CHAPTER 1

THREAT LANDSCAPE:

LINUX ISN'S SUSCEPTIBLE TO TYPICAL WINDOWS VIRUS INFECTIONS, BUT STILL HAS FLAWS

BOTNET MALWARE - REMOTE-CONTROL MALWARE. EXAMPLES INCLUDE A LINUX-SERVER DDoS BOTNET

RANSOMWARE - ENCRYPTS USER DATA & EXPECTS A PAYOUT.

CRYPTOCOIN MINING SOFTWARE - USES SYSTEM CPUS TO MINE CRYPTOCURRENCY FOR THE ATTACKER

PRIMARY CAUSES OF SECURITY BREACHES COME FROM SECURITY BUGS AND POORLY CONFIGURED SERVERS

LABS USE UBUNTU SERVER & CENTOS 7 VMS IN VIRTUAL BOX

CENTOS 7 EPEL INSTALL INSTRUCTIONS

SUDO YUM INSTALL YUM-PLUGIN-PRIORITIES EPEL-RELEASE

NAVIGATE TO /ETC/YUM.REPOS.D

~$ CD /ETC/YUM.REPOS.D

OPEN CENTOS-BASE.REPO IN A TEXT EDITOR

/ETC/YUM.REPOS.D$ SUDO VIM CENTOS-BASE.REPO

AFTER THE FINAL LINE OF BASE, UPDATES, & EXTRAS, ADD PRIORITY=1

AFTER CENTOSPLUS ADD PRIORITY=2

OPEN EPEL.REPO

/ETC/YUM.REPOS.D$ SUDO VIM EPEL.REPO

AFTER EPEL ADD PRIORITY=10

AFTER ALL OTHERS ADD PRIORITY=11

~$ SUDO YUM UPGRADE

~$ SUDO YUM LIST > YUM_LIST.TXT