Linux Academy: Security Track – Triple Tools Video http://linuxacademy.com

ClamAV

- ☒ sudo apt-get install clamav
  - system update automatically run, but no daemon in background
- ☒ sudo apt-get install clamav-daemon
- ☒ update the definitions
  - sudo freshclam
- ☒ start the service
  - sudo service clamav-daemon start
- ☒ basic filesystem scan
  - sudo clamscan /path/to/folder
  - sudo clamscan -r –bell -i /path/to/folder
    - will flash the screen if there are any viruses

chkrootkit

- ☒ sudo apt-get install chkrootkit
  - will install application and supporting libraries
- ☒ sudo chkrootkit
  - will check for all the rootkits that are currently in its binary database
- ☒ Updates
  - sudo apt-get upgrade
  - will pull updates as they are published

LSAT (Linux Security Administration Tool)

- ☒ sudo apt-get install lsat
- ☒ sudo lsat
  - large number of scripts, will take some time (md5 package can take hours to complete)
- ☒ output file – lsat.out
  - human readable format, all module results that were run
- ☒ sudo lsat -o custom.out -m debian -x modules.exclude
  - custom output file
  - debian distribution
  - exclude modules file
- ☒ -w output.html
  - html formatted output in addition to log created with -o
- ☒ list of all modules
  - bpass
  - cfg
  - dotfiles
  - files
  - forward
  - ftpusers
  - inetd
  - inittab
  - ipv4
  - issue
  - kbd
  - limits
  - logging
  - md5
  - modules
  - net

  - open
  - passwd
  - perms
  - pkgs
  - promisc
  - rc
  - rpm
  - securetty
  - set
  - ssh
  - startx
  - umask
  - write
  - www

Linux Academy: Security Track – John the Ripper

John the Ripper

- sudo apt-get install john john-data
- Download the word list (free) at:
  - http://download.openwall.net/pub/wordlists/all.gz
- sudo gunzip all.gz
- create a test user for cracking with the tool

- ☒ combine the password files so that john can identify a user and password tandem
    - sudo unshadow /etc/passwd /etc/shadow > mypassword.list
- ☒ make sure john.ini exists
    - touch john.ini
    - place file in directory you will run the tool from
- ☒ john –format=crypt -wordlist:all mypassword.list
    - -format=crypt work with md5 encrypted hashes
    - -wordlist:all use wordlist called 'all'
    - mypassword.list unshadowed system password list
- ☒ tail john.pot
    - cracked password output file
- ☒ sudo cat mypassword.list | grep 'hashvaluecrackedabove'
    - identifies username matching the cracked password
- ☒ Running with the 27mb 'all' file against a large number of users can/will take hours to run
- ☒

Linux Academy: Security Track – NMap

NMap

- ☒ sudo apt-get install nmap sysstat
- ☒ sudo nmap localhost
    - simple scan on localhost for all open ports and services
- ☒ sudo nmap -p22 localhost
    - is port 22/ssh open?
- ☒ sudo nmap -p22,23,80,443
    - are any of those ports open?
        - comma delimited means are any of them running
        - range will test all and report only those open

- ☒ sudo nmap 192.168.1.0/24 > results.txt
    - ping scan, what ips are running on the subnet in question
    - cat results.txt
        - will show all ips on that network
- ☒ sudo nmap -p1-340 -sV 192.168.1.250
    - in that range of ports, what version are those services
    - -o what operating system is the system in question
- ☒ sudo -oA scanresults.txt
    - 3 results file
        - .gnmap – grep format file
        - .nmap – human readable/plain text format
        - .xml – extended markup format (great for database import)
    - add -vv for more verbose information included in each of those files

Linux Academy: Security Track – Netstat

Netstat

- ☒ Installed by default on all Linux systems
- ☒ sudo ifconfig
- ☒ sudo netstat -ie (same output on interface)
- ☒ sudo netstat -i
    - abbreviated interface information
- ☒ sudo netstat -rn
    - kernel routing table without name resolution
- ☒ netstat -a
    - all (tcp, rdp, etc) and all states current and sum
- ☒ netstat -aute
    - all tcp, udp, established connections with extended information
- ☒ netstat -lt
    - listening status by application

- netstat -s
    - complete protocol summary since last reboot/interface restart
- netstat -pt
    - run as sudo to get all processes
    - PID and name by all current states
- netstat -c
    - running netstat repeated every few seconds (fast scroll)
- netstat -ap
    - all applications running with the associated service and ports on system
- netstat -an
    - all applications by port
- netstat –tcp –listening –programs
    - more human readable options (matches the -atpe)

Linux Academy: Security Track – Wireshark

Wireshark

- sudo apt-get wireshark
- network interface needs to have permission and be running in permiscuous mode in order to listen to all passive traffic on the network your interface is on
- sudo wireshark
    - sudo necessary to have permission to the interfaces to set the packet captures on
- start capture on eth0
    - filters at the top, simple
        - tcp, http, ftp, ssh, etc – green will indicate valid filter
    - filters, custom (tools)
        - tcp.receive exists
        - http.cookie exists, etc
        - again, green will indicate a valid filter type
- captures can be stopped after a period of time and then reviewed and filtered or can be done and applied various filters live
- in configuration, turn on reverse DNS lookup so that outgoing/incoming connections have associated names when available
    - note: will slow down capture over time or when DNS systems are not performant
- all seven levels of the network OSI model are viewable by packet, disassociated or assembled

    - OSI model layers:
        - application layer
        - presentation layer
        - session layer
        - transport layer
        - network layer
        - data link layer
        - physical layer
- can be set to log output live, filtered or unfiltered

Linux Academy: Security Track – IPTraf

IPTraf

- sudo apt-get iptraf
- more of a 'local network troubleshooting' system
- can scan passive network traffic on the network if set to permiscous mode (and can be set to log) but interface makes live capture of passive network traffic difficult to follow
- sudo iptraf
    - configuration, permiscuous, name resolution, etc
    - ip traffic monitor
        - by connection with some summary statistics
    - general interface statistics
        - by interface with some summary statistics
    - detailed interface statistics
        - by protocol, in detail and total and in/out bandwidth utilization
    - statistical breakdowns
        - live view of all connections by port, protocol, in detail and summary
    - filter
        - include/exclude
        - by port, protocol
        - by source, destination
        - apply filter to view results
- logging to file
    - sudo iptraf -s eth0 -B
        - -s interface
        - -B background run

- /var/log/iptraf
    - rvnamed.log
    - tcp_udp_services-eth0.log
-