T.C. SAĞLIK BAKANLIĞI
SAĞLIK BİLGİ SİSTEMLERİ
GENEL MÜDÜRLÜĞÜ

Siber Olaylara Müdahale (SOME) Birimi

KURUMSAL AĞLARDA ALINACAK GÜVENLİK ÖNLEMLERİ DOKÜMANI v.1.0

09.09.2019

İçindekiler Tablosu

Sistem Yönetimi ve Bilgi Güvenliği Dairesi Başkanlığı / Siber Olaylara Müdahale (**SOME**) Birimi FD-01-2019-05-05
Üniversiteler Mah. Dumlupınar Bul. 6001 Cad. No:9 Kat:3 06800 Çankaya / ANKARA
Tel: +90 (312) 471 83 50 Dahili 8183 – 81 86 – 81 88
some@saglik.gov.tr https://some.saglik.gov.tr

ÖZET

Bu dökümanda kurumlara ait iç ağda bulunan cihazların sıkılaştırılmasıyla ilgili adımlar yer almaktadır. İlgili sistemlerde kullanılan web, veri tabanı gibi sunucuların gerekli sıkılaştırmalarının yapılması gerekmektedir. İlgili sistemlere yapılabilecek siber saldırılar yalnızca web uygulamaları üzerinden gelmeyebilir. İlgili sistemlere iç ağlardan erişimler de dikkate alınarak gerekli sıkılaştırmaların (güvenlik ayarları, sıkılaştırmalar, güncellemeler, ağ katmanında erişim kısıtlaması vb.) yapılması büyük önem taşımaktadır:

1. Uygulamanın veri tabanı kullanıcılarının yetki kontrollerinin yapılması başta olmak üzere gerekli sıkılaştırmalarının yapılması

2. Uygulamanın çalıştığı işletim sisteminin yetki düzenlemesi baştan olmak üzere gerekli sıkılaştırmalarının yapılması

3. Ağ katmanında yalnızca ihtiyaç kapsamında gerekli izinlerin verilmesi, gerekli sıkılaştırmalarının yapılması

4. İşletim sistemi kapsamında erişimlerin ve kullanıcı hesaplarının ihtiyaca yönelik açılması, mümkünse internete çıkışın kapatılması başta olmak üzere gerekli sıkılaştırmalarının yapılması

