NMAP Network Scanning

Ağ Keşfi ve Güvenlik Taraması için Resmi Nmap Projesi Kılavuzu

Table of Contents (İçindekiler)

        - RPM-based Distributions (Red Hat, Mandrake, SUSE, Fedora) (RPM tabanlı dağıtımlar (Red Hat, Mandrake, SUSE, Fedora))
        - Updating Red Hat, Fedora, Mandrake, and Yellow Dog Linux with Yum (Red Hat, Fedora, Mandrake ve Yellow Dog Linux'un Yum ile Güncellenmesi)
        - Debian Linux and Derivatives such as Ubuntu (Debian Linux ve Ubuntu gibi türevleri)
        - Other Linux Distributions (Diğer Linux Dağıtımları)
    - Windows
        - Windows Self-installer (Windows Kendi Kendine Yükleyici)
        - Command-line Zip Binaries (Komut Satırı Zip İkilileri)
            - Installing the Nmap zip binaries (Nmap zip ikili dosyalarının yüklenmesi)
        - Compile from Source Code (Kaynak Koddan Derleme)
        - Executing Nmap on Windows (Windows'ta Nmap Çalıştırma)
    - Apple Mac OS X
        - Executable Installer (Yürütülebilir Yükleyici)
        - Compile from Source Code (Kaynak Koddan Derleme)
            - Compile Nmap from source code (Nmap'i kaynak koddan derleme)
            - Compile Zenmap from source code (Zenmap'i kaynak koddan derleme)
        - Third-party Packages (Üçüncü Taraf Paketleri)
        - Executing Nmap on Mac OS X (Mac OS X üzerinde Nmap Çalıştırma)
    - Other Platforms (BSD, Solaris, AIX, AmigaOS) (Diğer Platformlar (BSD, Solaris, AIX, AmigaOS))
        - FreeBSD / OpenBSD / NetBSD (FreeBSD / OpenBSD / NetBSD)
            - OpenBSD Binary Packages and Source Ports Instructions (OpenBSD İkili Paketleri ve Kaynak Portları Talimatları)

        - FreeBSD Binary Package and Source Ports Instructions (FreeBSD İkili Paket ve Kaynak Portları Talimatları)
        - NetBSD Binary Package Instructions (NetBSD İkili Paket Talimatları)
      - Oracle/Sun Solaris (Oracle/Sun Solaris)
      - IBM AIX
      - AmigaOS
      - Other proprietary UNIX (HP-UX, IRIX, etc.) (Diğer tescilli UNIX (HP-UX, IRIX, vb.))
    - Removing Nmap (Nmap'i Kaldırma)
- **Chapter** 3. Host Discovery (“Ping Scanning”) (Bölüm 3. Ana Bilgisayar Bulma ("Ping Taraması"))
    - Introduction (Giriş)
    - Specifying Target Hosts and Networks (Hedef Ana Bilgisayarları ve Ağları Belirleme)
      - Input From List (`iL`) (Listeden Giriş (-iL))
      - Choose Targets at Random (`iR` `<numtargets>`) (Hedefleri Rastgele Seçme (-iR <numtargets>))
      - Excluding Targets (`-exclude` , `-excludefile` `<filename>`) (Hedefleri Hariç Tutma (--exclude, --excludefile <dosya adı>))
      - Practical Examples (Pratik Örnekler)
    - Finding an Organization's IP Addresses (Bir Kuruluşun IP Adreslerini Bulma)
      - DNS Tricks (DNS Hileleri)
      - Whois Queries Against IP Registries (IP Kayıtlarına Karşı Whois Sorguları)
      - Internet Routing Information (İnternet Yönlendirme Bilgileri)
    - DNS Resolution (DNS Çözünürlüğü)
    - Host Discovery Controls (Ana Bilgisayar Bulma Kontrolleri)

        - List Scan (`sL`) (Liste Taraması (-sL))
        - Disable Port Scan (`sn`) (Port Taramasını Devre Dışı Bırak (-sn))
        - Disable Ping (`Pn`) (Ping'i Devre Dışı Bırak (-Pn))
    - Host Discovery Techniques (Ana Bilgisayar Bulma Teknikleri)
        - TCP SYN Ping (`PS` *<port list>*) (TCP SYN Ping (-PS<port listesi>))
        - TCP ACK Ping (`PA` *<port list>*) (TCP ACK Ping (-PA<port listesi>))
        - UDP Ping (`PU` *<port list>*) (UDP Ping (-PU<port listesi>))
        - ICMP Ping Types (`PE` , `PP` , and `PM`) (ICMP Ping Türleri (-PE, -PP ve -PM))
        - IP Protocol Ping (`PO` *<protocol list>*) (IP Protokolü Ping (-PO<protokol listesi>))
        - ARP Scan (`PR`) (ARP Taraması (-PR))
        - Default Combination (Varsayılan Kombinasyon)
    - Putting It All Together: Host Discovery Strategies (Hepsini Bir Araya Getirme: Ana Bilgisayar Bulma Stratejileri)
        - Related Options (İlgili Seçenekler)
        - Choosing and Combining Ping Options (Ping Seçeneklerini Seçme ve Birleştirme)
            - Most valuable probes (En değerli problar)
            - TCP probe and port selection (TCP probu ve port seçimi)
            - UDP port selection (UDP port seçimi)
            - ICMP probe selection (ICMP prob seçimi)
            - Designing the ideal combinations of probes (İdeal prob kombinasyonlarını tasarlama)
    - Host Discovery Code Algorithms (Ana Bilgisayar Bulma Kodu Algoritmaları)
- **Chapter** 4. Port Scanning Overview (Bölüm 4. Port Taramaya Genel Bakış)
    - İçindekiler

- TCP Connect Scan (`sT`) (TCP Bağlantı Taraması (-sT))
- UDP Scan (`sU`) (UDP Taraması (-sU))
  - Distinguishing Open from Filtered UDP Ports (Açık ve Filtrelenmiş UDP Portlarını Ayırt Etme)
  - Speeding Up UDP Scans (UDP Taramalarını Hızlandırma)
- TCP FIN, NULL, and Xmas Scans (`sF` , `sN` , `sX`) (TCP FIN, NULL ve Xmas Taramaları (-sF, -sN, -sX))
- Custom Scan Types with `-scanflags` (--scanflags ile Özel Tarama Türleri)
  - Custom SYN/FIN Scan (Özel SYN/FIN Taraması)
  - PSH Scan (PSH Taraması)
- TCP ACK Scan (`sA`) (TCP ACK Taraması (-sA))
- TCP Window Scan (`sW`) (TCP Window Taraması (-sW))
- TCP Maimon Scan (`sM`) (TCP Maimon Taraması (-sM))
- TCP Idle Scan (`sI`) (TCP Idle Taraması (-sI))
  - Idle Scan Step by Step (Idle Taraması Adım Adım)
  - Finding a Working Idle Scan Zombie Host (Çalışan Bir Boşta Tarama Zombi Ana Bilgisayarı Bulma)
  - Executing an Idle Scan (Boşta Tarama Yürütme)
  - Idle Scan Implementation Algorithms (Idle Taraması Uygulama Algoritmaları)
- IP Protocol Scan (`sO`) (IP Protokolü Taraması (-sO))
- TCP FTP Bounce Scan (`b`) (TCP FTP Sıçrama Taraması (-b))
- Scan Code and Algorithms (Tarama Kodu ve Algoritmaları)
  - Network Condition Monitoring (Ağ Durumu İzleme)
  - Host and Port Parallelization (Ana Bilgisayar ve Bağlantı Noktası Paralelleştirme)
  - Round Trip Time Estimation (Gidiş Dönüş Süresi Tahmini)

