

Açıklık Tarama ve Sızma Testi

MSÜ-2020

Deniz DEMİRCİ

Sızma Testi Süreci

- ▶ Hazırlık
 - ▶ Gizlilik Sözleşmesi (NDA)
 - ▶ Hedef Kurum için en önemli alanların kurum personeli ile ortaya çıkarılması
 - ▶ Angajman Kuralları (Rules of Engagement) , test nasıl yapılacak?
 - ▶ Test kapsamının belirlenmesi
 - ▶ [Resmi izin belgesi \(Jail Free Card\)](#)
 - ▶ Takımı belirleme
- ▶ Test
 - ▶ Testin Gerçekleştirilmesi
- ▶ Sonuç
 - ▶ Detaylı Analiz ve Tekrar Test Gerçekleştirilmesi
 - ▶ Raporlama

Gizlilik Sözleşmesi (NDA)

- ▶ Hassas/Kritik Veri tanımı
- ▶ Erişim halinde uygulanacak hareket tarzı
- ▶ Hukuki düzenlemelere uyumluluk kapsamında olan ancak erişilebilen veriler olması halinde uygulanacak hareket tarzı (HIPPA veya PCI)
- ▶ Açıklıkların elde ediliş şekilleri ve uygulanan yöntemler
- ▶ Sızma Testi Raporunun muhafazası
- ▶ İletişim kuralları
- ▶ Sorumluluk sınırları

Angajman Kuralları

- ▶ Test nasıl icra edilecek?
 - ▶ Black Box, Crystal Box (White box, Gray box)
 - ▶ Ping sweep, Port scan (yapılacak mı? Liste üzerinden mi gerçekleştirilecek?)
 - ▶ Zafiyet taraması ne şekilde gerçekleştirilecek?
 - ▶ Mesai saatlerinde mi?
 - ▶ Production sistemlerde yapılacak mı? (Kesinti olma ihtimali nedir?)
 - ▶ Sniffing yoluyla sızma, İstemci tarafında kullanılan bir uygulama ile derin tarama
 - ▶ Hangi istemciler dahil olacak
 - ▶ Uygulama seviyesi manipölasyon gerçekleştirilecek mi?
 - ▶ Fiziksel sızma testi yapılacak mı? Ne şekilde?
 - ▶ Sosya Mühendislik uygulanacak mı? Ne şekilde?
- ▶ Bilgilendirme ve iletişim kuralları
- ▶ Test başlangıç-bitiş tarihleri

Test kapsamının belirlenmesi

- ▶ Belirli domain adresleri
- ▶ Network adres aralığı
- ▶ İstemciler, belirli sunucular
- ▶ Angajman kuralları içerisinde belirlenen hedefler sadece tespit mi edilecek?
Ne kadar derine inilecek? DOS?
- ▶ 3. taraflar:
 - ▶ Web Barındırma yapılan bir sunucuda test ne seviyede yapılacak?
 - ▶ Buluttaki uygulamalar kapsam içinde mi? ([AWS](#))
 - ▶ ISP
- ▶ Özellikle kaçınılması gereken alanlar nelerdir

Resmi izin belgesi (Jail Free Card)

- ▶ Erişim izni
 - ▶ Kullanıcı veya sistem seviyesinde
 - ▶ Sistem ve sistem odası
 - ▶ Ağ cihazları ve yönetim cihazları
- ▶ Ağ paketlerin dinlenmesinin izni
- ▶ Bant genişliği kullanımı ve darboğaz oluşma durumu
- ▶ Ele geçen veriler ile ilgili bilgi talep hakkı (kritiklik, hassaslık) ve bilgilendirilme
- ▶ İzin süresi

