis devre dışı bırakılmalı, yerine SSH kullanılmalıdır.

- **Plugin ID 90509: Samba Badlock Vulnerability (Port 445/SMB)**
  - **Açıklama:** Sistemdeki Samba versiyonu (3.0.20-Debian), "Badlock" (CVE-2016-2118) zafiyetine sahiptir.
  - **CVE:** CVE-2016-2118.
  - **Risk Faktörü:** Yüksek (CVSS v2.0 Base Score 6.8).
  - **Öneri:** Samba versiyonu acilen güncellenmelidir.

3.6. Potansiyel Metasploit Sömürü Senaryoları

Nessus tarafından Metasploitable host (10.10.1.2) üzerinde tespit edilen kritik ve yüksek seviyeli zafiyetlerin birçoğu, Metasploit Framework içerisinde bulunan modüller kullanılarak sömürülebilir. Aşağıda bazı örnek zafiyetler ve bunlara karşılık gelebilecek potansiyel Metasploit modülleri ve senaryoları listelenmiştir:

- **vsftpd 2.3.4 Backdoor (Plugin ID 10092, 52703; Nmap Çıktısı)**
  - **Zafiyet:** vsftpd'nin 2.3.4 versiyonunda, zararlı bir kullanıcı adı ile giriş denemesi sonucu 6200/TCP portunda bir komut satırı (shell) açan bir arka kapı bulunmaktadır.
  - **Potansiyel Metasploit Modülü:** `exploit/unix/ftp/vsftpd_234_backdoor`.
  - **Senaryo:** Saldırgan, bu modülü kullanarak hedef sistemde root yetkilerinde bir komut satırı oturumu elde edebilir.
- **UnrealIRCd Backdoor (Plugin ID 11156, 17975; Nmap Çıktısı)**
  - **Zafiyet:** UnrealIRCd 3.2.8.1 versiyonunda, `AB;` komut dizisi ile tetiklenebilen ve sistemde komut çalıştırılmasına olanak tanıyan bir arka kapı bulunmaktadır.
  - **Potansiyel Metasploit Modülü:** `exploit/unix/irc/unreal_ircd_3281_backdoor`.
  - **Senaryo:** Saldırgan, bu modülü kullanarak hedef IRC sunucusu üzerinden sistemde komut çalıştırabilir.
- **Java RMI Server Insecure Default Configuration (Plugin ID 22227; Nmap Çıktısı - Port 1099, 60347)**
  - **Zafiyet:** Java RMI Registry, uygunsuz yapılandırılmışsa uzaktan kod çalıştırmaya olanak tanıyabilir.
  - **Potansiyel Metasploit Modülü:** `exploit/multi/misc/java_rmi_server`.
  - **Senaryo:** Saldırgan, RMI servisi üzerinden hedef sisteme zararlı bir Java payload'u yükleyebilir.

---

4. Windows Host (10.10.1.29) Zafiyet Analizi (Kredisiz Tarama)

Windows Host (IP: 10.10.1.29) üzerinde Nessus ile kredisiz (uncredentialed) bir tarama gerçekleştirilmiştir. Bu tür bir tarama, sistem üzerinde çalışan ve dışarıdan erişilebilen servisler hakkında bilgi toplar ve bunlarla ilişkili zafiyetleri tespit etmeye çalışır.

4.1. Sistem Bilgileri (Nessus Çıktılarından)

- **İşletim Sistemi Tahmini (Plugin ID 11936, 209654):** Microsoft Windows 10 (Güven Seviyesi: %56, Metot: MLSinFP).
- **Ana Bilgisayar Adı (Plugin ID 53513 - LLMNR):** Std19.
- **MAC Adresi (Plugin ID 35716, 86420):** BC:24:11:FD:15:D3 (Proxmox Server Solutions GmbH).

4.2. Ağ Servisleri ve Port Bilgileri (Nessus Çıktılarından)

- **Port 3389/TCP:** Remote Desktop Protocol (RDP) servisi aktif. (Plugin ID 10840, 11219).
- **Port 5355/UDP:** Link-Local Multicast Name Resolution (LLMNR) aktif. (Plugin ID 53513).

4.3. Yüksek Seviye Zafiyetler

- **Plugin ID 42873: SSL Medium Strength Cipher Suites Supported (SWEET32) (Port 3389/RDP)**
  - **Açıklama:** RDP servisi, 3DES gibi orta kuvvette şifreleme paketlerini desteklemektedir.
  - **CVE:** CVE-2016-2183.
  - **Risk Faktörü:** Yüksek (CVSS v2.0 Base Score 5.0).
  - **Öneri:** Orta kuvvetteki şifreleme paketleri devre dışı bırakılmalı, güçlü şifreleme paketleri tercih edilmelidir.

