



Bilgi Sistemleri ve Güvenliđi Dersi
Bireysel Rapor

190542007

Bedirhan TUNCER

Giriş

Bu rapor, Bilgi Sistemleri ve Güvenliđi dersinin iřleyiři geređi 01.08.2022 – 26.08.2022 tarihleri arasında grup halinde gerekleřtirdiđimiz tarama araları kullanımı ve sızma testlerinde bireysel olarak neler yapıp, neler yapamadıđımı ierendetaylı bir rapordur.

Yaptıđımız alıřmalar sonucunda bilgi farkındalıđı ve bilgi gvenliđini nemini sonu olarak elde etmiř oldum. Yazılım Mhendisi olarak tarama araları ve Kali iřletim sistemine olan yabancılıđımı giderdim. Bir web sayfasının gvenliđini temel seviyede kontrol edecek ve nlem alacak bilgim var.

Özet

Grup dağılımları sonucu bulunduğum 4 numaralı grup içerisinde iletişimi sağlayan, grup üyeleri arasında köprü niteliğinde bir rolde bulundum. Grup sayımızın 17 kişi olması sebebiyle etkin bir çalışma yapabilmemiz için dörtlü grupları ayrılmaya karar kıldık. Grup dağılımı ve görev dağılımını yaptıktan sonra içerisinde bulunduğum ekip ise Nessus tarama aracını tanıttı.

***Bu grup içerisinde Nessus kurulumu, tarama işlemi ve sunum noktasında yardımcı oldum. Bunun yanı sıra sunucu bendim.**

Tüm tarama araçları ile Muş Ticaret ve Sanayi Odası'nın taraması yapıldıktan sonra **raporlama ve Nessus tarama aracından elde ettiğimiz sonuçlarının sunumunu yaptım.**

Yaptığım Tarama ve Araştırmalar

1. Nessus Kurulumu
2. Nessus ile Güvenlik Açıklarının tespiti
3. Basic Network Scan

1. Nessus Kurulumu

Nessus'u bir sunucuya kurmak, eğitimsiz bir yönetici için oldukça zordur. Her şeyden önce, Unix için önceden yüklenmiş bir sürüme ihtiyaç vardır. Ayrıca, bir bağlantı noktası tarayıcısı için kabul edilen bir standart **NMAP**, iyi bir şifre test cihazı Hydra ve son olarak iyi bir CGI tarayıcısı **Nikto** gibi bazı ek uygulamaların yüklenmesi önerilir. Bu programların yüklenmesi gerekmeseyse de, Nessus'un performansını büyük ölçüde artıracaklar. UNIX sistemleri için sınıflarında en iyi yardımcı programlar olarak kabul edildikleri için önerilir.

Kali'ye girdikten sonra terminal kısmına:

```
Lynx -source http://install.nessus.org | sh
```

2. Nessus ile Güvenlik Açıklarının tespiti

- Hassas verilere erişmesine veya bunları kontrol etmesine veren güvenlik açıklarının tespiti,
- Yanlış yapılandırma sorunlarının önceden bilinmesi,
- Varsayılan şifre ya da kolay şifre kullanımı gibi sistem üzerindeki sorunların tespiti,
- DDoS (Hizmet dışı bırakma) saldırılarına izin veren TCP/IP sorunlarının çözümü,
- Yüksek hızda varlık keşfi,
- Yama ve yapılandırma denetlemesinin yapılması,
- Varlık profili çıkarma,
- Hassas veri keşfi,
- Yama yönetimi entegrasyonu,
- Çoklu tarayıcı yönetimi ve zafiyet analizi.

