KADİFE TEKSTİL SIZMA TESTİ RAPORU

İçindekiler

Sayfa no

1-) YÖNETİCİ ÖZETİ

Kadife tekstil domaini hem dış hem iç sızma testine tabi tutulmuş olup aşağıdaki açıklanmış olan açık ciddiyetine göre ilgili açıklar ip-network bazlı belirtilmiştir.Her açık için ilgili çözüm ya da öneri her açık sistem için ayrıca verilmiştir.

Açığın ciddiyeti şu şekilde sembolize edilmiştir.

Kırmızı(Critical) :Ciddiyeti en yüksek açıktır,sistem yöneticisi (administrator/root) haklarında sistemin ele geçirilip istenilen zararlı aktiviteler yapılabilir.

Turuncu(High) :Ciddiyeti ikinci derece olan açıktır,herhangi bir teknikle açık başarılı bir şekilde kırılabilirse sistemler sistem yöneticisi haklarında ele geçirilebilir.

Sarı(Medium) :Genelde phishing(oltalama),man in the middle(ortadaki adam) saldırılarına açık oluşturup,Client(sunucudan istekte bulanan kullanıcı) tarafının bilgilerini ifşa etme,onu başka bir zararlı siteye vs yönlendirme gibi ataklara olanak sağlar,sunucu tarafında ise sunucudan fazla bilgi edinilmesini ve sonrasında daha komplex ataklara olanak sağlar.

Yeşil(low) :Daha çok ilgili sistem hakkında fazla bilgi edinilmesini sağlayan,tek başına tehdit olmayacak açıklardır.

Mavi(informational) :Sadece en basit toplanabilen bilgilerdir,açık port/servisler gibi,tek başına bir tehdit oluşturmayan açıklardır.

Yukarıdaki kriterlere göre ,bulunan açıkların ciddiyetleri ve hangi ip ya da network de olduğu aşağıda özetlenmiştir.

Critical	6 192.168.1.110 ,192.168.1.61 ,192.168.0.0-192.168.3.255,94.102.1.96
High	6 192.168.1.1,192.168.1.110,212.57.17.125,192.168.1.50,192.168.1.60
Medium	10 192.168.1.1 , 212.57.17.122 ,212.57.17.126,192.168.0.0/23 ,192.168.1.110,192.168.1.61,94.102.1.96
Low	3 192.168.1.110,94.102.1.96,212.57.17.125
Informational	4 212.57.17.122,212.57.17.123,212.57.17.124,212.57.17.126

2-) AÇIKLARIN IP/NETWORK BAZLI DETAYLARI

A-)İnternet üzerinden açıklar

--212.57.17.122

1-)Medium:Güvenilmeyen sertifika kullanımı;

phishing(oltalama) ve mitm(ortadaki adam) saldırılarına olanak tanımaktadır.

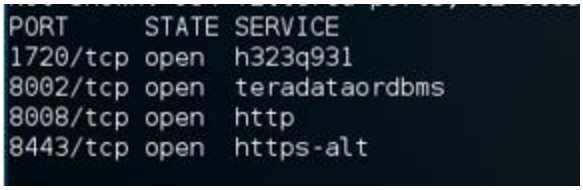
Çözüm:Güvenilir bir sertifika otoritesinden sertifika alınması gerekmektedir.

2-)Medium:Kullanılan yazılımın-programın ifşası;

bu yazılımın üzerinde daha detaylı çalışılarak daha kompleks atakların yapılmasına olanak sağlar.

Çözüm:İlgili sayfanın değiştirilmesi ve kullanılan programın ne olduğunun anlaşılmamasını sağlamak

3-)Informational:Açık port tespiti



--212.57.17.126

1-)Medium:Güvenilmeyen sertifika kullanımı;

phishing(oltalama) ve mitm(ortadaki adam) saldırılarına olanak tanımaktadır.

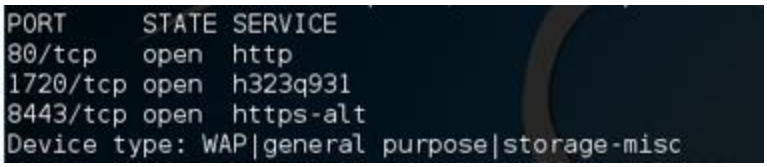
Çözüm:Güvenilir bir sertifika otoritesinden sertifika alınması gerekmektedir.

