Soru 1 : Gateway Holding bünyesinde SEDDK ‘a tabi bir şirket bulunmakta. Bu şirkete ait siber ortamda hangi bilgileri (Hacklemek için bulabileceğiniz her türlü bilgi) bulabileceksiniz.

Cevap 1:
Hangi portlarının açık olduğunu, sunucu adı, işletim sistemi, firewall tespiti, çalışan servisler (nmap)

nmaple bulduğum bilgiler ile metasploit ile zafiyeti sömürme,

ip adresini bu suretle lokasyonunu,
burpsuite ile genel web güvenliği kontrolü,

maltego ile ağ haritası, kişisel bilgiler, organizasyonel bilgiler, ip adresi analizi, e posta analizi bulunabilir.

recon-ng ile alt alan adları,

Son olarak nessus, owasp zap veya openvas gibi güçlü toollar ile baştan aşağı tarama yapılabilir. Bu toollar otomatik olarak zafiyet tespiti yapabiliyor. Fakat manuel tarama yapmak genelde daha etkili olur.

Bulabileceğim bilgiler: Hangi portlarının açık olduğunu, sunucu adı, işletim sistemi, firewall tespiti, çalışan servisler, log analizi, ağ haritası, kişisel bilgiler, organizasyonel bilgiler, ip adresi analizi, e posta analizi, alt alan adları(ağ topolojisi) vs. bulunabilir.

NOT: Daha fazla uzun olmasını istemediğim için özet yazdım.

Soru 2: Black-Box (Soru-1 deki aktivite) aktivitelerinde kullanılan araçlara verilen genel isim nedir ?

Cevap 2:

Kullanılan araçlara genel olarak "penetration testing tools" denir. Bu araçlar, sistemlerin güvenlik açıklarını tespit etmek ve sızma testi yapmak için kullanılır. Bu araçlar, güvenlik açıklarının belirlenmesine ve düzeltilmesine katkı sağlar.

Soru 3: Sizin de bildiğiniz gibi T.C. vatandaşlarına ait bir çok bilgiye (Nitelikli kişisel veri) undergroundsitelerinden paralı veya parasız erişilebiliniyor. Bir kişiye ait recetesine ulaşabildiğiniz düşünün. Bu bilgiden neler elde edebilirsiniz ?

Cevap 3:
Bu reçeteden kişinin adını soyadını öğrenmemiz dahi yeterli olabiliyor. Çünkü bilgiler, veritabanında ad soyad ile ilişkilendirilmiş olabiliyor. Bu reçeteden ad soyad veya tc kimlik no bulunduğu takdirde kişinin adresine, soy ağacına hatta aracının plakasına kadar bilgilere erişebilir. Kısaca kişiye ait tüm bilgileri ad soyad aracılığıyla bile bulabiliyorsa, alışveriş fişinden bile tüm bilgilerine erişebilir.

Soru 4: aşağıdaki logu yorumlayınız (log u okuyun !!!) .
OS_USERNAME: "gwadmin" USERNAME: "GTHUMAN" USERHOST: "GATEWAY\GWEBDEV01" TERMINAL: "WEBDEV01" TIMESTAMP: "2019-08-01 16:21:25.0" OWNER: "GTHUMAN" OBJ_NAME: "EXTERNELREPORT" ACTION: "12" ACTION_NAME: "DROP TABLE" NEW_OWNER: "null" NEW_NAME: "null" OBJ_PRIVILEGE: "null" SYS_PRIVILEGE: "null" ADMIN_OPTION: "null" GRANTEE: "null" AUDIT_OPTION: "null" SES_ACTIONS: "null" LOGOFF_TIME: "null" LOGOFF_LREAD: "null" LOGOFF_PREAD: "null" LOGOFF_LWRITE: "null" LOGOFF_DLOCK: "null" COMMENT_TEXT: "null" SESSIONID: "58557840" ENTRYID: "3" STATEMENTID: "228" RETURNCODE: "0" PRIV_USED: "null" CLIENT_ID: "null" ECONTEXT_ID: "null" SESSION_CPU: "null" EXTENDED_TIMESTAMP: "2019-08-01 16:21:25.790671 Turkey" PROXY_SESSIONID: "null" GLOBAL_UID: "null" INSTANCE_NUMBER: "0"

