Read on the below topics.

- Things should do before enabling auditing in a company
- Blackjacking tool (BBProxy)
- SOAP communication
- ACL list configured on a server
- Shellshock vulnerability
- POODLE attack
- Heartbleed – fetch OpenSSL Private keys..
- Time to Live Exceeded packets
- ISO 27002 – Guidelines
- RSA & AES encryption
- Identify port scan (Printing Ports – 9100,613,515)
- Banner grabbing
- Google hacking techniques
- NMAP
- Nmap UDP scanning
- Nmap log analysis and identifying it as port scanning
- Hping2/3
- Firewalk
- Idle scan – zombie
- Virus – stealth scan
- TCP Ack scan
- Burpsuite
- BBProxy – Blackjack
- Snort rules
- IDS/ NIDS
- Exploit framework automation – Nessus/ metasploit
- DNS Sec
- IP SEC
- Msfencode – metasploit evasion from AV
- Netcat tool
- ADS (Alternate Data Stream)
- Covert channel
- Botnet
- Wireshark filters
- OS Fingerprinting is an Active scanning methodology
- DNS Zone transfer & Dig command
- Bash exploit to see the etc/password file
- Fetching /etc/password file in Linux. Circumstances?
- John the ripper tool
- DNS poisoning – malware infecting linux machines hosts file
- N-tier architecture layer that is responsible for data transmission & data processing
- Click jacking attack
- Cross Site Request Forgery attack
- Wireless analysis which comes in Linux machines – wireshark airpcap
- Evil Twin attack – WIFI attacks
- Session Splicing & IP fragmentation
- SHA1 message digest produces 160 bit msg
- PKI Infrastructure – CA – Issues & verifies digital certificates