Nmap Post Port Scans

Task 1 Introduction (Görev 1 Giriş)

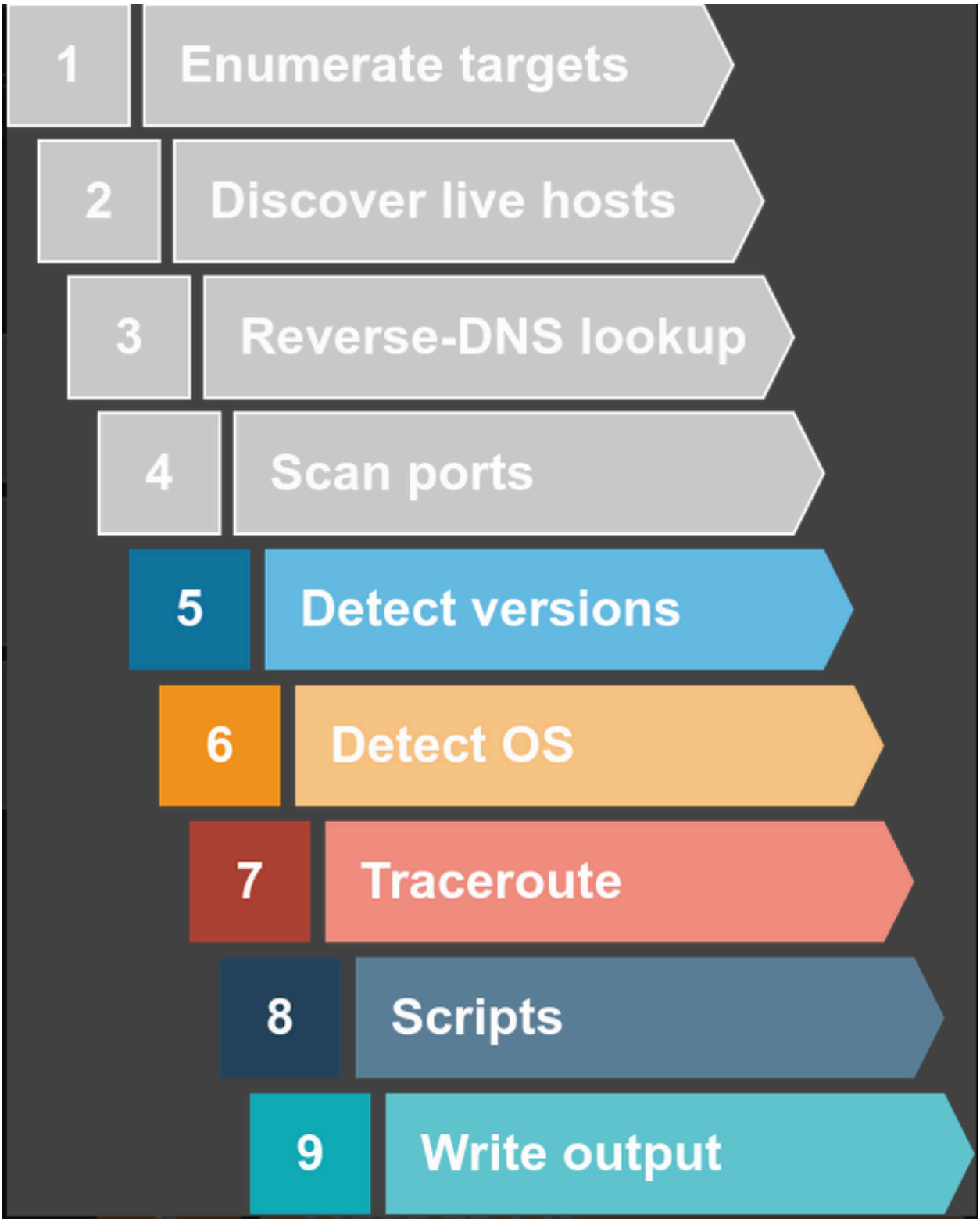
Bu oda, Nmap serisinin (Ağ Güvenliğine Giriş modülünün bir parçası) sonuncusudur. Bu odada, port taramasını takip eden adımlara odaklanıyoruz: özellikle, hizmet algılama, işletim sistemi algılama, Nmap komut dosyası motoru ve tarama sonuçlarını kaydetme.

1. Nmap Live Host Discovery (Nmap Canlı Ana Bilgisayar Keşfi)
2. Nmap Basic Port Scans (Nmap Temel Port Taramaları)
3. Nmap Advanced Port Scans (Nmap Gelişmiş Port Taramaları)
4. Nmap Post Port Scans (Nmap Post Port Taramaları)

Bu serinin ilk odasında, Nmap'in hedefleri nasıl listeleyebileceğini, canlı ana bilgisayarları nasıl keşfedebileceğini ve ilginç isimleri bulmak için ters-DNS'yi nasıl kullanabileceğini öğrendik. Serinin ikinci ve üçüncü odaları ağ portları için temel ve gelişmiş tarama türlerine odaklandı.

