Netcat ile Sistem Ele Geçirme Senaryosu

Adım adım bir sistem kabaca şu şekilde ele geçirilebilir:

- Web açikligi bulunur.
- Açiklik kullanilarak reverse_shell yerlestirilir.
- Reverse_shell+nc kullanilarak sistemde komut satirina ulasilir.
- Hedef sistemde kernel yamalari eksikse (%80) uygun exploit bulunarak sistemde root haklari elde edilir. (Privilage Escelation)

Şimdi bu aşamaları teker teker izah edelim. Hedef sistemdeki Reverse shell payload'u bizim sisteme durmadan bağlantı sunacaktır. nc ile kendi makinamızdaki ilgili portu tıpkı metasploit'in multi/handler'ı gibi dinleyerek hedef sistemden gelen bağlantıyı yakalayacağız ve sonra bir bakmışız komut satırımızdaki nc hedef sistemin komut satırı haline gelivermiş olur. Hedef sisteme attığımız hak yükseltme payload dosyasını ise komut satırından ./priv_esc şeklinde hedef sistemde çalıştırarak komut satırımız deneme@hedef_sistem iken root@hedef_sistem oluvericektir ve böylelikle root izni elde etmiş olacağız.

Hak Yükseltme Örneği

Exploit indirilir ve hedef sisteme atılır. Ardından exploit hedef sistemde derlenir.

test@hedefSistem > gcc 15704.c -o priv_esc

Daha sonra derlenen dosya hedef sistemde çalıştırılır:

test@hedefSistem > ./priv_esc

Output:
Hey Congratulations... You are root.t

Böylece root yetkisine ulaşırız:

root@hedefSistem > ...

NOT: Sızılan sistemde gcc derleyicisinin var olduğu varsayılmıştır.

Kaynak

Tez Raporu/Literatür Taraması/BGA/Pentest Sunumu.docx
Tez Raporu/Literatür Taraması/BGA/Pentest Sunumu.docx