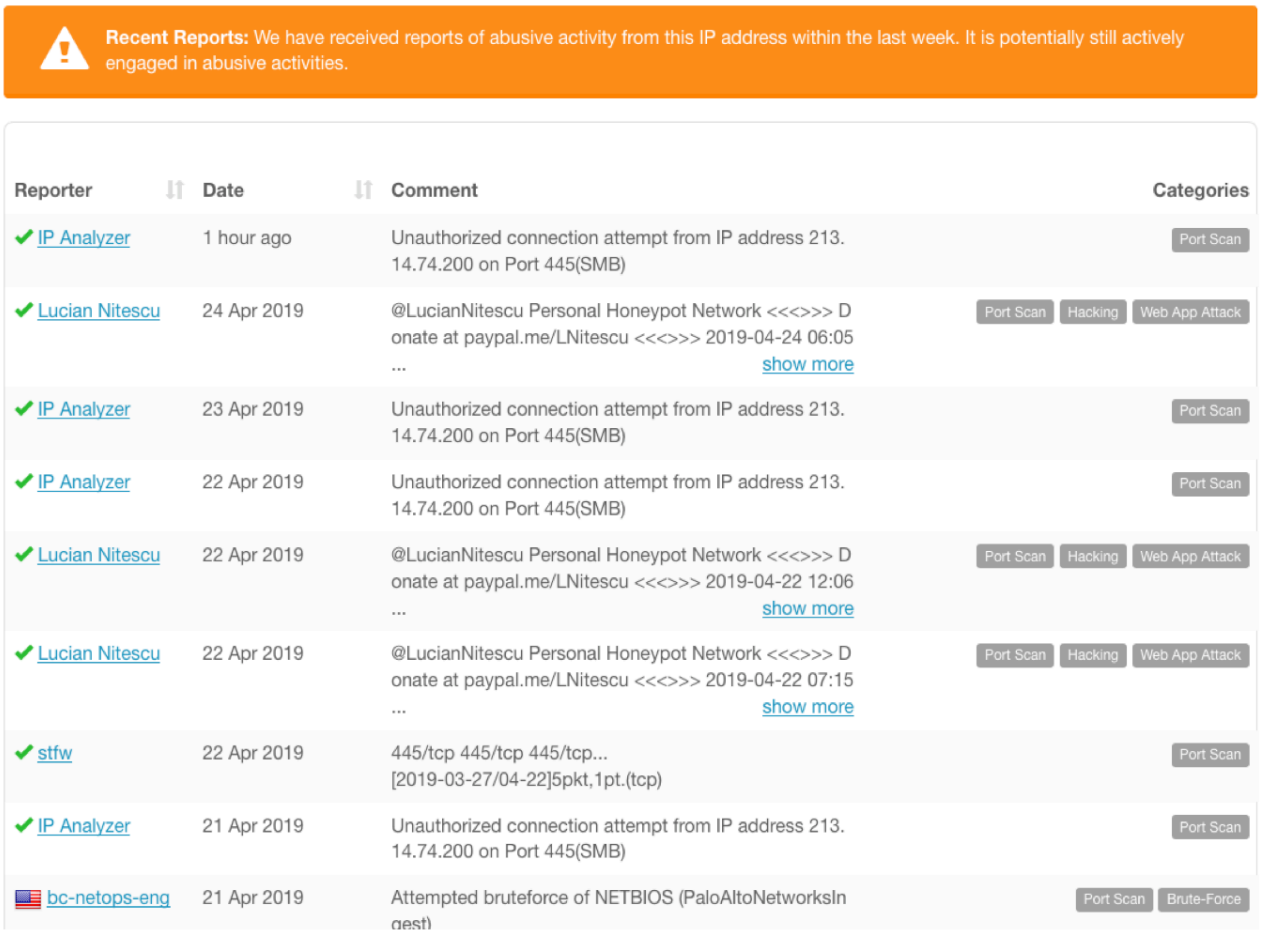
Sistem Yönetimi ve Bilgi Güvenliği Dairesi Başkanlığı / Siber Olaylara Müdahale (**SOME**) Birimi FD-01-2019-05-05
Üniversiteler Mah. Dumlupınar Bul. 6001 Cad. No:9 Kat:3 06800 Çankaya / ANKARA
Tel: +90 (312) 471 83 50 Dahili 8183 – 81 86 – 81 88
some@saglik.gov.tr https://some.saglik.gov.tr

YAPILMASI GEREKENLER

A)REEL (DIŞ) IP ADRESİ KONTROLÜ

DIŞ IP adresi üzerinden yapılan istekler kontrol edilmelidir. Aşağıdaki ekran görüntüsünde de örnek bir IP üzerinden dünya da bulunan birçok bilgisayara 445(SMB) portu üzerinden saldırı isteğinde bulunulduğu gözükmektedir. Bu IP adresi şikâyet edildiği zaman kara listeye eklenmektedir. IP belirli otoritelerce kendisine gelen bildirimlerden soran blacklict'e alınmaktadır. IP adresi kara listeden çıkarılma işlemi çok uzun sürmektedir. Yukarıda yer alan önlemler alındıktan sonra https://www.abuseipdb.com/ sitesi üzerinden dış IP adresiniz kontrol edilmelidir. Alınan önlemlerden sonra iç networkte bulunan bilgisayarlardan herhangi bir saldırı isteğinde bulunup bulunmadığı kontrolü yapılabilir. Bu kontrol güvenlik cihazı üzerinden de kontrol edilebilir. 445 Portu ile iletişim kapatıldıktan sonra dışarıya istekte bulunan bilgisayarlar bu şekilde tespit edilebilir.

https://www.abuseipdb.com/



Recent Reports: We have received reports of abusive activity from this IP address within the last week. It is potentially still actively engaged in abusive activities.