OS_PROCESS: "14006" TRANSACTIONID: "07001F0069C00500" SCN: "341565375019" SQL_BIND: "null" SQL_TEXT: "drop table externelReport" OBJ_EDITION_NAME: "null" DBID: "3491572080"

Cevap 4:
GTHUMAN kullanıcısı, "EXTERNELREPORT" adlı tabloyu silen bir işlem gerçekleştirmiş. Bu işlem, "DROP TABLE" komutu ile gerçekleştirilmiş ve ilgili log bu eylemi kaydetmiştir. Veritabanı güvenliği açısından, bu tür kritik işlemlerin izlenmesi önemlidir ve kullanıcı aktivitelerinin denetlenmesi bu tür potansiyel güvenlik tehditlerini belirlemede yardımcı olabilir.

Soru 5 : Bir şirkette çalışan turn-over rate çok yüksek ise hangi tür yetkilendirme yöntemi kullanmalıyım? Neden ?

Cevap 5:
Yüksek turn-over rate'i azaltmak için çalışanlardan düzenli geri bildirim alın, çıkış mülakatları düzenleyin, performans değerlendirmeleri yapın. Mentorluk ve koçluk programlarıyla yeni çalışanları entegre edin, insan kaynakları departmanını güçlendirin.

Soru 6 : " ilgili varlıkların (özne ve nesne) eylemlerinin özniteliklerine ve ortama göre kuralları değerlendirerek nesnelere erişimi kontrol ettiği için ayırt edilebilen mantıksal bir erişim kontrol modeli" Nedir ?

Cevap 6:
Bu kavram "mantıksal erişim kontrol modeli"dir. Bu model, öznenin ve nesnenin eylemlerini belirli özniteliklere ve ortama göre değerlendirerek nesnelere erişimi kontrol eder. Sistem içindeki kaynaklara yapılan erişimleri düzenlemek ve kontrol etmek için kullanılır.

Soru 7 : Google Hacking nedir ?

Cevap7: Google Hacking, özel veya hassas bilgileri bulma amacı taşıyan arama tekniklerini içeren bir kavramdır. Bu yöntemler, Google ve diğer arama motorlarını kullanarak özel sorgular ile istenilen bilgileri çıkarmayı hedefler.

Soru 8 : 5651 sayılı kanun nedir ? Gateway 'I bağlar mı?

Cevap 8:

Temel amacı, internet üzerinden yapılan yayınları düzenlemek ve suçlarla mücadele etmektir. Türk hukuk sistemine tabi olduğu sürece 5651 sayılı Kanun'un kapsamına girebilir.Fakat bu kanun, özellikle çocukların cinsel istismarı, suç teşkil eden içeriklerin yayınlanması gibi konulara odaklanır.

Soru 9: Siz bir siber güvenlikçisiniz ve bizim şirkette çalışıyorsunuz. Bir kullanıcı size telefonla arayıp, kendisine vergi borcu olduğuna dair e-mail geldiğini, mail içerisindeki linke tıkladığını. Makinasında bir hata mesajı çıktığını söyledi. İlk iş ne yaparsınız ?
Not. Unutmayın siz daha junior bir güvenlikçisiniz.

Cevap 9:

Kullanıcıdan gelen bilgiye göre, ağ bağlantısının kesilmesini öneririm. Ardından güvenlik taraması yaparak bilgisayarı temizlerim. Saldırı yöntemini anlamak için olayı analiz eder ve kullanıcıya sosyal mühendislik saldırıları konusunda bilgi veririm.

Soru 10: Size Cuma günü akşam mesai bitiminde bir iş verdim. Sizin bu işi 48 saat çalışıp bitirme şansınız yok. Ne yaparsınız ?

Cevap 10:
Verilen işin 48 saat içinde tamamlanması mümkün değilse, sizinle iletişime geçerim, durumu detaylı bir şekilde açıklar ve gerçekçi bir zaman çerçevesi belirlerim. Acil durumlarda ek destek talep ederim ve işin etkili bir şekilde tamamlanmasını sağlarım.