Son odada, aşağıdaki şekilde gösterildiği gibi, Nmap'in nasıl kullanılabileceğine odaklanıyoruz:

- Detect versions of the running services (on all open ports) (Çalışan hizmetlerin sürümlerini tespit edin (tüm açık portlarda))
- Detect the OS based on any signs revealed by the target (Hedef tarafından ortaya çıkarılan herhangi bir işarete dayanarak işletim sistemini tespit edin)
- Run Nmap’s traceroute (Nmap'in traceroute'unu çalıştırın)
- Run select Nmap scripts (Seçili Nmap komut dosyalarını çalıştırın)
- Save the scan results in various formats (Tarama sonuçlarını çeşitli formatlarda kaydedin)



Bu oda bu adımlara ve port taramasından sonra bunların nasıl yürütüleceğine odaklanacaktır.

Soru ⇒ Nmap taramasının nasıl ilerlediğini ve izlediği adımları ve aşamaları sağlam bir şekilde anladığınızdan emin olun. AttackBox'ı Başlat düğmesini kullanarak AttackBox'ı başlatın, çünkü daha sonraki görevlerdeki soruları yanıtlamak için buna ihtiyacınız olacak.

Cevap ⇒ Cevap Gerekmemektedir.

Task 2 Service Detection (Görev 2 Hizmet Tespiti)

Nmap açık portları keşfettiğinde, çalışan servisi tespit etmek için mevcut portu araştırabilirsiniz. Açık portların daha fazla araştırılması, pentester hizmetin bilinen herhangi bir güvenlik açığı olup olmadığını öğrenmek için kullanabileceği için önemli bir bilgi parçasıdır. Güvenlik açığı olan hizmetleri arama hakkında daha fazla bilgi edinmek için Güvenlik Açıkları 101'e katılın.

Nmap komutunuza -sV eklemek, açık portlar için servis ve sürüm bilgilerini toplayacak ve belirleyecektir. Yoğunluğu --version-intensity LEVEL ile kontrol edebilirsiniz; burada seviye en hafif olan 0 ile en eksiksiz olan 9 arasında değişir. -sV --version-light 2 yoğunluğa sahipken, -sV --version-all 9 yoğunluğa sahiptir.

sV kullanımının Nmap'i TCP 3 yönlü el sıkışmasına devam etmeye ve bağlantı kurmaya zorlayacağına dikkat etmek önemlidir. Bağlantı kurulması gereklidir çünkü Nmap tam olarak bir bağlantı kurmadan ve dinleyen servisle iletişim kurmadan sürümü keşfedemez. Başka bir deyişle, -sV seçeneği seçildiğinde gizli SYN taraması -sS mümkün değildir.

Aşağıdaki konsol çıktısı -sV seçeneği ile basit bir Nmap gizli SYN taramasını göstermektedir. sV seçeneğinin eklenmesi, çıktıda tespit edilen her hizmet için sürümü gösteren yeni bir sütuna yol açar. Örneğin, TCP bağlantı noktası 22'nin açık olması durumunda, 22/tcp open ssh yerine 22/tcp open ssh OpenSSH 6.7p1 Debian 5+deb8u8 (protokol 2.0) elde ederiz. TCP port 22 açık olduğu için SSH protokolünün servis olarak tahmin edildiğine dikkat edin; Nmap'in onaylamak için port 22'ye bağlanması gerekmedi. Ancak -sV, hizmet başlığını ve nginx 1.6.2 gibi alabileceği herhangi bir sürüm bilgisini almak için bu açık bağlantı noktasına bağlanmayı gerektirdi. Dolayısıyla, hizmet sütununun aksine, sürüm sütunu bir tahmin değildir.

```
pentester@TryHackMe$ sudo nmap -sV MACHINE_IPStarting Nmap 7.60 ( htt
ps://nmap.org ) at 2021-09-10 05:03 BST
Nmap scan report for MACHINE_IP
Host is up (0.0040s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 6.7p1 Debian 5+deb8u8 (protocol 2.0)
25/tcp  open  smtp    Postfix smtpd
80/tcp  open  http    nginx 1.6.2
110/tcp open  pop3    Dovecot pop3d
111/tcp open  rpcbind 2-4 (RPC #100000)
MAC Address: 02:A0:E7:B5:B6:C5 (Unknown)
Service Info: Host:  debra2.thm.local; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nm
ap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.40 seconds
```

Birçok Nmap seçeneğinin root ayrıcalıkları gerektirdiğini unutmayın. Nmap'i root olarak çalıştırmadığınız sürece, yukarıdaki örnekte olduğu gibi sudo kullanmanız gerekir.

Sanal makineyi başlatın. Hazır olduğunda, aşağıdaki soruları yanıtlamak için AttackBox üzerindeki terminali açın.

Soru ⇒ Bu görev için hedef makineyi başlatın ve AttackBox'ı başlatın. AttackBox üzerinden nmap -sV --version-light MACHINE_IP komutunu çalıştırın. Port 143 için algılanan sürüm nedir?