2-)Medium:Kullanılan yazılımın-programın ifşası;

bu yazılımın üzerinde daha detaylı çalışılarak daha kompleks atakların yapılmasına olanak sağlar.

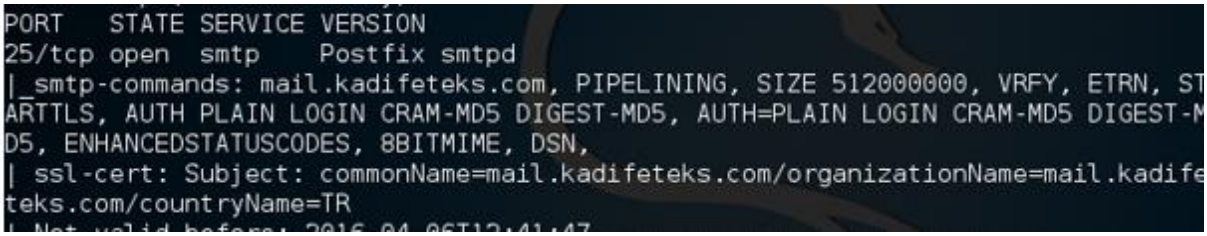
Çözüm:İlgili sayfanın değiştirilmesi ve kullanılan programın ne olduğunun anlaşılmamasını sağlamak

3-)Informational:Açık port tespiti



--212.57.17.125

1-)Low:Kullanılan yazılımın/servisin tespiti;



Çözüm:Yazılımın/servisin karşılama mesajının değiştirilmesi

--212.57.17.124

1-)Informational:Açık port tespiti;

--212.57.17.123

1-)Informational:Açık port tespiti;

B-)Yerel Ağ ve Sistem alt yapısı açıkları

--192.168.1.110

1-)Critical :MS14-066 açığı;

Sistem üzerinde remote code execution(uzaktan sistem üzerinde kod çalıştırabilme) açığı,sisteme administrator/root haklarında authentication sağlanıp istenilen kodun çalıştırılabilmesi.

Çözüm:Bu açık yaması(patch) çıkmış bir açık olup,yamanın zamanında yüklenmemesinden kaynaklı çok ciddi bir açıktır.Otomatik yama yönetimi(patch management) yapan programların kullanılması gerekmektedir.

2-)Hİgh:MS16-047 açığı;

Sam database inin el geçirilebilmesi,bu açığı başarıyla exploit eden biri sam database hash tablosunu ele geçirerek,hash kıran programları da kullanarak bilgisayarın local kullanıcı şifrelerini elde edebilir.

Çözüm:Bu açık yaması(patch) çıkmış bir açık olup,yamanın zamanında yüklenmemesinden kaynaklı bir açıktır.Otomatik yama yönetimi(patch management) yapan programların kullanılması gerekmektedir.

3-)Medium:Güvenilmeyen sertifika kullanımı;

phishing(oltalama) ve mitm(ortadaki adam) saldırılarına olanak tanımaktadır.

Çözüm:Güvenilir bir sertifika otoritesinden sertifika alınması gerekmektedir

4-)Low:Servis/versiyon tespiti;

Bu açık kullanılarak,ilgili servise daha kapsamlı ataklar yapılabilir,dhcp serverin banner grabing yapılarak çalışan servis ve versiyonu tespit edilebilmektedir.

Çözüm:Banner grabing in (isteği karşılama mesajının) değiştirilmesi

4-) Medium: SMB null session açığı;

Bu açık kullanılarak domain de olmayan bir PC üzerinden bile tüm domain kullanıcıları,grupları,şifre politikaları,domain admin kullanıcıları tespit edilebilir

yapılan testler sonucunda elde edilen bilgilerin az bir kısmı aşağıdadır.