Reporter	Date	Comment	Categories
IP Analyzer	1 hour ago	Unauthorized connection attempt from IP address 213.14.74.200 on Port 445(SMB)	Port Scan
Lucian Nitescu	24 Apr 2019	@LucianNitescu Personal Honeypot Network <<<>>> Donate at paypal.me/LNitescu <<<>>> 2019-04-24 06:05 ... show more	Port Scan, Hacking, Web App Attack
IP Analyzer	23 Apr 2019	Unauthorized connection attempt from IP address 213.14.74.200 on Port 445(SMB)	Port Scan
IP Analyzer	22 Apr 2019	Unauthorized connection attempt from IP address 213.14.74.200 on Port 445(SMB)	Port Scan
Lucian Nitescu	22 Apr 2019	@LucianNitescu Personal Honeypot Network <<<>>> Donate at paypal.me/LNitescu <<<>>> 2019-04-22 12:06 ... show more	Port Scan, Hacking, Web App Attack
Lucian Nitescu	22 Apr 2019	@LucianNitescu Personal Honeypot Network <<<>>> Donate at paypal.me/LNitescu <<<>>> 2019-04-22 07:15 ... show more	Port Scan, Hacking, Web App Attack
stfw	22 Apr 2019	445/tcp 445/tcp 445/tcp... [2019-03-27/04-22]5pkt,1pt.(tcp)	Port Scan
IP Analyzer	21 Apr 2019	Unauthorized connection attempt from IP address 213.14.74.200 on Port 445(SMB)	Port Scan
bc-netops-eng	21 Apr 2019	Attempted bruteforce of NETBIOS (PaloAltoNetworksIngest)	Port Scan, Brute-Force

Sistem Yönetimi ve Bilgi Güvenliği Dairesi Başkanlığı / Siber Olaylara Müdahale (**SOME**) Birimi FD-01-2019-05-05
Üniversiteler Mah. Dumlupınar Bul. 6001 Cad. No:9 Kat:3 06800 Çankaya / ANKARA
Tel: +90 (312) 471 83 50 Dahili 8183 – 81 86 – 81 88
some@saglik.gov.tr https://some.saglik.gov.tr

Botnet bilgisayarlarla ile ilgili olarak iç ağda bulunan yukarıdaki zafiyetlerin keşfi, alınacak önlemler ve bu saldırıya tekrar maruz kalınmaması adına iç ağı daha güvenli hale getirmek için aşağıdaki adımlar uygulanmalıdır.

Saldırganlar daha çok MS17-10, oltalama saldırıları ve RDP'nin dışa açılarak basit parola kullanılmasından kaynaklı sistemlere sızmaktadırlar. Saldırganlar kullanıcıların bilgisayarını şifreleyip para istemenin yanında bilgisayarlara uzaktan kontrol komut çalıştırmaktadır. Kullanıcı farkında olmadan saldırganın yönlendirdiği yere saldırı isteğinde bulunmaktadır. Saldırgan bu şekilde kullanıcının bilgisi dışında zombi bilgisayarlar oluşturmaktadır.