Cevap ⇒ Dovecot imapd

Soru ⇒ Hangi hizmetin --version-light ile algılanan bir sürümü yoktu?

Cevap ⇒ rpcbind

Task 3 OS Detection and Traceroute (Görev 3 İşletim Sistemi Algılama ve Traceroute)

OS Detection (İşletim Sistemi Algılama)

Nmap, İşletim Sistemini (OS) davranışına ve yanıtlarındaki herhangi bir belirtiye dayanarak tespit edebilir. OS tespiti -O kullanılarak etkinleştirilebilir; bu OS'de olduğu gibi büyük O harfidir. Bu örnekte, AttackBox üzerinde nmap -sS -O MACHINE_IP komutunu çalıştırdık. Nmap işletim sisteminin Linux 3.X olduğunu tespit etti ve daha sonra 3.13 çekirdeğini çalıştırdığını tahmin etti.

```
pentester@TryHackMe$ sudo nmap -sS -O MACHINE_IPStarting Nmap 7.60 ( https://nmap.org ) at 2021-09-10 05:04 BST
Nmap scan report for MACHINE_IP
Host is up (0.00099s latency).
Not shown: 994 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
80/tcp  open  http
110/tcp open  pop3
111/tcp open  rpcbind
143/tcp open  imap
MAC Address: 02:A0:E7:B5:B6:C5 (Unknown)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3.13
OS details: Linux 3.13
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.91 seconds
```

Taradığımız ve işletim sistemi sürümünü tespit etmeye çalıştığımız sistem 3.16 kernel sürümünü çalıştırıyor. Nmap bu durumda yakın bir tahmin yapabildi. Başka bir durumda, 5.13.14 çekirdekli bir Fedora Linux sistemini taradık; ancak Nmap

bunu Linux 2.6.X olarak algıladı. İyi haber şu ki, Nmap işletim sistemini doğru algıladı; o kadar da iyi olmayan haber ise çekirdek sürümünün yanlış olmasıydı.

İşletim sistemi tespiti çok kullanışlıdır, ancak birçok faktör doğruluğunu etkileyebilir. Her şeyden önce, Nmap'in güvenilir bir tahminde bulunabilmesi için hedef üzerinde en az bir açık ve bir kapalı port bulması gerekir. Ayrıca, sanallaştırma ve benzeri teknolojilerin artan kullanımı nedeniyle konuk işletim sistemi parmak izleri bozulabilir. Bu nedenle, işletim sistemi sürümünü her zaman bir tuz tanesi ile alın.

Traceroute

Nmap'in sizinle hedef arasındaki yönlendiricileri bulmasını istiyorsanız, --traceroute eklemeniz yeterlidir. Aşağıdaki örnekte, Nmap tarama sonuçlarına bir traceroute eklemiştir. Nmap'in traceroute'unun Linux ve macOS'ta bulunan traceroute komutundan veya MS Windows'ta bulunan tracert'ten biraz farklı çalıştığını unutmayın. Standart traceroute düşük TTL'li (Time to Live) bir paketle başlar ve hedefe ulaşana kadar artmaya devam eder. Nmap'in traceroute'u yüksek TTL'li bir paketle başlar ve bunu azaltmaya devam eder.

Aşağıdaki örnekte, AttackBox üzerinde nmap -sS --traceroute MACHINE_IP komutunu çalıştırdık. Doğrudan bağlı oldukları için ikisi arasında herhangi bir yönlendirici/atlama olmadığını görebiliriz.

```
pentester@TryHackMe$ sudo nmap -sS --traceroute MACHINE_IPStarting Nm
ap 7.60 ( https://nmap.org ) at 2021-09-10 05:05 BST
Nmap scan report for MACHINE_IP
Host is up (0.0015s latency).
Not shown: 994 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
80/tcp  open  http
110/tcp open  pop3
111/tcp open  rpcbind
143/tcp open  imap
MAC Address: 02:A0:E7:B5:B6:C5 (Unknown)
```

```
TRACEROUTE
HOP RTT     ADDRESS
1   1.48 ms MACHINE_IP

Nmap done: 1 IP address (1 host up) scanned in 1.59 seconds
```

Birçok yönlendiricinin ICMP Time-to-Live aşımı göndermeyecek şekilde yapılandırıldığını belirtmek gerekir, bu da IP adreslerini keşfetmemizi engelleyecektir. Daha fazla bilgi için Aktif Keşif odasını ziyaret edin.

Soru ⇒ MACHINE_IP'ye karşı -O seçeneği ile nmap çalıştırın. Nmap hangi işletim sistemini tespit etti?