        - Congestion Control (Tıkanıklık Kontrolü)
        - Timing probes (Zamanlama Probları)
        - Inferred Neighbor Times (Çıkarılan Komşu Süreleri)
        - Adaptive Retransmission (Uyarlanabilir Yeniden İletim)
        - Scan Delay (Tarama Gecikmesi)
- **Chapter** 6. Optimizing Nmap Performance (Bölüm 6. Nmap Performansını Optimize Etme)
    - Introduction (İçindekiler)
    - Scan Time Reduction Techniques (Tarama Süresini Azaltma Teknikleri)
        - Omit Non-critical Tests (Kritik Olmayan Testleri Atlayın)
        - Optimize Timing Parameters (Zamanlama Parametrelerini Optimize Edin)
        - Separate and Optimize UDP Scans (UDP Taramalarını Ayırın ve Optimize Edin)
        - Upgrade Nmap (Nmap'i Yükseltin)
        - Execute Concurrent Nmap Instances (Eşzamanlı Nmap Örnekleri Yürütün)
        - Scan From a Favorable Network Location (Uygun Bir Ağ Konumundan Tarayın)
        - Increase Available Bandwidth and CPU Time (Kullanılabilir Bant Genişliğini ve CPU Süresini Artırın)
    - Coping Strategies for Long Scans (Uzun Taramalar için Başa Çıkma Stratejileri)
        - Use a Multi-stage Approach (Çok Aşamalı Bir Yaklaşım Kullanın)
        - Estimate and Plan for Scan Time (Tarama Süresini Tahmin Edin ve Planlayın)
    - Port Selection Data and Strategies (Port Seçimi Verileri ve Stratejileri)
    - Low-Level Timing Controls (Düşük Seviyeli Zamanlama Kontrolleri)

    - Timing Templates (`T`) (Zamanlama Şablonları (-T))
    - Scanning 676,352 IP Addresses in 46 Hours (46 Saatte 676.352 IP Adresi Tarama)
- **Chapter 7.** Service and Application Version Detection (Bölüm 7. Hizmet ve Uygulama Sürümü Algılama)
    - Introduction (İçindekiler)
    - Usage and Examples (Kullanım ve Örnekler)
    - Technique Described (Açıklanan Teknik)
        - Cheats and Fallbacks (Hileler ve Geri Dönüşler)
        - Probe Selection and Rarity (Prob Seçimi ve Nadirlik)
    - Technique Demonstrated (Gösterilen Teknik)
    - Post-processors (Son işlemciler)
        - Nmap Scripting Engine Integration (Nmap Scripting Engine Entegrasyonu)
        - RPC Grinding (RPC Taşlama)
        - SSL Post-processor Notes (SSL Post-işlemci Notları)
    - `nmap-service-probes` File Format (nmap-service-probes Dosya Formatı)
        - `Exclude` Directive (Hariç Tutma Yönergesi)
        - `Probe` Directive (Prob Yönergesi)
        - `match` Directive (match Yönergesi)
        - `softmatch` Directive (softmatch Yönergesi)
        - `ports` and `sslports` Directives (ports ve sslports Yönergeleri)
        - `totalwaitms` Directive (totalwaitms Yönergesi)
        - `tcpwrappedms` Directive (tcpwrappedms Yönergesi)
        - `rarity` Directive (nadirlik Yönergesi)
        - `fallback` Directive (fallback Yönergesi)

        - Putting It All Together (Hepsini Bir Araya Getirme)
    - Community Contributions (Topluluk Katkıları)
        - Submit Service Fingerprints (Servis Parmak İzlerini Gönder)
        - Submit Database Corrections (Veritabanı Düzeltmelerini Gönder)
        - Submit New Probes (Yeni Probları Gönder)
    - SOLUTION: Find All Servers Running an Insecure or Nonstandard Application Version (ÇÖZÜM: Güvensiz veya Standart Olmayan Uygulama Sürümü Çalıştıran Tüm Sunucuları Bulun)
        - Problem (Sorun)
        - Solution (Çözüm)
        - Discussion (Tartışma)
    - SOLUTION: Hack Version Detection to Suit Custom Needs, such as Open Proxy Detection (ÇÖZÜM: Açık Proxy Algılama gibi Özel İhtiyaçlara Uygun Sürüm Algılamayı Hackleyin)
        - Problem (Sorun)
        - Solution (Çözüm)
        - Discussion (Tartışma)
- **Chapter 8.** Remote OS Detection (Bölüm 8. Uzak İşletim Sistemi Algılama)
    - Introduction (Giriş)
        - Reasons for OS Detection (İşletim Sistemi Algılama Nedenleri)
            - Determining vulnerability of target hosts (Hedef ana bilgisayarların güvenlik açığını belirleme)
            - Tailoring exploits (Terzilik açıkları)
            - Network inventory and support (Ağ envanteri ve desteği)
            - Detecting unauthorized and dangerous devices (Yetkisiz ve tehlikeli cihazların tespit edilmesi)
            - Social engineering (Sosyal mühendislik)

- Usage and Examples (Kullanım ve Örnekler)
- TCP/IP Fingerprinting Methods Supported by Nmap (Nmap Tarafından Desteklenen TCP/IP Parmak İzi Yöntemleri)
  - Probes Sent (Probes Sent)
    - Sequence generation (`SEQ`, `OPS`, `WIN`, and `T1`) (Sekans oluşturma (SEQ, OPS, WIN ve T1))
    - ICMP echo (`IE`) (ICMP yankısı (IE))
    - TCP explicit congestion notification (`ECN`) (TCP açık tıkanıklık bildirimi (ECN))
    - TCP (`T2`–`T7`)
    - UDP (`U1`)
  - Response Tests (Yanıt Testleri)
    - TCP ISN greatest common divisor (`GCD`) (TCP ISN en büyük ortak bölen (GCD))
    - TCP ISN counter rate (`ISR`) (TCP ISN sayaç oranı (ISR))
    - TCP ISN sequence predictability index (`SP`) (TCP ISN sıra tahmin edilebilirlik endeksi (SP))
    - IP ID sequence generation algorithm (`TI`, `CI`, `II`) (IP ID dizisi oluşturma algoritması (TI, CI, II))
    - Shared IP ID sequence Boolean (`SS`) (Paylaşılan IP Kimliği sırası Boolean (SS))
    - TCP timestamp option algorithm (`TS`) (TCP zaman damgası seçeneği algoritması (TS))
    - TCP options (`O`, `O1`–`O6`) (TCP seçenekleri (O, O1-O6))
    - TCP initial window size (`W`, `W1`–`W6`) (TCP başlangıç pencere boyutu (W, W1-W6))
    - Responsiveness (`R`) (Duyarlılık (R))
    - IP don't fragment bit (`DF`) (IP parçalama biti (DF))

- Don't fragment (ICMP) (`DFI`) (Parçalama (ICMP) (DFI))
- IP initial time-to-live (`T`) (IP ilk yaşam süresi (T))
- IP initial time-to-live guess (`TG`) (IP ilk zaman-canlı tahmin (TG))
- Explicit congestion notification (`CC`) (Açık tıkanıklık bildirimi (CC))
- TCP miscellaneous quirks (`Q`) (TCP çeşitli tuhaflıklar (Q))
- TCP sequence number (`S`) (TCP sıra numarası (S))
- TCP acknowledgment number (`A`) (TCP onay numarası (A))
- TCP flags (`F`) (TCP bayrakları (F))
- TCP RST data checksum (`RD`) (TCP RST veri sağlama toplamı (RD))
- IP total length (`IPL`) (IP toplam uzunluğu (IPL))
- Unused port unreachable field nonzero (`UN`) (Kullanılmayan bağlantı noktası ulaşılamaz alanı sıfır olmayan (UN))
- Returned probe IP total length value (`RIPL`) (İade edilen prob IP toplam uzunluk değeri (RIPL))
- Returned probe IP ID value (`RID`) (İade edilen prob IP kimlik değeri (RID))
- Integrity of returned probe IP checksum value (`RIPCK`) (İade edilen prob IP sağlama toplamı değerinin bütünlüğü (RIPCK))
- Integrity of returned probe UDP checksum (`RUCK`) (İade edilen prob UDP sağlama toplamının bütünlüğü (RUCK))
- Integrity of returned UDP data (`RUD`) (İade edilen UDP verilerinin bütünlüğü (RUD))
- ICMP response code (`CD`) (ICMP yanıt kodu (CD))

◦ IPv6 fingerprinting (IPv6 parmak izi)

▪ Probes Sent (Problar Gönderimi)

- Sequence generation (`S1` – `S6`) (Dizi oluşturma (S1-S6))
- ICMPv6 echo (`IE1`)

