/Rooted

Red Team Operations (One day edition)

LISBOA

May 24, 2024

TRAINING DOSSIER

/Rooted

Lisboa 2024

Presentations presented by international speakers and technical experts.

Presentation

- **Mission**: we want to share knowledge, attract different cultures, expose local talent and make a difference.
- **Vision**: be responsible by doing something different, sharing culture and building a knowledge network. Be an honest, reliable, beneficial event and establish alliances and collaborations with partners, clients and competitors.
- **Our winning culture and our values live**: collaboration, diversity, talent everywhere, passion, quality and focus on clients (every person who attends our conferences).

Teacher: Eduardo Arriols

- CEO and Offensive Director at SilentForce, a start-up specialized in Adversarial Simulation and product development for the protection and management of the attack surface on the Internet.
- 13 years of experience in offensive security, and more than 8 years developing and coordinating Red Team exercises on large national and international organizations.
- Graduate and postgraduate professor in Cybersecurity for various universities.
- Author of the book "CISO: The Company's Red Team", from the 0xWord publishing house.
- Speaker at national and international conferences such as Defcon, RootedCON, Navaja Negra, STIC Conference (CCN-Cert) or 8.8 Security Conference (Chile and Bolivia).
- Computer Engineer from the UAM and master in Cybersecurity from the UOC.

Goals

The goal of this Bootcamp is to provide attendees with the capabilities to develop intrusion exercises and real attack simulations, understanding the process, phases and actions, as well as the techniques, tools and guidelines.

During the training, students will work on the main aspects to develop an intrusion, from the recognition of assets on the perimeter and search for access vectors, to internal actions such as lateral movement between systems, compromise of infrastructure or deployment of persistence, among others. Due to time limitations, techniques and actions for intrusion on internal infrastructure will be prioritized.

The bootcamp has a clear objective of showing in a practical way a useful methodology and techniques for developing targeted attacks, which is why it will not delve into techniques that go beyond this. Students will be provided with a laboratory both locally and in the Cloud on which to simulate all the techniques learned.

Who is it addressed to?

The training is not intended to serve as an introduction to ethical hacking, since the objective is to delve into advanced techniques that allow the development of real intrusions. Therefore, the bootcamp is focused especially on professionals in the Cybersecurity sector, and especially those related to security auditing and pentesting.

The training is also open, in any case, to all those who already have auditing knowledge that will be presented later, such as: students, developers, system and/or network administrators, Security Forces and Corps, as well as anyone who is interested in learning and deepening the development of Red Team exercises.

Knowledge requirements

Basic knowledge of:

- ✔ Administration and management of Windows or Linux systems.
- ✔ Basic programming in languages such as Bash scripting and Python.
- ✔ Functioning and operations of Microsoft environments with Active Directory.
- ✔ Use of ethical hacking tools such as Metasploit, Nmap, Sqlmap,…
- ✔ Process of intrusion and exploitation of vulnerabilities in systems and networks.
- ✔ Exploitation of web vulnerabilities such as SQL Injection, XSS, RCE or File Upload.

For maximum use of the training, theoretical material on the development of the exercises and basic aspects that the student must read will be provided before the start.

Technical requirements

For the training to function correctly, it will be necessary for students to have computers with administrator access to be able to add, delete software or change any of its configuration.

The machines must have the following minimum characteristics:

- ✔ Administrator access to personal equipment that will be used in the laboratory.
- ✔ Wired and wireless connection capability.
- ✔ Able to run three virtual machines simultaneously using VMware Workstation/Player or VirtualBox (machines will be provided in .ova).
- ✔ 120 GB of free disk space.
- ✔ At least 12GB of RAM.

Agenda

1. Introduction and basic concepts
2. Infrastructure deployment
3. Attack surface recognition
4. Vectors of access
5. Obtaining credentials and password cracking
6. Lateral movement and pivoting techniques
7. Domain attack techniques
8. Persistence deployment

The training will focus and delve deeper into those techniques that are novel or that are currently widely used in the development of intrusion scenarios. Attendees will be provided access to private SilentForce tools for automating actions during the intrusion process.