Cevap ⇒ Linux

Task 4 Nmap Scripting Engine (NSE) (Görev 4 Nmap Komut Dosyası Motoru (NSE))

Kod, derlenmesi gerekmeyen bir kod parçasıdır. Başka bir deyişle, orijinal insan tarafından okunabilir formunda kalır ve makine diline dönüştürülmesi gerekmez. Birçok program komut dosyaları aracılığıyla ek işlevsellik sağlar; dahası, komut dosyaları yerleşik komutlar aracılığıyla mevcut olmayan özel işlevsellik eklemeyi mümkün kılar. Benzer şekilde, Nmap Lua dilini kullanan komut dosyaları için destek sağlar. Nmap'in bir parçası olan Nmap Scripting Engine (NSE), Nmap'in Lua dilinde yazılmış Nmap komut dosyalarını yürütmesini sağlayan bir Lua yorumlayıcısıdır. Ancak, Nmap komut dosyalarından yararlanmak için Lua öğrenmemize gerek yoktur.

Nmap varsayılan kurulumunuz kolayca 600'e yakın komut dosyası içerebilir. Nmap kurulum klasörünüze bir göz atın. AttackBox'ta /usr/share/nmap/scripts adresindeki dosyaları kontrol ettiğinizde, hedefledikleri protokolle başlayan yüzlerce komut dosyası olduğunu göreceksiniz. AttackBox üzerinde HTTP ile başlayan tüm betikleri aşağıdaki konsol çıktısında listeledik; http ile başlayan yaklaşık 130 betik bulduk. Gelecekteki güncellemelerle, yüklü komut dosyası sayısının artmasını bekleyebilirsiniz.

```
pentester@AttackBox /usr/share/nmap/scripts# ls http*
http-adobe-coldfusion-apsa1301.nse      http-passwd.nse
http-affiliate-id.nse                   http-php-version.nse
http-apache-negotiation.nse             http-phpmyadmin-dir-traversal.nse
http-apache-server-status.nse           http-phpself-xss.nse
http-aspnet-debug.nse                   http-proxy-brute.nse
http-auth-finder.nse                    http-put.nse
http-auth.nse                           http-qnap-nas-info.nse
http-avaya-ipoffice-users.nse           http-referer-checker.nse
http-awstatstotals-exec.nse             http-rfi-spider.nse
http-axis2-dir-traversal.nse            http-robots.txt.nse
http-backup-finder.nse                  http-robtex-reverse-ip.nse
http-barracuda-dir-traversal.nse        http-robtex-shared-ns.nse
http-brute.nse                          http-security-headers.nse
http-cakephp-version.nse                http-server-header.nse
http-chrono.nse                         http-shellshock.nse
http-cisco-anyconnect.nse               http-sitemap-generator.nse
http-coldfusion-subzero.nse             http-slowloris-check.nse
http-comments-displayer.nse             http-slowloris.nse
http-config-backup.nse                  http-sql-injection.nse
http-cookie-flags.nse                   http-stored-xss.nse
http-cors.nse                           http-svn-enum.nse
http-cross-domain-policy.nse            http-svn-info.nse
http-csrf.nse                           http-title.nse
http-date.nse                           http-tplink-dir-traversal.nse
http-default-accounts.nse               http-trace.nse
http-devframework.nse                   http-traceroute.nse
http-dlink-backdoor.nse                 http-unsafe-output-escaping.nse
http-dombased-xss.nse                   http-useragent-tester.nse
http-domino-enum-passwords.nse          http-userdir-enum.nse
http-drupal-enum-users.nse              http-vhosts.nse
http-drupal-enum.nse                    http-virustotal.nse
http-enum.nse                           http-vlcstreamer-ls.nse
http-errors.nse                         http-vmware-path-vuln.nse
http-exif-spider.nse                    http-vuln-cve2006-3392.nse
```

```
http-favicon.nse                    http-vuln-cve2009-3960.nse
http-feed.nse                       http-vuln-cve2010-0738.nse
http-fetch.nse                      http-vuln-cve2010-2861.nse
http-fileupload-exploiter.nse       http-vuln-cve2011-3192.nse
http-form-brute.nse                 http-vuln-cve2011-3368.nse
http-form-fuzzer.nse                http-vuln-cve2012-1823.nse
http-frontpage-login.nse            http-vuln-cve2013-0156.nse
http-generator.nse                  http-vuln-cve2013-6786.nse
http-git.nse                        http-vuln-cve2013-7091.nse
http-gitweb-projects-enum.nse       http-vuln-cve2014-2126.nse
http-google-malware.nse             http-vuln-cve2014-2127.nse
http-grep.nse                       http-vuln-cve2014-2128.nse
http-headers.nse                    http-vuln-cve2014-2129.nse
http-huawei-hg5xx-vuln.nse          http-vuln-cve2014-3704.nse
http-icloud-findmyiphone.nse        http-vuln-cve2014-8877.nse
http-icloud-sendmsg.nse             http-vuln-cve2015-1427.nse
http-iis-short-name-brute.nse       http-vuln-cve2015-1635.nse
http-iis-webdav-vuln.nse            http-vuln-cve2017-1001000.nse
http-internal-ip-disclosure.nse     http-vuln-cve2017-5638.nse
http-joomla-brute.nse               http-vuln-cve2017-5689.nse
http-litespeed-sourcecode-download.nse  http-vuln-cve2017-8917.nse
http-ls.nse                         http-vuln-misfortune-cookie.nse
http-majordomo2-dir-traversal.nse   http-vuln-wnr1000-creds.nse
http-malware-host.nse               http-waf-detect.nse
http-mcmp.nse                       http-waf-fingerprint.nse
http-method-tamper.nse              http-webdav-scan.nse
http-methods.nse                    http-wordpress-brute.nse
http-mobileversion-checker.nse      http-wordpress-enum.nse
http-ntlm-info.nse                  http-wordpress-users.nse
http-open-proxy.nse                 http-xssed.nse
http-open-redirect.nse
```

