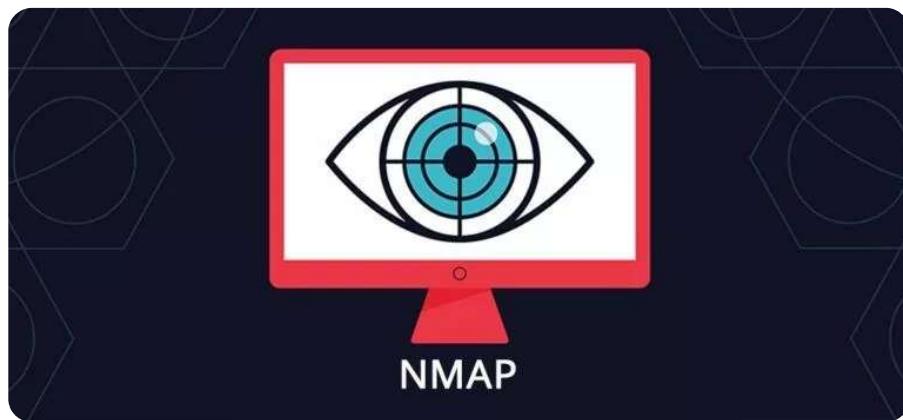


Kurumunuza Özel **Sızma Testi Pentest Hizmeti İndirim Fırsatı!**



Nmap Nedir? – Temel ve İleri Seviye – Part 3

30/01/2020



Nmap, ağ tarama ve zafiyet tespiti için kullanılan açık kaynaklı bir araçtır. Bu araç birçok sisteme yönelik taramaları gerçekleştirerek esnek, hızlı ve anlamlı bir şekilde sonuç üretmektedir. Sistemlerin açık olup olmadığını, açık olan sistemlerin portlarını durumları, hangi servislerin çalıştığı ve kullanılan işletim sistemi gibi birçok bilgiyi verebilmektedir.

Nmap ile tespit edilen servislerin güvenlik açığı barındırıp barındırmadığı ve kullanılan servisler hakkında bilgi elde edilebilir. Ayrıca içerisinde barındırmış olduğu scriptler ile hedef sisteme yönelik tarama gerçekleştirildiğinde hedef sistem hakkında detaylı bilgi ve güvenlik açığı olup olmamasına yönelik sonuç üretmektedir. Nmap aracı, alanının en iyi araçları araçları arasında yer almaktadır.

NMAP SCRIPTING ENGINE

Nmap Scripting Engine (NSE), Nmap'in en güçlü ve esnek özelliklerinden biridir. Kullanıcıların ağ üzerinde yapmak istediği işlemleri otomatize eder. İçerisindeki komut dosyaları, Nmap ile paralel çalışmakta olup taramaya hız ve verimlilik katar. Nmap Scripting Engine, ağ keşiflerinde hedef hakkında bilgiler toplamak, açık olan portlara yönelik gelişmiş sürüm tespitini yapmak, hedef sistemde bulunan güvenlik açıklıklarının tespitini yapmak, sistem üzerinde çalışan backdoorların tespitini yapmak ve tespit edilen güvenlik açıklıklarını exploit etmek için Lua dilinde yazılmış olan bazı scriptleri kullanmak gibi işlemleri gerçekleştiren modülleri içerir.

NSE, -sC parametresi ile kullanılır. Ayrıca özel script belirtilmek istendiğinde “–script” veya “–sC” parametresinden sonra kullanılacak script adının yazılması gereklidir. Elde edilen sonuçları Nmap normal ve XML çıktısına eklenir.

Şekil 7.a – NSE (-sC) parametresinin Kullanılması

Şekil 7.a'da çıktı üreten servis komut dosyaları, sistemin RSA ve DSA SSH anahtarlarını sağlayan ssh-hostkey ve portmapper'ı mevcut hizmetleri numaralandırmayı sorgulayan rpcinfo'dur. Bu örnekte, çıktı üreten tek host komut dosyası, SMB sunucularından çeşitli bilgiler toplayan smb-os-discovery'dir.

Kullanım Şekilleri

-script <filename>|<category>|<directory>|<expression>[,...]: Virgülle ayrılmış dosya adı, script kategorileri ve dizin listesini kullanarak script taraması yapılır. Her öğe önce bir ifade, sonra bir kategori ve en sonunda bir dosya ya da dizin adı olarak yorumlanır. Script ifadesi listesindeki her öğeye, verilen

script/kodları, script veya hostrule işlevlerindeki koşullardan bağımsız olarak çalışması için bir **+** karakteri eklenebilir. Nmap'ın mssql servisini tanıabilmesi için kapsamlı sürüm tespiti (**-sV -version-all**) çalıştırarak Nmap taramasını yavaşlatmak yerine, **ms-sql-config** scriptini tüm hedeflenen hostlara ve portlara karşı çalıştırabilir. **-script + ms-sql-config** olarak yapılabilir.

-script-args <args>, -script-args-file<filename>: Scriptlere argümanlar sağlanır. “–script-args-file” parametresi, argümanların bir dosyada belirtilmesinde kullanılır.

