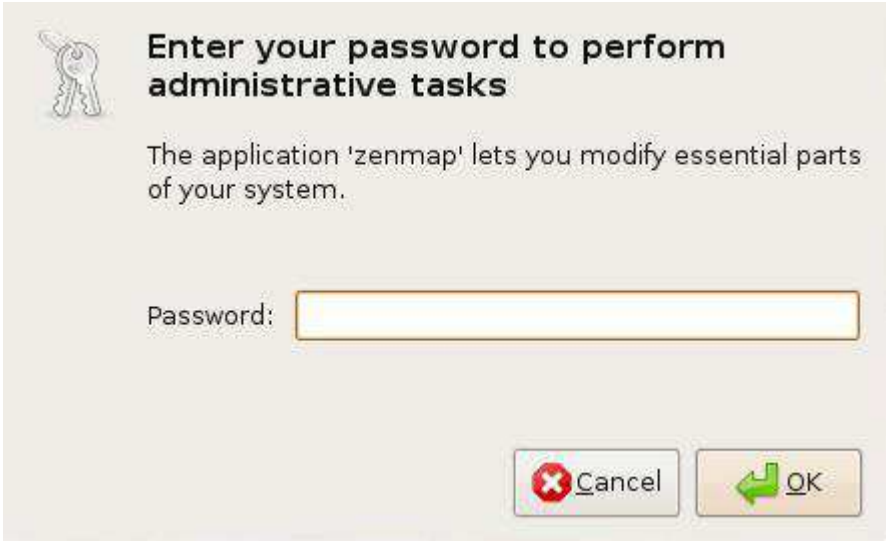
SAMURAİ FRAMEWORK İLE HACKİNG-1 (FOOTPRINTING)

Merhaba arkadaşlar. Samurai Framework ile Temel Hacking makale serisinin ikinci kısmını bu ve devamında ki makalelerimizde inceleyeceğiz. Bu makalemizde temel hacking aşaması konularından olan footprinting (Bilgi Toplama)'i işleyeceğiz. Kısaca değinecek olursak; saldırı yapılacak sistem hakkında temelden derinlemesine bilgi toplama nasıl gerçekleştirilir, hangi bilgiler gereklidir ve son olarakta bu bilgileri saldırı amaçlı nasıl kullanılabileceğini öğreneceğiz. Özellikle bir sistem hakkında ne kadar bilgi sahibi iseniz, o sisteme erişim ve yönetim o kadar rahat ve kolay olur. Biz bu makalede değinilen bilgi toplama işlemlerini bir mail sunucusu üzerinde test edeceğiz. Böylelikle sunucu hakkında detaylı bilgileri toplayıp saldırı aşamasına zemin hazırlayacağız.

Not: Samurai Framework ile Temel Hacking makalesinde anlatmış olduğum kullanım bilgileri aynı şekilde bu makalemizde de geçerlidir.

Bu bilgi toplama aşamasında bize sunucu hakkında kritik bilgileri toplamak gerekecektir. Kritik bilgilerden kastım; sunucu üzerinde hangi işletim sistemi bulunduğu, sunucunun çalıştırmış olduğu servisler, sunucuda aktif olarak kullanılan portlar, sunucu network yapısı v.s gibi bilgilerdir. Bu bilgiler bir hacking saldırısından önce en çok ihtiyaç duyulan kritik bilgilerdir. Bu bilgileri elde eden bir saldırgan sunucuya saldırı planlaması yaparak, yol haritasını derlemiş olduğu bu bilgiler çerçevesinde çizer.