Bu yüklü komut dosyalarından herhangi birini veya bir grubunu kullanmayı belirleyebilirsiniz; dahası, diğer kullanıcıların komut dosyalarını yükleyebilir ve taramalarınız için kullanabilirsiniz. Varsayılan komut dosyalarıyla başlayalım. Varsayılan kategorideki komut dosyalarını --script=default kullanarak veya sadece

-sC ekleyerek çalıştırmayı seçebilirsiniz. Varsayılana ek olarak, kategoriler arasında auth, broadcast, brute, default, discovery, dos, exploit, external, fuzzer, intrusive, malware, safe, version ve vuln bulunur. Kısa bir açıklama aşağıdaki tabloda gösterilmektedir.

Script Category	Description
`auth`	Authentication related scripts
`broadcast`	Discover hosts by sending broadcast messages
`brute`	Performs brute-force password auditing against logins
`default`	Default scripts, same as `-sC`
`discovery`	Retrieve accessible information, such as database tables and DNS names
`dos`	Detects servers vulnerable to Denial of Service (DoS)
`exploit`	Attempts to exploit various vulnerable services
`external`	Checks using a third-party service, such as Geoplugin and Virustotal
`fuzzer`	Launch fuzzing attacks
`intrusive`	Intrusive scripts such as brute-force attacks and exploitation
`malware`	Scans for backdoors
`safe`	Safe scripts that won’t crash the target
`version`	Retrieve service versions
`vuln`	Checks for vulnerabilities or exploit vulnerable services

Bazı komut dosyaları birden fazla kategoriye aittir. Dahası, bazı betikler hizmetlere karşı kaba kuvvet saldırıları başlatırken, diğerleri DoS saldırıları başlatır ve sistemleri istismar eder. Bu nedenle, hizmetleri çökertmek veya istismar etmek istemiyorsanız, çalıştırılacak komut dosyalarını seçerken dikkatli olmak çok önemlidir.

MACHINE_IP'ye karşı bir SYN taraması yapmak ve aşağıda gösterilen konsolda varsayılan komut dosyalarını çalıştırmak için Nmap kullanıyoruz. Komut sudo nmap -sS -sC MACHINE_IP şeklindedir, burada -sC Nmap'in SYN taramasını takiben varsayılan komut dosyalarını çalıştırmasını sağlayacaktır. Aşağıda görünen yeni ayrıntılar var. Port 22'deki SSH hizmetine bir göz atın; Nmap çalışan sunucuyla ilgili dört genel anahtarın tümünü kurtarmıştır. Başka bir örnek olarak 80 numaralı

bağlantı noktasındaki HTTP hizmetini ele alalım; Nmap varsayılan sayfa başlığını aldı. Sayfanın varsayılan olarak bırakıldığını görebiliriz.

```
pentester@TryHackMe$ sudo nmap -sS -sC MACHINE_IPStarting Nmap 7.60 ( https://nmap.org ) at 2021-09-10 05:08 BST
Nmap scan report for ip-10-10-161-170.eu-west-1.compute.internal (10.10.161.170)
Host is up (0.0011s latency).
Not shown: 994 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
| ssh-hostkey:
|   1024 d5:80:97:a3:a8:3b:57:78:2f:0a:78:ae:ad:34:24:f4 (DSA)
|   2048 aa:66:7a:45:eb:d1:8c:00:e3:12:31:d8:76:8e:ed:3a (RSA)
|   256 3d:82:72:a3:07:49:2e:cb:d9:87:db:08:c6:90:56:65 (ECDSA)
|_  256 dc:f0:0c:89:70:87:65:ba:52:b1:e9:59:f7:5d:d2:6a (EdDSA)
25/tcp  open  smtp
|_smtp-commands: debra2.thm.local, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
| ssl-cert: Subject: commonName=debra2.thm.local
| Not valid before: 2021-08-10T12:10:58
|_Not valid after:  2031-08-08T12:10:58
|_ssl-date: TLS randomness does not represent time
80/tcp  open  http
|_http-title: Welcome to nginx on Debian!
110/tcp open  pop3
|_pop3-capabilities: RESP-CODES CAPA TOP SASL UIDL PIPELINING AUTH-RESP-CODE
111/tcp open  rpcbind
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4       111/tcp  rpcbind
|   100000  2,3,4       111/udp  rpcbind
|   100024  1         38099/tcp  status
|_  100024  1         54067/udp  status
143/tcp open  imap
```

```
|_imap-capabilities: LITERAL+ capabilities IMAP4rev1 OK Pre-login ENABLE ha
ve LOGINDISABLEDA0001 listed SASL-IR ID more post-login LOGIN-REFERRAL
S IDLE
MAC Address: 02:A0:E7:B5:B6:C5 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 2.21 seconds
```