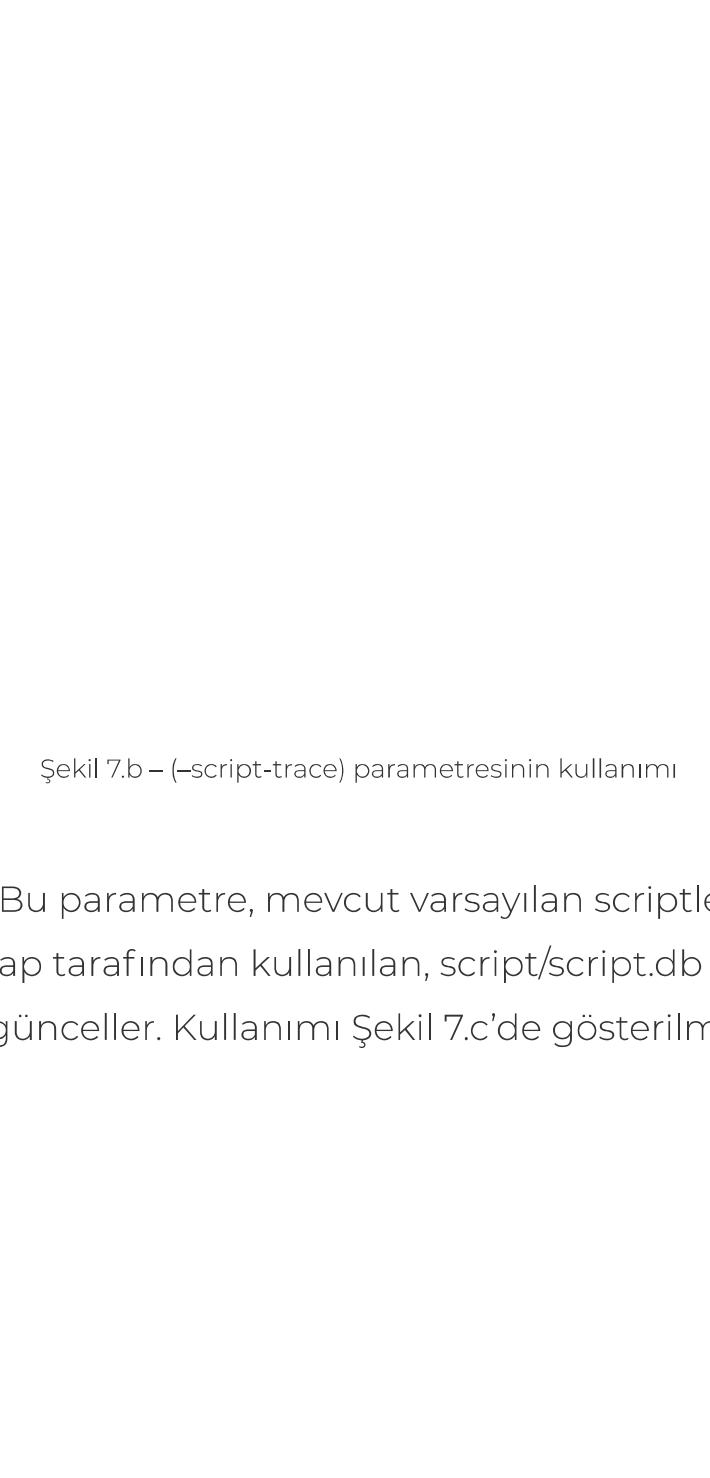
-script-help <filename>|<category>|<directory>|<expression>|all[,...]: Scriptler hakkında bilgi elde etmek için –script-help kullanılır. Belirtilen öğe ile eşleşen her bir script için Nmap, script adını, kategorilerini ve açıklamasını yazdırır. Özellikler **-script** tarafından kabul edilenlerle aynıdır; Örneğin, **nmap –script-help ssl-enum-ciphers** komutunu çalıştırılabilir.

-script-trace: Bu parametre, **-packet-trace** ögesine benzemektedir. Ancak paket yerine uygulama düzeyinde çalışır. Bu parametre belirtilirse, scriptler tarafından gerçekleştirilen, tüm gelen ve giden iletişim yazdırılır. Görüntülenen bilgiler iletişim protokolünü, kaynak ve hedef adreslerini ve iletilen verileri içerir. iletilen verilerin %5'inden fazlası yazdırılamazsa, bunun yerine hex dökümleri yapılır. –packet-trace parametresinin belirlenmesi, script izlemeyi de sağlar. Kullanımı, Şekil 7.b'de gösterilmiştir.



Şekil 7.b – (`-script-trace`) parametresinin kullanımı

`-script-updatedb`: Bu parametre, mevcut varsayılan scriptleri ve kategorileri belirlemek için Nmap tarafından kullanılan, `script/script.db` içinde bulunan script veritabanını günceller. Kullanımı Şekil 7.c'de gösterilmiştir.



Şekil 7.c – (`-script-updatedb`) parametresinin kullanımı

Script Kategorileri

NSE scriptleri, ait oldukları kategorilerin bir listesini tanımlar. Şu anda tanımlanmış kategoriler; auth, broadcast, brute, default, discovery, dos, exploit, external, fuzzer, intrusive, malware, safe, version ve vuln. Kategori adlarının büyük/küçük harf duyarlılığı yoktur.

✓ **Auth:** Hedef sisteme yönelik kimlik doğrulama işlemini yapan scriptlerin kategorisidir.

✓ **Broadcast:** Genellikle listelenmeyen hostları yerel ağıda yayinallyarak keşfeden scriptlerdir.

✓ **Brute:** Uzak bir sunucunun kimlik doğrulama bilgilerini tahmin etmek için bruteforce saldırıları kullanan script kategorisidir.

✓ **Default:** Nmap'in -A parametresi ile kullanılan varsayılan scriptlerin kategorisidir. Bu kategori, **-script=default** kullanılarak belirtilir.

Speed: Bruteforce, kimlik doğrulama, crackleme, web dizin tespiti ve tek bir hizmeti taramak için hızlı sonuç veren default scriptleri kullanılır.

Usefulness: Default kategorisindeki değerli ve işlem yapılabılır bilgiler üreten scriptleri belirtir.

Verbosity: Nmap çıktısı çok çeşitli amaçlar için kullanılıp okunaklı ve özlü olması gereklidir. Sık sık çıktılarla dolu sayfalar üreten bir scripti, default kategorisinden çıkartır.

Reliability: Hedef host veya hizmetle ilgili sonuçlara ulaşmak için sezgisel ve bulanık imza eşleştmeleri için kullanılan scriptleri belirtir. Örneğin, sniffer tespiti ve sql injection scriptlerini içerir.

Intrusiveness: Sistemi veya hizmeti çekertebilen veya uzak yöneticilerin saldırısı olarak algılanan scriptleridir.

Privacy: Üçüncü şahıslara bilgi veren scriptlerdir. Örneğin, whois betiği hedef IP adresini bölgesel whois kayıtlarına göstermelidir.

✓ **Discovery:** Ağ ve ağa bağlı bütün cihazlar hakkında bilgi elde etmek için kullanılan scriptlerin kategorisidir.

✓ **Dos:** Denial Of Service scriptlerinden oluşur. Servislerin çökeltilmesine yönelik bir zafiyet olup olmadığını test etmek için kullanılan scriptlerdir.

✓ **Exploit:** Hedef sistemde bulunan bir güvenlik açığını sömürmek için kullanılan scriptlerdir. Örnekler arasında **jdwp-exec** ve **http-shellshock** bulunur.

✓ **External:** Bir üçüncü taraf veritabanına veya başka bir ağ kaynağına veri gönderen scriptlerdir. Örneğin, whois sunucularına hedefin adresi hakkında bilgi edinmek için bir bağlantı kuran whois-ip'tir.