        - ICMPv6 echo (`IE2`)
        - Node Information Query (`NI`) (Düğüm Bilgisi Sorgusu (NI)
        - Neighbor Solicitation (`NS`) (Komşu İsteği (NS))
        - UDP (`U1`)
        - TCP explicit congestion notification (`TECN`) (TCP açık tıkanıklık bildirimi (TECN))
        - TCP (`T2`–`T7`)
      - Feature extraction (Özellik çıkarma)
        - List of all features (Tüm özelliklerin listesi)
      - Differences from IPv4 (IPv4'ten Farklılıklar)
    - Fingerprinting Methods Avoided by Nmap (Nmap Tarafından Kaçınılan Parmak İzi Yöntemleri)
      - Passive Fingerprinting (Pasif Parmak İzi)
      - Exploit Chronology (İstismar Kronolojisi)
      - Retransmission Times (Yeniden İletim Süreleri)
      - IP Fragmentation (IP Parçalanması)
      - Open Port Patterns (Açık Bağlantı Noktası Kalıpları)
      - Retired Tests (Emekli Testler)
    - Understanding an Nmap Fingerprint (Nmap Parmak İzini Anlama)
      - Decoding the Subject Fingerprint Format (Denek Parmak İzi Formatının Şifresini Çözme)
        - Decoding the `SCAN` line of a subject fingerprint (Bir deneğin parmak izinin TARAMA satırının kodunun çözülmesi)
      - Decoding the Reference Fingerprint Format (Referans Parmak İzi Formatının Kodunu Çözme)
        - Free-form OS description (`Fingerprint` line) (Serbest biçimli işletim sistemi açıklaması (Parmak izi satırı))

        - Command-line Arguments (Komut Satırı Bağımsız Değişkenleri)
        - Script Selection (Komut Dosyası Seçimi)
        - Arguments to Scripts (Komut Dosyalarına Bağımsız Değişkenler)
        - Complete Examples (Tam Örnekler)
    - Script Format (Komut Dosyası Biçimi açıklaması)
        - `description` Field (Alan kategorileri)
        - `categories` Field ()
        - `author` Field (Alan yazarı)
        - `license` Field (Alan lisansı)
        - `dependencies` Field (Alan bağımlılıkları)
        - Rules (Alan Kuralları)
        - Action (Eylem)
        - Environment Variables (Ortam Değişkenleri)
    - Script Language (Komut Dosyası Dili)
        - Lua Base Language (Lua Temel Dil)
    - NSE Scripts (NSE Komut Dosyaları)
    - NSE Libraries (NSE Kütüphaneleri)
        - List of All Libraries (Tüm Kütüphanelerin Listesi)
        - Hacking NSE Libraries (NSE Kütüphanelerini Hackleme)
        - Adding C Modules to Nselib (Nselib'e C Modülleri Ekleme)
    - Nmap API (Nmap API)
        - Information Passed to a Script (Bir Komut Dosyasına Aktarılan Bilgiler)
        - Network I/O API (Ağ G/Ç API)
            - Connect-style network I/O (Bağlan-stil ağ G/Ç)
            - Raw packet network I/O (Ham paket ağ G/Ç)

        - Structured and Unstructured Output (Yapılandırılmış ve Yapılandırılmamış Çıktı)
        - Exception Handling (İstisna İşleme)
        - The Registry (Kayıt Defteri)
    - Script Writing Tutorial (Komut Dosyası Yazma Eğitimi)
        - The Head (Baş)
        - The Rule (Kural)
        - The Action (Eylem)
    - Writing Script Documentation (NSEDoc) (Komut Dosyası Yazma Belgeleri (NSEDoc))
        - NSE Documentation Tags (NSE Belgeleri Etiketler)
    - Script Parallelism in NSE (Komut Dosyası NSE'de Paralellik)
        - Worker Threads (Çalışan İş Parçacıkları)
        - Mutexes (Muteksler)
        - Condition Variables (Koşul Değişkenleri)
        - Collaborative Multithreading (İşbirlikçi Çoklu İş Parçacığı)
            - The base thread (Temel iplik)
    - Version Detection Using NSE (NSE Kullanarak Sürüm Algılama)
    - Example Script: `finger` (Örnek Kod: parmak)
    - Implementation Details (Uygulama Detayları)
        - Initialization Phase (Başlatma Aşaması)
        - Script Scanning (Komut Dosyası Taraması)
- **Chapter 10**. Detecting and Subverting Firewalls and Intrusion Detection Systems (Bölüm 10. Güvenlik Duvarlarını ve Saldırı Tespit Sistemlerini Tespit Etme ve Yıkma)
    - Introduction (Giriş)

- Why Would Ethical Professionals (White-hats) Ever Do This? (Etik Profesyonelleri (Beyaz Şapkalılar) Bunu Neden Yapsın?)
- Determining Firewall Rules (Güvenlik Duvarı Kurallarını Belirleme)
  - Standard SYN Scan (Standart SYN Taraması)
    - Sneaky firewalls that return RST (RST döndüren sinsi güvenlik duvarları)
  - ACK Scan (ACK Scan)
  - IP ID Tricks (IP Kimliği Hileleri)
  - UDP Version Scanning (UDP Sürüm Taraması)
- Bypassing Firewall Rules (Güvenlik Duvarı Kurallarını Atlama)
  - Exotic Scan Flags (Egzotik Tarama Bayrakları)
  - Source Port Manipulation (Kaynak Bağlantı Noktası Manipülasyonu)
  - IPv6 Attacks (IPv6 Saldırıları)
  - IP ID Idle Scanning (IP Kimliği Boşta Tarama)
  - Multiple Ping Probes (Çoklu Ping Probları)
  - Fragmentation (Parçalanma)
  - Proxies (Proxyler)
  - MAC Address Spoofing (MAC Adresi Sahtekarlığı)
  - Source Routing (Kaynak Yönlendirme)
  - FTP Bounce Scan (FTP Sıçrama Taraması)
  - Take an Alternative Path (Alternatif Bir Yol İzleyin)
  - A Practical Real-life Example of Firewall Subversion (Güvenlik Duvarı Subversion'ının Gerçek Hayattan Pratik Bir Örneği)
- Subverting Intrusion Detection Systems (İzinsiz Giriş Tespit Sistemlerini Yıkmak)
  - Intrusion Detection System Detection (İzinsiz Giriş Tespit Sistemi Tespiti)

    - Reverse probes (Ters problar)
    - Sudden firewall changes and suspicious packets (Ani güvenlik duvarı değişiklikleri ve şüpheli paketler)
    - Naming conventions (Adlandırma kuralları)
    - Unexplained TTL jumps (Açıklanamayan TTL atlamaları)
- Avoiding Intrusion Detection Systems (İzinsiz Giriş Tespit Sistemlerinden Kaçınma)
    - Slow down (Yavaşla)
    - Scatter probes across networks rather than scanning hosts consecutively (Ana bilgisayarları art arda taramak yerine probları ağlara dağıtın)
    - Fragment packets (Paketleri parçalama)
    - Evade specific rules (Belirli kurallardan kaçınmak)
    - Avoid easily detected Nmap features (Kolayca tespit edilen Nmap özelliklerinden kaçının)
- Misleading Intrusion Detection Systems (Yanıltıcı Saldırı Tespit Sistemleri)
    - Decoys ()
    - Port scan spoofing (Port tarama sahtekarlığı)
    - Idle scan (Boşta tarama)
    - DNS proxying (DNS proxyleme)
- DoS Attacks Against Reactive Systems (Reaktif Sistemlere Karşı DoS Saldırıları)
- Exploiting Intrusion Detection Systems (İzinsiz Giriş Tespit Sistemlerinden Yararlanma)
- Ignoring Intrusion Detection Systems (İzinsiz Giriş Tespit Sistemlerini Görmezden Gelmek)