Ayrıca --script "SCRIPT-NAME" veya ftp-brute içeren --script "ftp*" gibi bir kalıp kullanarak betiği adıyla da belirtebilirsiniz. Bir betiğin ne yaptığından emin değilseniz, betik dosyasını less gibi bir metin okuyucu veya bir metin düzenleyici ile açabilirsiniz. ftp-brute dosyasında şöyle yazıyor: "FTP sunucularına karşı kaba kuvvet parola denetimi gerçekleştirir." Bazı betikler oldukça müdahaleci olduğu için dikkatli olmalısınız. Dahası, bazı betikler belirli bir sunucu için olabilir ve rastgele seçilirse hiçbir fayda sağlamadan zamanınızı boşa harcayacaktır. Her zamanki gibi, hedef sunucuda bu tür testleri başlatma yetkiniz olduğundan emin olun.

Http sunucusunun tarih ve saatini alacağını tahmin ettiğimiz http-date adlı iyi huylu bir betiği ele alalım ve bu gerçekten de açıklamasında doğrulanmaktadır: "HTTP benzeri servislerden tarihi alır. Ayrıca, tarihin yerel saatten ne kadar farklı olduğunu yazdırır..." AttackBox üzerinde, aşağıdaki konsolda gösterildiği gibi sudo nmap -sS -n --script "http-date" MACHINE_IP komutunu çalıştırıyoruz.

```
pentester@TryHackMe$ sudo nmap -sS -n --script "http-date" MACHINE_IPSt
arting Nmap 7.60 ( https://nmap.org ) at 2021-09-10 08:04 BST
Nmap scan report for MACHINE_IP
Host is up (0.0011s latency).
Not shown: 994 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
80/tcp  open  http
|_http-date: Fri, 10 Sep 2021 07:04:26 GMT; 0s from local time.
110/tcp open  pop3
111/tcp open  rpcbind
143/tcp open  imap
MAC Address: 02:44:87:82:AC:83 (Unknown)
```

```
Nmap done: 1 IP address (1 host up) scanned in 1.78 seconds
```

Son olarak, Nmap'in işlevselliğini resmi Nmap betiklerinin ötesine genişletebilirsiniz; betiğinizi yazabilir veya İnternet'ten Nmap betikleri indirebilirsiniz. İnternetten bir Nmap betiği indirmek ve kullanmak belirli bir düzeyde risk taşır. Bu nedenle, güvenmediğiniz bir yazardan gelen bir betiği çalıştırmamak iyi bir fikirdir.

Soru ⇒ Nmap komut dosyalarının AttackBox üzerinde /usr/share/nmap/scripts dosyasına kaydedildiğini bilerek. http-robots.txt betiği neyi kontrol eder?

Cevap ⇒ disallowed entries

Soru ⇒ MS15-034 (CVE2015-1635) uzaktan kod çalıştırma güvenlik açığını kontrol eden betiğin adını bulabilir misiniz (İpucu ⇒ Bu komut dosyası HTTP kapsamına girer.)?

Cevap ⇒http-vuln-cve2015-1635

Soru ⇒ Henüz başlatmadıysanız AttackBox'ı başlatın. Sanal makineyi Görev 2'den sonlandırdığınızdan emin olduktan sonra, bu görev için hedef makineyi başlatın. AttackBox üzerinde, Nmap'i varsayılan komut dosyaları -sC ile MACHINE_IP'ye karşı çalıştırın. Port 53'ü dinleyen bir servis olduğunu fark edeceksiniz. Tam sürüm değeri nedir?

Cevap ⇒ 9.18.28-1~deb12u2-Debian

Soru ⇒ Açıklamasına göre, ssh2-enum-algos betiği "hedef SSH2 sunucusunun sunduğu algoritma sayısını (şifreleme, sıkıştırma vb. için) bildirir." SHA2-512'ye dayanan ve MACHINE_IP tarafından desteklenen sunucu ana bilgisayar anahtar algoritmasının adı nedir(İpucu ⇒ Şu komutu çalıştırın: nmap -script "ssh2-enum-algos" MACHINE_IP)?