✓ **Fuzzer:** Hedefin cevap vermemesine yönelik rastgele hazırlanmış paketlerle istek yapılmasını sağlayan scriptlerdir. Örneğin, bir DNS sunucusunu, sunucu çökene veya kullanıcı tarafından belirlenen bir zaman sınırı doluncaya kadar yavaşça hatalı DNS istekleriyle bombalayan **dns-fuzz**'dır.

✓ **Intrusive:** Hedef sistemi çökertecek veya hedef sistemin zararlı olarak algılayacağı scriptlerdir. Örnekler **http-open-proxy** (hedef sunucuyu bir HTTP proxy'si olarak kullanmaya çalışır) ve **snmp-brute** (genel, özel ve cisco gibi ortak değerler göndererek bir cihazın SNMP topluluk dizesini tahmin etmeye çalışır).

✓ **Malware:** Hedef platformun zararlı yazılımlara veya backdoorlara bulaşıp bulaşmadığını tespit eden scriptler malware kategorisinde yer alır. Örneğin, 25 numaralı port dışındaki farklı portlarda çalışan SMTP sunucularını izleyen **smtp-strangeport** ve herhangi bir istek almadan, istek almış gibi davranışın cevap veren kimlik doğrulama scripti **auth-spoof'tur**.

✓ **Safe:** Servisleri çökertmek, büyük miktarda ağ bant genişliği kullanmak veya güvenlik açıklarından yararlanmak için tasarlanmamış scriptlerdir. Örneğin, **ssh-hostkey** (bir SSH host anahtarı alır) ve **html-title** (başlığı bir web sayfasından alır). Sürüm kategorisindeki scriptler güvenlik açısından sınıflandırılmaz.

✓ **Version:** Sürüm tespit etme özelliğinin bir uzantısıdır. Açıkça seçilemez. Yalnızca sürüm tespiti (-sV) istendiğinde çalışacak şekilde seçilirler. Çıktıları sürüm tespit çıktısından ayırt edilemez ve hizmet ya da host script sonuçları üretmezler. Örneğin, **skypev2 sürümü, pptp sürümü ve iax2 sürümü**.

✓ **Vuln:** Bilinen bazı güvenlik açıklarının hedef platformda olup olmadığını tespit etmek için kullanılan scriptleridir. Örneğin, **realvnc-auth-bypass** ve **afp-path-vuln, smb-vuln-ms17-010** scriptleri bulunur.

Script Seçimi

-script parametresi, virgülle ayrılmış kategorilerin, dosya adlarının ve dizin adlarının gösterimiyle kullanılır.

nmap -script default, safe: Default ve Safe kategorilerindeki scriptler kullanılır. Örnek olarak Şekil 7.3'te gösterilmiştir.



Şekil 7.3 – Varsayılan script kategorisinin belirlenmesi

nmap –script smb-os-discovery: Yalnızca smb-os-discovery scripti kullanılır. .nse uzantısını eklemek zorunlu değildir.

nmap –script default, banner, /home/user/customscripts: Default kategorisindeki scriptler, banner scripti ve /home/user/customscripts dizininde bulunan scriptler kullanılır.

nmap –script “http-*”: Http-auth ve http-open-proxy gibi, adı http- ile başlayan tüm scriptler kullanılır. **–script** parametresi, wildcard karakterleri kabuktan korumak için tırnak içinde olmalıdır. Boolean ifadeleri oluşturmak için ve/veya operatörleri kullanılarak daha karmaşık komut dosyası seçimi yapılabilir.

nmap –script “not intrusive”: intrusive kategorisi dışındaki scriptlerin kullanılmasını sağlar.

nmap –script “default or safe”: İşlevsel olarak nmap **–script “default, safe”** komutu ile eşdeğerdir. Default ya da safe kategorisindeki scriptler veya her ikisindeki scriptler kullanılır.

nmap –script “default and safe”: Hem default hem de safe kategorisindeki scriptler kullanılır.

nmap –script “(default or safe or intrusive) and not http-*”: http- ile başlayan scriptler hariç, default, safe ya da intrusive kategorisindeki scriptler kullanılır.

Script Tipleri ve Aşamaları

NSE, aldıkları hedeflerin türü ve çalıştırıldığı tarama aşaması ile ayırt edilen dört tür script destekler. Bireysel scriptler, çoklu işlem türlerini destekleyebilir.

Prerule Scriptleri: Herhangi bir Nmap'ın tarama aşamasından önce yayınlanır. Bu nedenle Nmap henüz hedefleri hakkında herhangi bir bilgi toplamayabilir. DHCP ve DNS SD sunucularını sorgulamak için ağ yayın istekleri yapmak gibi belirli tarama hedeflerine bağlı olmayan görevler için faydalı olabilirler. Bu scriptlerden bazıları, Nmap'ın taraması için yeni hedefler oluşturabilir. Örneğin, **dns-zone-transfer**, zone transfer isteğini kullanarak bir alandaki IP'lerin listesini alabilir ve bunları otomatik olarak Nmap'ın tarama hedefi listesine eklemektedir.

Host Scriptleri: Bu aşamadaki scriptler, Nmap host bulma, port tarama, sürüm tespiti ve hedef hostlara karşı işletim sistemi tespiti gerçekleştirdikten sonra Nmap'ın normal tarama işlemi sırasında çalışır. Bu tür

scriptler, **hosrule** işleviyle eşleşen her hedef hosta karşı bir kez çağrıılır. Örneğin, bir hedef IP için ownership bilgilerini arayan whois-ip ve parçalanma gerektirmeden hedefe ulaşabilecek maksimum IP paket boyutunu belirlemeye çalışan yol **mtu**'dur.

Servis Scriptleri: Bu scriptler, bir hedef hostta dinleyen belirli servislere karşı çalıştırılır. Örneğin, Nmap, web sunucularına karşı çalıştmak için 15'ten fazla http hizmeti scripti içerir. Bir hostta birden fazla portta çalışan web sunucuları varsa, bu komut dosyaları birden çok kez çalışabilir. Bunlar en çok kullanılan Nmap komut dosyası türündür ve bir komut dosyasının hangi algılayıcılara karşı çalıştırılacağına karar vermek için bir **portrule** işlevi içерerek ayrıt edilirler.