Samurai Framework v0.9.5 sürümünü VMware Workstation üzerinden çalıştırıp sisteme login oluyoruz (Ben bu şekilde makaleyi hazırladım. Siz fiziki bilgisayarınızda yapacaksanız ona göre ayarlarsınız). Daha sonra Application menüsünden Samurai/Recon & Mapping kısmından ZenMap (as root)'u açıyoruz. ZenMap genel mantıkta komut satırı ile çalışmakta olup ayrıca ZenMap GUI'de mevcuttur. ZenMap GUI komut satırı kullanamayanlar için arayüze sahiptir. ZenMap (as root) ZenMap GUI olarak çalışmaktadır. ZenMap programı ile çok detaylı taramalar yapabilirsiniz. İşletim sistemi tespiti, servis tespiti, port tarama gibi çok detaylı özelliklere sahip olup penetration testlerinde en güçlü footprinting araçlarının başında gelir. Linux ve Windows işletim sistemlerinde çalışan komut ve GUI sürümleri mevcuttur. Sizden ZenMap'ı root yetkileri ile çalıştırmak için root şifresi isteyecektir. Şifreye **samurai** yazarak OK'i tıklayın.



ZenMap programı çalışacaktır. Tarama yapacağınız sistemi belirledikten sonra Target (hedef) kısmına sunucu adını yazıyoruz. Örneğin www.eyupcelik.com.tr, 192.168.1.8 gibi tarama

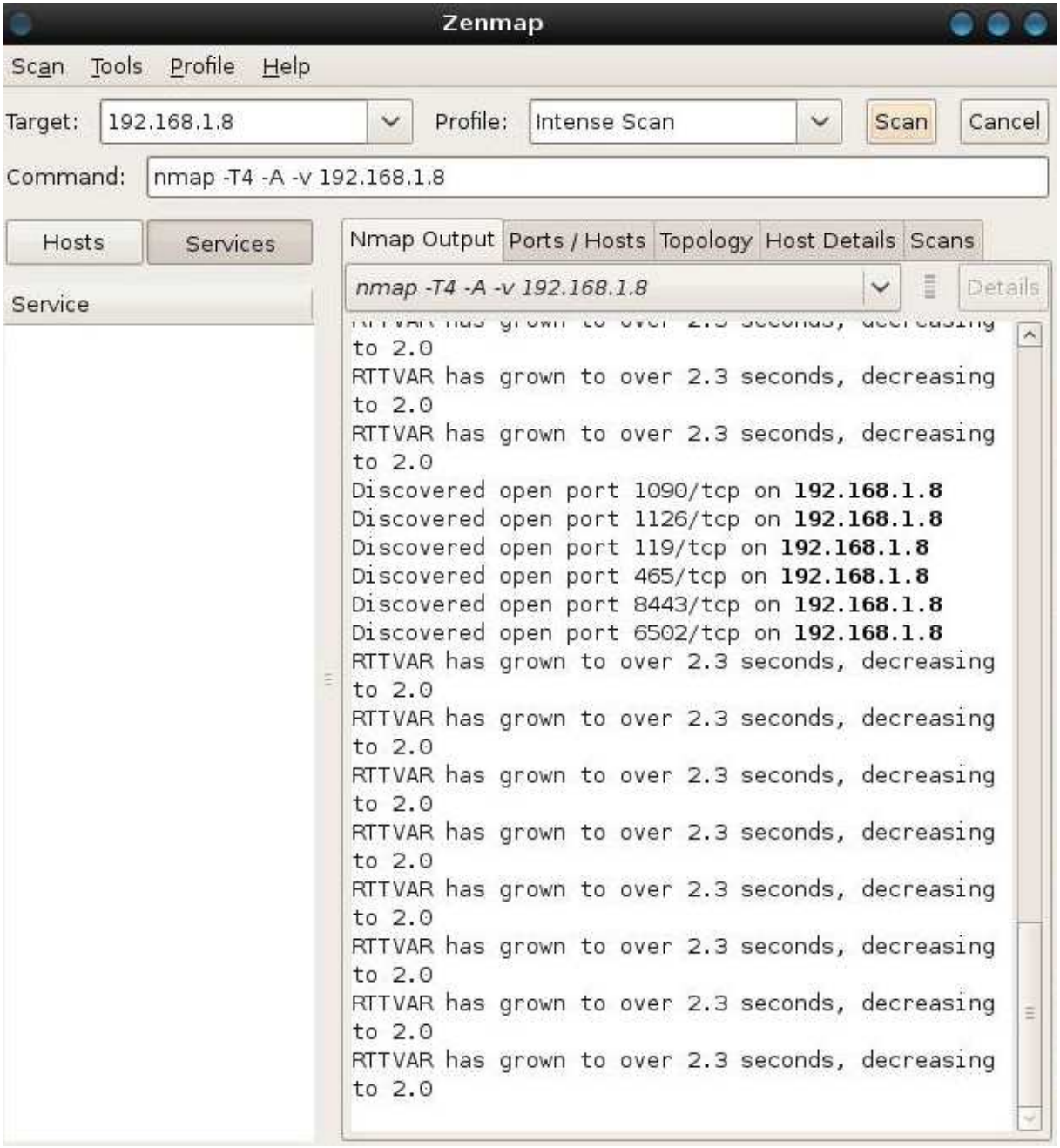
yapacağımız sunucu adresini yazıyoruz. Bu local bir sunucu yahut uzak bir sunucu olabilir. Sunucu adresini yazdıktan sonra Profile kısmından nasıl bir tarama yapmak istediğimizi seçiyoruz. Eğer detaylı bir tarama istiyorsak Intense Scan'i seçiyoruz.

