

Program and Rules

Segurança em Redes de Comunicações

**Mestrado em Cibersegurança
Mestrado em Engenharia de Computadores e
Telemática
DETI-UA**



Professores

- Prof. Paulo Salvador
 - ♦ Email: salvador@ua.pt
- Prof. João Paulo Barraca
 - ♦ Email: jparraca@ua.pt
- Prof. António Nogueira
 - ♦ Email: nogueira@ua.pt



UC Informations

- All materials, documents and software will be available on eLearning.ua.pt (Moodle).
 - Subjected to weekly updates.

Flexible office hours

- Email (to discuss any topic or schedule a meeting).
- Discord: Invite <https://discord.gg/bPPpKy5>
 - ➔ **Change your nick to your real name** (First and Last names).
 - ➔ **Ask SRC student role.**
 - ➔ Only after you will have access the course contents.



Program

- Corporate network architecture (resilience and redundancy).
- Network vulnerabilities (known and unknown), attack vectors and attack phases. Network management good practices and introduction to security architecture
 - ◆ Networks and services isolation.
 - ◆ Cybersecurity KPI.
- Virtualization (device and network).
- Access Layer control (802.1X+RADIUS/TACACS).
- Firewalls, Load Balancers and Orchestrators. Secure zones. Network deployment and integration.
- DoS and DDoS (Attacks and Defenses).
- IDS and IPS.
- Privacy and anonymity.
- Certificate Authority (CA) characteristics and deployment.
- Secure communication (SSL/TLS).
- Secure communication (SSH and IPsec). VPN (site-to-site and user).
- Network monitoring (SNMP, Netflow, rsyslog,...). SIEM.



Planning (tentative)

| Semana | Teórica | | Prática | Terça | Sexta |
|--------|--|--|--|---------------|------------------|
| 07/Mar | T1: Program and Rules. Corporate Network Topics. | | P1: Corporate Network Fundamentals. | T1+P1 | T1+P1 |
| 14/Mar | T2: Introduction to Network Security. | | P1: Corporate Network Fundamentals. | T2+P1 | T2+P1 |
| 21/Mar | T3: Network Access Control. | | P2: Layer2 Access Control (802.1X & RADIUS). | T3+P2 | T3+P2 |
| 28/Mar | T4: Network Flow Control. | | P3: Introduction to Firewall Deployment. | T4+P3 | T4+P3 |
| 04/Apr | | | P3: Introduction to Firewall Deployment. | P3 | P3 |
| 11/Apr | | | P4: High-Availability Firewalls Scenarios. | Sexta-Feira | P4 (terça-feira) |
| 18/Apr | | | P4: High-Availability Firewalls Scenarios. | P4 | P4 |
| 25/Apr | Feriado/Sem.Académica | | Sem.Académica | Sem.Académica | Sem.Académica |
| 02/May | T5: Secure IP Connections. | | P5: Overlay IP and IPsec Networks. | P4 | T5+P5 |
| 09/May | | | P5: Overlay IP and IPsec Networks. | T5+P5 | P5 |
| 16/May | T6: Remote Access. | | P6: Network Remote Access (OpenVPN). | P5 | T6+P6 |
| 23/May | | | P6: Network Remote Access (OpenVPN). | T6+P6 | P6 |
| 30/May | T7: Intrusion Detection and Prevention | | P7: Intrusion Detection (Suricata). | P6 | T7+P7 |
| 06/Jun | | | P7: Intrusion Detection (Suricata). | T7+P7 | Feriado |
| 13/Jun | T8: Network Monitoring. SIEM. | | P8: Network Monitoring. | T8+P8 | T8+P8 |
| 20/Jun | | | P8: Network Monitoring. | P8 | |



