214-Final-Review

Cyber-related laws covered in the book.

Social Engineering - types? What does a social engineer prey upon?

dumpster diving, shoulder surfing, reverse-social-engineering, persuasion/coercion

Social Networking and Company Security. What percentage of companies have a defined social networking policy?

Footprinting people: what tools can you use to search info on people?

Incident Responce phases and their characteristics/definition.

Types of evidence: ??? Know the types and definitions. What is Chain of Custody? Why is it important?

Know BCP, BIA, DRP, IRP, SLA.

What types of DRP testing exist? Differentiate the types listed in the book.

Fault tolerance vs. Redundancy

IDS vs IPS - Signature vs Anomoly...

HIDS vs NIDS and their components.

Firewall types and how they examinine traffic: packet filtering/stateful inspection/application proxy

Honeypot/Honeynet

Permissions: MAC, DAC, RBAC, etc... from book. Misuse vs Abuse vs Intrusion

Controls: TAP

Kali Linux: directories, commands. Book content areas.

Session hijacking, XSS, Buffer overflows, SQL-injections, DoS vs DDoS, Botnets, ARP poisoning, MAC flooding, hubs vs switches,

Passive vs Active sniffing

Netcat - what is it good for?

Viruses/Malware/Trojans, worms, rootkits, polymorphic, poly-???, etc...

Virtualization: PaaS/SaaS/IaaS...

SQL vs NoSQL

Encryption Algorithms/Ciphers

NCC SQuirreL, AppDetectivePro and ...

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

SKILLS -REVIEW

Review the Shellshock lab and how BASH is vulnerable. Two types of attacks.

Review SQL Injection lab and how you construct a query..

Steganography- what is it. How does Steghide work, in general terms.

MSF, in general. Reviewing labs should refresh the relevant info.

nmap command and switches from Kali.

NetCat: construct a command with –help

Review John the Ripper, Metasploit Commands, SQL Injections