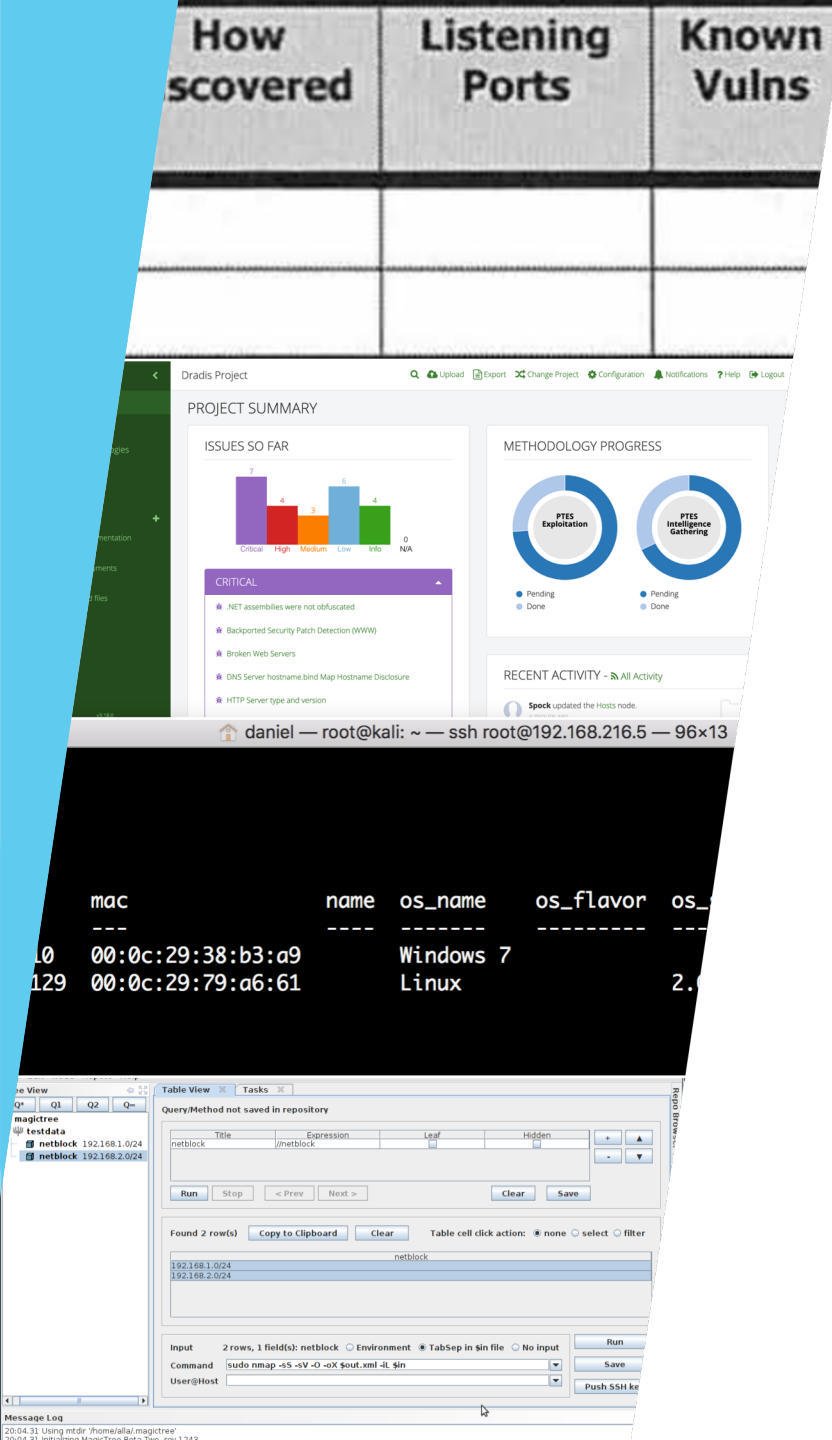
Rapor Formatı

- ▶ Yönetici Özeti: Kısa ve öz, en önemli başlıklar
- ▶ Giriş: Ne için yapıldı, testin maksadı
- ▶ Yöntem: Ne yapıldı, sızma testi sürecinin detayları
- ▶ Bulgular: En kritikten en düşüğe doğru, detaylı teknik anlatım, çözümler.
- ▶ Sonuçlar: Özet ve yönetici özeti ile uyumlu sonuçlar.

Keşif / Bilgi Toplama

► Envanter:

- Excel
- MagicTree
- MediaWiki
- Dradis Server
- Metasploit DB
-



Keşif / Bilgi Toplama

- ▶ Hedef kurum hakkında açık kaynaklardan bilgi edinilmesi
- ▶ Kurum içi erişim var ise kurum web sayfalarından bilgi edinilmesi
- ▶ Hedef kurum teknik altyapısı
- ▶ Kurumsal kültürü, jargonu, ürünleri
- ▶ Kurumun öne çıkan özellikleri

Skip Tracing Framework

A directory of information gathering tools and websites

Start

About

Links

I have a...