1. Intense Scan (Yoğun Tarama): Tarama yapacağımız sistem hakkında gerekli tüm bilgileri (İşletim sistemi, port v.s) getirmeye çalışır.
2. Operation System Detection (İşletim Sistemi Algılama): Hedef bilgisayarda bulunan işletim sistemi hakkında detaylı bilgileri toplamaya çalışır.
3. Quick Full Version Detection Scan (Hızlı tam sürüm algılama): Hedef bilgisayar üzerinde hızlı bir şekilde bilgi toplama taraması için kullanılır.
4. Quick Operation System Detection (Hızlı İşletim Sistemi Algılama): Hedef bilgisayarın işletim sistemini hızlı bir şekilde bulmak için kullanılır.
5. Quick Scan (Hızlı Tarama): Hedef bilgisayar üzerinde hızlı bir şekilde genel bir tarama yapar.
6. Quick Services Version Detection (Hızlı Servis Algılama): Hedef bilgisayar üzerinde bulunan servis sürümlerini hızlı bir şekilde taramak için kullanılır.
7. Quick and Verbose (Hızlı ve Gereksiz Bilgiler): Hedef bilgisayar üzerinde hızlı bir tarama gerçekleştirerek en temel bilgileri toplamaya çalışır.
8. Regular (Düzenli): Hedef üzerinde periyodik tarama gerçekleştirmek için kullanılır.

Ayrıca kendinizde bir tarama kuralı oluşturmak isterseniz; Profile menüsünden New Profile or Command'ı tıklayarak kendinize özel bir tarama kuralı oluşturabilirsiniz. Bu menüye erişmen için CTRL+P kısa yolunu da kullanabilirsiniz.

Profile kısmının hemen altında command bölümü mevcuttur. Hedef sisteme karşı yapacağınız taramanın komut satırına dökülmüş halidir. GUI kullanmadan komut satırı ile tarama yapmanız için gereken komutları size gösterir.

Target ve Profile kısmını seçtikten sonra Scan diyoruz. Profile kısmını genel olarak yapacağınız taramalarda Intense Scan olarak seçerseniz hedef hakkında daha çok bilgi toplama şansınız doğar. Ben bu şekilde tarama yapmanızı tavsiye ederim.



Yukarda ki gibi tarama başlayacaktır. Tarama esnasında sol tarafta Hosts ve Services adı altında iki bölüm mevcuttur. Hosts kısmı tarama yaptığımız sunucu adını gösterirken, Services kısmı tarama yaptığımız hedef sistemin çalışan servislerini göstermektedir. Servisleri tek tek tıklayarak hangi servis üzerinde kaç tane çalışır durumda port olduğunu görüntüleyebilirsiniz.

Bunun dışında yukarda 5 (beş) ayrı bölüm mevcuttur. Nmap Output, Ports/Hosts, Topology, Hosts Details ve Scans bölümleri vardır.

Nmap Outputs: Hedef sistem üzerinde yapılan taramaların çıktısını gösterir. Taramada işlenen kuralların hedef sunucu üzerinde verdiği cevaplar ve sonuçları print eder.