==========

| Target Information |

==========

Target 192.168.1.110

RID Range 500-550,1000-1050

[+] Got OS info for 192.168.1.110 from smbclient: Domain=[KADIFETEKS] OS=[Windows Server 2008 R2 Standard 7601 Service Pack 1] Server=[Windows Server 2008 R2 Standard 6.1]

index: 0x81ee RID: 0x132e acb: 0x00000210 Account: adem.akyol Name: Adem AKYOLDesc: An

index: 0x1b79 RID: 0xc7e acb: 0x00000210 Account: adem.ciftci Name: Adem CIFTCI Desc: (null)

index: 0x1805 RID: 0xc32 acb: 0x00000010 Account: adem.karaca Name: Adem KARACA Desc: (null)

index: 0x17ec RID: 0x4e5 acb: 0x00000010 Account: adem.mutlu Name: Adem MUTLUDesc: (null)

index: 0x17db RID: 0x6d8 acb: 0x00000010 Account: adem.saglam Name: Adem SAGLAM

Group 'Domain Admins' (RID: 512) has member: KADIFETEKS\Administrator

Group 'Domain Admins' (RID: 512) has member: KADIFETEKS\mustafa.arat

Group 'Domain Admins' (RID: 512) has member: KADIFETEKS\reha.erdag

Group 'Domain Admins' (RID: 512) has member: KADIFETEKS\karani.ince

Group 'Domain Admins' (RID: 512) has member: KADIFETEKS\samet.yesil

Group 'Domain Admins' (RID: 512) has member: KADIFETEKS\cuneyt.erdil

Group 'Domain Admins' (RID: 512) has member: KADIFETEKS\gazi.becit

Group 'Domain Admins' (RID: 512) has member: KADIFETEKS\sedat.ozturk

Group 'Domain Admins' (RID: 512) has member: KADIFETEKS\runit.as

Group 'CYBER_RESMISITELER' (RID: 3230) has member: KADIFETEKS\emre.karacuha

Group 'CYBER_RESMISITELER' (RID: 3230) has member: KADIFETEKS\perstajyer

Group 'CYBER_RESMISITELER' (RID: 3230) has member: KADIFETEKS\boyalab2

Group 'CYBER_RESMISITELER' (RID: 3230) has member: KADIFETEKS\muh.stajyer

Group 'CYBER_RESMISITELER' (RID: 3230) has member: KADIFETEKS\elektrik1

Group 'CYBER_RESMISITELER' (RID: 3230) has member: KADIFETEKS\tasarim.takip

Çözüm:SMB null session inaktif hale getirilmelidir.

Referans: https://social.technet.microsoft.com/Forums/windows/en-US/52899d34-0033-41f5-b5e0-2325dd827244/disabling-null-sessions-on-windows-server-20032008?forum=winserverGP

--192.168.1.61

1-)Critical:MS11-030 açığı;

Sistem üzerinde remote code execution(uzaktan sistem üzerinde kod çalıştırabilme) açığı,sisteme administrator/root haklarında authentication sağlanıp istenilen kodun çalıştırılabilmesi.

Çözüm:Bu açık yaması(patch) çıkmış bir açık olup,yamanın zamanında yüklenmemesinden kaynaklı çok ciddi bir açıktır.Otomatik yama yönetimi(patch management) yapan programların kullanılması gerekmektedir

2-)Critical:MS14-066 açığı;

Sistem üzerinde remote code execution(uzaktan sistem üzerinde kod çalıştırabilme) açığı,sisteme administrator/root haklarında authentication sağlanıp istenilen kodun çalıştırılabilmesi.

Çözüm:Bu açık yaması(patch) çıkmış bir açık olup,yamanın zamanında yüklenmemesinden kaynaklı çok ciddi bir açıktır.Otomatik yama yönetimi(patch management) yapan programların kullanılması gerekmektedir

3-) Critical:MS12-020 açığı;

Sistem üzerinde remote code execution(uzaktan sistem üzerinde kod çalıştırabilme) açığı,sisteme administrator/root haklarında authentication sağlanıp istenilen kodun çalıştırılabilmesi.

Çözüm:Bu açık yaması(patch) çıkmış bir açık olup,yamanın zamanında yüklenmemesinden kaynaklı çok ciddi bir açıktır.Otomatik yama yönetimi(patch management) yapan programların kullanılması gerekmektedir

4-)High: MS16-047;Sam database inin el geçirilebilmesi;

Bu açığı başarıyla exploit eden biri sam database hash tablosunu ele geçirerek, sonrasında hash kıran programları da kullanarak bilgisayarın local kullanıcı şifrelerini elde edebilir.