The screenshot displays the Nessus Essentials interface for configuring a new scan. The left sidebar contains navigation options: FOLDERS (My Scans, All Scans, Trash) and RESOURCES (Policies, Plugin Rules). The main content area is titled 'New Scan / Host Discovery' and includes a 'Back to Scan Templates' link. The 'Settings' tab is active, showing a 'BASIC' section with 'General', 'Schedule', and 'Notifications' sub-sections. The 'Schedule' sub-section is selected, showing a toggle for 'Enabled' (checked), a note about scheduling, and fields for 'Frequency' (Once), 'Starts' (20:00 on 2021-10-10), 'Timezone' (America/New York), and a 'Summary' line: 'Once on Sunday, October 10th, 2021 at 8:00 PM'. At the bottom are 'Save' and 'Cancel' buttons.

Schedula sekmesinde hangi tarih ve saat aralığında scan'ı başlatacağımızı seçebiliyoruz. Aynı anda birden fazlascan ekleyebilmek için profesyonel paketi yüklememiz gerekiyor

FOLDERS

My Scans

All Scans

Trash

RESOURCES

Policies

Plugin Rules

TENABLE

Community

Research

Plugin Release Notes

New Scan / Host Discovery

[← Back to Scan Templates](#)

Settings

Plugins 

BASIC

DISCOVERY

REPORT

ADVANCED

Scan Type

Host enumeration

Host enumeration

OS Identification

Port scan (common ports)

Port scan (all ports)

Custom

TCP

ARP

ICMP (2 retries)

Save

Cancel

Tenable News

CVE-2021-41773: Path
Traversal Zero-Day in
Apache ...

3. Basic Network Scan

Nessus

ScansSchedulesPoliciesUsers

paul

Basic Network Scan

Audit Trail

Filter Hosts

Scans > Hosts 24 Vulnerabilities 102 Remediations 5

Hide Details

Host	Vulnerabilities ▲	
192.168.1.1	<div><div>18</div><div>7</div><div>57</div></div>	✓
192.168.1.242	<div><div>4</div><div>41</div></div>	✓
192.168.1.16	<div><div>6</div><div>40</div></div>	✓
192.168.1.81	<div><div>3</div><div>31</div></div>	✓
192.168.1.98	<div><div>2</div><div>4</div><div>24</div></div>	✓
192.168.1.10	<div><div>3</div><div>21</div></div>	✓
192.168.1.67	<div><div>2</div><div>23</div></div>	✓
192.168.1.20	<div><div>2</div><div>14</div></div>	✓
192.168.1.21	<div><div>2</div><div>14</div></div>	✓
192.168.1.22	<div><div>2</div><div>14</div></div>	✓

Scan Details

Name: Basic Network Scan

Folder: My Scans

Status: Running

Policy: Basic network scan

Targets: 192.168.1.0/24

Start time: Sun Dec 8 09:46:36 2013

Vulnerabilities

Severity	Count
Info	57
Low	7
Medium	18
High	4
Critical	2

Sonuç

Yaz dönemi itibariyle Bilgi Sistemleri ve Güvenliği dersinden elde ettiğim çıkarımlar:

- Bilgi Güvenliği Farkındalığı noktasında yetkin bir noktaya geldiğimi düşünüyorum.
- Dersin üçgenin bir köşesinde bulunan kriptoloji kısmında hala derse başladığımız noktadayım.
- Penetrasyon testi kısmında ise yaptığımız laboratuvar uygulamaları, grup çalışmaları ve tarama araçlarının kullanımı ile oldukça verim aldım ve kendimi geliştirdim.
- Ekip ile çalışmanın zorlukları ve kolaylıkları kısmında gözlemlene yapabildim.
- Üyeler ve gruplar arası iletişim noktasında kendimi geliştirdiğimi düşünüyorum.
- Ders işleyişi gereği fazlasıyla sunum yaptığımızdan dolayı bu noktada tecrübelenmekten dolayı oldukça mutluyum.
- Tarama araçları ve kali işletim sisteminin herkesin ulaşabileceği şeyler olduğunu gördüm. Doğrusu yalnızca kapüşonlu gözleri kapalı kod yazan insanların uğraşı olduğu algımı yıktım diyebilirim.
- Raporlama noktasında başladığım noktaya nazaran yol kat ettiğimi düşünüyorum