Postrule Scriptleri: Nmap tüm hedeflerini taradıktan sonra yayınlanır. Nmap çıktısını biçimlendirmek ve sunmak için faydalı olabilirler. Örneğin, **ssh-hostkey**, SSH sunucularına bağlanan, genel anahtarlarını keşfeden ve bunları basan hizmet (**portrule**) scriptleriyle en iyi bilinir. Ancak, taranan tüm hostlar arasında yinelenen anahtarları denetleyen, ardından bulunanları yazdırın bir posta kodu da içerir. Bir **postrule** scripti için bir başka kullanım, Nmap çıktısının ters bir indeksini basmaktadır. Hangi hostların yalnızca her bir hosttaki hizmetleri listelemek yerine belirli bir servisi çalıştırıldığını gösterir. Postrule scriptleri, postrule işlevi içерerek tanımlanır. Birçok script, bir ön hazırlık ya da önyükleme dosyası olarak çalıştırılabilir. Bu durumlarda, tutarlılık için bir primer kullanmanız faydalı olacaktır.

Scriptlerden Bağımsız Değişkenler

Argümanlar **-script-args** parametresi kullanılarak NSE scriptlerine iletilebilir. Argümanlar bir **key-value** çiftleri tablosunu ve muhtemelen dizi değerlerini açıklar. Argümanlar, scriptlere **nmap.registry.args** adlı kayıt defterinde bir tablo olarak tutulur.

Ancak normalde **stdnse.get_script_args** işleviyle erişilebilirler. Komut satırı bağımsız değişkenlerinin sözdizimi, Lua'nın tablo yapıcısının sözdizimine benzemektedir.

Bağımsız değişkenler, virgülle ayrılmış bir ad listesidir: Değer çiftleridir. Adlar ve değerler, boşluk içermeyen dizeler veya '{, }', '=' veya ';' karakterleri olabilir. Alıntı yapılan bir dizgede '\' bir alıntıdan kaçar.

Bir ters eğik çizgi yalnızca bu özel durumda tırnak işaretlerinden kaçmak için kullanılır; Diğer tüm durumlarda, ters eğik çizgi tam anlamıyla yorumlanır. Komut satırındaki **-script-args** komutundaki argümânları iletmek yerine, bunları bir dosyada (virgül veya yeni satırlarla ayrılmış) saklayabilir ve **-script-args-file** ile sadece dosya adını belirleyebilirsiniz. Komut satırında **-script-args** ile belirtilen parametreler, dosyada verilenlerden önceliklidir. Dosya adı mutlak bir yol olarak veya Nmap'ın normal arama yoluna (NMAPDIR, vs.) göre görülebilir. Argüman kullanımına örnek olarak Şekil 7.5 verilmiştir.

Şekil 7.5- Nmap komut satırında argüman kullanımı

Script Dili

Nmap Scripting Engine çekirdeği gömülebilir bir Lua yorumlayıcısıdır. Lua, genişletilebilirlik için tasarlanmış hafif bir dildir. Nmap gibi diğer yazılımlarla arayüz oluşturmak için güçlü ve iyi belgelenmiş bir API sunmaktadır. Nmap Scripting Enginenin ikinci kısmı, Lua ile Nmap'ı birbirine bağlayan NSE kütüphanesidir. Bu katman, Lua yorumlayıcısının başlatılması, paralel komut

dosyası çalışma zamanlaması, komut dosyası alımı ve daha fazlası gibi sorunları ele alır. Aynı zamanda NSE ağ I/O framework ve yönetim mekanizmasının kalbidir. Ayrıca, komut dosyalarını daha güçlü ve kullanışlı hale getirmek için yardımcı program kitaplıklarını da içerir.

Nmap script dili, Nmap ile arabirim oluşturmak için kütüphanelerle genişletilen gömülü bir Lua yorumlayıcısıdır. Nmap API, Lua namespace'inde nmap adıyla bulunur. Bu, Nmap tarafından sağlanan tüm kaynaklara yapılan çağrıların bir nmap ön ekine sahip olduğu anlamına gelmektedir. **nmap.new socket()**, örneğin, yeni bir soket sarmalayıcı nesnesi döndürür. Nmap kütüphane katmanı aynı zamandaLua içeriğini başlatmayı, paralel kodları planlamayı ve tamamlanmış kodlar tarafından üretilen çıktıyı toplamayı da önemsemektedir. Planlama aşamalarında, Nmap script için temel olarak birkaç programlama dili düşünüldü. Diğer bir seçenek ise tamamen yeni bir programlama dili uygulamaktı. NSE'nin kullanımı kolay, küçük boyutlu, Nmap lisansı ile uyumlu, ölçeklenebilir, hızlı ve paralelleştirilebilir olması gerekiyordu. Perl, Python ve Ruby dillerde daha kapsamlı interpreterlar vardır. Ancak, Nmap içerisinde verimli bir şekilde gömülmesi zordur. Ama, Lua Nmap içerisinde gömülü geldiği gibi, Wireshark sniffer ve Snort IDS gibi diğer popüler açık kaynaklı güvenlik araçlarında bile gömülü geliyor.

Lua'nın önemli yerleşik özelliklerine ek olarak, senaryo yazmayı daha güçlü ve kullanışlı hale getiren birçok uzantı kütüphanesi yazılmış entegre edilmiştir. Gerekirse bu kütüphaneler (bazen modüller olarak da adlandırılır) derlenir ve Nmap ile birlikte kurulur. Yapılandırılmış Nmap veri dizinine yüklenen kendi dizinleri nselib vardır. NSE Kütüphaneleri Şekil 7.6'da gösterilmiştir.

Şekil 7.6 – NSE Kütüphaneleri

GÜVENLİK DUVARLARI VE IDS SİSTEMLERİNİN TESPİTİ

Yapılan taramalarda güvenlik duvarları ağın haritalanmasını zorlaştırmaktadır. Sistemler hakkında keşif taramaları gerçekleştirildiğinde güvenlik duvarları ve IDS sistemleri bu tarama işlemlerini engelleyemektedir. Nmap, bu karmaşık ağları anlamaya yardımcı olmak ve filtrelerin amaçlandığı gibi çalıştığını doğrulamak için birçok özellik sunmaktadır. Tüm büyük IDS'ler Nmap taramalarını tespit etmek için tasarlanmış kurallarla birlikte gelmektedir. Çünkü taramalar bazen saldırılara öncülük etmektedir.

Güvenlik Duvarı Kurallarını Belirlemek

Güvenlik duvari kurallarını atlamak için nasıl çalışıklarını bilmek gereklidir. Nmap ulaşılabilir, ancak kapalı olan ve aktif olarak filtrelenen portları birbirinden ayırır. Etkili bir teknik, normal bir SYN port taraması ile başlamak, daha sonra ağın daha iyi anlamak için ACK taraması ve IP ID sıralaması gibi teknikler kullanmaktadır.

