UNIVERSIDADE CATÓLICA DE BRASÍLIA

Pós-graduação Lato Sensu em Perícia Digital

Turma 11 - Análise de tráfego em redes TCP/IP - Prof. Eriberto

- Atualizado em 20 ago. 2015 -

Cronograma de aulas

Aula	Data	Previsão de aula	Obs
1	**21 ago**	• SANS Pocket reference e guia tcpdump. • CORE Network (simulador). • Introdução às redes de computadores. • Introdução às redes TCP/IP. • **Temas para trabalhos em grupo.** • Protocolo IPv4.	• Exercícios para casa: 1, 2 e 3.
2	**28 ago**	• Retirada de dúvidas dos exercícios 1 e 2. • Correção do exercício 3. • Protocolo TCP.	• Exercício para casa: 4.
3	**04 set**	• Correção do exercício 4. • **Escolha dos temas pelos grupos.** • Fluxo TCP. • Protocolo UDP. • Protocolo ICMP.	• Exercícios para casa: 5 e 6.
4	**11 set**	• Correção dos exercícios 5 e 6. • Modelo OSI. • Protocolos Ethernet e ARP. • Problemas de segurança na camada 2.	• Exercício para casa: 7.
5	**25 set**	• Correção do exercício 7. • Payloads que falam. • Demonstração. • netmate, wireshark, windump, packit, netdude, driftnet e pcredz. • Seguindo streams com wireshark e chaosreader.	
6	**02 out**	• Roteamento em redes TCP/IP. • Utilização de gateways. • Lei da proximidade. • Lei do menor esforço. • Bridges em GNU/Linux. Demonstração. • MRTG. • Vlans.	• Exercícios para casa: 8 e 9.
7	**09 out**	• Correção dos exercícios 8 e 9. • Protocolo IPv6.	• Exercício para casa: 10.

8	**23 out**	• Correção do exercícios 10. • Serviço DNS. • Sistemas de firewall.	• Exercícios para casa: 11 e 12.
9	**06 nov**	• Correção dos exercícios 11 e 12. • Filme WOTN. • Controle de tráfego em redes TCP/IP.	
10	**13 nov**	• Exercício prático de infraestrutura de redes de computadores. • Itens: criação das redes; estabelecimento do roteamento; implementação de uma bridge; análise de tráfego; solução de problemas. • Criação de uma rede automática.	---
11	**16 nov**	• Prova teórica individual. • Entrega do resultado da prova.	• Prova individual, com consulta apenas ao "TCP/IP and tcpdump Pocket Reference Guide" (IPv4 e IPv6). • Nota mínima: 7,0. Tempo de prova: 1 hora.
12	**20 nov**	• Trabalho em grupo (30 min cada).	---
REC	**11 dez**	• Prova de recuperação.	---

Temas para trabalhos em grupo:

- Protocolos SMB, NMB e CIFS (citar SAMBA e operações de “browseamento”).

- Protocolos ATM, PPP e Frame Relay (citar PPPoE, PPPoA e LLC).

- Protocolos RIP, OSPF e BGP (citar Bird e Quagga).

- Redes Zeroconf.

- OpenVAS, Zabbix, Cacti (citar vulnerabilidades do SNMP).