B) ALINACAK ÖNLEMLER

1) Sunucuların hiçbir kontrol olmadan internete açılmaları ve iç ağda gerekli ağ izolasyonlarının yapılmaması güvenlik açısından büyük sıkıntı oluşturmaktadır. Sunucu ve bilgisayarların 21(FTP), 22(SSH), 23Telnet, 25(SMTP), 445(SMB), ve 3389(RDP) portları kapatılmalıdır. Yetkisiz erişim için kullanılabilecek bu portların internete kapatılmasına önem verilmelidir.Güvenlik duvarından dışarıdan ve içeriden erişim için sadece 80 ve 443 portuna izin verilmelidir. (Örneğin http://10.10.10.10:8090/liste/liste2.asp adresindeki gibi kullanılan portlara da izin verilebilir.) İçerde kullanılan uygulamalara göre port izinleri belirlenebilir. İç ağda kullanılan suncuların ağı, kullanıcıların kullandığı ve misafir kullanıcıların eriştiği ağ izole edilmelidir. Misafir ağına bağlanan kullanıcı iç ağda bunun hiçbir sunucuya ve kurumsal ağda bulunan cihazlara ulaşmamalıdır. Kullanılan RDP ve SSH servislerine bilgisayarı uzaktan yönetmek için bağlanma izni olan kullanıcılara SSL VPN üzerinden erişmelidir. Ayrıca RDP ve SSH bağlantıları için kullanıcılar basit parola oluşturamayacakları şekilde **Group Policy**'den parola politikası oluşturulmalıdır. Sunucudaki ve bilgisayardaki açık portları kontrol etmek için nmap programı kullanılabilir. Windows işletim sistemine kurulabilecek Zenmap(https://nmap.org/dist/nmap-7.80-setup.exe) programı kullanılabilir.
Bu portları engelledikten sonra güvenlik duvarına dışarıya saldırı isteği yapan bilgisayar varsa aşağıda belirtildiği gibi temiz kurulum yapılmalıdır. İç ağda bulunan bilgisayarlarda kullanıcılar arasında dosya paylaşımı yapılacaksa sadece izin verilen IP adreslere izin verilmelidir. Bu madde kritik önem taşımaktadır saldırıların çoğu dışa açık sunuculara gelmektedir. Burada salıdırı isteği olarak port taraması, 445 wanna cry saldırısı, karaliste de olan adreslere(IP ve URL) erişim isteği ve kritik portlara parola kırma saldırısı(TELNET,FTP,SSH,SMB ve RDP yapılmasıdır.
SMB(445) MS17-010 ve RDP(3389) BlueKepp zafiyetinden windows bilgisayarlarda yetkisiz komut çalıştırılabilmesine imkan sağlamaktadır. Bu iki zafiyet için windows bilgisayarlara gerekli güncellemelerin yüklenmesi gerekmektedir.

https://support.microsoft.com/tr-tr/help/4013389/title
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708

2) İşletim sistemi güncellemesi yapılamayacak Windows XP gibi eski işletim sistemine sahip hastanelerde kullanılan Sağlık Cihazları genel ağ yerine farklı bir segment'teki ağa dahil olmalıdır.

Kritik sunucularda farklı bir blokta yer almalıdır. (Sağlık Cihazları üzerindeki bazı cihazların işletim sistemi güncellemesi yapılamadığı için bu önlem alınmalıdır.)

3) Sunucuların dışarıya RDP bağlantısına izin verilmemelidir. Kullanıcılar özellikle dışarıdan sunucuya SSL VPN üzerinden erişmelidir. Saldırganlar RDP'ye brute-force(kaba-kuvvet saldırısı) ile saldırıp parolaya erişmeye çalışıyor. Parola elde edildikten sonra ise sunucudaki verileri şifreleyip para istemektedirler (Fidye Virüsü). Bu şekilde saldırganların sunucuya direk erişmesi engellenmiş olur. Teamviewer ve Anydesk gibi programlar izin verilmeden kullanılamamalıdır.

4) İlgili IP adresinde bulunan sunucu üzerindeki tüm Microsoft güncellemeleri yapılmalıdır. İsteği yapan kullanıcı bilgisayarıysa aşağıdaki adımları da tespit edilen kullanıcı bilgisayarlarına yapılmalıdır.

5) Sunucu bir antivirüs yazılımı ile taratılmalıdır ve sunucu üzerinde güncel bir antivirüs yazılımı kullanılmalıdır. Antivirüs belirli aralıklarla güncellemeleri yapılmalıdır.