TCP SYN Scan

TCP SYN(Stealth) Scan, TCP portlarını taramanın en hızlı yolu olduğu için en popüler tarama türündür. Connect taramasından daha gizlidir ve tüm işlevsel TCP yığınlarına karşı çalışmaktadır. SYN veya Stealth taraması, bir SYN paketi gönderip gelen cevabı göz önüne alarak bu prosedürü kullanmaktadır. SYN/ACK geri gönderilirse, TCP connection bağlantısı ile açık porta uzaktan bağlanmaya çalışır. Tarayıcı tamamen kurulmadan önce bağlantıyı down etmek için bir RST gönderir; genellikle uygulama logları bağlantı girişiminin görünmesini önlemektedir. Port kapalıysa, bir RST gönderilir. Eğer filtre edilirse, SYN paketi düşürülmüş olacak ve herhangi bir cevap gönderilmeyecektir. Bu şekilde, Nmap portun açık, kapalı ya da filtreli olup olmadığını tespit etmektedir. Şekil 8.1.1.a'da 956 tane portun kapalı, 40 tane portun filtreli olduğu belirtilmektedir. Varsayılan tarama yaptığımız için 1000 portu taradığına göre 4 portu da açık olarak belirledi.

A screenshot of a network traffic capture tool showing a SYN scan. The interface displays a list of hosts or ports being scanned, with various status indicators such as 'Open', 'Closed', and 'Filtered'. The tool also shows packet statistics and configuration settings.

Şekil 8.1.1.a – Varsayılan SYN Scan Örneği

RST döndüren gizli güvenlik duvarları: Kapalı TCP portları (bir RST paketi döndüren) ve filtrelenmiş portlar (hiçbir şey veya bir ICMP hatası döndürmeyen) arasındaki Nmap ayrimı genellikle doğru olsa da, birçok güvenlik duvarı cihazı şimdi RST paketlerini hedef hosttan geliyormuş gibi yapabilir ve portun kapalı olduğunu iddia edebilir. Bu özelliğin bir örneği, istenmeyen paketleri reddetmek için birçok yöntem sunan Linux iptables sistemidir. Iptables kılavuzu özelliği, **-reject-with** tipi olarak belirtmektedir. Verilen tip uygun ICMP hata mesajını döndüren icmp-net-unreachable, icmp-host-unreachable, icmp-port-unreachable, icmp-proto-unreachable, icmp-net-prohibited veya icmp-host-prohibited olabilir, unreachable varsayılandır). **Tcp-reset** parametresi yalnızca TCP protokolüyle eşleşen kurallarda kullanılabilir: bu bir TCP RST paketinin geri gönderilmesine neden olur. Bu, çoğunlukla bozuk posta hostlarına, posta gönderirken sıkça oluşan ident (113/tcp) problemini engellemek için kullanışlıdır (aksi halde postanızı kabul etmeyecektir). RST paketlerini güvenlik duvarları ve IDS/IPS ile oluşturmak, ağ operatörlerinin kafasını karıştırabildiğinden ve tarayıcıların, düşmüş paketlerin neden olduğu zaman aşımını beklemeden hemen bir sonraki porta geçmesine izin verdiğiinden özellikle 113 numaralı port dışında

yaygın değildir. Böyle bir sahtecilik, RST paketinin, makine tarafından gönderilen diğer paketlerle karşılaştırıldığında dikkatli bir şekilde analiz edilmesiyle tespit edilebilir.

TCP ACK Scan

TCP ACK Scan, güvenlik duvarı kurallarının durumlu olup olmadığını ve hangi portlarınfiltrelendiğini belirlemek için kullanılır. Dezavantajı ise açık portları kapalı portlardan ayırt edememesidir. **-scanflags** parametresini kullanmıyorsanız, varsayılan olarak bu tarama türü problkardaki ACK bayrağını ayarlamaktadır. Filtrelenmemiş sistemleri tararken, açık ve kapalı portların her ikisi de bir RST paketi döndürmektedir. Nmap aracı da bunları unfiltered olarak etiketlemektedir. Bu durum, ACK paketleri tarafından erişilebilecekleri anlamına gelmektedir. Ancak Açık veya kapalı olup olmamaları belirsizdir. Yanıt vermeyen veya belirli ICMP hata mesajlarını geri gönderen portlar (type 3, codes 0, 1, 2, 3, 9, 10 veya 13),filtrelenmiş olarak etiketlenir. Ayrıca bu taramayı gerçekleştirmek için **-sA** parametresini kullanmanız yeterli olacaktır. Şekil 8.1.2 ‘de gösterilmiştir.

Şekil 8.1.2 – TCP ACK Scan Gösterimi

IP ID Püf Noktaları

IP başlıklarındaki ID alanında şaşırtıcı miktarda bilgi açığa çıkabilir. Idle Scan tekniğide kullanıldığı gibi güvenlik duvarlarını kandırmak için RST paketlerinin saldırıcı bir sistemden gelmediğini göstermeye çalışılır. Bir başka yol da, güvenlilik kaynak adreslerinin güvenlik duvarının kontrol mekanizmalarına takılmadan çalışmasıdır. Örneğin, bir şirketin üretim ağındaki makineler, şirket ağındaki IP adreslerine güvenebilir veya bir sistem yöneticisinin kişisel makinesine güvenebilir. Güvenilir kaynak adres sorununun somut bir örneği, bir şirketin özel UDP hizmetinin, bir yapılandırma dosyasına girilen özel bloklardan geliyorsa, kullanıcıların kimlik doğrulaması mekanizması atlatılabilir. Bu ağ blokları farklı kurumsal konumlara karşılık gelip bu özellik yönetimi ve hata ayıklamayı kolaylaştırmaktadır. Bu güvenlik duvarı kurallarını belirleme tekniği olarak Nmap kullanılmamalıdır. Ama Nmap taramalarının

çıktıları önemlidir. Örneğin, bu test bazı kod çözüçüler kullanılıp kullanılmayacağını gösterebilir (-D).

UDP Sürüm Taraması

UDP ile çalışmak genellikle daha zordur. Çünkü protokol, TCP gibi açık portların onaylanması yapmamaktadır. Birçok UDP uygulaması beklenmedik paketleri görmezden gelmektedir. Nmap, portların açık veya filtrelenmiş olup olmadığını öğrenmek amacıyla açık portlardan yanıt alabilmek için birbirinden farklı UDP hizmetine birçok UDP probu gönderir. Şekil 8.1.4’te 53 numaralı portun açık ve üzerinde bir servisin çalışıyor olduğu görülmektedir. Diğer portlar hala open|filtered,’dır. Çünkü probaların hiçbirine cevap dönmemektedir.

