**Linux**

1. Kill networking and Firewall setup (iptables)
   1. Service network stop
   2. Ifconfig <interface-name> down
   3. Iptables -F
   4. Iptables –P INPUT DROP
   5. Iptables –P OUTPUT ACCEPT
   6. Iptables –P FORWARD DROP
   7. Iptables –A INPUT –p tcp –s <ip-address of scoring engine> --dport <scored port number> -m state –state NEW,ESTABLISHED –j ACCEPT
2. Rotate Creds and delete unnecessary accounts
   1. Passwd <username>
   2. Check users – cat /etc/passwd, /etc/shadow
   3. Userdel –rf <username>
3. What services and processes are running on the box and listening ports
   1. Service –status-all
   2. Ps -aux
   3. Ps –ef
   4. Service <service-name> stop
   5. Netstat –tulpan
   6. Chkconfig --list
4. Backup configs for scored service
   1. Cp <file path> <new file path>
5. Check environ for suspicious
   1. Cron jobs
   2. Vi ~/.bashrc
   3. ENV
   4. Echo $PATH
   5. Vi /etc/rc.local
6. Check service configs for vulns
   1. ~/.ssh/authorized\_keys
   2. /etc/dhcp/dhcpd.conf
   3. /etc/named.conf or /var/named/
7. Restart services and turn on interfaces
   1. Service <service-name> restart
   2. Ifconfig <interface-name> up
8. Audit System
   1. Github.com/ppil/nixaa.sh
   2. Sticky Bits
   3. Groups
   4. Permissions
   5. Inventory all executables or scripts
9. Check for other bads
   1. Netcat listener