6) Sunucuların giriş parolası güçlü olmalı, 3389(RDP), 445 portu dışarı açılmamalı ve kullanıcılar sunucuya VPN üzerinden erişmelidir. Saldırganlar RDP'ye brute-force(kaba-kuvvet saldırısı) ile saldırıp parolaya erişmeye çalışıyor. Parola elde edildikten sonra ise sunucudaki verileri şifreleyip para istemektedirler.

7) Buradaki zafiyetin adı MS17-010'dur. Saldırganlar SMB portundaki zafiyetten yararlanarak Windows bilgisayarları şifrelemektedir. Bu yüzden bilgisayarların MS17-10 yamasının geçildiğinden emin olunmalıdır.

https://support.microsoft.com/tr-tr/help/4023262/how-to-verify-that-ms17-010-is-installed

8) Kritik veriler için düzenli olarak yedeklerinin alınmalıdır.

9) https://www.abuseipdb.com sitesi üzerinden belirli aralıklarla dış IP adresinizin herhangi bir saldırı isteğinde bulunup bulunmadığı kontrolü yapılmalıdır.

Sistem Yönetimi ve Bilgi Güvenliği Dairesi Başkanlığı / Siber Olaylara Müdahale (**SOME**) Birimi FD-01-2019-05-05
Üniversiteler Mah. Dumlupınar Bul. 6001 Cad. No:9 Kat:3 06800 Çankaya / ANKARA
Tel: +90 (312) 471 83 50 Dahili 8183 – 81 86 – 81 88
some@saglik.gov.tr https://some.saglik.gov.tr

10) Aşağıda yer alan zararlı URL ve IP adresleri güvenlik duvarı tarafından engellenmelidir. Bu listeler belirli aralıklarla güncellenmektedir ve Kurumsal SOME Ekipleri ile paylaşılmaktadır.

https://www.usom.gov.tr/url-list.txt

11) Bilgisayara ya da sunuculara temiz kurulum (format) yapılacaksa aşağıdaki adımlar takip edilmelidir.

Temiz Kurulum için aşağıdaki hususlara dikkat edilmelidir;

a) Yeni kurulum için Windows 10 ya da Server 2016 işletim sistemi tercih edilmesi tavsiye edilmektedir.(Bu saldırılar özellikle Windows 7 ve Server 2008/R2 bilgisayarlara daha kolay yapılabilmektedir) Kurulum yapıldıktan sonra bilgisayarın tüm Windows güvenlik güncellemelerini yapıldığından emin olunmalıdır. Temiz kurulumda kullanılacak ISO dosyaları Micsosoft'un sitesinden indirilmelidir

(https://www.microsoft.com/tr-tr/software-download/windows10ISO).

b) Temiz kurulum işlemi yapılacak olan iso dosyası eski olabileceği için Windows işletim sistemi güncellemelerini almamış olacaktır. Bu yüzden işletim sisteminin tüm güncelleme işlemlerinin yapılması gerekmektedir.

c) Kurulumdan sonra bilgisayara lisanslı ve güncel bir antivirüs yüklenmelidir. Eğer antivirüs yüklenmeyecekse Windows 10 ve Server 2016'daki Windows Defender güncellenerek kullanılabilir. Önemli dosyalar Windows Defender'daki dosya koruma tarafına eklenildiğinde bu saldırılardan etkilenmeyecektir.

d) Temiz kurulumdan (format) sonra kurulacak programlarında güncel versiyonu kurulmalıdır.

e) Özellikle kritik verilerin bulunduğu sunucularda ya da bilgisayarlarda Windows Sandbox etkileştirilmelidir. Windows Sandbox kullanıcıların şüpheli bir uygulamayı Windows'tan yalıtılmış, sanal bir bilgisayarda çalıştırmasını sağlayan özelliğin kurulumdan sonra açılmalıdır. Windows sandbox kurulumuna http://www.mshowto.org/kurtulus-windows-sandbox-nedir.html sitesi üzerinden ulaşılabilir. Sandbox işlemi kritik önem taşıyan sunucularda yapılması önerilmektedir.