Çözüm:Bu açık yaması(patch) çıkmış bir açık olup,yamanın zamanında yüklenmemesinden kaynaklı bir açıktır.Otomatik yama yönetimi(patch management) yapan programların kullanılması gerekmektedir.

5-)Medium: Güvenilmeyen sertifika kullanımı ;

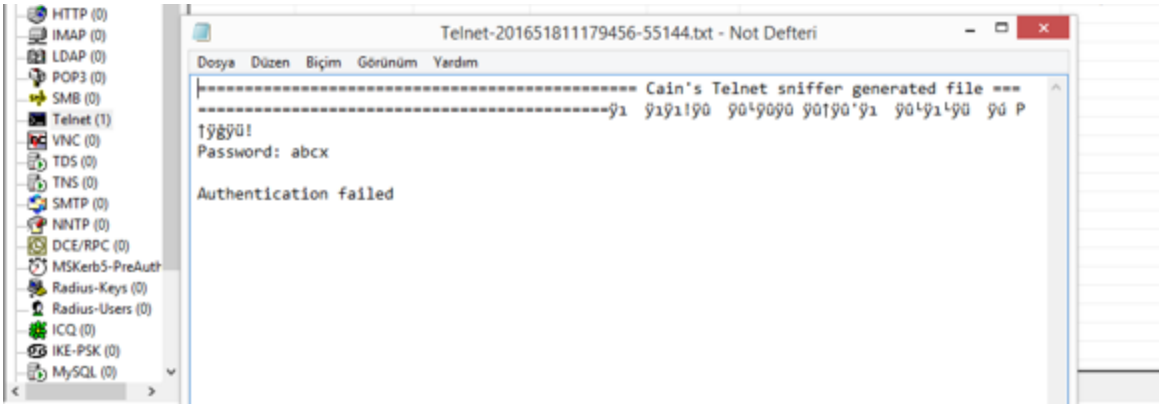
phishing(oltalama) ve mitm(ortadaki adam) saldırılarına olanak tanımaktadır.

Çözüm:Güvenilir bir sertifika otoritesinden sertifika alınması gerekmektedir

--192.168.0.0-192.168.3.255

1-)Critical:Arp zehirlenmesi açığı;

Bu açık kullanılarak atak eden kişi istediği trafiği kendi bilgisayarı üzerinden geçirip ,trafiği sniff (koklama) ederek istediği hassas veriyi ele geçirebilir,Session hijacking(oturum çalma) yaparak otantike olmuş oturumları kendisi otantike olmuş gibi yönlendirebilir.



Çözüm:İçerde kullanılan switch lerde Port security özelliğinin açılması

Referans: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/port_sec.html

2-)Medium:Gereksiz servislerin açık olması ve default (öntanımlı) değerleriyle hizmet vermesi;

Network te bir çok bilgisayarın snmp servisinin açık olduğu ve Readonly community olarak default değeri olan public olarak bırakıldığı tespit edilmiştir,bu açık ,bilgisayarların bir çok bilgilerinin ele geçirilmesine olanak sağlar.

ess	Host Name	MAC Address	Response Time	Hostname	Uptime
192.168.1.19		B8-AF-67-9E-3...	6 ms	HP V1910 Switc...	1298091345 (15(
192.168.3.203		CC-3E-5F-05-B...	6 ms	HP V1910 PLAN...	3748583973 (43
192.168.3.202		D0-7E-28-18-A...	10 ms	HP V1910 EGITI...	2299363009 (26(
192.168.1.122		00-C0-FF-1A-8...	0 ms		3361070004 (38
192.168.1.123		00-C0-FF-1A-4...	1 ms	HPMSA2040	3361070291 (38
192.168.1.36	NPIF192A8	00-11-0A-F1-9...	1 ms	NPIF192A8	378039690 (43d
192.168.1.190	RNKYP1	00-1A-4B-1C-8...	8 ms	RNKYP1	27312042 (3d 3h
192.168.1.251	NPI83C0A0	00-1E-0B-0A-2...	1 ms	NPI83C0A0	18018015 (2d 2h
192.168.1.252	NPI83C0A0	00-21-5A-83-C...	1 ms	NPI83C0A0	16133761 (1d 20
192.168.0.76	idea-PC.KADIF...	20-89-84-3A-3...	0 ms	idea-PC	34671441 (4d 0h

Çözüm:İlgili servisin açık olması gerekse bile default değerleri değiştirilmeli,snmp için ise snmp versiyon 3 kullanılmalıdır.

