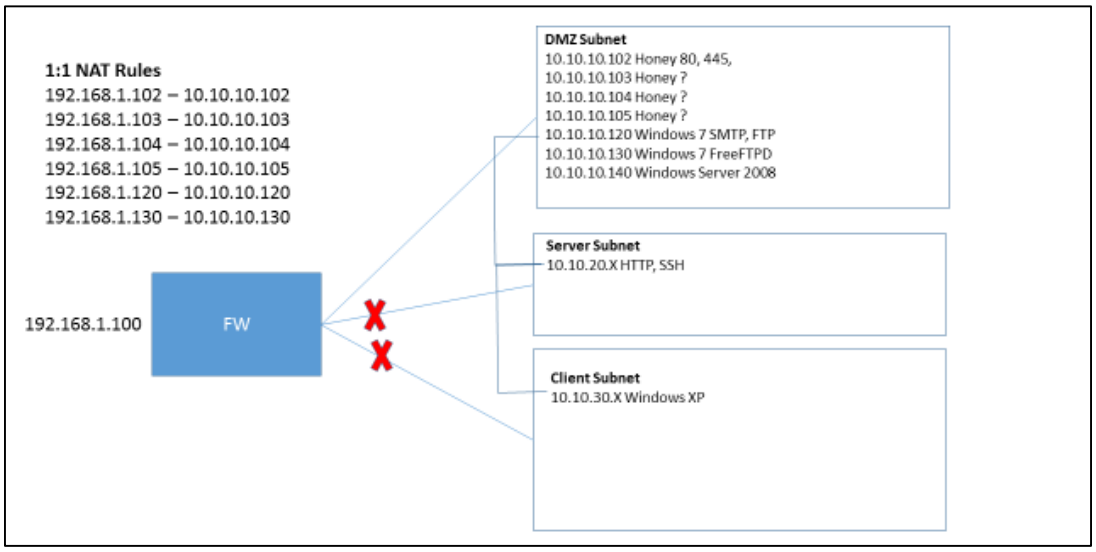
Network Soruları

Merhaba Arkadaşlar. Network sorularında mümkün olduğunca gerçek durumu yansıtmaya çalıştım. Network içerisinde bir tane Firewall vardı. Firewall ile 3 tane subnet oluşturulmuştu. Genel network yapısını aşağıdaki şekilde şekilde görebilirsiniz. Sizlere verilen 192.168.1.0/24 subnet aslında hedef sistemin DMZ subnetinin IP aralığı idi. 192.168.1.X IP'ler 10.10.10.X li IP'lere 1:1 NAT ile eşleştirildi.



DMZ üzerinde 10.10.10.101-10.10.10.105 arasındaki sunucular aslında tuzak sistemdi. Dış network üzerinden sadece DMZ network'üne erişim mümkündü. Diğer subnetlere geçiş engellendi.

1 ve 2. Sorular

1 ve 2. Sorular DMZ'te bulunan 2 adet sunucunun ele geçirilmesi idi. Bir tanesi FreeFtpd serverda yer alan password buffer overflow açıklığının kullanarak 10.10.10.130 IP'li bilgisayarın ele geçirilmesiydi. Bu açıklığa denk gelen exploit Metasploit içerisinde yer almaktadır.

Diğer soru SLMAIL server pop3 buffer overflow açıklığı idi. Bu açıklığın exploit kodu Windows XP için Metasploit içerisinde yer almaktadır. Ancak yarışmada SLMail uygulaması Windows 7 işletim sistemi üzerine çalışordu. Bu nedenle exploit kodunda EIP adresi gibi ufak değişikliklere ihtiyacamız olacaktı.

3. Soru

3 soruda yer alan sunucu (10.10.20.X) sunucuların bulunduğu subnet içerisinde yer almaktaydı. Bu sunucuya erişim sadece 10.10.10.130 IP'li sunucudan sağlanmaktaydı. 10.10.10.130 sunucusunu ele geçirenlerin makina üzerinde keşif yaptığında iki tane interface tanımlı olduğunu tespit edip, 10.10.20.X subnete geçiş sağlıyabileceğini tespit etmesi bekleniyordu.

Pivoting yaparak, 10.10.20.X li IP ye sahip sunucuda TCP 80 ve 22'nci portların tespit edilmesi, bu sunucuda yer alan web sayfasındaki duyurularda yer alan kullanıcı adlarının tespiti, ve bu kullanıcı adları kullanılarak SSH password bruteforce ile (macar,password123) sunucu ele geçirilebilecekti.

4. Soru

Bu soruda yer alan sunucu DMZ networkü üzerinde yer alan 10.10.10.140 IP'li Windows Server 2008 di. Bu sunucu kurulumdan itibaren hiç güncelleme almamış network içinde unutulmuş bir sunucuydu. Dış network'den veya diğer subnetlerden erişim yoktu. Sadece 10.10.10.130 ve 10.10.10.120 IP'li sunuculardan erişim mümkündü. Bu sunucu üzerinde bir çok kritik seviyeli exploit kodu public olmayan açıklık vardı. Ya bu exploit kodları bulunarak bu sunucun ele geçirilmesi bekleniyordu yada pass the hash tipinde bir saldırı ile daha önceki bilgisayarlarda tespit edilen password hash değerleri ile exploit edilmesi bekleniyordu.

5. Soru

Bu soruda yer alan 10.10.30.X IP client bilgisayarına erişim sadece 10.10.20.X'li bilgisayardan sağlanabiliyordu. Bu nedenle double pivoting yaparak bu bilgisayara erişim sağlamabilinirdi. Bu bilgisayarda herkesce bilinin MS08-067 açıklığı bulunuyordu. Metasploit kullanarak bu açıklık rahatlıkla exploit edilinebilinirdi. Burada esas hedef double pivoting yaparak 3. Subnete erişim sağlamanızdı.

Gayretlerinizden dolayı hepinize teşekkür ederiz. Umarım network soruları zevkli ve öğretici olmuştur. Daha detaylı sorularınız için emre.caliskan@metu.edu.tr adresinden bana ulaşabilirsiniz. Umarım ilerleyen dönemlerde yine aynı şekilde buluşma imkanı buluruz. Bu alanda çalışmalarınızın devamını diliyorum.