NETITUDE

AN LRQA COMPANY

Red Team Training

Advanced Threat Actor Simulation (ATAS)

Contents

Course Audience: Those already operating as Red Teamers

Course Length: Four Days

Location: Remote or Onsite

01 Introduction

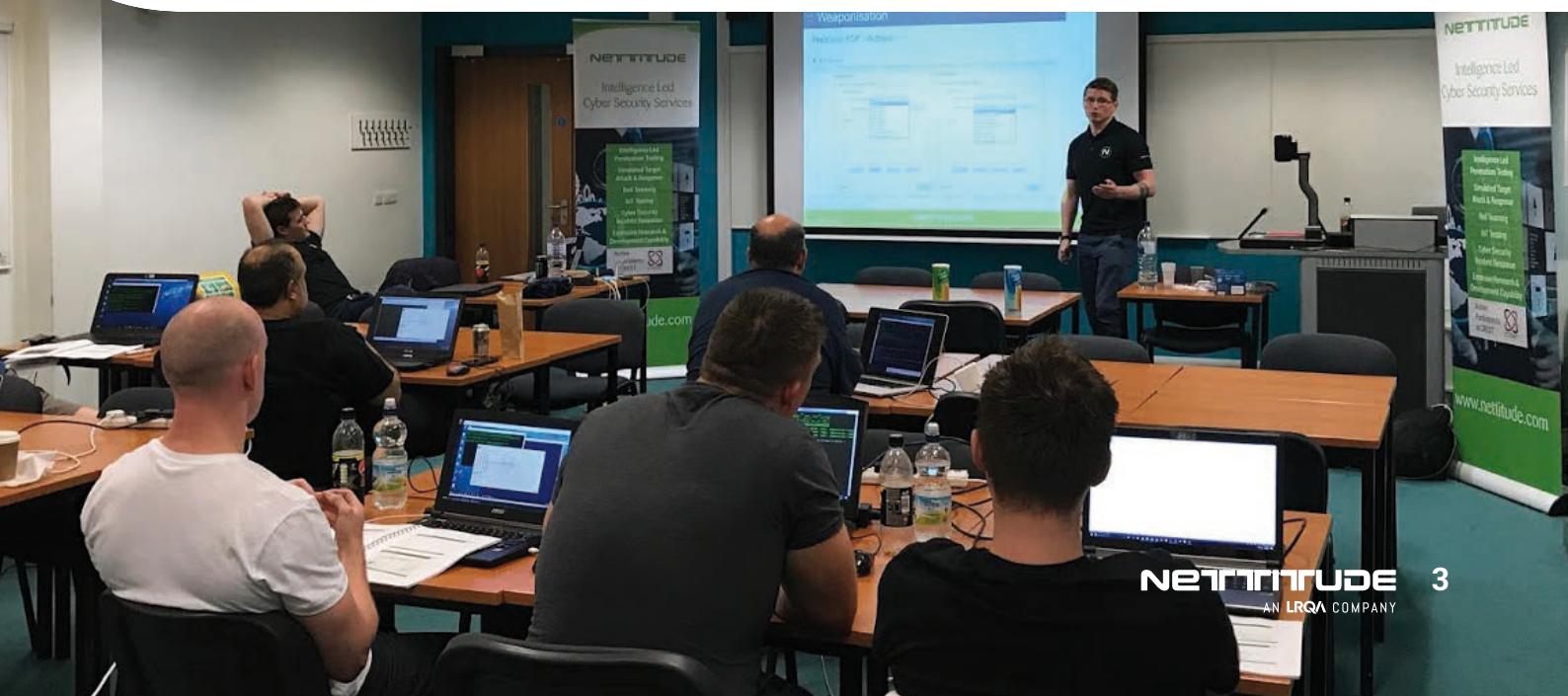
The Red Team Training -Advanced Threat Actor Simulation course aims to train an already inquisitive mind on how to operate and simulate real-world threat actors. The course is fast paced and highly intensive, teaching delegates an in-depth methodology and approach while operating as a professional Red Teamer. We not only show delegates how to perform advanced tactics, techniques and procedures (TTP's) but further cover how to run a successful end-to-end engagement with a focus on operational security and risk.

What is included?

The tactics and techniques taught in this course are constantly updated and adapted to keep up-to-date with the latest techniques used by known threat actors in the wild. The latest TTPs being used by real-world threat actors will be demonstrated on a practical level. This includes stealthily bypassing defensive security controls (Common EDR's and next gen AV), which are typically operating within modern enterprise environments and the pitfalls and lessons learned through many engagements and built-up experience across our Red Team. The instructors will impart knowledge from the field including wins, losses, improvements, optimisations and most importantly operational security.

The course includes both a theory element as well as hands on practical exercises, where the techniques learned can be practiced in a training lab environment specifically designed to replicate a typical corporate network. While the course focuses heavily on the latest offensive techniques used by a Red Team, it also covers common defensive techniques that are deployed by the blue team, such as host-based event logging and monitoring, strict egress filtering, application whitelisting and various other endpoint protections, such as EDR and next generation AV.

The course is four days long, broken down into three days of teaching, including four structured sessions a day mixed with multiple labs and demo's after each session. The following breakdown outlines an overview of the course with some highlights detailed per-session. The final day concludes the training and allows you to bring all your accumulated knowledge to the test and simulate this in a real-world assault course.