    - Detecting Packet Forgery by Firewall and Intrusion Detection Systems (Güvenlik Duvarı ve Saldırı Tespit Sistemleri ile Paket Sahteciliğinin Tespiti)
        - Look for TTL Consistency (TTL Tutarlılığına Bakın)
        - Look for IP ID and Sequence Number Consistency (IP Kimliği ve Sıra Numarası Tutarlılığına Bakın)
        - The Bogus TCP Checksum Trick (Sahte TCP Checksum Hilesi)
        - Round Trip Times (Gidiş Dönüş Süreleri)
        - Close Analysis of Packet Headers and Contents (Paket Başlıklarının ve İçeriklerinin Yakın Analizi)
        - Unusual Network Uniformity (Olağandışı Ağ Tekdüzeliği)
- **Chapter 11.** Defenses Against Nmap (Bölüm 11. Nmap'e Karşı Savunmalar)
    - Introduction (Giriş)
    - Scan Proactively, Then Close or Block Ports and Fix Vulnerabilities (Proaktif Olarak Tarayın, Ardından Bağlantı Noktalarını Kapatın veya Engelleyin ve Güvenlik Açıklarını Düzeltin)
    - Block and Slow Nmap with Firewalls (Güvenlik Duvarları ile Nmap'i Engelleme ve Yavaşlatma)
    - Detect Nmap Scans (Nmap Taramalarını Algılama)
    - Clever Trickery (Zeki Hileler)
        - Hiding Services on Obscure Ports (Belirsiz Bağlantı Noktalarındaki Hizmetleri Gizleme)
        - Port Knocking (Liman Vuruntusu)
        - Honeypots and Honeynets (Honeypotlar ve Honeynetler)
        - OS Spoofing (İşletim Sistemi Sahtekarlığı)
        - Tar Pits (Tar Pits)
        - Reactive Port Scan Detection (Reaktif Port Tarama Algılama)
        - Escalating Arms Race (Tırmanan Silahlanma Yarışı)

- **Chapter 12.** Zenmap GUI Users' Guide (Bölüm 12. Zenmap GUI Kullanıcı Kılavuzu)
  - Introduction (Giriş)
    - The Purpose of a Graphical Frontend for Nmap (Nmap için Grafiksel Önyüzün Amacı)
  - Scanning (Tarama)
    - Profiles (Profiller)
    - Scan Aggregation (Tarama Birleştirme)
  - Interpreting Scan Results (Tarama Sonuçlarını Yorumlama)
    - Scan Results Tabs (Tarama Sonuçları Sekmeleri)
      - The “Nmap Output” tab ("Nmap Çıktısı" sekmesi)
      - The “Ports / Hosts” tab ("Bağlantı Noktaları / Ana Bilgisayarlar" sekmesi)
      - The “Topology” tab ("Topoloji" sekmesi)
      - The “Host Details” tab ("Ana Bilgisayar Ayrıntıları" sekmesi)
      - The “Scans” tab ("Taramalar" sekmesi)
    - Sorting by Host (Ana Bilgisayara Göre Sıralama)
    - Sorting by Service (Hizmete Göre Sıralama)
  - Saving and Loading Scan Results (Tarama Sonuçlarını Kaydetme ve Yükleme)
    - The Recent Scans Database (Son Taramalar Veritabanı)
  - Surfing the Network Topology (Ağ Topolojisinde Gezinme)
    - An Overview of the “Topology” Tab ("Topoloji" Sekmesine Genel Bir Bakış)
    - Legend (Gösterge)
    - Controls (Kontroller)
      - Action controls (Eylem kontrolleri)

        - Interpolation controls (Enterpolasyon kontrolleri)
        - Layout controls (Düzen kontrolleri)
        - View controls (Görünüm kontrolleri)
        - Fisheye controls (Balıkgözü kontrolleri)
      - Keyboard Shortcuts (Klavye Kısayolları)
      - The Hosts Viewer (Ana Bilgisayarlar Görüntüleyici)
    - The Profile Editor (Profil Düzenleyici)
      - Editing a Command (Komut düzenleme)
        - Script selection (Senaryo Seçimi)
      - Creating a New Profile (Yeni Profil Oluşturma)
      - Editing or Deleting a Profile (Profili Düzenleme veya Silme)
    - Host Filtering (Ana Bilgisayar Filtreleme)
    - Searching Saved Results (Kaydedilen Sonuçları Arama)
    - Comparing Results (Sonuçları Karşılaştırma)
    - Zenmap in Your Language (Kendi Dilinizde Zenmap)
      - Creating a new translation (Yeni bir çeviri oluşturma)
    - Files Used by Zenmap (Zenmap Tarafından Kullanılan Dosyalar)
      - The `nmap` Executable (nmap Çalıştırılabiliri)
      - System Configuration (Files Sistem Yapılandırma Dosyaları)
      - Per-user Configuration Files (Per-kullanıcı Yapılandırma Dosyaları)
      - Output Files (Çıktı Dosyaları)
    - Description of `zenmap.conf` (zenmap'in açıklaması.conf)
      - Sections of `zenmap.conf` (zenmap.conf'un Bölümleri)
    - Command-line Options (Komut Satırı Seçenekleri)
      - Synopsis (Özet)
      - Options Summary (Seçenekler Özeti)

        - Error Output (Hata Çıktı)
    - History (Geçmiş)
- **Chapter 13.** Nmap Output Formats (Bölüm 13. Nmap Çıktı Biçimleri)
    - Introduction (Giriş)
    - Command-line Flags (Komut Satırı Bayrakları)
        - Controlling Output Type (Çıktı Türünü Kontrol Etme)
        - Controlling Verbosity of Output (Çıktının Ayrıntılarını Kontrol Etme)
        - Enabling Debugging Output (Hata Ayıklama Çıktısını Etkinleştirme)
        - Enabling Packet Tracing (Paket İzlemeyi Etkinleştirme)
        - Resuming Aborted Scans (Durdurulan Taramaları Sürdürme)
    - Interactive Output (Etkileşimli Çıktı)
    - Normal Output (`oN`) (Normal Çıktı (-oN))
    - $crIpT kIddI3 0uTPut (`oS`) ($crIpT kIddI3 0uTPut (-oS))
    - XML Output (`oX`) (XML Çıktısı (-oX))
        - Using XML Output (XML Çıktısını Kullanma)
    - Manipulating XML Output with Perl (XML Çıktısını Perl ile Yönetme)
    - Common Platform Enumeration (CPE) (Ortak Platform Numaralandırma (CPE))
        - Structure of a CPE Name (CPE Adının Yapısı)
    - Output to a Database (Veritabanına Çıktı)
    - Creating HTML Reports (HTML Raporları Oluşturma)
        - Saving a Permanent HTML Report (Kalıcı HTML Raporunu Kaydetme)
    - Grepable Output (`oG`) (Grepable Çıktısı (-oG))
        - Grepable Output Fields (Greplenebilir Çıktı Alanları)
            - `Host` field (Ana Bilgisayar alanı)
            - `Status` field (Durum alanı)

        - `Ports` field (Bağlantı Noktaları alanı)
        - `Protocols` field (Protokoller alanı)
        - `Ignored State` field (Yoksayılan Durum alanı)
        - `OS` field (İşletim Sistemi alanı)
        - `Seq Index` field (Seq Dizini alanı)
        - `IP ID Seq` field (IP Kimliği Seq alanı)
    - Parsing Grepable Output on the Command Line (Komut Satırında Grepable Çıktısını Ayrıştırma)
- **Chapter 14.** Understanding and Customizing Nmap Data Files (Bölüm 14. Nmap Veri Dosyalarını Anlama ve Özelleştirme)
    - Introduction (Giriş)
    - Well Known Port List: `nmap-services` (İyi Bilinen Bağlantı Noktası Listesi: nmap-services)
    - Version Scanning DB: `nmap-service-probes` (Sürüm Tarama DB: nmap-service-probes)
    - SunRPC Numbers: `nmap-rpc` (SunRPC Numaraları: nmap-rpc)
    - Nmap OS Detection DB: `nmap-os-db` (Nmap İşletim Sistemi Algılama DB: nmap-os-db)
    - MAC Address Vendor Prefixes: `nmap-mac-prefixes` (MAC Adresi Satıcı Önekleri: nmap-mac-prefixes)
    - IP Protocol Number List: `nmap-protocols` (IP Protokol Numarası Listesi: nmap-protocols)
    - Files Related to Scripting (Scripting ile İlgili Dosyalar)
    - Using Customized Data Files (Özelleştirilmiş Veri Dosyalarını Kullanma)
- **Chapter 15.** Nmap Reference Guide (Bölüm 15. Nmap Referans Kılavuzu)
    - Description (Açıklama)
    - Options Summary (Seçenekler Özet)
    - Target Specification (Hedef Belirleme)