Ports/Hosts: Hedef sistem üzerinde bulunan açık portları gösterir. Böylece servisler ve portlar hakkında detaylı bilgiler bu kısımda saklanır.

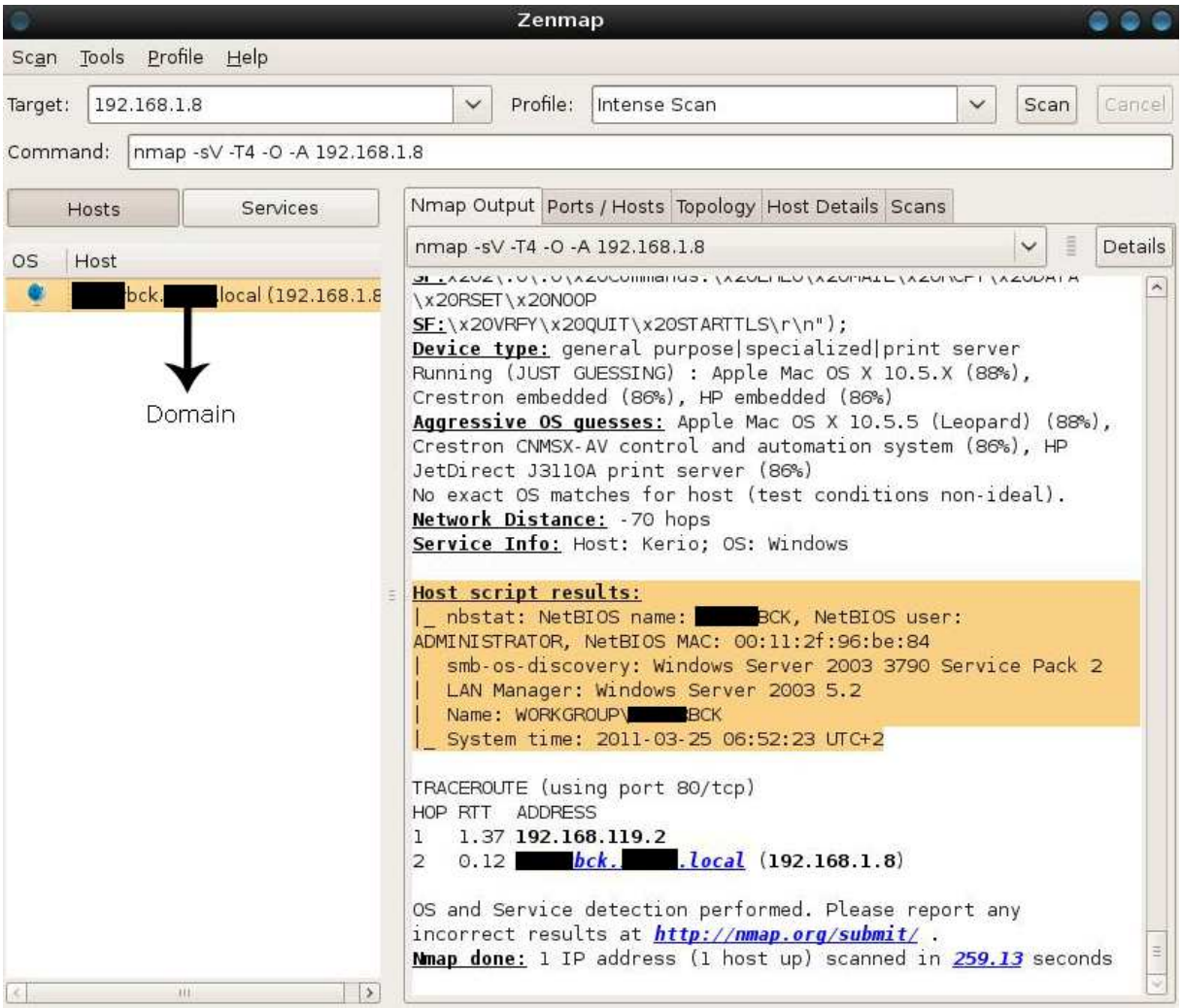
Topology: Hedef sistemin ağ tapolojisini gösterir. Hedef sistemin network'ünde bulunan diğer bilgisayarları map düzeninde göstermeye çalışır.