Şekil 8.1.4 – UDP sürüm taraması örneği

Güvenlik Duvarı Kurallarını Atlatma Teknikleri

Güvenlik duvari kurallarını belirlemek değerli olsa da kuralları atlamak çoğu zaman öncelikli hedeftir. Nmap bunu yapmak için birçok teknik kullanarak kötü yapılandırılmış güvenlik duvarlarını atlayabilmektedir. Saldırganın başarılı olabilmesi için oluşturulan yanlış yapılandırmaların birini bulması gereklidir, ağ yöneticilerinin yanlış yapılandırmaların hepsini tespit edip düzeltmeleri gerekmektedir.

Egzotik Tarama Bayrakları

Ağ portlarından hangisininfiltrelendiğini belirlemek için bir ACK taraması kullanılabilir. Ancak, erişilebilir portlardan hangisinin açık veya kapalı olduğu bilinmemektedir. Nmap, istenen port durumu bilgilerini verirken güvenlik duvarlarını gizlice atlatmak için iyi olan birkaç tarama yöntemi sunmaktadır. FIN taraması böyle bir tekniktir. `-sF` parametresi kullanılarak FIN taraması gerçekleştirilir. Şekil 8.2.1'de, bu kez bir FIN taraması kullanarak FIN taraması yapılmıştır. Bir FIN paketi ayarlandığında, SYN paketlerini engelleyen kuralların ötesine geçmektedir. Bir SYN taraması 100'ün altında yalnızca bir açık port bulurken, FIN taraması ikisini de bulmaktadır.

Şekil 8.2.1 – Egzotik tarama bayraklarının kullanımı

Diğer birçok tarama türü denenmeye değer tarama türleridir. Çünkü hedef güvenlik duvari kuralları ve hedef host türü hangi tekniklerin çalışacağını

belirlemektedir. Bazı değerli tarama türleri FIN, Maimon, Window, SYN/FIN ve NULL taramalardır.

Kaynak Port Manipülasyonu

Yaygın olarak yapılan yanlış yapılandırmalardan biri, yalnızca kaynak port numarasına dayanan trafiğe güvenmektir. Bir yönetici, uygulamaları durdurmak kullanıcıların şikayetleri ile ilgilenecek şekilde yeni bir güvenlik duvarı kurarken, UDP DNS harici sunuculardan gelen yanıtlar artık ağa giremediğinden DNS çökebilir. Ayrıca FTP protokolü üzerinden dosya paylaşımlarında proxyler, sunucular görevlendirilir. Bazı sistem ve ağ yöneticilerinin FTP protokolü üzerinden saldırı yapılmayacağını varsayılmaktadır. Aynı durum 53 numaralı DNS portu içinde geçerlidir. Nmap, bu zayıflıklardan yararlanmak için **-g** ve **-source-port** seçeneklerini sunmaktadır. Bir port numarası verip bu porta paketler gönderilmektedir. Nmap, belirli işletim sistemi tespit testlerinin düzgün çalışması için farklı port numaraları kullanmalıdır. SYN taraması dâhil olmak üzere çoğu TCP taraması, UDP taraması gibi seçeneği tamamen desteklemektedir. Şekil 8.2.2'de gösterildiği gibi kaynak port manipülasyon işlemini gerçekleştirmiştir. Bunun için **-g** parametresi kullanılmıştır. **-sS** parametresi ile SYN taraması, **-v** parametresi ile detaylı sonuç getirmesini, ikinci **-v** parametresi ile çıktıları detaylı bir şekilde getirmesi sağlanmıştır. Ayrıca **-n** parametresi ile dns çözümleme yapmaması için kullanılmıştır. **-Pn** parametresini kullanarak pingsiz tarama yapmasını ve **-p1-100** parametresini belirterek ilk 100 portu taraması istenilmiştir.



Şekil 8.2.2 – Kaynak port manipülasyonu gösterimi

IPv6 Saldırıları

IPv6 tam olarak dünyanın her yerinde olmasa bile, Japonya ve diğer bazı bölgelerde oldukça popülerdir. IPv6'yi filtrelemek bazen IPv4'ten daha kritik olabilir. Çünkü genişletilmiş adres alanı, genel olarak adreslenebilir IPv6 adreslerinin genellikle RFC 1918 tarafından belirtilen özel IPv4 adreslerini kullanmak zorunda kalacak makinelere tahsis edilmesini sağlar. IPv4 varsayılanı yerine IPv6 taraması gerçekleştirmek çoğu zaman komut satırına **-6** eklemek kadar kolaydır. İşletim sistemi tespiti ve UDP tarama gibi bazı özellikler bu protokol için henüz desteklememektedir. Ancak en popüler özellikler çalışmaktadır.

IP ID Idle Scan

IP ID Idle scan, hedefinize hiçbir adres gönderilmez. Çünkü en gizli tarama türlerinden biridir. Açık portlar, seçilen bir zombi makinesinin IP ID sequencelerinden çıkarılır. Idle scan'nın daha az bilinen bir özelliği, elde edilen sonuçların, eğer zombinin doğrudan hedef host taraması durumunda elde edeceğiniz sonuçlardır. **-g** parametresinin güvenilir kaynak portlarından yararlanmasına izin verdiği gibi, Idle scan bazen güvenilir kaynak IP adreslerinden de yararlanabilir.

Çoklu Ping Problemleri

Güvenlik duvari ağlarını taramaya çalışırken, atılan ping problemleri hostlardan cevap alamayabilir. Bu sorunu azaltmak için Nmap, çok çeşitli problemlerin paralel olarak gönderilmesine izin verir.

Fragmentation (Parçalama)

Parçalama işlemi güvenlik duvarlarını atlatmak için kullanılan tekniklerden biridir. Bazı güvenlik duvarları paketleri boyutlarını göz önüne alarak paketin incelenmesini yapmaktadır. Paket boyutlarının parçalanması ile güvenlik duvari paketleri tek bir paket halinde inceleyemediği için kolaylıkla güvenlik duvarı atlatılır. Paketlerin parçalanması için **-f** parametresi kullanılır. Nmap, paketlerin parçalanması işleminde her parçalanan paketin boyutunu 8 bayt olarak belirler. Bu nedenle tipik bir 20 veya 24 bayt TCP paketi üç küçük parça halinde gönderilir. **-f** parametresinin kullanımı her parçanın 8 bayt olduğunu belirtir. Yani **-f -f**, her bir parça içerisinde 16'ya kadar veri baytı sağlar. Alternatif olarak, **-mtu** parametresini belirtebilir. **-mtu** argümanı sekizin bir katı olmalı ve **-f** parametresiyle birleştirilmemelidir.