C-) DOS/DDOS açıkları

--94.102.1.96(www.kadifeteks.com)

Uygulama bazlı http Dos saldırısı gerçekleştirilmiş olup kullanılan tool slowloris perl scriptidir,web server in 5 dk süresince http isteklerine cevap verememesi sağlanmıştır.

Açıklama:slowloris uygulaması bir çok ids/ips/firewall tarafından farkedilemeyen,sunucuda ki anlık bağlantı sayısını çok fazla artırarak,maksimum anlık bağlantı sınırını doldurur,sunucunun yeni gelen isteklere cevap verememesini sağlar.Gönderilen paketler kötü amaçlı bir istek olmadığından ips gibi sistemler bunu algılayamaz.

Çözüm: aşağıdaki linkte çözüm önerileri vardır

http://www.acunetix.com/blog/articles/slow-http-dos-attacks-mitigate-apache-http-server/

D-)Webserver açıkları

--94.102.1.96(www.kadifeteks.com)

1-)Critical:Uygulama bazlı http dos saldırısı;

Detaylar yukarıda açıklanmıştır

2-)Medium:Güvensiz protokollerin kullanılması;

ftp servisi güvensiz bir protokol olup,trafiğin sniff(koklama) edilmesiyle kullanıcı adı ve paraloların ele geçirilmesine olanak sağlar.

```
20/tcp   closed ftp-data
21/tcp   open   tcpwrapped
```

Çözüm:ftp yerine sftp(kriptolu) servisin kullanılması

3-)Low:Kullanılan yazılımın/servisin tespiti

```
root@kali2016:~# ftp 94.102.1.96
Connected to 94.102.1.96.
220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
220-You are user number 2 of 50 allowed.
```

Çözüm:Yazılımın karşılama mesajının değiştirilmesi

E-)Mail Server açıkları

--192.168.1.1 (yerel ağdan)

1-)High:Smtp otantikasyonun yapılmaması;bu açık içeriden birinin istediği kişi adına istediği kişiye mail atabilmesini dolayısıyla phishing(oltalama),sosyal mühendislik(kişilerin özel bilgilerini ele geçirme vb .. gibi) ataklarına olanak tanır.

```
220 mail.kadifeteks.com
mail from:karani@kadifeteks.com
250 2.1.0 Ok
rcpt to:reha@kadifeteks.com
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
test
test
ste
.
250 2.0.0 Ok: queued as 5664D66EBB
```

Çözüm:Sadece pop3 gibi mail alma protokol otantikasyonlarının yanında mail gönderme için de smtp otantikasyonun mail server da enable edilmesi.

--212.57.17.125 mail.kadifeteks.com (internet üzerinden)

1-) High :Reverse DNS lookup açığı:Mail server da Reverse DNS kontrolü yapılmamaktadır. Bu açık kullanılarak internet üzerinden herhangi bir ip den,istenilen domain adına mail gönderilebilmektedir,Bu açık phishing(oltalama) saldırılarına olanak sağlamaktadır.

Yapılan testte billy.gates@microsoft.com dan reha@kadifeteks.com adresine başarılı bir şekilde mail atılabildiği tespit edilmiştir.

Çözüm:Mail server ya da SMTP gateway de Reverse DNS lookup özelliğinin aktif hale getirilmesi.

F-) Wireless sistemler

İç tarama ile sistemdeki,kadifeteks ve visitor wireless ağlarına aircrack-ng tool u ile saldırılar gerçekleştirilmiş olup herhangi bir bulguya rastlanmamıştır.