- Host Discovery (Ana Bilgisayar Bulma)
- Port Scanning Basics (Bağlantı Noktası Tarama Temelleri)
- Port Scanning Techniques (Bağlantı Noktası Tarama Teknikleri)
- Port Specification and Scan Order (Bağlantı Noktası Belirleme ve Tarama Sırası)
- Service and Version Detection (Hizmet ve Sürüm Algılama)
- OS Detection (İşletim Sistemi Algılama)
- Nmap Scripting Engine (NSE) (Nmap Scripting Engine (NSE))
- Timing and Performance (Zamanlama ve Performans)
- Firewall/IDS Evasion and Spoofing (Güvenlik Duvarı/IDS Kaçırma ve Aldatma)
- Output (Çıktı)
- Miscellaneous Options (Çeşitli Seçenekler)
- Runtime Interaction (Çalışma Zamanı)
- Examples (Etkileşim Örnekleri)
- Nmap Book (Nmap Kitabı)
- Bugs (Hatalar)
- Authors (Yazarlar)
- Legal Notices (Yasal Bildirimler)
    - Nmap Copyright and Licensing (Nmap Telif Hakkı ve Lisanslama)
    - Creative Commons License for this Nmap Guide (Bu Nmap Kılavuzu için Creative Commons Lisansı)
    - Source Code Availability and Community Contributions (Kaynak Kodu Kullanılabilirliği ve Topluluk Katkıları)
    - No Warranty (Garanti Yok)
    - Inappropriate Usage (Uygunsuz Kullanım)

NMAP Preface (önsöz)

- Introduction (Giriş)
- Intended Audience and Organization
- Conventions
- Other Resources
- Request for Comments
- Acknowledgements
    - Technology Used to Create This Book
- TCP/IP Reference

Introduction (Giriş)

1 Eylül 1997'de, adını taşıyan bir güvenlik tarayıcısı yayınladım. *Prack* dergisinin elli birinci sayısında Nmap. Benim hedefim Özel amaçlı port tarayıcılarının parçalanmış alanını konsolide
Tutyar bir arayüz sağlayan güçlü ve esnek bir ücretsiz araç tüm pratik port taramasının verimli bir şekilde uygulanması Teknikler. Nmap daha sonra üç dosyadan oluşuyordu (sıfırdı
2.000 satır kod) ve yalnızca Linux işletim sistemini destekledi. Kendi amaçlarım için yazılmıştı ve umudumla serbest bırakıldı. Diğerleri bunu yararlı bulurdu.

Bu mütevazı başlangıçlardan ve açıkların gücünden Kaynak geliştirme, Nmap dünyanın en popüler ağına dönüştü Güvenlik tarayıcısı, milyonlarca insanla Dünya çapında kullanıcılar. Yıllar geçtikçe, Nmap gelişmiş eklemeye devam etti. uzaktan işletim sistemi algılama, sürüm / hizmet algılama gibi işlevsellik, Ve Nmap Senaryo Motoru. Artık tüm büyük Unix, Windows ve Mac OS'yi destekliyor
Hem konsol hem de grafik arayüzleri olan platformlar.
Linux Journal dahil yayınlar,

Bilgi Dünyası,LinuxQuestions.Org, ve the *Codetalker Digest,* Nmap'ı tanıdı
“Yılın güvenlik aracı”. Hatta içinde bile yer aldı
The Matrix dahil dokuz filmYeniden *yüklendi, Ejderha Dövmeli Kız, The Bourne Ultimatum* ve *Die Hard* 4.

Nmap (“Ağ Haritalayıcısı”) ücretsiz ve açık bir kaynak faydasıdır. Ağ arama ve güvenlik denetimi. Birçok sistem ve ağ Yöneticiler ayrıca ağ gibi görevler için yararlı buluyor
envanter, hizmet yükseltme programlarını yönetme ve ev sahibini izleme Servis çalışma zamanı. Nmap, çiğ IP paketlerini belirlemek için yeni yollarla kullanıyor Ağda hangi ev sahiplerinin mevcut olduğu, hangi hizmetler (ipkis İsim ve versiyon) bu ev sahipleri, hangi işletim sistemleri sunuyor
(ve OS versiyonları) koşuyorlar, ne tür bir paket Filtreler / güvenlik duvarları ve düzinelerce başka özelliktedir. O Büyük ağları hızla taramak için tasarlandı, ancak karşı iyi çalışıyor
Tek ev sahibi. Nmap son derece güçlü olsa da, aynı zamanda karmaşıktır. 100 komut satırı seçeneği, ağ guruları için ifadeler ekler, ancak Acemileri karıştırabilir. Bazı seçenekleri hiç olmadı bile Belgelenmiş. Bu kitap tüm harita özelliklerini ve daha fazlasını belgeliyor Daha da önemlisi, onları kullanmanın en etkili yollarını öğretir. var Nmap'ın sahip olduğu gibi sürekli güncelleme ile yazmak için yaklaşık dört yıl sürdü. Evrimleşmiştir. Bu kitap, kullanıcıların ve geliştiricilerin Nmap topluluğuna adanmıştır. Tutkunuz, fikirlerininiz, yamalarınız, özellik istekleri, alev savaşlarınız, böcek
Raporlar ve gece yarısı rantları Nmap'ı bugün olduğu gibi şekillendirdi.

Intended Audience and Organization (Hedef Kitle ve Organizasyon)

Bu kitap, limandan ücretsiz Nmap Güvenlik Tarayıcısı'na belgeliyor Acemiler için temelleri, paket hazırlamanın kullandığı paket hazırlama türlerine tarama Gelişmiş bilgisayar korsanları. Nmap kullanıcılarına (veya potansiyel kullanıcılara) fayda sağlamalıdır Tüm deneyim seviyeleri.

Temel bilgilerle başlayarak, bu kitap Nmap'a genel bir bakış sunuyor. 1. Bölümde örnek. Sonra Bölüm 2, elde etmeyi, derlemeyi ve Nmap'ı kurmak. Bölümler 3 ila 5 kapak özellikleri size sırayla
Penetrasyon testi yaparken bunları kullanabilir. İlk geliyor ev sahibi Keşif (“ping taraması”), bu da belirleyici Bir ağdaki ev sahipleri. Ardından, port taraması kapsanıyor Derinlik. Bölüm 5'te, tüm Nmap tarama teknikleri ayrıntılıdır, Tavsiye ve

örneklerle. Büyük bir ağı taramak uzun sürebilir
Zaman, yani Bölüm 6 performans optimizasyonu tavsiyesiyle doludur. Bölüm 7 ayrıntıları hizmet ve uygulama sürüm algılama, Nmap, portları tam olarak neyin çalıştırın yerine çalıştırılabileceğini belirlemek için sorgular Sadece liman numarasına göre tahmin etmek. Bölüm 8 bir tanesini kapsar
Nmap'ın en sevilen özellikleri: uzaktan işletim sistemi tespiti. Bölüm 9 detayları Kullanıcıların yazmalarını sağlayan Nmap Scripting Engine (NSE) Paylaş) çok çeşitli ağ görevlerini otomatikleştirmek için basit komut dosyaları. En sevdiğim bölüm 10 numara:
Tespit ve Altyazılı
Güvenlik duvarları ve saldırı tespit sistemleri
. Denge için, Bunu, Nmap taramalarına karşı savunma konusunda bir bölüm takip ediyor. Bölüm 12 daha sonra Zenmap çoklu platform Nmpa GUI'yi tam olarak belgeliyor ve Sonuç izleyicisi. Sonraki iki bölüm çıkış formatlarını ve verilerini kapsar
Dosyalar. Son dört bölüm bütün için referans rehberleridir. Araç ailesi: Nmap, Ndiff, Ccat ve Nping. Bunlar hızlı Belirli komut satırı seçeneklerini veya kısa arama kaynakları özellik özetleri. Kitap boyunca dağınık ayrıntılı talimatlardır Bir ağı belirli bir şekilde taramak gibi ortak görevleri yerine getirmek tek açık TCP port veya tarama ile kablosuz erişim noktalarını tespit etmek Kablo tarafından. Önce her sorun tarif edilir, sonra bir Etkili çözüm sağlanır. Nihai bir tartışma bölümü tarif etti Çözüm daha derinlemesine ve alternatif çözümler sağlayabilir ve Benzer problemler hakkında bilgi.

Conventions (Sözleşmeler)

Nmap çıktısı bu kitap boyunca prensipleri ve özellikleri göstermek için kullanılmıştır. Çıktı genellikle anlatılan konuyla ilgisi olmayan satırları kesmek için düzenlenmiştir. Nmap tarafından yazdırılan tarihler/saatler ve sürüm numaraları da genellikle kaldırılır, çünkü bazı okuyucular bunları dikkat dağıtıcı bulur. Ana bilgisayar adları, IP adresleri ve MAC adresleri gibi hassas bilgiler değiştirilebilir veya kaldırılabilir. Diğer bilgiler kesilebilir veya satırlar yazdırılan bir sayfaya sığacak şekilde sarılabilir. Benzer düzenlemeler diğer uygulamaların çıktıları için de

yapılır. Örnek 1, Nmap'in yeteneklerine bir bakış sunarken çıktı biçimlendirmesini de göstermektedir.

