Sosyal Mühendislik

> Bilgi güvenliği bağlamında sosyal mühendislik, eylemleri gerçekleştirmeye veya gizli bilgileri ifşa etmeye yönelik olarak insanların psikolojik manipülasyonudur.

Storm Breaker Kurulumu

> https://github.com/ultrasecurity/Storm-Breaker.git linkinyle terminalden klonlanır.(`git clone` `https://github.com/ultrasecurity/Storm-Breaker.git`)

- Sonrasında ilgili klasöre geçilir. `cd Storm-Breaker`
- `sudo bash install.sh` ile ilk indirme yapılır.
- **Eğer hata alınırsa** `python3 -m venv .venv` komutuyla sanal bir çevre oluşturulur.
- `source .venv/bin/activate` komutuyla çalıştırılır.
- Eğer hata hala devam ederse `python3 -m pip install -r requirements.txt` komutu çalıştırılır.
- En son ise p`ython3 st.py` çalıştırılır ve işlem tamamlanır.

---

ngrok kurulumu

> Tünelleme yapmak için kullanılır.

- ngrok.com sitesine kayıt olunur ve indirilir.

- Zip dosyasından çıkılır ve kullanıcı token kullanmak için dosyanın olduğu klasöre gidilir.
- `./ngrok <token>` komutu ayrı bir terminalde çalıştırılır.(sitedeki aşamaları takip et)
- `./ngrok http 2525` ile çalıştırılır.
- Forwarding kısmındaki linkten siteye gidilebilir.
- admin hem şifre hem isim olarak kullanılıp giriş yapılabilir.
- Buradaki linklerle çeşitli hack işlemleri yapılabilir.

Kötü Amaçlı Yazılımlar

1. **Virüs**
   - Kendini başka dosyalara veya programlara ekleyerek yayılır.
   - Genellikle dosyalar çalıştırıldığında aktifleşir.
2. **Solucan (Worm)**
   - Ağ üzerinden kendini çoğaltarak yayılır.
   - Genellikle kullanıcı etkileşimine gerek kalmadan sistemleri etkiler.
3. **Truva Atı (Trojan Horse)**
   - Zararsız bir yazılım gibi görünür ama arka planda kötü amaçlı işlevler gerçekleştirir.
   - Genellikle sistemlere arka kapı bırakır.
4. **Casus Yazılım (Spyware)**
   - Kullanıcının bilgilerini (şifreler, kredi kartı verileri vb.) gizlice toplar.
   - Klavye dinleyiciler (keylogger) bu kategoriye girer.
5. **Reklam Yazılımı (Adware)**
   - Kullanıcıya istenmeyen reklamlar gösterir.
   - Genellikle sistem performansını düşürür ve kullanıcı davranışlarını izler.
6. **Fidye Yazılımı (Ransomware)**

- Dosyaları şifreler veya sisteme erişimi engeller.
- Kullanıcıdan para karşılığında (fidye) dosyaları açmak için anahtar ister.

7. **Kökkit (Rootkit)**
    - Sisteme sızarak kötü amaçlı yazılımların gizli kalmasını sağlar.
    - Genellikle sistem dosyalarına erişimi değiştiren derinlemesine kontrol sağlar.
8. **Botnet ve Zombi Bilgisayarlar**
    - Bilgisayarlar uzaktan kontrol edilerek bir ağa (botnet) katılır.
    - Spam gönderme, DDoS saldırıları gibi amaçlarla kullanılır.
9. **Korsan Yazılım (Rogue Security Software)**
    - Sahte güvenlik yazılımı gibi davranır.
    - Tehdit olmadığını iddia ettiği virüsleri kaldırmak için ödeme ister.
10. **Dosyasız Zararlı Yazılımlar (Fileless Malware)**

- Geleneksel antivirüslerin tespit etmesi zor olan bu yazılım türü, sistem belleğinde (RAM) çalışır ve dosya sistemiyle çok az veya hiç etkileşime girmez.

Görsel ve Backdoor Birleştirme

- İlgili icon ve jpg-png görselleri indirilir.
- Backdoor oluşturulur ve tüm dosyalar aynı yere atılır.(www içindeki oluşturulan klasöre)
- Windows'a autoit kurulur.
- TrojanFactory githubda bulunur ve oradaki txt dosyası kopyalanıp alınır.
- Backdoor sunucu sitesine gidilir.(Kaliden `service apache2 start` komutuyla sunucu çalıştırılabilir.)
- Windows'a icon dosyası indirilir.
- txt dosyasındaki url1 ve url2 kısımlarına sırasıyla birleştirilmek istenen görsel ve exe dosyasının linkleri yazılır.

- Arama kısmından compile script exe çalıştırılır.
- Source kısmından txt dosyası seçilir,icon kısmından icon eklenir ve dönüştürülür.

🖋**Ömer Faruk Baysal**