---

5. Genel Güvenlik Önerileri

Her iki sistem için de aşağıdaki genel güvenlik önlemleri tavsiye edilir:

- **Yama Yönetimi ve Güncelleme:** Tespit edilen tüm sistemlerde işletim sistemi ve üzerinde çalışan tüm servisler acilen en güncel ve güvenli versiyonlarına yükseltilmelidir. Özellikle Metasploitable host gibi destek süresi dolmuş (Ubuntu 8.04) sistemler derhal desteklenen güncel bir işletim sistemine geçirilmelidir.
- **Güvenli Yapılandırma:**
  - Gereksiz veya güvensiz servisler (Telnet, rlogin, rsh, güvensiz FTP versiyonları) devre dışı bırakılmalıdır.
  - Tüm SSL/TLS kullanan servislerde (HTTPS, SMTPS, RDP vb.) zayıf protokoller (SSLv2, SSLv3, TLS 1.0, TLS 1.1) ve güvensiz şifreleme takımları (RC4, 3DES, EXPORT dereceli şifreler) devre dışı bırakılmalıdır. Sadece TLS 1.2 ve üzeri, güçlü şifreleme takımları (AES-GCM gibi) kullanılmalıdır.
- **Kimlik Doğrulama ve Yetkilendirme:**
  - Tüm hesaplarda güçlü ve benzersiz parolalar kullanılmalıdır. Varsayılan parolalar derhal değiştirilmelidir.
  - SSH erişiminde parola tabanlı kimlik doğrulama yerine anahtar tabanlı kimlik doğrulama tercih edilmelidir.
- **Arka Kapılar ve Güvensiz Yapılandırmalar:** Metasploitable sistemindeki port 1524'te çalışan root shell gibi kritik arka kapılar derhal kapatılmalı ve sistemin bütünlüğü detaylı olarak incelenmelidir.
- **Ağ Güvenliği:**
  - Güvenlik duvarları (firewall) kullanılarak gereksiz portlar ve servisler dışarıdan erişime kapatılmalıdır.
  - SMBv1 protokolü her iki sistemde de devre dışı bırakılmalıdır.
- **Düzenli Güvenlik Taramaları:** Sistemlerin güvenlik duruşunu sürekli izlemek için düzenli olarak yetkili (credentialed) ve yetkisiz (uncredentialed) zafiyet taramaları yapılmalıdır.

---

6. Projeden Kazanımlar

Bu proje, sağlanan Nessus tarama çıktıları ve sistem komut verileri üzerinden iki farklı test sisteminin (bir Linux tabanlı Metasploitable ve bir Windows ana bilgisayarı) güvenlik açıklarını ve yapılandırma detaylarını analiz etme fırsatı sunmuştur. Özellikle Metasploitable sistemi üzerinde çok sayıda kritik ve yüksek seviyeli zafiyetin (arka kapılar, uzaktan kod çalıştırma açıkları, güncel olmayan yazılımlar, zayıf SSL/TLS yapılandırmaları, güvensiz servisler) nasıl tespit edildiği ve raporlandığı incelenmiştir. Potansiyel Metasploit modülleri ve sömürü senaryolarının değerlendirilmesi, tespit edilen zafiyetlerin pratik etkilerini anlamada yardımcı olmuştur. Windows ana bilgisayarı üzerindeki kredisiz tarama ise, özellikle SSL/TLS yapılandırmaları ve eski protokollerin kullanımı gibi dışarıdan tespit edilebilen risklere odaklanmıştır. Bu çalışma, mevcut tarama verilerini yorumlama, farklı işletim sistemleri ve servislerdeki yaygın zafiyet türlerini anlama ve bu zafiyetlere yönelik temel iyileştirme önerileri geliştirme konularında pratik bir deneyim sağlamıştır.

7.Gerçekleşmeyen Hedefler (Unrealized Targets)

Sağlanan raporda, projenin hedeflerine ulaşılamadığına veya kapsam dışında bırakılan, gerçekleştirilemeyen herhangi bir hedefe dair bir bilgi bulunmamaktadır. Rapor, mevcut verilerin başarıyla analiz edildiğini ve sonuçların raporlandığını belirtmektedir.

