### Linux Hak Yükseltme Yontemleri ( Privilege Escalation )

Bir sistemde, belli kullanıcı haklarını kullanarak oturum elde etmek mümkündür. Ancak, eğer bir sonraki adımımız daha büyük amaçlar taşıyorsa, yani en yüksek kullanıcı haklarını kullanarak yapılabilecek işlemler ise, o zaman hak yükseltmemiz gerekmektedir. Hak yükseltme için gerekli olan durum ise hedef sistemde çalışan servislerde, uygulamalarda vb. bulunan yapılandırma eksiklikleridir. Bu eksiklikleri istismar ederek hak yükseltme dediğimiz en yüksek kullanıcı haklarına sahip olmamız mümkündür.

Burada temel adımları; hedef sistem hakkında bilgi toplamak, işimize yarayacak olanları seçmek ve eğer gerekli ise exploit hazırlayarak her türlü yolu denemek olarak sıralayabiliriz.

Linux bir sistemde ilk iş olarak versiyon bilgisi, hangi dağıtımın kullanıldığı, kernel sürümü gibi bilgiler edinilebilir.Kullanılabilecek komutlardan bazıları;S

ürüm bilgileri: cat /etc/\*-release

Sistem hakkında bilgi: uname -a

Hangi servislerin çalıştığı : top

Root çalışan işlemler: ps aux | grep root

Hangi uygulamaların kurulu olduğu: ls -alh /usr/bin/

Hatalı veya yanlış konfigürasyonlar kontrol edilebilir: cat /etc/syslog.conf

Planlanmış iş var mı: crontab -l

Diğer hostların sistem ile ilişkileri vb.: netstat -antup

gibi birçok bilgi toplanarak bunlara uygun senaryolar düşünülebilir. Eksiklikler, hatalar belirlenerek bunlar istismar edilebilir.

Zafiyet Olabilecek sistemler ( Yapılması gereken kotroller ):

* Çekirdek (kernel) ve işletim sistemi sürümü
* Sonradan veya varsayılan olarak kurulu olan uygulamaların sürümü
* “root” yetkisi ile çalışan servisler ve uygulamalar
* Kullanıcılar ve gruplar
* Çalışan prosesler
* Yapılandırma ayarları
* Aygıtlar
* Dosya içerisinde yazılı bilgiler (parola gibi)
* Herkes tarafından çalıştırılabilir veya yazılabilir dosyalar (özellikle betikler) ve içerikleri
* SUID veya GUID biti etkin dosyalar ve işlevleri
* Servisler
* Zamanlanmış görevler
* Çevresel değişkenler
* Uzaktan erişim (SSH, R\* servisleri, VNC,…) için kimlik bilgileri veya anahtarlar

En temelde bu kontrollerin yapılması ile hak yükseltme için gerekli açıklar bulunabilir.

Belirtilen kontroller için çalıştırılabilecek komutların listesi aşağıdaki sitelerden elde edilebilir.

* G0tmi1k: <http://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation>
* RebootUser: <https://www.rebootuser.com/?page_id=1721>
* Xapax: <https://github.com/xapax/security/blob/master/privilege_escalation_-_linux.md>
* Cybrary: <https://www.cybrary.it/0p3n/penetration-testing-checklist-linux-machine-intrusion-discovery/>

**Toolar ( Tavsiye edilmez ) :**

En çok kullanılan toolar :

* **Linenum (RebootUser):** <http://www.siberportal.org/red-team/linux-penetration-tests/linenum-betigi-ile-tespit-edilen-zamanlanmis-gorev-betiginde-hatali-joker-karakteri-kullanimi-tar-araci-ile-hak-yukseltme/>
* **Unix-Privesc-Check (PentestMonkey):** <http://www.siberportal.org/red-team/linux-penetration-tests/unix-privesc-check-betigi-ile-tespit-edilen-zafiyetli-chkrootkit-paketindeki-zafiyet-istismar-edilerek-root-yetkileri-ile-komut-satirinin-elde-edilmesi/>
* **LinuxPrivChecker:** <http://www.siberportal.org/red-team/mysql-database-penetration-tests/linuxprivchecker-betigi-ile-tespit-edilen-mysql-kullanici-tanimli-fonksiyon-raptor_udf-hak-yukseltme-zafiyetinin-istismari/>
* **Linux-Local-Enum:** <http://www.siberportal.org/red-team/linux-penetration-tests/linux-local-enum-betigi-ile-tespit-edilen-hatali-yapilandirma-zafiyeti-istismar-edilerek-root-yetkileri-ile-komut-satirinin-elde-edilmesi/>
* **Linux-Exploit-Suggester:** <http://www.siberportal.org/red-team/linux-penetration-tests/linux-exploit-suggester-betigi-ile-tespit-edilen-isletim-sistemi-zafiyeti-istismar-edilerek-root-yetkileri-ile-komut-satirinin-elde-edilmesi/>
* **KernelPop:** <https://www.siberportal.org/red-team/linux-penetration-tests/kernelpop-betigi-ile-tespit-edilen-isletim-sistemi-zafiyetinin-istismar-edilerek-root-yetkileri-ile-komut-satirinin-elde-edilmesi>
* **Linux\_Exploit\_Suggester:** <https://github.com/PenturaLabs/Linux_Exploit_Suggester> VEYA <https://github.com/InteliSecureLabs/Linux_Exploit_Suggester> (Güncel değildir. Linux-Exploit-Suggester kullanılması tavsiye edilir.)
* **LinExpSuggester & LinPrivChecker & LinExpChecker:** <https://github.com/reider-roque/linpostexp> (Diğer orijinal betiklerin yedekleri bulunmaktadır.)
* **LARE:** <https://github.com/m4lv0id/LARE>
* **Auto-Root-Exploit**: <https://github.com/nilotpalbiswas/Auto-Root-Exploit> (LARE betiğinin sadece internetten istismar kodu indirme özelliği olan koddur)
* **Elevator:** <https://github.com/guifre/Elevator>
* **Inspector:** <https://github.com/graniet/Inspector>
* **Linux Soft Exploit Suggester:** <https://www.kitploit.com/2017/11/linux-soft-exploit-suggester-search.html>
* **PrivEscalation:** <https://github.com/expl0i13r/privescalation/blob/master/privescalation.sh> (Sadece genel sorgular bulunur)
* **MSF**: post/multi/recon/local\_exploit\_suggester