Cevap ⇒ rsa-sha2-512

Task 5 Saving the Output (Görev 5 Çıktıyı Kaydetme)

Ne zaman bir Nmap taraması yapsanız, sonuçları bir dosyaya kaydetmek mantıklıdır. Dosya adlarınız için iyi bir adlandırma kuralı seçmek ve benimsemek de çok önemlidir. Dosya sayısı hızla artabilir ve önceki bir tarama sonucunu bulmanızı engelleyebilir. Üç ana format şunlardır:

1. Normal
2. Grepable (`grep`able)
3. XML

Tavsiye edemeyeceğimiz dördüncü bir tane daha var:

- Script Kiddie

Normal

Adından da anlaşılacağı gibi, normal format bir hedefi tararken ekranda aldığınız çıktıya benzer. Taramanızı -oN FILENAME kullanarak normal formatta kaydedebilirsiniz; N normal anlamına gelir. İşte sonucun bir örneği.

```
pentester@TryHackMe$ cat MACHINE_IP_scan.nmap # Nmap 7.60 scan initiat
ed Fri Sep 10 05:14:19 2021 as: nmap -sS -sV -O -oN MACHINE_IP_scan MAC
HINE_IPNmap scan report for MACHINE_IP
Host is up (0.00086s latency).
Not shown: 994 closed ports
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 6.7p1 Debian 5+deb8u8 (protocol 2.0)
25/tcp  open  smtp    Postfix smtpd
80/tcp  open  http    nginx 1.6.2
110/tcp open  pop3    Dovecot pop3d
111/tcp open  rpcbind 2-4 (RPC #100000)
143/tcp open  imap    Dovecot imapd
MAC Address: 02:A0:E7:B5:B6:C5 (Unknown)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3.13
OS details: Linux 3.13
Network Distance: 1 hop
Service Info: Host:  debra2.thm.local; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
OS and Service detection performed. Please report any incorrect results at htt
ps://nmap.org/submit/ .
# Nmap done at Fri Sep 10 05:14:28 2021 -- 1 IP address (1 host up) scanned i
n 9.99 seconds
```

Grepable

Grepable formatı adını grep komutundan alır; grep, Global Regular Expression Printer anlamına gelir. Basit bir ifadeyle, tarama çıktısını belirli anahtar kelimeler veya terimler için filtrelemeyi verimli hale getirir. Tarama sonucunu -oG FILENAME kullanarak grepable formatında kaydedebilirsiniz. Yukarıda normal formatta görüntülenen tarama çıktısı, grepable format kullanılarak aşağıdaki konsolda gösterilir. Normal çıktı 21 satırdır; ancak greplenebilir çıktı yalnızca 4 satırdır. Bunun temel nedeni, Nmap'in kullanıcı grep uyguladığında her satırı anlamlı ve eksiksiz hale getirmek istemesidir. Sonuç olarak, greplenebilir çıktıda satırlar çok uzundur ve normal çıktıya kıyasla okunması uygun değildir.

```
pentester@TryHackMe$ cat MACHINE_IP_scan.gnmap # Nmap 7.60 scan initi
ated Fri Sep 10 05:14:19 2021 as: nmap -sS -sV -O -oG MACHINE_IP_scan MA
CHINE_IPHost: MACHINE_IP Status: Up
Host: MACHINE_IP Ports: 22/open/tcp//ssh//OpenSSH 6.7p1 Debian 5+deb8u8
(protocol 2.0)/, 25/open/tcp//smtp//Postfix smtpd/, 80/open/tcp//http//nginx 1.
6.2/, 110/open/tcp//pop3//Dovecot pop3d/, 111/open/tcp//rpcbind//2-4 (RPC #1
00000)/, 143/open/tcp//imap//Dovecot imapd/  Ignored State: closed (994)  O
S: Linux 3.13   Seq Index: 257   IP ID Seq: All zeros
# Nmap done at Fri Sep 10 05:14:28 2021 -- 1 IP address (1 host up) scanned i
n 9.99 seconds
```

Örnek bir grep kullanımı grep KEYWORD TEXT_FILE şeklindedir; bu komut verilen anahtar kelimeyi içeren tüm satırları görüntüleyecektir. Normal çıktı ve greplenebilir çıktı üzerinde grep kullanmanın çıktısını karşılaştıralım. Birincisinin ana bilgisayarın IP adresini vermediğini fark edeceksiniz. Bunun yerine, 80/tcp open http nginx 1.6.2 döndürür, bu da birden fazla sistemin tarama sonuçlarını inceliyorsanız çok elverişsiz hale getirir. Bununla birlikte, ikincisi, her satırda ana bilgisayarın IP adresi gibi eksiksiz olması için yeterli bilgi sağlar.

```
pentester@TryHackMe$ grep http MACHINE_IP_scan.nmap 80/tcp  open  http
nginx 1.6.2
OS and Service detection performed. Please report any incorrect results at htt
ps://nmap.org/submit/ .
```

```
pentester@TryHackMe$ grep http MACHINE_IP_scan.gnmap Host: MACHINE_
IP Ports: 22/open/tcp//ssh//OpenSSH 6.7p1 Debian 5+deb8u8 (protocol 2.0)/,
25/open/tcp//smtp//Postfix smtpd/, 80/open/tcp//http//nginx 1.6.2/, 110/open/t
cp//pop3//Dovecot pop3d/, 111/open/tcp//rpcbind//2-4 (RPC #100000)/, 143/o
pen/tcp//imap//Dovecot imapd/   Ignored State: closed (994)  OS: Linux 3.13
Seq Index: 257   IP ID Seq: All zeros
```

XML

Üçüncü format XML'dir. Tarama sonuçlarını -oX FILENAME kullanarak XML formatında kaydedebilirsiniz. XML formatı, çıktıyı diğer programlarda işlemek için en uygun format olacaktır. Yeterince uygun bir şekilde, normal, grepable ve XML için -oN, -oG ve -oX komutlarını birleştirmek için -oA FILENAME komutunu kullanarak tarama çıktısını her üç formatta da kaydedebilirsiniz.