Örnek 1. Tipik bir Nmap taraması

```
# nmap -A -T4 scanme.nmap.org

Starting Nmap ( https://nmap.org )
Nmap scan report for scanme.nmap.org (64.13.134.52)
Host is up (0.034s latency).
Not shown: 994 filtered ports
PORT      STATE  SERVICE VERSION
22/tcp    open   ssh     OpenSSH 4.3 (protocol 2.0)
| ssh-hostkey: 1024 60:ac:4d:51:b1:cd:85:09:12:16:92:76:1d:5d:27:6e (DSA)
|_2048 2c:22:75:60:4b:c3:3b:18:a2:97:2c:96:7e:28:dc:dd (RSA)
53/tcp    open   domain
70/tcp    closed gopher
80/tcp    open   http    Apache httpd 2.2.3 ((CentOS))
| http-methods: Potentially risky methods: TRACE
|_See https://nmap.org/nsedoc/scripts/http-methods.html
|_html-title: Go ahead and ScanMe!
113/tcp   closed auth
31337/tcp closed Elite
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.18 (CentOS 5.4)
Network Distance: 10 hops

TRACEROUTE (using port 113/tcp)
HOP RTT      ADDRESS
[Cut first eight hops for brevity]
9   20.29 ms xe6-2.core1.svk.layer42.net (69.36.239.221)
10  19.58 ms scanme.nmap.org (64.13.134.52)

Nmap done: 1 IP address (1 host up) scanned in 25.97 seconds
```

Dosya adları ve uygulama komutları gibi belirli simgeler için özel biçimlendirme sağlanmıştır. Tablo 1 en yaygın biçimlendirme kurallarını göstermektedir.

Tablo 1. Biçimlendirme stili kuralları

Token type	Example
Literal string	Açık durumdaki portlar beni kapalı veya filtrelenmiş olarak bildirilenlerden çok daha fazla heyecanlandırıyor.
Command-line options	En havalı, ancak en az anlaşılan Nmap seçeneklerinden biri --packet-trace'dir.
Filenames	C:\net\dhcp-leases.txt veya /home/h4x/hosts-to-pwn.lst gibi girdi dosya adı ile -iL seçeneğini izleyin.
Emphasis	Bankalara ve askeri hedeflere saldırmak için iş veya okul bilgisayarınızdan Nmap kullanmak kötü bir fikirdir.
Application commands	Trinity Matrix'i nmap -v -sS -O 10.2.2.2 komutu ile taradı.

Replaceable variables	<kaynak> Nmap çalıştıran makine ve <hedef> microsoft.com olsun.

Other Resources (Diğer Araştırmalar)

Bu kitap Nmap için önemli bir referans olsa da, tek referans değildir. https://nmap.org adresindeki Nmap web sayfası sadece indirmeler için değildir. Aynı zamanda Nmap geliştiricilerinden ve üçüncü taraflardan önemli belgeler de sağlar. Örneğin, bir düzine dile çevrilmiş Nmap Referans Kılavuzunu burada bulabilirsiniz. Nmap'i kapsayan başka kitaplar, videolar ve makaleler de mevcuttur.

Bu kitabın resmi web sitesi https://nmap.org/book/'dur. Hatalar, güncellemeler ve birçok örnek bölüm için oraya gidin.

Her ciddi Nmap kullanıcısı, Nmap ve Insecure.Org ile ilgili duyurular için nmap-hackers posta listesine abone olmalıdır. Trafik çok azdır (yılda yaklaşık altı gönderi) çünkü yalnızca en önemli duyurular için ayrılmıştır. Geliştiriciler ve özellikle sadık kullanıcılar nmap-dev posta listesine de abone olabilirler. Trafik çok daha yüksektir (ayda yüzlerce gönderi), ancak yeni özellikleri yayınlanmadan önce öğrenmek ve denemek ve ileri düzey kullanıcılardan ipuçları almak için harika bir yerdir. Her iki liste için abonelik bilgileri ve arşivler https://seclists.org adresinde mevcuttur.

Nmap faydalı olsa da, tüm güvenlik sorunlarınızı çözmeyecektir. Her birkaç yılda bir binlerce Nmap kullanıcısıyla başka hangi araçları sevdiklerini belirlemek için bir anket yapıyorum. Liste, en popüler web sitelerimden biri haline gelen https://sectools.org adresinde yayınlanıyor. Listeyi okuduğunuzda daha önce hiç duymadığınız pek çok cevherle karşılaşacağınızdan emin olabilirsiniz. Araçların çoğu ücretsiz ve açık kaynak kodludur.

Request for Comments (Yorum Talebi)

Bu kitabın kapsamlı, doğru ve güncel olması için elimden gelenin en iyisini yapmaya çalışsam da, hepimiz hata yapabiliriz. Herhangi bir sorun bulursanız veya bu kitabı daha iyi hale getirmek için önerileriniz varsa, lütfen fyodor@nmap.org

adresine e-posta göndererek bana bildirin. Birçok okuyucu ve katkıda bulunanın açık kaynak ilkesi, yazılım için olduğu kadar dokümantasyon için de geçerlidir. Bir sonraki bölümün de kanıtladığı gibi, düzinelerce insan bu kitabın başarılı olması için zamanlarını ve becerilerini cömertçe ortaya koymuştur.

Nmap hakkında bir sorunuz veya yorumunuz varsa (bu kitabın kendisi yerine), en iyisi "Hatalar" adlı bölümde açıklandığı gibi Nmap geliştirme listesine göndermenizdir.

Acknowledgements (Teşekkür)

Bir Nmap kitabı yazma fikrini ilk kez nmap-hackers e-posta listesine sunduğumda, öneriler ve yardım teklifleriyle dolup taştım. Bu coşku seli beni devam etmeye ikna etti. Ne kadar çok çalışmanın söz konusu olduğu konusundaki saflığım da kararıma katkıda bulundu. Oldukça büyük bir girişim oldu, ancak beni bölüm bölüm devam ettiren şey nmap-yazarları adlı özel bir inceleme grubuydu. Süreç boyunca çok değerli geri bildirimler, tavsiyeler ve ayrıntılı inceleme notları sağladılar. Özellikle aşağıdaki kişilere teşekkür etmek isterim:

- David Fifield ilk sırada yer alıyor (diğer herkes alfabetik olarak sıralanmıştır) çünkü kitabın yazım sürecinde çok büyük yardımları oldu. Bir dizi teknik DocBook sorununu çözdü, benim berbat taslaklarımdan nihai resimlerin çoğunu yarattı, dizini önemli ölçüde geliştirdi, düzeltme okumasına yardımcı oldu ve hatta Bölüm 12, Zenmap GUI Kullanıcı Kılavuzu'nu yazdı.
- Matt Baxter, güzel TCP/IP başlık diyagramlarının ("TCP/IP Referansı" adlı bölümde) kullanılmasına izin verdi. Bu kitaptaki diğer bazı diyagramlar da buna uygun olarak bu tarzda yapılmıştır.
- Saurabh Bhasin düzenli olarak ayrıntılı geri bildirimde bulundu.
- Mark Brewis'e her zaman iyi tavsiyeler için güvenilebilir.
- Ellen Colombo en başından beri çok yardımcı oldu.
- Patrick Donnelly Bölüm 9, Nmap Scripting Engine'in geliştirilmesine yardımcı oldu.
- Brandon Enright tüm kitabın çıktısını aldı ve bölüm bölüm gözden geçirdi.