**Yapılandırma Zafiyetleri :**

* **Sudo yetkisi**
* **Sudo enjeksiyonu:** <https://github.com/nongiach/sudo_inject>
* **Yazılabilir /etc/passwd dosyası:** <http://www.siberportal.org/red-team/linux-penetration-tests/erisim-izinleri-uygun-ayarlanmamis-etc-passwd-dosyasinin-kotuye-kullanilarak-hak-yukseltilmesi/>
* **Yazılabilir /etc/sudoers dosyası**
* **“history” geçmişleri**
* **Yapılandırma dosyaları**
* **/root/.bashrc dosyası:** <https://null-byte.wonderhowto.com/how-to/use-misconfigured-suid-bit-escalate-privileges-get-root-0173929/>
* **PATH Çevresel Değişkeni:** <http://www.siberportal.org/red-team/linux-penetration-tests/linux-isletim-sisteminde-suid-biti-zafiyeti-istismar-edilerek-cevresel-degiskenlerin-degistirilmesi-ve-root-yetkilerine-hak-yukseltilmesi/> && <http://www.hackingarticles.in/linux-privilege-escalation-using-path-variable/>
* **SUID biti etkin dosyada çevresel değişken:** <https://bitvijays.github.io/LFC-VulnerableMachines.html#environment-variable-abuse>
* **SUID biti etkin “donpcgd” aracı:** <http://www.siberportal.org/red-team/linux-penetration-tests/linux-isletim-sisteminde-suid-biti-zafiyeti-istismar-edilerek-zamanlanmis-gorev-olusturulmasi-ve-root-yetkilerine-hak-yukseltilmesi/>
* **SUID biti etkin “procwatch” aracı:** <http://www.siberportal.org/red-team/linux-penetration-tests/linux-isletim-sisteminde-suid-biti-zafiyeti-istismar-edilerek-cevresel-degiskenlerin-degistirilmesi-ve-root-yetkilerine-hak-yukseltilmesi/>
* **SUID biti etkin “nmap” aracı:** <http://www.siberportal.org/red-team/linux-penetration-tests/suid-biti-etkin-olan-nmap-araci-ile-hak-yukseltme-isleminin-gerceklestirilmesi/>
* **SUID biri etkin “vim.basic” aracı:** <https://null-byte.wonderhowto.com/how-to/use-misconfigured-suid-bit-escalate-privileges-get-root-0173929/>
* **SUID biti etkin “tcpdump” aracı:**https://bitvijays.github.io/LFC-VulnerableMachines.html#tcpdump
* **SUID biti etkin “tee” aracı:** <https://bitvijays.github.io/LFC-VulnerableMachines.html#tee-suid>
* **SUID biti etkin “strace” aracı:** <http://mannulinux.blogspot.com/2018/07/vulnhub-linux-vm-linsecurity-1.html>
* **SUID biti etkin “wget” aracı:** <https://bitvijays.github.io/LFC-VulnerableMachines.html#wget> && sudo wget -i /etc/shadow 2>&1
* **SUID biti etkin “pip” && “npm” aracı:** <https://bitvijays.github.io/LFC-VulnerableMachines.html#package-installation>
* **IFS:** <http://www.dankalia.com/tutor/01005/0100501004.htm>
* **Symlink:** <https://bitvijays.github.io/LFC-VulnerableMachines.html#symlink-creation>
* **Zamanlanmış görevde Joker kullanılmış “tar” aracı:** <http://www.siberportal.org/red-team/linux-penetration-tests/linenum-betigi-ile-tespit-edilen-zamanlanmis-gorev-betiginde-hatali-joker-karakteri-kullanimi-tar-araci-ile-hak-yukseltme/>
* **Openssh 4.7 <–> 7.1:** <https://dustri.org/b/how-to-radare2-a-fake-openssh-exploit.html>
* **LD\_Preload Çevresel Değişkeni:** <http://www.hackingarticles.in/linux-privilege-escalation-using-ld_preload/>
* **Docker grubu üyesi iken docker komutları ile hak yükseltme:**mannulinux.blogspot.com/2018/07/vulnhub-linux-vm-linsecurity-1.html
* **apt ve dpkg araçları:** <https://bitvijays.github.io/LFC-VulnerableMachines.html#unattended-apt-upgrade>

temelde bunlardır.

SUID/GUID bitini kontrol eden uygulamalar vardır . Bu uygulamalar aracılığı ile sistemlerde hak yükseltilebilir.

Bzılar:

* nmap
* vim
* less
* more
* nano
* sudoedit
* tar
* zip
* cp
* mv
* find