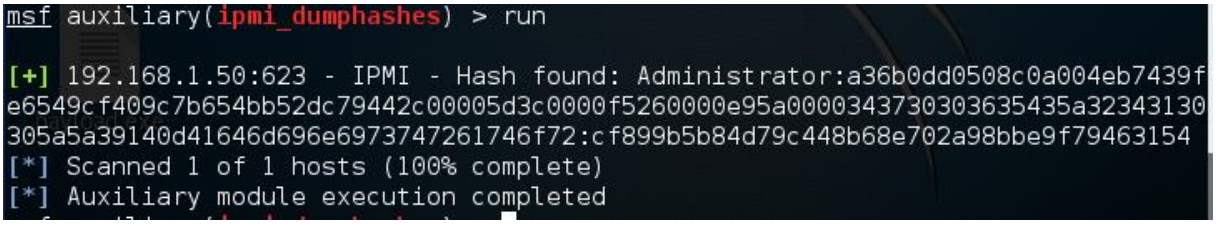
G-)Sosyal Mühendislik Testleri

Sosyal Mühendislik testleri,bir takım firma çalışanlarının mail adreslerine Social Engineering Toolkit(SET) yazılımı ile sahte domainlerden,içerisinde kurban makineye uzaktan reverse shell bağlantısı açılmasını sağlayan zararlı link bulunan sahte emailler ile yapılmıştır,ancak herhangi bir reverse shell(ters kabuk) bağlantısına ulaşılamamıştır.

H-)Vmware sistemler

--192.168.1.50

1-)High:ipmi_dumphashes açığı,bu açık uzaktan sistemin user larının hash tablolarının çıkarılmasına olanak sağlar,sonrasında hash decoder programlar kullanılarak sistem kullanıcılarının şifreleri ele geçirilebilir.



Çözüm:bu açık bilinen bir açık olup,sistem yamalarının geçilmesiyle açık kapatılabilir.

--192.168.1.60

1-)High:ipmi_dumphashes açığı,bu açık uzaktan sistemin user larının hash tablolarının çıkarılmasına olanak sağlar,sonrasında hash decoder programlar kullanılarak sistem kullanıcılarının şifreleri ele geçirilebilir.

```
msf auxiliary(ipmi_dumphashes) > run

[+] 192.168.1.60:623 - IPMI - Hash found: Administrator:93238b8e508c0a004151713d
89a67335e68e6d8d0f5bfd21d171000065600000911e000087240000343730303635435a32343039
3035424c140d41646d696e6973747261746f72:592285ae8f3ee5170f82e608789ac4e5ea1a36bf
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(ipmi_dumphashes) >
```

Çözüm:bu açık bilinen bir açık olup,sistem yamalarının geçilmesiyle açık kapatılabilir.

I-)DNS Server açıkları

--94.102.1.96

1-)Medium:Kullanılan yazılımın-programın ifşası;

Bu yazılımın üzerinde daha detaylı çalışılarak daha kompleks atakların yapılmasına olanak sağlar.

```
PORT   STATE SERVICE VERSION
53/udp open  domain  ISC BIND 9.8.2rc1 (RedHat Enterprise Linux 6)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel:6
```

Çözüm:Yazılımın/servisin karşılama mesajının değiştirilmesi

3-)SONUÇLAR VE ÖNERİLER

Yapılan çalışmalar neticesinde Özellikle internal (iç) bölgedeki açık seviyesi Critical olarak çıkmıştır,dışarıdan yapılan sızma çalışmalarının neticesi Medium seviyededir.

Öneriler aşağıdaki gibidir.

**Yama yönetiminin (patch management) yapılması, insan müdahalesine gerek duyulmadan otomatik olarak update/upgrade leri geçecek bir yazılımın kullanılması.

**İnternal (iç network) da port security veya 802.1x gibi bir yapılanmaya gidilmesi .

**Güvenilir Sertifika Otoritelerinden sertifika alınması.

**Güvensiz kriptosuz servislerin/protokollerin kullanılmaması,bunların yerine kriptolu servislerin kullanılması.

**Mail sunucuda smtp için de otantikasyonun yapılması,Reverse DNS lookup özelliğinin aktif hale getirilmesi

**Kullanılan yazılımların/servislerin markası veya versiyonun gizlenmesi.

**Uygulama bazlı DoS saldırıları için dışarıya açık sunucularda referans verilen linklerdeki çözümlerin uygulanması gerekmektedir.