02 The Syllabus

DAY 1:

Session 1: Introduction / C2 Proxy and Supporting Infrastructure Setup

- Cyber Kill Chain, Scoping & Pre-Engagement, Legal & Ethics, Reconnaissance & OSINT, Threat Intelligence
- C2 architecture, Rewrite rules, controlling traffic and user behaviour, Red Team monitoring

Session 2: Domain Fronting and Proxy Reputation

- Purchasing collateral, Staying Anonymous, Fronting and Domain Reputation
- Certificates, Phishing, Email Security, Information Leakage and Burners

Session 3: C2 Communications / Implant Configurations

- C2 communication, C2 safety and Operational security
- Inner Workings of an Implant, Security Bypasses and Defensive Considerations (AMSI, ETW, Hooking etc)

Session 4: C2 Frameworks & Introduction to PoshC2

- Overview of many C2 frameworks
- Introduction to PoshC2

DAY 2:

Session 1: Weaponisation

- Weaponisation handlers, Macro embedded office document / Excel4.0 SLK, OLE (Office 2013 / Office 2016+)
- Windows Script Hosting (JS&HTA), ClickOnce / Java applets and Document and application signing

Session 2: Download Cradles

- Downloaders, One Liners and Code snippets

Session 3: Execution

- Bypassing whitelisting, Custom C++/C# droppers and AMSI/ETW bypass techniques

Session 4: Mac OS X Execution & Delivery

- Phishing, social engineering, USB, network devices, physical
- Delivery evasion (HTML smuggling), Delivery tracking and live experiences

DAY 3:

Session 1: Situational Awareness & Persistence

- Understanding your Environment, Finding hidden defensive products
- Laying persistence, advanced persistence, custom droppers

Session 2: Privilege Escalation / Active Directory Attacks

- Host Based Attacks, Elevating Privileges, Network Attacks
- Active Directory Attack (Kerb / Deleg etc), ACL Abuse common vulnerabilities

Session 3: Active Directory Trusts / Cloud Tenancy and Lateral Movement

- Understanding Trusts, Attacking Trusts and Hybrid Cloud Environment
- Common Lateral Movement Techniques, Stealth and Advanced Methods

Session 4: Database Intrusion / Memory Abuse

- Attacking Databases, Common weaknesses and Interacting through C2
- Stealing Data from Memory and other commonly found memory artefacts

DAY 4:

- Assault Course

The training lab environment is built with defensive security controls and countermeasures deployed, which will require the candidates to use their newly acquired skills to bypass them.

The objective of the assault course is to use your newly acquired skills to run a Red Team assessment with an objective of penetrating the Blorebank network defenses via phishing, then abusing many typical weaknesses (such as those highlighted throughout the course) with the ultimate objective of gaining access to a critical non-domain joined and segregated database server to retrieve credit card information.

Key Takeaways

- Perform a simulated phishing attack against a typical corporate environment with standard defenses, such as EDR (Microsoft Defender and Kaspersky), mail filtering and AppLocker restrictions (use the knowledge you have gained through the course to obtain a foothold).
- Perform situational awareness and lay persistence to secure your initial foothold. Users are simulated and may reboot their workstations from time to time to ensure they have the latest updates.
- Perform reconnaissance against a multi-domain environment and attempt to enumerate Active Directory and find any vulnerabilities that may or may not exist within the environment, keeping OpSec in mind.
- Attempt privilege escalation on-host and against the environment using your C2 framework of choice and aim to perform multi-layered network pivoting to access multiple targets in a highly monitored network.
- Enumerate the target objective and attempt to compromise the critical system in scope for the Red Team. This will include multiple levels of privilege escalation and lateral movement in order to gain access to the objective system.

How is the training conducted?

The training is conducted either remotely or onsite utilising cloud-based infrastructure to support the deployment of a complex and real-life lab. The course comprises a fast paced and comprehensive syllabus delivered by multiple instructors and supported by many labs that will build on each phase of a Red Team, from preparation to execution.

Each delegate will be presented with a copy of the training materials, lab guides and scripts. Should the training be remote the training will be conducted over Microsoft Teams while utilising Slack for comms, questions and chatting before during and after the training is finished.

Prerequisites

Remote pre-requisites differ for an onsite delivery as the labs and assault course can be brought with the team for onsite delivery.

Remote:

- Stable Internet Access
- Outbound SSH and RDP Access

Onsite:

Delegate laptops should have the ability to run two Virtual Machines, preferably on VMWare with permission to bridge the network interface to the Internet. These VMs will be provided prior to the course via a download link that we will supply.

All student must have administrative rights over the laptop in order to install any software that may be required and have webcams and audio dial in via MS Teams.

Laptop Hardware requirements:

- 8 GB RAM minimum
- 100 GB of available HDD space
- Internet connection with over 5Mb download speed

NETTITUDE

AN LRQA COMPANY

UK Head Office
Jephson Court, Tancred Close, Leamington Spa, CV31 3RZ

Americas
50 Broad Street, Suite 403, New York, NY 10004

Asia Pacific
1 Fusionopolis Place, #09-01, Singapore, 138522

Europe
Leof. Siggrou 348 Kallithea, Athens, 176 74 +30 210 300 4935

Follow Us

solutions@nettitude.com
www.nettitude.com