CCDC – “First Fifteen” Checklist

Splunk Station

1. CHANGE PASSWORDS. TAKE SCREENSHOTS OF THE UNALTERED FILES.
   1. First, check the **passwd** binary to ensure that it has not been swapped out with password scraper. Use [whereis ] to locate the binary files and [ cat ] to see if they are in fact binary executables or Bash scripts. If cat shows a readable text file, something is wrong.
   2. Review the /etc/passwd and /etc/shadow files to determine which users have logins.
      1. You can use [ cat /etc/passwd | grep bash or cat/etc/passwd | grep -v nologin ] to exclude disabled/unaccessible accounts in /etc/passwd.
      2. You can use [ sudo awk -F: '{if ($2 != "\*") print}' /etc/shadow ] to filter out daemon accounts that have no passwords (“\*” in field 2 of the shadow file).
   3. **Change the passwords** of accounts with logins**, according to the team’s agreed-on password scheme,** and **record your station’s “extension” of the password on the board.** (ex, Cvber123###\_ \_ \_ or something else).
   4. Recommended – disable the Root user entirely by changing the shell in the passwd file from “bash” to “nologin”.
2. CAPTURE SCREENSHOTS OF INITIAL STATES
   1. The /etc/passwd file
   2. Current listening connections [ netstat | grep LISTEN ]
   3. Look for processes started recently or after the flag drop that you didn’t make [ ps aux ]
3. MAKE A BACKUP OF CONFIG FILES
   1. Tarball the /etc folder. This command [ sudo tar czf splunk\_etc\_backup.tar.gz /etc ] will archive the entire /etc file into splunk\_sysconfig\_backup.tar.gz into the current working directory.
   2. Secure shell copy the tarball to the local Linux box. [ scp splunk\_etc\_backup.tar.gz student@linux.ncstech.org ]
4. SET UP FIREWALL
   1. sudo firewall-cmd --zone=public --add-masquerade –permanent
   2. sudo firewall-cmd --zone=public --set-default=drop
   3. sudo firewall-cmd --zone=public --add-port=8000/tcp --permanent
   4. sudo firewall-cmd --zone=public --add-port=514/tcp --permanent
   5. sudo firewall-cmd --zone=public --add-port=514/udp --permanent
   6. sudo firewall-cmd –reload
   7. (This is all assuming that the Splunk is on RHEL 9.3 – separate iptables doc will be attached for an older distro that doesn’t support frontend config).
5. CONFIGURE DEFAULT GW (If necessary)
   1. ip route 0.0.0.0/0 172.20.241.254
6. START REMOTE SYSLOG SERVICE FOR LOG COLLECTION
   1. Separate document included. May need adjustment because the Linux distro in the practice and invitational environments are not the same as the qualifier and beyond.