Hosts Details: Hedef sistemin kısa bir özetini gösterir.

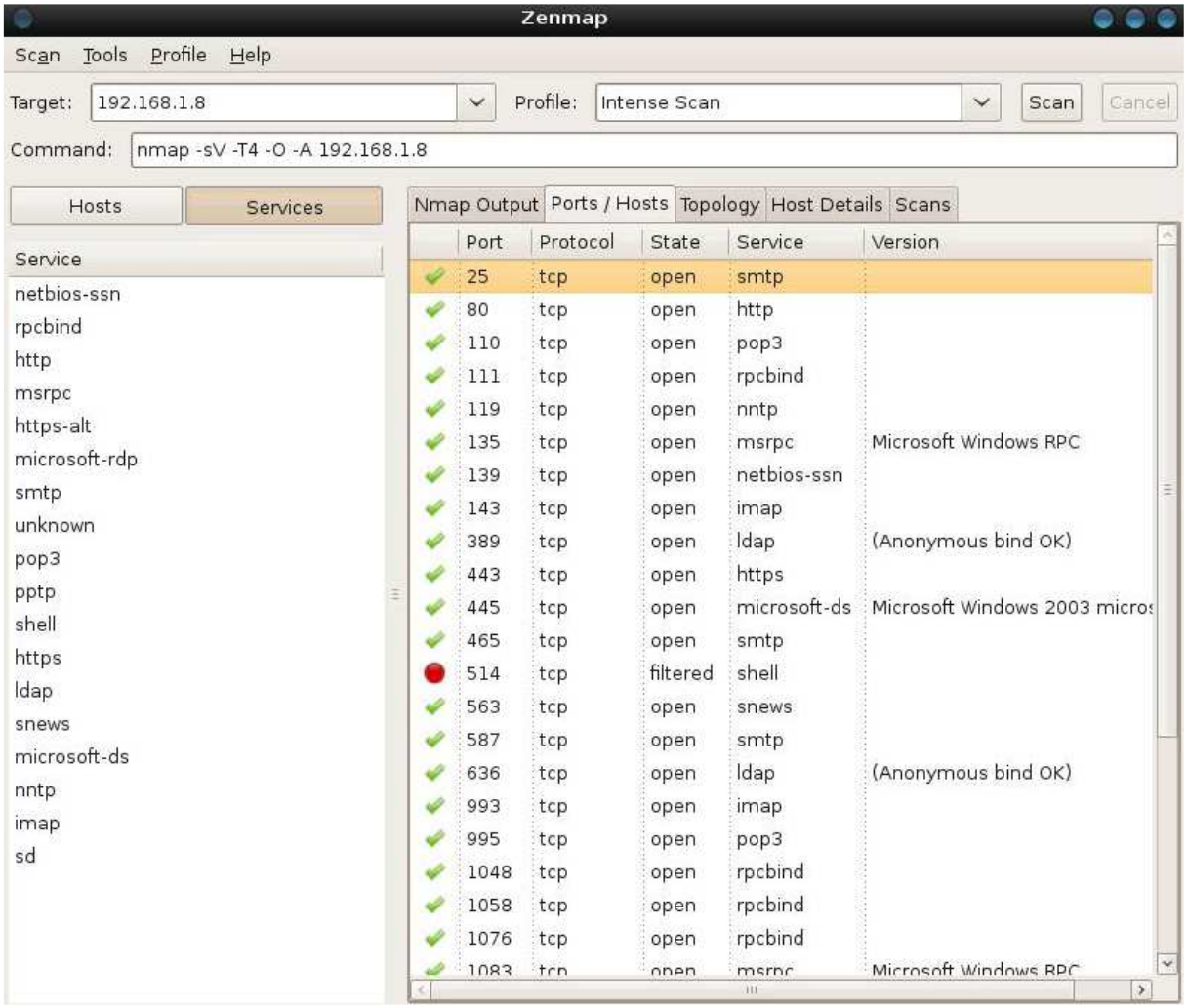
Scans: Hedef sistem üzerinde yapılan tarama çıktılarını ve komutlarını gösterir.

