Privilige Escaltion Methods

Not:Aşağidaki yazdiğim her maddeyi okuyup yazmadim direk,onla nasil privilege escalation yukseltirim dive duşundum hemen hemen hepsinin,escaltion işlemdinde nasi işe yarayacağini biliyorum

1. Hangi işletim sistemi,hangi versiyonu,kernel versiyonu

   Bu veriler kullanirak o versiyona uygun bir exploit,zayifet araştirlmasi yapilabilir

2. Mounted filesystem kontrol et,eğer herhangi unmounted file varsa,onu mount etmeye çaliş

   mount –l,bunla ne yapablirim şuan bir fikrim yok araştiriyorum,ancak mount komutunu suid bit set edilmiş ordan bişeyler çikar gibime geldi

3. Enviremnet variable kontrol et,yanliş bir şekilde configure edilmiş olabilir,Yanliş yerlere Path export etmiş olabilir,onlari kullanrak oraya normalde /bin dizine arancak bir komutu koyariz,bin dizine gitmeden ordan çaliştirir,admin bizim programi çaliştiri yanlişlamaya

4. Development tools kontrol et hangileri var,python g++ hangileri ne yapbilmeye iznim var,

   python,perl,g++,gcc,ruby

5. Yuklu package kontrol et,belki zayifiyertli bir package yuklenmiştir

6. Eğer /etc,/var gibi dizinlere erişebiliyorsam,ordaki tum configurasyanlar bak,yanliş configure edilmişleri ara

7. Çalişan Servisleri Proccesleri kontrol et

8. Özelikle Root olarak çalişan servisler processler

9. Cron joblar bak,onlarin neler caliştirdiğina bak,eğer çaliştirdiklar file yazma iznim varsa ordan yuruyebilirim

   ls /etc/cron*

   ls /var/spool/cron

10. Sistem de bağli device lar varmi,yazicidir felan file

11. Kernel modules kontrol et,

12. /Bin dizindeki programlari kontrol et,izinleri bak,bunlardan yazma değiştirme iznim var mi

13. Shared libray kontrol et,file permisionlari kontrol,ben shared libray ekliyebiliyorum onu kontrol et,eğer eklersem ,ordan bişeyler yapabilirim

14. LD_PRELOAD diye bir env variable varmiş,shared library ilk burda yukluyormuş ,yani ben fgets,scannf,fopen gibi çok kullanilan library ,ayni isimde bura eklerim,adam onu çaliştirken benim kodu çaliştir,

    ->If you set `LD_PRELOAD` to the path of a shared object, that file will be loaded **before** any other library (including the C runtime, `libc.so`).

15. File  kontrol et,sensitive file olabilir ,SUID guıd bitleri set edilmiş olanlar olabilir,izileri yanliş configure edilmiş olabilirler,izinlerini sahibi root olup

    777 izinleri olan

16. suid biti set edilmiş olan file write iznim varsa işim çok kolay dosyanin içeriğini değiştirim amacima gore

    Ancak sadace 400 izni olan bir file  varsa,Shell escape sequence denerim,her ne kadar bunlar eskide kalsa bi ihtimal,kendi makinemde denedim olmuyor vi yi acan useri izinleri escape shell komutlari çaliştiriyor,dosyanin sahibi ve ya suid biti set edilip edilmediğine bakmiyor.Ancak onceden yiyormuş bunu neyse gene deneyip gormuş oldum

17. Network ayarlari kontrol,belkim bunun bağli olduğu ağa sizarim bundan bişey olmaz,diğerleri uzerinde yuruyebilirim

18. Eğer paketleri dinleyebiliyorsam,aği dinlerim belki ordan bişeyler

19. İçinde user and password gibi  keyword içeren file aranir

20. Sistemde tum userlarin listesini çikarim,Özellikle duzenli olarak giriş yapanlari ve bilgisayarda bunlara ait data ararim ,ordan brute force denerim,bash historilerine bakarim