Domain name

IP Address/Range

Company name

Website

Name

Email address

Phone number

Nick or ID

Hostname

Password/Hash

Image

URL

Regional/Country specific

Other data

Available information about IP addresses or network ranges:

IP Neighbors

★★★★★

Spam lists

★★★★★

Mailing Lists

★★★★★

Machine specific tools

★★★★★

Anonymous Networks

★★★★★

SSL certificates

★★★★★

Whois

★★★★★









Geolocation

★★★★★

AS Information

★★★★★

Whois protocol databases

- Domain Tools ★★★★★
- DNSStuff ★★★★★
- Robtex Tools ★★★★★
- Whois Archive Volumes ★★★★★
- CentralOps ★★★★★
- Fixed Orbit ★★★★★
- IP Tools ★★★★★
- Whois Archive Volumes (alt mirror) ★★★★★



Keşif / Bilgi Toplama

► Doküman Üst Bilgileri (Metadata):

- Kullanıcı adları
- Dosya yolları
- E-posta adresleri
- İstemci uygulamaları

Metadata Yönünden Zengin Dokümanlar:

- ▶ pdf
- ▶ doc, dot, and docx
- ▶ xls, xlt, and xlsx
- ▶ ppt, pot, pptx
- ▶ jpg, jpeg
- ▶ html and htm

Size	22 kB
File Type	DOCX
File Extension	docx
File Type	application/vnd.openxmlformats-officedocument.wordprocessingml.document
Required Version	20
Bit Flag	0x0006
Compression	Deflated
Modify Date	1980:01:01 00:00:00
Crc	0x82872409
Compressed Size	385
Uncompressed Size	1422
Zip File Name	[Content_Types].xml
Creator	ABDULLAH KÖKSAL(J.ASB.KD.BÇVŞ.) (JGNK)
Last Modified By	AYHAN AŞIK (J.MU.ASB.KD.ÜÇVŞ.)
Revision Number	13
Create Date	2017:03:07 06:07:00Z
Modify Date	2017:08:17 09:18:00Z
Template	Normal
Total Edit Time	15 minutes
Pages	2

Metadata

- ExifTool
- FOCA
- NLNZ
- strings
-



filetype:docx site:jandarma.gov.tr

[All](#) [Images](#) [News](#) [Shopping](#) [Maps](#) [More](#)

1 result (0.32 seconds)

vatandas.jandarma.gov.tr › personel1 ▾ [DOC](#) [Translate this page](#)

[İlk ve Acil Yardım Teknikeri Astsubay Adayı Yüklenm](#)

*In order to show you the most relevant results, we have omitted the 1 already displayed.
If you like, you can [repeat the search with the omitted results in](#)*

whois

- ▶ Kurum IP adreslerinin tespiti
- ▶ Kaydeden kullanıcı tespiti
- ▶ IP Bloğu tespiti

nslookup
dig



Record Type	Description
A	Points to a host's IP address
MX	Points to domain's mail server
NS	Points to host's name server
CNAME	Canonical naming allows aliases to a host
SOA	Indicate authority for domain
SRV	Service records
PTR	Maps IP address to a hostname
RP	Responsible person
HINFO	Host information record includes CPU type and OS
TXT	Unstructured text records

Çalışanlar

- ▶ LinkedIn
- ▶ Facebook
- ▶ Twitter
- ▶ ...

What Organizations Do	What Attacker Gets
User surveys	Business strategies
Promote products	Product profile
User support	Social engineering
Recruitment	Platform/technology information
Background check to hire employees	Type of business



Google Hacking Database

Filters Reset All

Show 15

Quick Search

Date Added	Dork	Category	Author
2020-12-15	intext:"user name" intext:"orion core" -solarwinds.com	Vulnerable Servers	Juan Christian
2020-12-15	intitle:("Index of" AND "wp-content/plugins/boldgrid-backup/=")	Sensitive Directories	Alexandros Pappas
2020-12-11	inurl:ldp/prp.wsf	Pages Containing Login Portals	Javier Bernardo
2020-12-11	"-- Dumped from database version" + "-- Dumped by pg_dump version" ext:txt ext:sql ext:env ext:log	Sensitive Directories	Alexandros Pappas
2020-12-11	"mailer_password:" + "mailer_host:" + "mailer_user:" + "secret:" ext:yaml	Files Containing Passwords	Alexandros Pappas
2020-12-11	inurl:nidp/idff/sso	Pages Containing Login Portals	Javier Bernardo
2020-12-07	"Powered by vBulletin(R) Version 5.6.3"	Advisories and Vulnerabilities	Alexandros Pappas
2020-12-07	ext:yaml ext:txt ext:env "Database Connection Information Database server ="	Files Containing Juicy Info	Alexandros Pappas
2020-12-07	intitle:"NetCamXL"	Various Online Devices	Sanu Jose M
2020-12-07	intext:construct('mysql:host	Files Containing Passwords	Javier Bernardo
2020-12-07	"The SQL command completed successfully." ext:txt ext:log	Files Containing Juicy Info	Alexandros Pappas
2020-12-07	intitle:"web client: login"	Pages Containing Login Portals	Sanu Jose M
2020-12-07	/etc/config + "index of /" /	Sensitive Directories	Manish Solanki

Arama motorları

Linux-101



BACKBOX LINUX

KALI LINUX[™]

Matriux 



blackubuntu

PENTOO



NodeZero