Fidye Virüsü saldırılarının yaşanmaması adına aşağıdaki önlemlerin alınmalıdır. İçerde yer alan diğer zafiyetli makinaları bulmak için aşağıda nasıl kullanılacağı anlatılan zenmap aracını kullanabilirsiniz.

Sistem Yönetimi ve Bilgi Güvenliği Dairesi Başkanlığı / Siber Olaylara Müdahale (**SOME**) Birimi FD-01-2019-05-05
Üniversiteler Mah. Dumlupınar Bul. 6001 Cad. No:9 Kat:3 06800 Çankaya / ANKARA
Tel: +90 (312) 471 83 50 Dahili 8183 – 81 86 – 81 88
some@saglik.gov.tr https://some.saglik.gov.tr

C)ZAFİYETLİ MAKİNELERİ TESPİT ETME

- Wannacry ve bunun gibi fidye virüslerinin bilgisayara bulaşmasına olanak sağlayan zafiyetin adı ms17-010 dur.
- Wannacry zafiyetinin tespiti için gerekli programın indirme linki https://nmap.org/dist/nmap-7.70-setup.exe
- Zenmap Programının Kullanımı aşağıdaki gibidir. Bu program kullanılmadan önce Windows işletim sistemindeki Güvenlik Duvarı ve anvivirüs varsa devre dışı bırakılmalıdır. Daha iyi performans için linux işletim sistemi üzerinden nmap işlemlerinin yapılması tavsiye edilmektedir.
- Çalıştırılacak Script Aşağıdaki gibidir. 10.10.10.1/24 ise örnek subnet. Birden fazla subnet girilecekse boşluk konularak yeni subnetler girilebilir.

nmap -p445 --script smb-vuln-ms17-010 10.10.10.1/24

Aşağıdaki komutlardan ikisi de aynı sonucu verir.

nmap -p445 --script smb-vuln-ms17-010 10.206.104.1-255

nmap -p445 --script smb-vuln-ms17-010 10.206.104.0/24

Yukarıdaki komut zenmap' te command ekranına yazılacak target ekranına ise taranmak istenilen IP adresi yazılması gerekmektedir. Target yerine arada boşluk konularak birden fazla IP adresi ya da IP subnetleri yazılabilir.