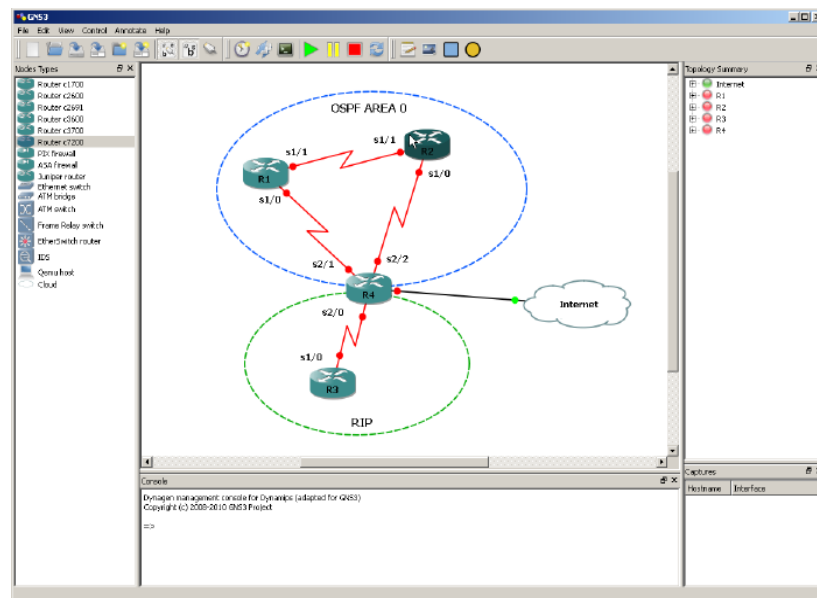
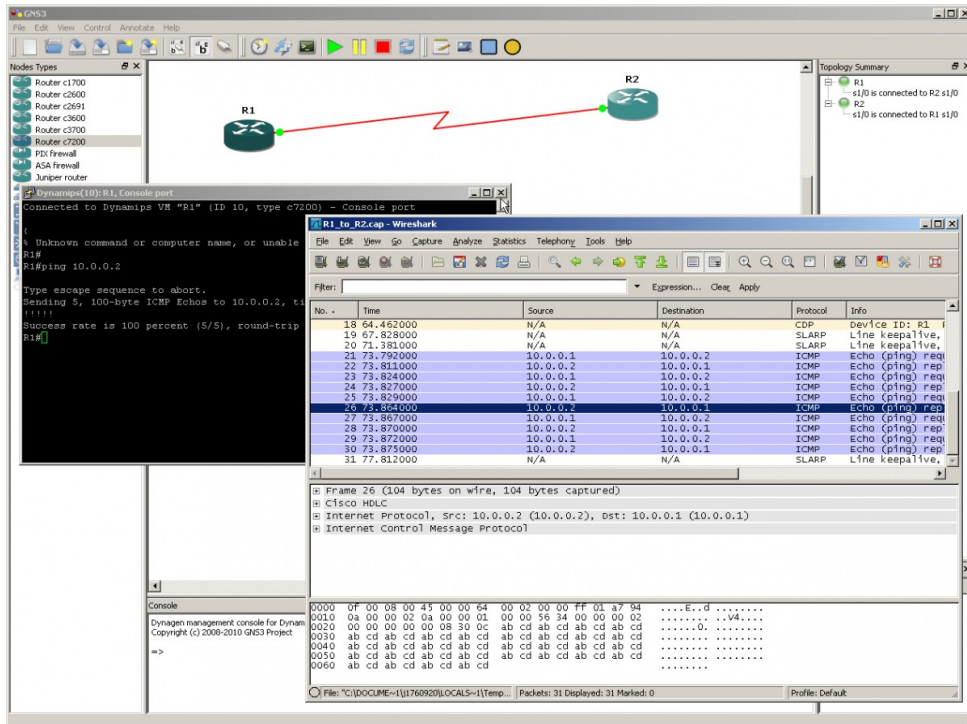
Evaluation

- Final Grade = 100% * Theoretical-Practice Written Exam
 - Final Exam and/or Extra/*Recurso* Exam
 - ➔ Practice and theoretical topics will be evaluated.
 - In the extra evaluation period (*recurso*) you can improve the grade of the regular exam. The best grade is considered.



GNS3

- Network Simulator + Device Emulator
 - ◆ Emulates Cisco devices(Routers)
 - ➔ Uses IOS/Firmware real with Dynamips
 - ◆ Emulates Servers and Firewalls with QEMU or VirtualBox.



Bibliography

- Ciampa, M. (2017). CompTIA Security+ Guide to Network Security Fundamentals - Standalone Book, 6th Edition. Cengage Learning, ISBN 1337288780
- Stallings, W. (2016). Cryptography and Network Security: Principles and Practice (7th Edition). Pearson. ISBN 978-0134444284
- Designing Cisco Network Service Architectures (ARCH), John Tiso, Cisco Press, ISBN-13: 978-1587142888, 3rd Edition, 2011.
- Yusuf Bhajji, Network Security Technologies and Solutions (CCIE Professional Development), Cisco Press, 1st edition, 2008.
- Network Security Through Data Analysis: From Data to Action, Michael Collins, O'Reilly Media; 2nd edition, ISBN-13: 978-1491962848, 2017.
- Crafting the InfoSec Playbook: Security Monitoring and Incident Response Master Plan, Jeff Bollinger, Brandon Enright, Matthew Valites, O'Reilly Media; 1st edition, ISBN-13: 978-1491949405, 2015
- A Practical Approach to Corporate Networks Engineering, António Nogueira, Paulo Salvador, River Publishers, ISBN-13: 978-8792982094, 2013.
- Computer Networks: A Systems Approach, Larry Peterson, Bruce Davie, Morgan Kaufmann, ISBN-13: 978-0123850591, 5th Edition, 2011.
- Jeff Doyle, Jennifer Carroll, Routing TCP/IP, Volume 1 (CCIE Professional Development), Cisco Press, 2nd, edition, 2005.
- Jeff Doyle, Jennifer Carroll, Routing TCP/IP, Volume 2 (CCIE Professional Development), Cisco Press, 2001.

