**Kybernetická bezpečnost**

1. Základy práce v textovém rozhraní
	1. terminál
	2. shell
	3. spouštění programů a skriptů
	4. přepínače a parametry
	5. standardní vtup/výstup/error
	6. přesměrování výstupu
2. Práce se soubory
	1. adresářová struktura
	2. vytváření a úprava souborů
	3. metadata
3. Oprávnění v GNU/Linux systémech
	1. uživatelé
	2. skupiny
	3. úrovně přístupu
	4. změna oprávnění
	5. sudo
4. Instalace softwaru v GNU/UNIX systémech
	1. balíčkovací správci
	2. sestavení ze zdroje
5. Síťování v GNU/Linux systémech
	1. network stack
	2. síťová konfigurace
	3. principy TCP/IP
6. Průzkum a sken sítě
	1. skenování sítě a síťových služeb
	2. navázání a příjem spojení pomocí nástroje netcat
7. Analýza síťového provozu
	1. tcpdump
	2. wireshark
8. Síťové protokoly
	1. síťové protokoly obecně
	2. DHCP
	3. DNS
	4. NTP
	5. ARP
	6. ICMP
	7. SSH (SCP)
9. Druhy síťových útoků
	1. ARP spoofing
	2. DHCP starvation
10. Bash skriptování
	1. proměnné
	2. cykly
	3. podmínky
	4. satus kódy
	5. parametry
11. Kryprografie
	1. základní principy
	2. starověké šifry
	3. symetrické kryptografické algoritmy
12. Asymetrická kryptografie
	1. principy
	2. hashování
13. Virtualizace
	1. typy virtualizace
	2. nastavení a instalace virtuálního stroje
	3. využití virtualizace při analýze škodlivého softwaru
14. Analýza škodlivého softwaru
	1. principy statické analýzy
	2. využití online nástrojů
	3. principy dynamické analýzy
15. Firewall
	1. principy firewallu
	2. nastavení firewallu
16. Procesy
	1. manipulace s procesy
	2. vyhledávání procesů
	3. analýza procesů
17. Webové technologie
	1. principy HTTP
	2. frontend technologie webových aplikací
	3. backend technologie webových aplikací
18. Bezpečnost webových technologií
	1. nastavení testovací proxy
	2. popis OWASP top 10
	3. metody testování
19. Síťový monitoring
	1. druhy síťového monitoringu
	2. analýza zachycených dat
20. IDS, IPS
	1. popis druhů a jejich využití
	2. nastavení nástrojů