1) **nmap -p445 --script smb-vuln-ms17-010 10.206.104.1-255** yerine

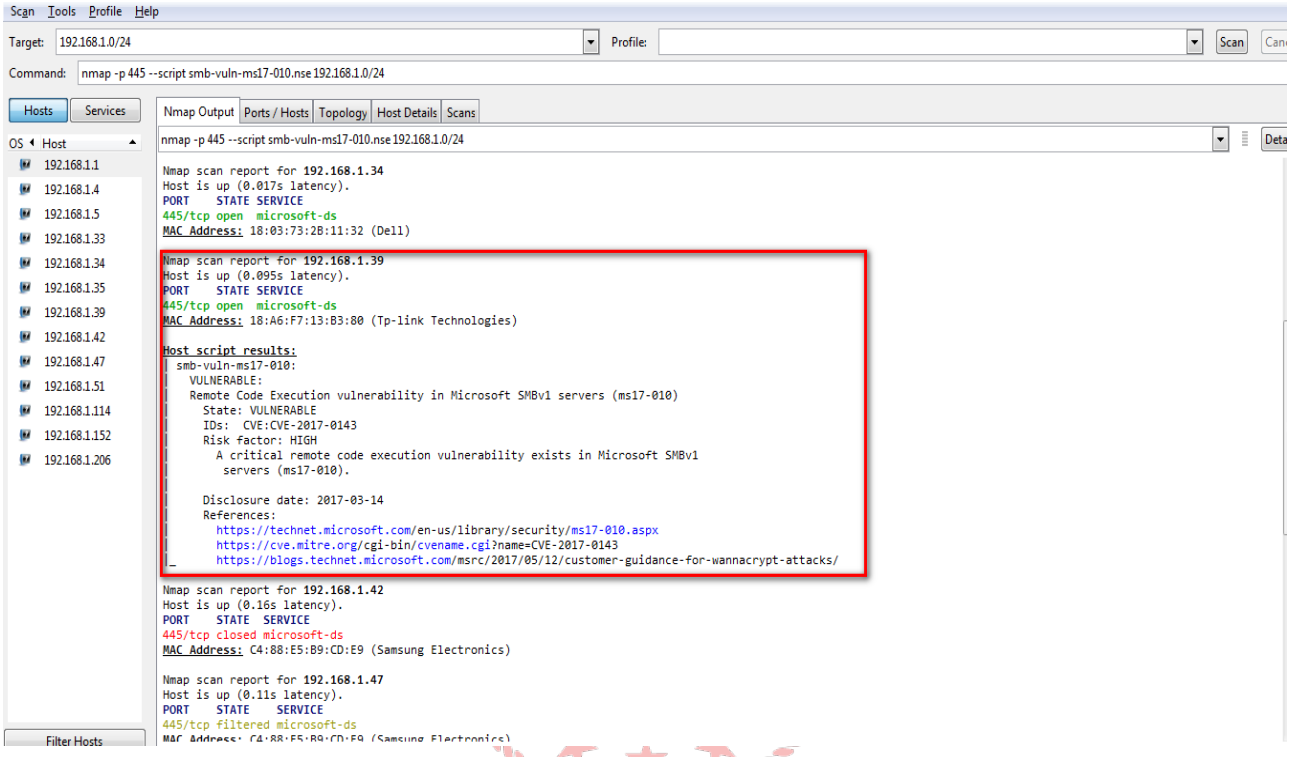
2) **nmap -p445 --script smb-vuln-ms17-010 10.206.104.0/24** (1.ye alternatif olarak buda kullanılabilir.)

3) **nmap -p445 --script smb-vuln-ms17-010 -iL C:\Users\cmd\Desktop\iplistesi.txt** (Bu şekilde subneti dosya olarakta verebilirsiniz. Subnetler alt alta olacak şekilde yapabilir. Dosya için örnek bir dizin yazdım). iplistesi.txt içerisindeki IP ve subnetler alt alta gelecek şekilde yazılmalıdır. iL parametresi kullanıldığında zenmap'te target kısmının doldurulmasına gerek yoktur.

4) **nmap -p445 --script smb-vuln-ms17-010 -iL C:\Users\cmd\Desktop\iplistesi.txt -T4** =>Taramanın daha hızlı yapılması için T4 kullanılabilir. Varsayılan olarak nmap'te -T3 parametresi ile tarama yapmaktadır. Çok hızlı bir tarama içinde -T5 parametresi de kullanılabilir.

Sistem Yönetimi ve Bilgi Güvenliği Dairesi Başkanlığı / Siber Olaylara Müdahale (**SOME**) Birimi FD-01-2019-05-05
Üniversiteler Mah. Dumlupınar Bul. 6001 Cad. No:9 Kat:3 06800 Çankaya / ANKARA
Tel: +90 (312) 471 83 50 Dahili 8183 – 81 86 – 81 88
some@saglik.gov.tr https://some.saglik.gov.tr

5) nmap -p445 --script smb-vuln-ms17-010 -iL C:\Users\cmd\Desktop\iplistesi.txt -T4 = nmap -p445 -T4 --script smb-vuln-ms17-010 -iL C:\Users\cmd\Desktop\iplistesi.txt => Argümanların kullanılması için herhangi bir sıra zorunluluğu yoktur.