Şekil 8.2.6 – Varsayılan bir taramada fragmentation kullanımı

IP katmanını atlamak ve raw ethernet frameleri göndermek için **-send-eth** parametresi kullanılabilir. Fragmentation, Nmap'in yalnızca TCP ve UDP port taramaları (connect scan ve FTP bounce scan hariç) ve işletim sistemi tespiti içeren ham paket özellikleri için deskeşeler. Sürüm tespiti ve Nmap Scripting Engine gibi özellikler genellikle parçalanmayı desteklemez. Çünkü hedef hizmetlerle iletişim kurmak için makinedeki TCP stack'e güvenir. Nmap, herhangi bir çakışma olmadan sırayla parçaları gönderir. Parçalanmış bir port taraması geçerse, ana makineye saldırmak için kullanılan diğer araçları ve istismarları parçalamak için fragroute gibi bir araç kullanılabılır.

Proxyler

Web için uygulama düzeyinde proxy'ler, algılanan güvenlik ve ağ verimliliği (önbelkleme yoluyla) yararları nedeniyle popüler hale gelir. Güvenlik duvarları ve IDS gibi, yanlış yapılandırılmış proxy'ler çözüdüklerinden çok daha fazla güvenlik sorununa neden olabilir. En sık karşılaşılan sorun uygun erişim kontrollerinin ayarlanamamasıdır. İnternette yüzbinlerce geniş açık proxy sunucusu bulunur. Bu sayede herhangi birinin başka internet sitelerine isimsiz atlamlı noktalar olarak kullanılmasına izin verir. Birçok kuruluş açık proxy'leri

bulmak ve IP adreslerini dağıtmak için otomatik tarayıcılar kullanır. Açık proxy'ler daha çok sitelere sızmak, kredi kartı sahtekârlığı yapmak ya da interneti spam ile doldurmak isteyen daha kötü insanlar tarafından kötüye kullanılır. İnternet kaynaklarında açık bir proxy barındırmak çok sayıda soruna neden olabilir. Ancak açık proxy'lerin korumalı ağa yeniden bağlantı kurmasına izin verilmesi daha ciddi bir durumdur. Dâhili ana makinelerin Internet kaynaklarına erişmek için bir proxy kullanması gerektiğine karar veren yöneticiler, istemeden de olsa trafiğe ters yönde de izin verir. **Hacker Adrian Lamo, genellikle bu reverse-proxy tekniğinden yararlanarak Microsoft, Excite, Yahoo, WorldCom, New York Times ve diğer büyük ağlara girdiği için ünlüdür.**

MAC Address Spoofing Tekniği

Ethernet cihazları, benzersiz bir altı bayt Media Access Control (MAC) adresiyle tanımlanır. İlk üç bayt organizasyonel olarak benzersiz bir tanımlayıcı (OUI) oluşturur. Bu ön ek, bir satıcıya IEEE tarafından atanır. Satıcı daha sonra kalan üç byte'ı sattığı adaptörlere ve cihazlara benzersiz bir şekilde atamaktan sorumludur. Nmap, OUI'leri atandıkları satıcı adlarıyla eşleştirilen bir veritabanı içerir. Bu, bir ağı tararken aygıtları tanımlamaya yardımcı olur. OUI veritabanı dosyası, nmap-mac-prefixes bulunur. MAC adresleri ethernet cihazlarına önceden atanmış olsalar da, mevcut donanımların çoğunda sürücü ile değiştirilebilir. Örneğin, çoğu Wireless Access Point, belirli bir MAC adresi grubuna erişimi sınırlamak için bir yapılandırma seçeneği sunar. Benzer şekilde, bazı ücretli veya özel ağlar, sizi bir web formu kullanarak bağlandıktan sonra doğrulamaya veya ödeme yapmaya zorlar. Ardından, MAC adresinize dayanarak ağın geri kalanına erişmenizi sağlar. MAC adreslerini spooflamanın ve MAC'in ağa yetkisiz erişim sağlamaası için spoofing yapmasının kolay olduğu göz önüne alındığında, bu erişim kontrolü şekli oldukça zayıftır. Bir yönlendiriciyi geçerken son sunucunun MAC adresi değiştirilir. Erişim

kontrolüne ek olarak, MAC adresleri bazen hesap verebilirlik için kullanılır. Ağ yöneticileri, DHCP lease aldıklarında veya yeni bir makine ağda iletişim kurduğunda MAC adreslerini kaydeder. Ağın kötüye kullanılması veya korsanlık şikayetleri alınırsa, IP adresini ve olay saatini temel alarak MAC adresini bulur. Sonra sorumlu makineyi ve sahibini bulmak için MAC kullanılır. Nmap, **–spoof-mac** parametresiyle MAC Address Spoofing işlemi yapar. Verilen argümân birkaç şekilde olabilir. Eğer sadece 0 ise, Nmap oturum için tamamen rasgele bir MAC adresi seçilir. Verilen dize çift sayıda onaltılk bir rakam ise, Nmap bunları MAC olarak kullanır. 12 hex basamaktan daha az rakam sağlanmışsa, Nmap altı baytin kalanını rasgele değerlerle doldurur. Arguman sıfır veya hexadecimal dize değilse, Nmap verilen dizeyi içeren bir satıcı adı bulmak için nmap-mac-öneklerine bakılır(büyük/küçük harf duyarsızdır). Bir eşleşme bulunursa, Nmap satıcının OUI'sini kullanır ve kalan üç baytı rastgele doldurur. Geçerli –spoof-mac argümân örnekleri Apple, 0, 01:02:03:04:05:06, deadbeefcafe, 0020F2 ve Cisco'dur. Bu parametre, Nmap'ın aslında ethernet düzeyinde paketler göndermesini sağlamak için **–send-eth** anlamına gelir. Bu parametre, sürüm tespiti veya Nmap Scripting Engine gibi bağlantı yönelik özellikleri değil, yalnızca SYN taraması veya işletim sistemi algılama gibi ham paket taramalarını etkiler. MAC Address Spoofing ağ erişimi için gerekli olmaya, aldatma için kullanılabilir.