Script Kiddie

Dördüncü bir format ise script kiddie'dir. Çıktıda ilginç anahtar kelimeler aramak veya sonuçları ileride başvurmak üzere saklamak istiyorsanız bu biçimin işe yaramadığını görebilirsiniz. Ancak, nmap -sS 127.0.0.1 -oS FILENAME taramasının çıktısını kaydetmek, çıktı dosya adını görüntülemek ve teknoloji meraklısı olmayan arkadaşlarınızın önünde 31337 olarak görünmek için kullanabilirsiniz.

```
pentester@TryHackMe$ cat MACHINE_IP_scan.kiddie $tart!ng nMaP 7.60 ( htt
pz://nMap.0rG ) at 2021-09-10 05:17 B$T
Nmap scan rEp0rt f0r |p-10-10-161-170.EU-w3$t-1.C0mputE.intErnaL (10.10.16
1.170)
HOSt !s uP (0.00095s LatEncy).
N0T $H0wn: 994 closed pOrtS
PoRT    st4Te SeRViC3 VERS1on
22/tcp  Open  ssH     Op3n$$H 6.7p1 Deb|an 5+dEb8u8 (pr0t0COl 2.0)
```

```
25/tCp  Op3n  SmTp    P0$Tf!x Smtpd
80/tcp  0p3n  http    Ng1nx 1.6.2
110/tCP 0pen  pOP3    d0v3coT P0p3D
111/TcP op3n  RpcbInd 2-4 (RPC #100000)
143/Tcp opEn  Imap    Dovecot 1mApd
mAC 4Ddr3sz: 02:40:e7:B5:B6:c5 (Unknown)
Netw0rk d!stanc3: 1 h0p
$3rv1c3 InFO: Ho$t:  dEBra2.thM.lOcal; 0s: Linux; cPe: cP3:/0:linux:l|nux_k3rn
el

0S and servIc3 D3tEcti0n pErf0rm3d. Plea$e r3p0rt any !nc0RrecT rE$ultz at
hTtpz://nmap.0rg/$ubmit/ .
Nmap d0nE: 1 |P addr3SS (1 hoSt up) $CaNnEd !n 21.80 s3c0Ndz
```

Sorular

Önceki görevin hedef makinesini sonlandırın ve bu görev için hedef makineyi başlatın. AttackBox terminalinde, hedef sanal makineden Nmap raporlarını normal ve grepable formatlarında indirmek için scp pentester@MACHINE_IP:/home/pentester/* . komutunu verin.

Pentester kullanıcı adının THM17577 parolasına sahip olduğuna dikkat edin

Soru ⇒ Ekteki Nmap günlüklerini kontrol edin. HTTPS bağlantı noktasını kaç sistem dinliyor?

Cevap ⇒ 3

Soru ⇒ 8089 numaralı bağlantı noktasını dinleyen sistemin IP adresi nedir?

Cevap ⇒ 172.17.20.147

Task 6 Summary (Görev 6 Özet)

Bu odada, ana bilgisayar işletim sistemi ile birlikte çalışan hizmetleri ve sürümlerini nasıl tespit edeceğimizi öğrendik. Traceroute'un nasıl etkinleştirileceğini öğrendik ve sızma testine yardımcı olmak için bir veya daha fazla komut dosyası seçmeyi ele aldık. Son olarak, tarama sonuçlarını ileride başvurmak üzere kaydetmek için

farklı formatları ele aldık. Aşağıdaki tablo, bu odada ele aldığımız en önemli seçenekleri özetlemektedir.

Option	Meaning
`-sV`	determine service/version info on open ports
`-sV --version-light`	try the most likely probes (2)
`-sV --version-all`	try all available probes (9)
`-O`	detect OS
`--traceroute`	run traceroute to target
`--script=SCRIPTS`	Nmap scripts to run
`-sC` or `--script=default`	run default scripts
`-A`	equivalent to `-sV -O -sC --traceroute`
`-oN`	save output in normal format
`-oG`	save output in grepable format
`-oX`	save output in XML format
`-oA`	save output in normal, XML and Grepable formats

Soru ⇒ Bu oda, 4 odadan oluşan Nmap serisini sonlandırmaktadır. Bu odada ve öncekilerde açıklanan tüm Nmap seçeneklerini not aldığınızdan emin olun.

Cevap ⇒ Cevap Gerekmemektedir.