Zafiyetli makina olduğu zaman Nmap Output ekranında aşağıdaki gibi çıktı verir.

```
| 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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
```

Aşağıdaki işlem Linux işletim siteminde yapılmıştır. Yukarıda gösterilen komutlar Windows işletim sistemine kurulan zenmap ile aynı işlemi görmektedir. Zenmap, nmap aracının aynısıdır. Kullanımı kolay olası açısından bir GUI ekranı bulunmaktadır.

Sistem Yönetimi ve Bilgi Güvenliği Dairesi Başkanlığı / Siber Olaylara Müdahale (**SOME**) Birimi FD-01-2019-05-05
Üniversiteler Mah. Dumlupınar Bul. 6001 Cad. No:9 Kat:3 06800 Çankaya / ANKARA
Tel: +90 (312) 471 83 50 Dahili 8183 – 81 86 – 81 88
some@saglik.gov.tr https://some.saglik.gov.tr

Aşağıda 192.168.254.99 IP adresi üzerinde nmap ile zafiyeti tespit için smb-vuln-ms17-010 script'i kullanılmıştır. Yapılan teste 192.168.254.99 IP adresinde zafiyet bulunduğu görülmektedir.

nmap -p445 --script smb-vuln-ms17-010 192.168.254.99

```
root@cmd:~# nmap -p445 --script smb-vuln-ms17-010 192.168.1.42

Starting Nmap 7.40 ( https://nmap.org ) at 2017-06-18 22:11 +03
Nmap scan report for 192.168.1.42
Host is up (0.015s latency).
PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 28:E3:47:27:66:C1 (Liteon Technology)

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://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Nmap done: 1 IP address (1 host up) scanned in 1.18 seconds
root@cmd:~#
```

Tespit edilen bilgisayarlara ilgili Windows Güncellemeleri yüklenmelidir.

(https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010)

Güncellemeler yüklendikten sonra bilgisayarın yeniden başlatılması gerekmektedir.

Güncellemenin yüklenip yüklenmediği kontrol edilmelidir.

(https://support.microsoft.com/tr-tr/help/4023262/how-to-verify-that-ms17-010-is-installed).

Doğrulama için tekrardan zenmap taraması da yapılabilir.

MS17-010 zafiyeti ile ilgili olarak saldırısı ile ilgili olarak daha ayrıntılı bilgi için aşağıdaki site incelenebilir.

https://canyoupwn.me/tr-ms17-010-zafiyeti-ve-korunma-yontemleri/

D)AĞ GÜVENLİĞİNDE KULLANILAN ZAFİYET TARAMA ARAÇLARI

Yukarıdaki yazıda yer alan nmap ağ tarama ile ağ da çalışan servislerle ilgili olarak versiyon bilgisine ve işletim sistemi tespiti için kullanılan ücretsiz açık kaynak kodlu yazılımdır. Bu yazılımı nmap betikleri(script) kullanılarak ms17-010 zafiyeti tespiti için kullanıldı. Nmap yazılımı yerine ağda bulunan tüm sistemler için zafiyet analizi yapan programlar kullanılabilir. Zafiyet keşfi için en çok kullanılan ücretli Nessus Pro ve NeXpose yazılımlarıdır. Nessus Pro ticari ürün olarak en fazla rağbet gören bir yazılımdır. https://www.tenable.com/products/nessus/nessus-professional adresinden kurumsal eposta adresi kullanılarak 1 haftalık deneme lisans koduna erişilebilir.

Bu iki yazılıma alternatif olarak Openvas programı kullanılabilir. Openvas(http://openvas.org) ağda bulunan tüm zafiyetleri tarar ve raporlama işlemini gerçekleştirir.

Nessus Pro Kurulum ve Kullanımı

http://www.mshowto.org/nessus-kurulumu-ve-nessus-ile-network-penetration-test.html

Openvas Kurulum ve Kullanımı

https://www.cozumpark.com/kali-linux-uzerinde-openvas-kurulumu-ve-kullanimi/