- Brian Hatch her zaman çok yardımcı olmuştur.
- Loren Heal sürekli bir fikir kaynağıydı.
- Lee "MadHat" Heath "MadHat Harikalar Diyarında" adlı bölümü ve ayrıca "Grepable Output (-oG)" adlı bölümün erken bir versiyonunu yazdı.
- Dan Henage tavsiyelerde bulundu ve birçok bölümü düzeltti.
- Tor Houghton her bölümü gözden geçirdi ve muhtemelen bana herkesten daha fazla geri bildirim verdi.
- Doug Hoyte, eklediği birçok Nmap özelliğini belgeledi ve ayrıca kitabın indekslenmesinin çoğunu üstlendi.
- Marius Huse Jacobsen birçok bölümü gözden geçirerek ayrıntılı geri bildirimde bulunmuştur.
- Kris Katterjohn birkaç bölüm üzerinde kapsamlı incelemeler yapmıştır.
- Eric Krosnes yararlı teknik inceleme geribildirimleri gönderdi ve ayrıca kitabın ilerleyişi hakkında düzenli olarak başımın etini yedi. Bunu yapacak geleneksel bir editörüm olmadığı için bu çok yardımcı oldu.
- Vlad Alexa Mancini kapak (ve Nmap web sitesi) için Nmap göz logosunu yarattı.
- Michael Naef birçok bölümü nazikçe gözden geçirmiştir.
- No Starch Press'ten Bill Pollock, onlarca yıllık deneyimine dayanarak tavsiyelerde bulunmaktan ve kitap yayıncılığına ilişkin soruları yanıtlamaktan her zaman mutluluk duydu.
- David Pybus en sık fikir ve redaksiyon katkısında bulunanlardan biriydi.
- Tyler Reguly, tam da en çok ihtiyaç duyulduğu anda birden fazla bölümü gözden geçirerek yardımcı oldu.
- Chuck Sterling hem üst düzey tavsiyelerde bulundu hem de bazı bölümlerin detaylı redaksiyonunu yaptı.
- Anders Thulin birçok bölümün detaylı incelemesini yapmıştır.
- Diman Todorov Bölüm 9, Nmap Scripting Engine'in ilk taslağını yazdı.

- Catherine Tornabene birçok bölümü okudu ve son derece ayrıntılı geri bildirimler gönderdi.

Bu Kitabı Oluşturmak İçin Kullanılan Teknoloji

Kendim de açık kaynak kodlu araçlar kullanan bir yazar olarak, bu araçların gücüne ve yeteneklerine çok inanıyorum. Bu yüzden bu kitabı oluştururken mümkün olan her yerde onları kullanmak için çaba sarf ettim. Microsoft Word'de yazıp sonra da Adobe FrameMaker ile mizanpajı halledecek değildim!

Nmap Ağ Taraması DocBook XML formatında GNU Emacs metin editörü ile yazılmıştır.

Ücretsiz çevrimiçi bölümler, Norman Walsh'un XSL Stil Sayfaları ve xsltproc XSL işlemcisi kullanılarak XML'den oluşturulmuştur.

Baskı versiyonu da Norman'ın stil sayfalarını ve xsltproc'u kullanır, ancak XSL-FO formatına çıktı verir. Daha sonra PDF oluşturmak için bir XSL-FO işlemcisi kullanılıyor. Bunun için Apache FOP kullanmak isterdim, ancak dipnotla ilgili bir hata bunu engelliyor, bu yüzden RenderX XEP Motoruna geçtim. XEP tescilli ama en azından Linux üzerinde çalışıyor. Dipnot hatası düzeltildikten sonra FOP'a geri dönmeyi umuyorum.

Kapak düzeni Scribus ve (baskı şirketinin format gereksinimleri nedeniyle) Adobe InDesign ile yapıldı. Kapak ve iç illüstrasyonlar için raster grafikler Gimp ile oluşturulurken, vektör grafikleri için Inkscape kullanıldı.

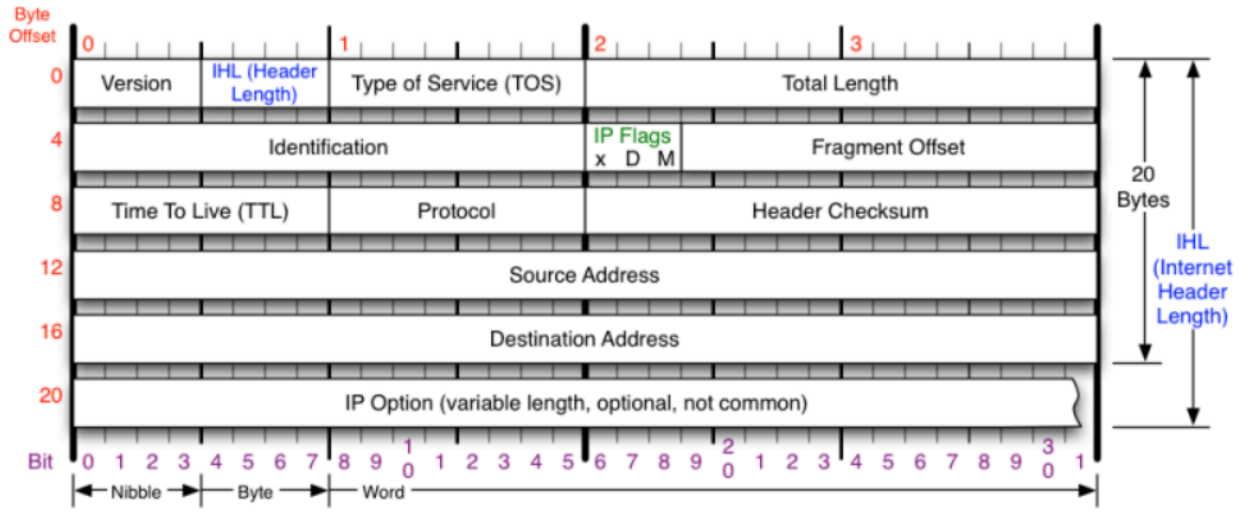
Revizyon kontrolü için Subversion kullanıldı ve ücretsiz web bölümlerine Apache httpd tarafından hizmet verildi.

TCP/IP Reference (TCP/IP Referansı)

Bu kitap TCP/IP ve ağ kavramlarına temel düzeyde aşina olunduğunu varsaymaktadır. Bu sayfalarda OSI yedi katman modeli ya da Berkeley Soket API'sinin bir özetini bulamayacaksınız. Kapsamlı bir TCP/IP rehberi için Charles Kozierok'un "The TCP/IP Guide" kitabını ya da W. Richard Stevens'ın eski bir klasik olan "TCP/IP Illustrated, Volume I" kitabını tavsiye ederim.

TCP/IP'ye aşina olunması beklenirken, en iyilerimiz bile zaman zaman paket başlığı alanları ve bayrakları için bayt ofsetlerini unutur. Bu bölüm IPv4, TCP, UDP ve ICMP protokolleri için hızlı referans diyagramları ve alan açıklamaları sağlar. Bu güzel diyagramlar yazar Matt Baxter'ın izniyle kullanılmıştır.

Şekil 1. IPv4 başlığı



Version

Version of IP Protocol. 4 and 6 are valid. This diagram represents version 4 structure only.

Header Length

Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.

Protocol

IP Protocol ID. Including (but not limited to):

1 ICMP	17 UDP	57 SKIP
2 IGMP	47 GRE	88 EIGRP
6 TCP	50 ESP	89 OSPF
9 IGRP	51 AH	115 L2TP

Total Length

Total length of IP datagram, or IP fragment if fragmented. Measured in Bytes.

Fragment Offset

Fragment offset from start of IP datagram. Measured in 8 byte (2 words, 64 bits) increments. If IP datagram is fragmented, fragment size (Total Length) must be a multiple of 8 bytes.