Tarama işlemi bittikten sonra ZenMap GUI bize detaylı bir şekilde footprinting bilgilerini gösterir. Bizi en çok ilgilendiren bilgilerin başında; hedef sunucunun işletim sistemi bilgileri, açık portlar, çalışan servisler, kullanıcı adı v.s gelmektedir. Tarama bittikten sonra ilk olarak hedef sunucunun host adını ve işletim sistemi bilgilerini kontrol ediyoruz. Bu aşamadan hedef sisteme sızıncaya kadar atacağımız her adımın temelini bu taramada elde ettiğimiz bilgiler doğrultusunda gerçekleştireceğiz. Bu açıdan footprinting hacking işleminin temelidir.

Şimdi hedef sistem üzerinde yaptığımız tarama raporunu inceleyelim.



Yukarıda ki resimde göreceğimiz gibi hedef sistemin NetBIOS adını, oturum açma yetkisine sahip kullanıcı adını, hedefin işletim sistemini, işletim sistemi sürümünü, hedef sistemin çalışma grubunu NetBIOS MAC adres bilgisini v.s aldık. Aşağıda ilerleyen bölümde hedef sistem üzerinde bulunan servisleri ve açık portları inceleyeceğiz.



Services bölümünü ve Ports/Hosts menüsünü tıkladıktan sonra karşımıza hedef sistem üzerinde bulunan servislerin yanı sıra açık portları da gösterecektir. Yukarıdaki resimden örnekleyecek olursak eğer; hedef üzerinde; netbios-ssn, rpcbind, http, msrpc, https-alt, microsoft-rdp, smtp, pop3, pptp, https, ldap, snews, microsoft-ds, nntp, imap dışında 2 servis ile birlikte toplamda 18 adet servis ve 25, 80, 110, 111, 119, 135, 139, 143, 389, 443, 445, 465, 514, 563, 587, 636, 993, 995, 1048, 1058, 1076, 1083, 1090, 1111, 1126, 1723, 3389, 6502, 8443, 8800, 9876 olmak üzere toplamda 31 adet açık port tespit edilmiş. Bu servisler ve portlar sistem, servisler ve programlar hakkında bize detaylı bilgiler vermeye yetecektir.

Servislere bakacak olursak eğer;

Netbios-ssn: Netbios Session Servisidir. 139'uncu portu kullanmaktadır. Netbios-ssn servisi hedef bilgisayar üzerinde çalıştığında 139'uncu portun açılmış olduğunuda anlayabiliriz.

Smtp, pop3 ve imap servislerinden hedef sistem üzerinde bir mail sunucusu olduğunu öğreniyoruz.

Pptp (Point to Point Tunneling Protocol) servisi ile hedef sistem üzerinde VPN (Sanal Özel Ağ) çalıştığını anlıyoruz.

http ve https, https-alt servisleri hedef sistem üzerinde web yayını yapan servislerdir. Hedef sistemin 80, 443 8800, 8443 portlarının açık olduğunu anlıyoruz.

Microsoft-rdp servisi 3389 portunun açık olduğunu ve Remote Desktop Connection'ın açık olduğunu görebiliyoruz.

En önemlisi 514 portunun açık olduğu ve sistem üzerinde çalışan bir shell olduğunu görüyoruz. Shell kullanarak sistemi uzaktan elegeçirmek bizim bir sonraki hedefimiz olacaktır.

Bir sonraki makalemizde Samurai Framework v9.0.5 ile Hacking-2 // Discovery (Keşif) saldırı yapacağız. Penetration (Sızma) testleri sonunda sisteme nasıl sızılabileceğini göstereceğim.

Sabırla okuduğunuz için teşekkür ederim. Herkese güvenli günler.

Eyüp ÇELİK
Bilgi Teknolojileri Güvenlik Uzmanı
http://www.eyupcelik.com.tr