Phoenix Linux User Group Security Team

HackFesting: Linux Attack Vectors demonstrated in Videos from reverse engineers and the security community.

Attack vectors in linux follow two basic OSI paths; top down and bottom up.

Therefore our OSI vector will be either application based or network based except where our exploits employ more than one known hack. While this is far from a complete list of tools to obtain unauthorized access to linux systems, it will provide a realistic idea of current security and insecurity for linux desktop and ser ver.

Network

Ettercap

http://www.youtube.com/watch?v=ESGV9zlo0Zo&feature=related

SSLStrip

http://www.youtube.com/watch?v=Dd5qGS-5C0I&feature=related

Arp Poisoning

http://www.youtube.com/watch?v=9z8i9SQr_s8&feature=related

Cain Arp Poisoning

http://www.youtube.com/watch?v=dbxG1sT3MSI&feature=related

DNS

http://www.youtube.com/watch?v=2hMkSNiBPvE&feature=related

http://www.youtube.com/watch?v=ICnwsn8tpFU&feature=related

http://www.youtube.com/watch?v=IOKBPb6aI2k&feature=related

http://www.youtube.com/watch?v=Aak6-B3JORE

http://www.youtube.com/watch?v=UtEPfAgp2Xg

http://www.youtube.com/watch?v=B4NwtrWOxiU&feature=related

PDF

http://www.youtube.com/watch?v=T3g2EGdZygw&feature=related

http://www.youtube.com/watch?v=WidakWk34LE

JPG

http://www.youtube.com/watch?v=jt81NvaOj5Y

Browser

http://www.youtube.com/watch?v=PGpAZZW6lrc

http://www.youtube.com/watch?v=tfFq8n9fCUs&feature=related

http://www.youtube.com/watch?v=id9PXH_xOvE&feature=related

XSS Session Hijacking – Script Injection

http://www.youtube.com/watch?v=r79ozjCL7DA&feature=related

Opera

http://www.youtube.com/watch?v=qNM6_Pi8XqY

Firefox

http://www.youtube.com/watch?v=G_lNIByYXxE&feature=related

SHELL/Kernel

http://www.youtube.com/watch?v=UdkpJ13e6Z0

http://www.youtube.com/watch?v=ShoAOdx0K7I&feature=related

http://www.youtube.com/watch?v=fUNE5t-bqsQ&feature=related

SSH

http://www.youtube.com/watch?v=jaEmcfKdJZU

http://www.youtube.com/watch?v=weEZtBTfEMU&feature=related

SAMBA

http://www.youtube.com/watch?v=8pfFbEbHRbM

http://www.youtube.com/watch?v=eQ0DwB8S_GM&feature=related

FTPD

http://www.youtube.com/watch?v=m3ohrvDMcv4&feature=related

WWW

http://www.youtube.com/watch?v=fXdnciH-BFM&feature=related

http://www.youtube.com/watch?v=dOpPbpUeeAo&feature=related

MAIL

Keylogging/Phishing

http://www.youtube.com/watch?v=KjrNO2GW1Cc&feature=related

http://www.youtube.com/watch?v=f8_M6V3xILE&feature=related

http://www.youtube.com/watch?v=lKmSqcJm7RQ&feature=related

PHP

http://www.youtube.com/watch?v=z0D0CTflj5U&feature=related

http://www.youtube.com/watch?v=YyaQw0ae_7I&feature=relmfu

http://www.youtube.com/watch?v=e4EYkoLlSq0&feature=relmfu

http://www.youtube.com/watch?v=ZFQ1PAdI6AY&feature=related

SQL Injection

http://www.youtube.com/watch?v=WHtUismhgzQ&feature=related

Wireless

http://www.youtube.com/watch?v=Vnvb3NzjBxA&feature=fvsr

http://www.youtube.com/watch?v=vnGqZPI5EPk&feature=fvwrel

Workarounds

http://www.youtube.com/watch?v=li1QABi25Ao&feature=related

BASIC LINUX USE PROTECTION RULES

Always use a fully random 8 character password. Change your password often. Never use the same password on all systems. Always use stable patched sources for your distribution as well as your daemons. Disable or install services you do not use, like Bluetooth. Read your logs and understand your normal packet traffic.

Do not leave ports open for the world; use source and destination trust only in iptables for ftp, ssh or VNC. Never open any executable file that you do not trust. Browse only with javascript turned off to untrusted sites. Never access trusted websites or services on an untrusted network even with SSL unless you can risk having your credentials hijacked. Do not open OpenOffice, pdf or jpg files from any source you do not trust.

Do not use Wireless unless you have a radius server configured with WPA-Enterprise without understanding the risks. While additional MAC address connection controls can assist, they do not completely protect you under WEP or WPA2.

Scan your own systems and networks to understand what is available (via nmap) and use Rapid7 Nexpose community scanner to expose known exploits if you run home servers. Do not cache your router password in your browser, as it can be XSS accessed trivially.