21. Sistemde çalişan procceserin servislerin configurasyon dosyalari bak belki orda şifreleri vardir,tomcati kullandiğim için biliyorum,eğer adam tomcati root olarak çaliştiriyorsa,ve tomcat in conf dosyalari erişebiliyorsam,kesin ordan root shell alirim,conf dosyasinda tomcatin yönetim panelinin şifresi plaint olarak olmak zorunda,ordan onu aldikdan sonra o pc de çalişan tomcat yönetici paneline girip,bana reverse shell verecek bir Java war dosyasi koyarim,urlden gider ora girerim sonra elime root shell var ,bu yuzden root olarak çalişan proccesler serviscler ve  cron jobs lar çok onemli,yukardaki yapan çok avel vardir benim yaptiğim gibi ☺️

22. Bash history yokla ordan bişey çikar,bakarsin ordan şifre denemiştir plain text olarak

23. Ssh private key ararim

24. Loglari kariştir kesin bişey çikar,bazi servisleri şifresini girmiştir,ve ya yanliş girmiştir oraya duşer ordan buluruz

25. Dediğim gibi file permisionlardan yuru,farkli kombinasyonlari dene,

26. Bizim ctf yaptiğimiz gibi,sistemde olan .py .sh gibi dosyalarin permision gore ara,suid bitlerine bak

27. Aklima uçuk bir fikir geldi,Az bişeyler Operation system dersinden hatirliom,şimdi ben pc ye bir flash takacam,operating system bu flash ait driver ihtiyaci olduğunda kernel module olarak import ediyor,ben bu flashin driveri kendim yazacam,işletim sistemi bunu kernel duzeinde eklediğinde dolayi root felan olmamişim yalan,herşeyi yaparim kernel mode da,ancak eminim boyle amelece bir hata yoktur,kesin bir onlemi vardi

28. Bu uste dediğim tek flash için geçerli değil,Linux işletim sistem tum device file olarak tutuyor,ordan iletişim felan geçiyorum,merak ettiğim bu device nasil çaliştiriyor,bir sandbox gibi belirli bi kutu içindemi çaliştiriyor,öğrenmek lazim

29. Sizin yolladiğiniz makelede gibi,bu wildchart üzerinden yururum,system admin çok girdiği dizinleri tar gibi exec parametleri olan için,o parametre için o dizinlere o file eklerim parametre gore,ve ya farkli komutlarin farkli parametleri bakarim — reference gibi,Burda bu nun olmasinin sebebi execve dolayi olduğu belli,parametleri aliş şeklinden kaynaklaniyor,ancak şimdi adamlara neden değiştirmiyonuz bunu diyemedim,şunu ortada bir tradeoff var,hangi birini nasil ekleyecek,tek tek her argumani tarayip tarayip dosya olup olmadiğimi kontrol edecek,kontrol etsene bişey farketmez onun execve sistem call içinde değişmesi lazim,dunya kadar iş gibi duruyor

Onu öğrendindek farkli komutlar ile wildchart denemedim,strace baktim,cp komutunda execve sistem cal ini ayni şekilde çaliştiriyor o da o ayni şekilde etkileniyor,Önemli olan cp komutunun işimi yaran bir parametesi var mi

execve("/bin/cp", ["cp", "exploit.php", "fork.c", "fork.o", "test", "test/"], [/* 41 vars */]) = 0

Not:Doğrudan -rf ismiyle file oluşturamiyoz,touch -rf ,nano -rf,vi -rf diyerek ancak bizde çözum bitmiyor,echo ""> -rf ve ya gidip arayuz varsa ordan da değiştirebiliyoz ismi ,Bunun sebebide ordaki komutlari - ile başlayanlarin kendi argumanlari olduğu zannediyorlar,ancak stdout redict edince sadece file olduğunu duşunduğu problem yok

Bunu en çok kullanilan cd komuduna yapmaya çaliştim, strace komutu takip etmeye çaliştim ancak yemedi,sonra cd komutunu aradim which ile çikmadi,sonra nette aradim o buitin command miş,yeni bişeyler öğrendim guzel guzel ,buitin kasti şey yeni process oluşturmadan yapmasi,zaten cureent directory variable değiştirmek için gidip yeni procces oluştursa tam avvelik olurdu,ondan dolayi bu builtin komutlari hizli çalişir

Not:Bu yukarda dediklerim hepsini oto arayan scriptler buldum hepsini,Normalde hepsinin altina gereken komutlari yaziyordum baktim çok şişecek vazgeçtim ,Bu scriptleri github ekledim ,public yaptim kullancağim zaman ordan çekeceğim

->https://github.com/altuntasfatih/PrivilegeEscalation