Source Routing (Kaynak Yönlendirme)

Hedef ile aranızdaki bir router sorun yaşamana neden oluyorsa, çevresinde bir rota bulmaya çalışılır. Bu tekniğin etkinliği sınırlıdır. Çünkü paket filtreleme sorunları genellikle hedef ağ üzerinde veya yakınında meydana gelir. Bu makinelerin tüm kaynak yönlendirmeli paketlerini düşürmesi veya ağa girmesinin tek yoludur. Nmap, **–ip-options** parametresini kullanarak hem gevşek hem de katı kaynak yönlendirmesini desteklemektedir. Örneğin, –ip-options parametresi “L 192.168.0.7 192.168.30.9” olarak belirtilmesi, paketin,

verilen iki IP yol noktasından bu serbest kaynağın yönlendirilmesini talep eder. Kesin kaynak yönlendirmesi için L yerine S belirtilir. Sıkı kaynak yönlendirmeyi seçerseniz, yol boyunca her bir sekmeyi belirtmek zorunda kalacaktır. IPv4 kaynak yönlendirmesi çok sık engellenirken, kaynak yönlendirmenin IPv6 biçimi çok daha yaygındır. Nmap ile bir hedef makineye yönlendirilmiş bir kaynak yolu keşfedilirse, exploitability port taramasıyla sınırlı değildir. Ncat, kaynak yönlendirilmiş yollar üzerinden TCP ve UDP iletişimini etkinleştirebilir (-g parametresi kullanılabilir).

FTP Bounce Scan

FTP protokolünün bir özelliği (RFC 959) proxy FTP bağlantıları için destek sağlar. Bu, kullanıcının bir FTP sunucusuna bağlanmasını ve ardından dosyaların üçüncü taraf bir sunucuya gönderilmesini istemesini sağlar. Böyle bir özellik birçok düzeye saldırganlar tarafından kullanılmıştır. Bu nedenle çoğu sunucu bu özelliği destekler. Özelliğin diğer bir dezavantajı, FTP sunucusunun diğer hostları taramasına izin vermesidir. FTP sunucusundan, sırayla bir hostun portuna bir dosya göndermesini istemektedir. Hata mesajı portun açık olup olmadığını açıklamaktadır. Bu, güvenlik duvarlarını atlamak için iyi bir yoldur. Çünkü kurumsal FTP sunucuları, genellikle diğer tüm ana bilgisayarlara, eski herhangi bir Internet ana bilgisayarlarından daha fazla erişebilecekleri bir yere yerleştirilir. Nmap, **-b** seçeneğiyle birlikte FTP bounce taramasını deskeşler. “**kullanıcıadı:parola@ftpserver:port**” biçiminin bir argümanını alır. Server, güvenlik açığı bulunan bir FTP sunucusunun adı veya IP adresidir. Normal bir URL’de olduğu gibi, “**kullanıcıadı:parola**” ögesi atlanılabilir; bu durumda adsız oturum açma kimlik bilgileri (**kullanıcı:anonymous parola: -wwwuser@**) kullanılır. Port numarası ihmali edilebilir, bu durumda <server> üzerindeki varsayılan FTP port (21) kullanılır. Bir güvenlik duvarını atlamak amacınızsa, hedef ağı bağlantı noktası 21 için tarayın (veya sürüm algılamasıyla tüm bağlantı noktalarını tararsanız herhangi bir FTP

hizmeti için bile) ve ftp-bounce NSE komut dosyası kullanılabilir. Nmap hedefin savunmasız olup olmadığını söyler. İzlerinizi sadece kapatmaya çalışıyorsanız, kendinizi hedef ağdaki ana bilgisayarlarla sınırlandırmanız gerekmekz. Güvenlik açığı bulunan FTP sunucuları için rasgele internet adresleri taramaya gitmeden önce, sysadmins'in sunucularını bu şekilde kötüye kullanmanıza yardımcı olmaz.

Şekil 8.2.10 – TCP FTP Bounce Scan Gösterimi

Şekil 8.2.10 da gösterildiği gibi tarama işlemi gerçekleştirildi. Birazda FTP sunucusuna yönelik bir saldırı olarak da gösterilmektedir. Böyle bir girişimde yukarıdaki gibi kullanıcıadı parola FTP sunucusu adresi sonra hedefin adresi ve pingsiz tarama için -Pn parametresini kullanmıştır.

Güvenlik Duvarını Atlama Örneği

Şekil 8.2.11.a – Genel bir ağ taraması

Şekil 8.2.11.a'da bir ağ taraması gerçekleştiriliyor. Bu taramada –n parametresi ile dns çözümlemesini yapmamasını sağlanır. –sn parametresini kullanarak port tarama işlemini devre dışı bırakılır. –PE parametresini kullanarak bir ICMP echo taraması gerçekleştirilmesi ve –T4 parametresini kullanarak zamanlamasını ve performansını ayarlama işlemi gerçekleştiriliyor. Çünkü varsayılan olarak buradaki amaç ağdaki sistemlerin varlığını keşfetmektedir. Tabi, örnek olması amacıyla www.priviasecurity.com domain veriliyor. Ayrıca 192.168.16.0/24 veya 104.18.41.10 makinasının subnetinin hesaplandıktan sonra /24, /32 vb. opsiyonları kullanarak veriliip ağdaki sistemlerin keşfi sağlanabilir.

Şekil 8.2.11.b – Hedefin ek olarak –packet-trace parametresi ile taranması

Şekil 8.2.11.b'de ise gösterildiği –packet-trace parametresinin sağladığı avantajları kullanarak genel bir tarama gerçekleştiriliyor.

Şekil 8.2.11.c – Idle Scan İşleminin Kullanılması

Şekil 8.2.11.c'de ise idle scan işlemini kullanarak hedefin 80. portuna yönelik tarama gerçekleştiriliyor. Burada google.com adresinin bulunduğu makineyi zombie makina olarak belirleyip google.com makinesi üzerinden iletişime geçip tarama gerçekleştiriliyor.

Şekil 8.2.11.d – (ip-options) parametresinin kullanılması

Şekil 8.2.11.d'de gösterildiği gibi –ip-options parametresini avantajlarını kullanarak hedef makineye yönelik tarama işlemleri gerçekleştiriliyor.

Şekil 8.2.11.e – (-Pn) parametresinin kullanılması ile tarama

Şekil 8.2.11.e'de, Resim 8.2.11.d'deki avantajlara ek olarak Pingsiz tarama işlemi gerçekleştiriliyor.

- < [Nmap Nedir? – Temel ve İleri Seviye – Part 2](#)
- > [Avast Kullanıcı Verilerini Gizlice Satıyor #40](#)

Tel: +90 216 820 14 55

Posta: info@priviasecurity.com

Email Adresiniz

E-Bülten Abonelik

Gizlilik ve Çerez Politikası Bilgi Güvenliği Politikası

Privia Security © 2018 Privacy For You



Automated page speed optimizations for fast site performance