Header Checksum

Checksum of entire IP header

IP Flags

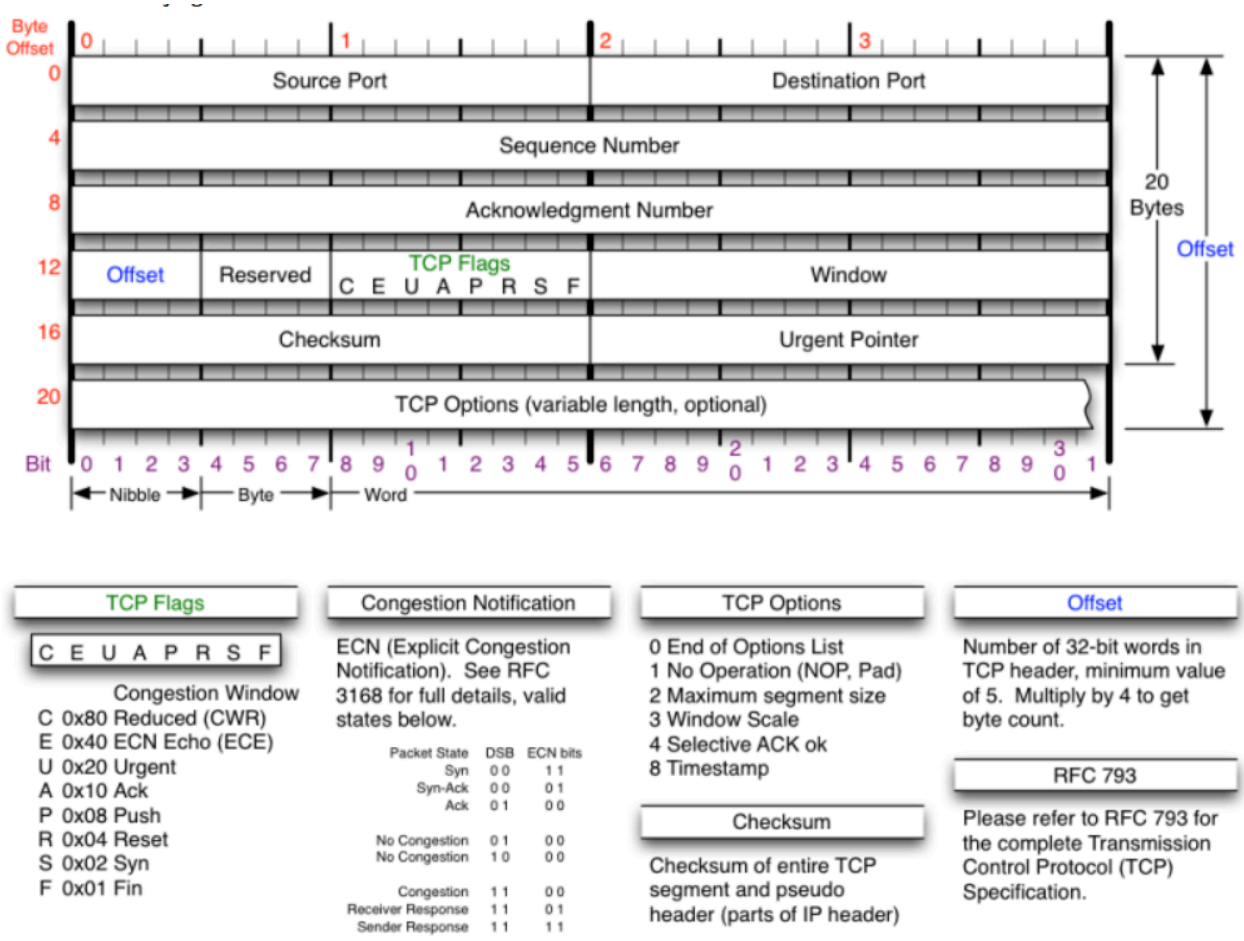
x D M

x 0x80 reserved (evil bit)
D 0x40 Do Not Fragment
M 0x20 More Fragments follow

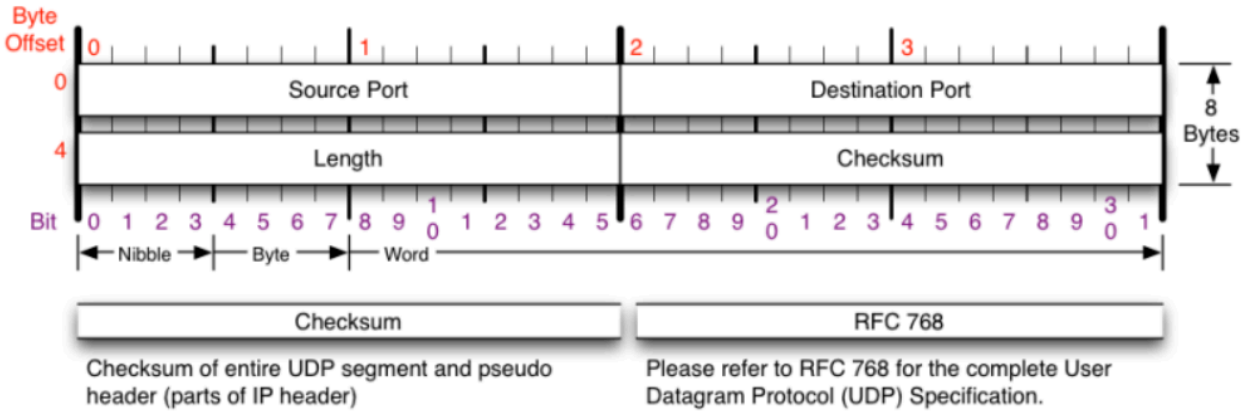
RFC 791

Please refer to RFC 791 for the complete Internet Protocol (IP) Specification.

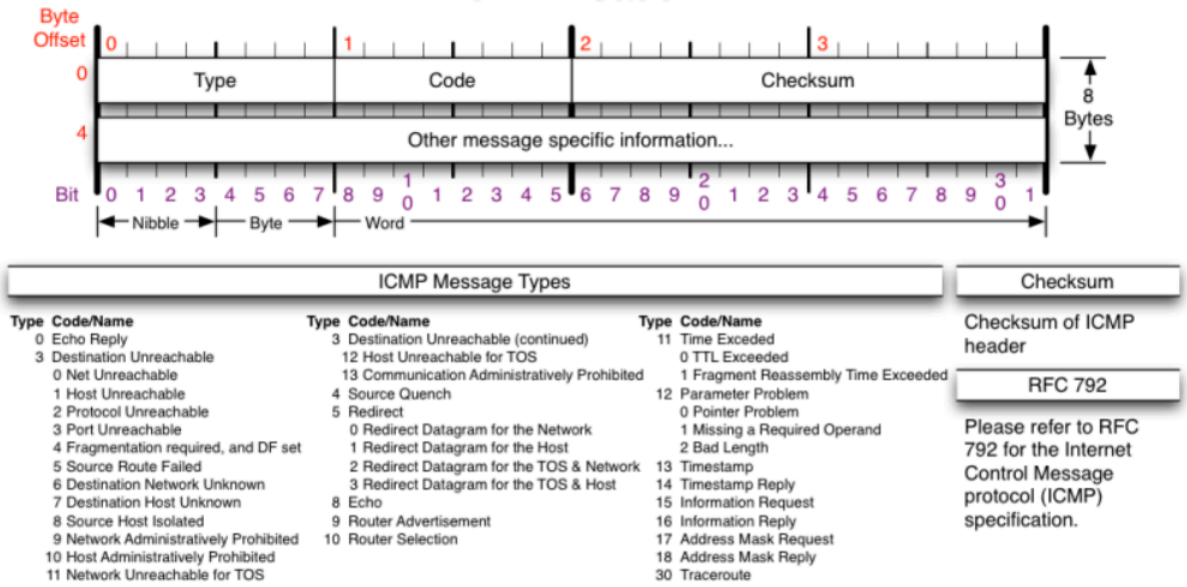
Şekil 2. TCP başlığı



Şekil 3. UDP başlığı



Şekil 4. ICMP başlığı



ICMP Message Types

Type	Code/Name
0	Echo Reply
3	Destination Unreachable
	0 Net Unreachable
	1 Host Unreachable
	2 Protocol Unreachable
	3 Port Unreachable
	4 Fragmentation required, and DF set
	5 Source Route Failed
	6 Destination Network Unknown
	7 Destination Host Unknown
	8 Source Host Isolated
	9 Network Administratively Prohibited
	10 Host Administratively Prohibited
	11 Network Unreachable for TOS
3	Destination Unreachable (continued)
	12 Host Unreachable for TOS
	13 Communication Administratively Prohibited
4	Source Quench
5	Redirect
	0 Redirect Datagram for the Network
	1 Redirect Datagram for the Host
	2 Redirect Datagram for the TOS & Network
	3 Redirect Datagram for the TOS & Host
8	Echo
9	Router Advertisement
10	Router Selection
11	Time Exceeded
	0 TTL Exceeded
	1 Fragment Reassembly Time Exceeded
12	Parameter Problem
	0 Pointer Problem
	1 Missing a Required Operand
	2 Bad Length
13	Timestamp
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply
30	Traceroute

Checksum

Checksum of ICMP header

RFC 792

Please refer to RFC 792 for the Internet Control Message protocol (ICMP) specification.

next next next