Tespitler ve Bulgular (Disclosures)

A. Metasploitable Host (10.10.1.2) Üzerindeki Bulgular

Kritik Seviye Zafiyetler:

- **SSLv2 ve SSLv3 Protokolleri:** SMTP (Postfix) ve PostgreSQL servisleri, güvensiz SSLv2 ve SSLv3 protokollerini desteklemektedir.
- **Zayıf SSH Anahtarları (Debian RNG Zafiyeti):** OpenSSH sunucusunun anahtarları, zayıf rastgele sayı üretimi nedeniyle tahmin edilebilir durumdadır (CVE-2008-0166). SMTP ve PostgreSQL servislerindeki SSL sertifikaları da bu zayıf anahtarlarla üretilmiştir.
- **Bind Shell Arka Kapısı:** 1524 numaralı portta, kimlik doğrulaması gerektirmeyen ve tam yetkili (`root`) erişim sağlayan bir komut satırı (shell) bulunmaktadır.
- **Bash "Shellshock" Zafiyeti:** Sistemdeki Bash versiyonu, ortam değişkenleri üzerinden uzaktan kod çalıştırmaya olanak tanıyan kritik "Shellshock" zafiyetine (CVE-2014-6271) sahiptir.
- **Apache Tomcat "Ghostcat" Zafiyeti:** AJP konnektörü üzerinden dosya okuma/içerme ve potansiyel uzaktan kod çalıştırmaya olanak tanıyan "Ghostcat" zafiyeti (CVE-2020-1938, CVE-2020-1745) mevcuttur.
- **Destek Süresi Dolmuş Apache Tomcat:** Kullanılan Apache Tomcat 5.5 versiyonunun destek süresi 30 Eylül 2012'de sona ermiştir ve artık güvenlik yaması almamaktadır.

Yüksek Seviye Zafiyetler:

- **rlogin Servisi:** Sistemde, şifresiz iletişim kuran ve zayıf kimlik doğrulama mekanizmalarına sahip `rlogin` servisi çalışmaktadır.
- **rsh Servisi:** `rlogin` ile benzer riskler taşıyan `rsh` servisi çalışmaktadır.

- **Zayıf Şifreleme Takımları (SWEET32):** SSL/TLS servisleri, 3DES gibi orta kuvvette şifreleme paketlerini destekleyerek "SWEET32" (CVE-2016-2183) saldırılarına karşı zafiyet oluşturmaktadır.
- **Samba "Badlock" Zafiyeti:** Sistemdeki Samba versiyonu (3.0.20-Debian), "Badlock" (CVE-2016-2118) zafiyetine sahiptir.
- **Güncel Olmayan İşletim Sistemi:** Metasploitable host, destek süresi Nisan 2013'te sona ermiş olan Ubuntu 8.04 Hardy Heron üzerinde çalışmaktadır ve yüzlerce kritik/yüksek seviyeli güvenlik güncellemesini almamıştır.

Potansiyel Sömürü Senaryoları:

- **vsftpd 2.3.4 Backdoor:** Zararlı bir kullanıcı adı ile giriş yapıldığında 6200/TCP portunda bir komut satırı açan bir arka kapı bulunmaktadır.
- **UnrealIRCd Backdoor:** `AB;` komut dizisi ile tetiklenebilen ve sistemde komut çalıştırılmasına izin veren bir arka kapı bulunmaktadır.
- **Java RMI Server:** Uygunsuz yapılandırıldığında uzaktan kod çalıştırmaya olanak tanıyabilir.
- **DistCC Daemon:** Uygunsuz yapılandırıldığında yetkisiz komut çalıştırmaya olanak tanır.
- **Apache Tomcat (Ghostcat):** AJP konnektörü üzerinden hassas konfigürasyon dosyaları okunabilir.

B. Windows Host (10.10.1.29) Üzerindeki Bulgular

Yüksek Seviye Zafiyetler:

- **Zayıf Şifreleme Takımları (SWEET32) [RDP]:** RDP servisi, 3DES gibi orta kuvvette şifreleme paketlerini desteklemektedir (CVE-2016-2183).

Orta Seviye Zafiyetler:

- **Güvenilmeyen SSL Sertifikası [RDP]:** RDP servisi için kullanılan SSL sertifikası kendinden imzalıdır ve güvenilir bir otorite tarafından doğrulanmamıştır.
- **TLS 1.0 Desteği:** RDP servisi, güvensiz kabul edilen TLS 1.0 protokolünü desteklemektedir.
- **TLS 1.1 Desteği:** RDP servisi, kullanımı sonlandırılmış (deprecated) olan TLS 1.1 protokolünü desteklemektedir.

Bilgilendirme Amaçlı Bulgular:

- **SMBv1 Desteği:** Sistem güvensiz kabul edilen SMBv1 protokolünü desteklemekte, ancak SMBv2 ve SMBv3'ü desteklememektedir.
- **RDP Sertifika Detayları:** RDP için kullanılan sertifikanın "CN=Std19" olduğu ve geçerlilik bitiş tarihinin 06 Temmuz 2025 olduğu raporlanmıştır.

Participant	*Training Institution*
Haydar Can Kotanoglu	*Oak Academy*