Details (i)

1. Introduction and basic concepts: All the necessary knowledge about the details of the methodology and phases of the intrusion, Threat and Breach model, potential vectors depending on the organization, techniques for measuring and analyzing the detection and response capabilities of the Blue Team, as well as aspects to take into account. account regarding OPSEC in Red Team exercises.

2. Infrastructure deployment: Details, guidelines and methodology for building enumeration, intrusion, persistence and anonymity infrastructure in the Cloud. The development of an anonymity platform for the concealment of actions, deployment of C&C systems for the reception of tunneled communications and persistence, as well as techniques such as Domain Fronting or IP Laundry will be further explored.

Details (ii)

3. Attack surface recognition: Set of techniques to map all the assets on which intrusion tests will be carried out to achieve an access vector, placing special emphasis on the detection of uncontrolled assets (Shadow IT) and asset prioritization.

4. Vectors of access: Main vectors of perimeter access and tunneling through tools such as reGeorg / NeoRegeorg, password spraying attacks, 2FA evasion or spoofing of Internet services.

5. Obtaining credentials and password cracking: Set of techniques to obtain credentials during the intrusion process, such as obtaining keys through local files, DPAPI, keys, hashes and tickets in memory or spoofing of services both locally and on the network. Additionally, the different techniques (dictionaries, use of rules, masks, combinations and hybrid attacks) for clear password recovery will be analyzed.

Details (iii)

6. Lateral movement and pivoting techniques: Set of access techniques to move between computers, networks and internal domains by accessing systems, with the use of permitted protocols such as SSH, SMB, WMI, WinRM or DCOM. The different possible techniques will be analyzed depending on the level of credentials obtained (pass-the-hash, overpass-the-hash, pass-the-ticket, ...). Additionally, commitment and lateral movement techniques in MSSQL will be analyzed.

7. Domain attack techniques: Main techniques to achieve control over the Microsoft infrastructure through the use of attacks such as Kerberoast, ASREPRoast, Unconstrained/Contraned Delegations, Alternate Service Name, Linux Cache Credentials, DACLs or trust relationships among others.

8. Persistence deployment: Técnicas para el despliegue de persistencia sobre la organización en todos los niveles (sistemas internos, Directorio Activo, DMZ, Cloud y técnicas alternativas). Se profundizará tanto en las técnicas para mantener persistencia, como las vías de comunicación o uso de dichas persistencias.

Costs

- The final price of this RootedLAB is €180

- You can register and make payment at: https://reg.rootedcon.com

IMPORTANT:

A minimum of **TEN (10)** attendees is required for the course to take place.

FAQ

- Dónde se celebra la formación?
  - A diferencia del Congreso RootedCON, las formaciones se celebran en el Hotel Eurostarts i-Hotel
  - Aquí puedes encontrar el mapa de la zona: Google Maps
- Qué diferencia hay entre BootCamp y RootedLab?
  - Diferenciamos los training por horas de formación. Un RootedLab tiene 8 horas de formación, mientras que un BootCamp tiene unas 24h.
- Qué horario tiene la formación?
  - La formación comienza a las 9 de la mañana, pero procura estar un poco antes para poder acreditarte y tener tu portátil preparado. El primer día recomendamos estar a las 8 :)
  - Las formaciones suelen acabar entre las 19h y 20h.
- Como puedo registrarme?
  - Para el registro, ve directamente al RootedManager: https://reg.rootedcon.com. Ahí, una vez registrado podrás seleccionar la formación y pagar directamente. Una vez se imparta la formación podrás solicitar la factura siguiendo los pasos indicados.
- Puedo pagar con transferencia bancaria?
  - Si, desde el propio RootedManager podrás gestionar el pago mediante transferencia bancaria.
- El training incluye comida?
  - Los training no incluyen comida. Pero hay varias opciones en la zona, y el profesor os dará más información.

/Rooted

Contact:

info@rootedcon.com