The Syllabus

Day 2

Situational Awareness
+ Operational security
+ Environmental checks

Persistence
+ User land persistence
+ System level persistence
+ Miscellaneous persistence - Outlook Rules, domain based persistence, etc.
+ Creating custom binaries

Acting on Objectives
+ Introduction to objective based testing
+ Reconnaissance
+ Exploiting user permissions
+ Elevating permissions
+ Workstation assessment
+ Domain and network assessment
+ Attack and enumerating Active Directory
+ Abusing domain trusts
+ Bypassing 2FA
+ Understanding UAC
+ Lateral movement
+ Tactical withdrawal
+ Keeping a small footprint

Reporting & Logging
+ What to log
+ How to log it
+ Why logging is important
+ Tips for team collaboration

Day 3

Assault Course - Objective Based Red Team Assessment
+ Perform simulated phishing
+ Persistence
+ Multi-domain environment
+ Multi-layered network pivoting
+ Gold build vulnerabilities
+ Active Directory weaknesses

Wrap Up
+ End-to- end assault course run through
+ Course wrap up
+ War stories
+ Questions and answers

NETTITUDE
A member of the Lloyd's Register group

UK Head Office
Jephson Court, Tancred Close,
Leamington Spa, CV31 3RZ
0345 52 000 85 solutions@nettitude.com

www.nettitude.com

ADVANCED THREAT ACTOR SIMULATION

(RED TEAM TRAINING)

DELIVERED BY NETTITUDE'S RED TEAM

NETTITUDE
A member of the Lloyd's Register group

The Syllabus

What is this course?

This course aims to train an already inquisitive mind on how to operate and simulate real-world threat actors, at various levels of sophistication. Candidates of the course will learn an in-depth methodology and approach, while operating at the standards required for a professional Red Teamer.

The tactics and techniques taught in this course are constantly updated; Nettitude's Red Team works side by side with Nettitude's Threat Intelligence Team to ensure Red Team operations are delivered with the utmost realism; "as real as it gets" by advanced threat actors nowadays.

The purpose of a Red Team engagement is primarily to assess an organizations ability to detect and respond to a real-world breach.

The latest tactics, techniques and procedures (TTPs) being used by real-world threat actors will be demonstrated on a practical level. This includes stealthily bypassing defensive security controls, which are typically operating within modern enterprise environments.

The course includes both a theory element as well as substantial hands on practical exercises, where the techniques learned can be practiced in a training lab environment specifically designed to replicate a typical corporate network. 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.

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 white-listing and various other endpoint protection controls.

Who is it for?

The course can be used to train both Red and Blue Teamers in the offensive techniques adopted by various threat actors and build a better understanding on how these techniques are used to bypass defensive measures and breach organizations security around the globe.

Nettitude deliver this course at various cyber security conferences, as well as in-house for various organizations in the private and government sector. For in-house training, additional pre-training sessions can be delivered (in the form of webcasts) in order to bridge any knowledge gaps that may exist with the student base. This will ensure that maximum value and knowledge is attained by the students during the delivery of the main course.

Nettitude's Advanced Threat Actor Simulation course best suits individuals with a general knowledge of offensive security and Microsoft Windows infrastructure within corporate environments. A basic knowledge of offensive and defensive tools would be beneficial but not mandatory.

> "Great course content delivered by extremely knowledgeable red teamers. The practical lab was a great environment where newly learned techniques can be applied."
>
> Sasha Raljic -Principal Security Consultant

Prerequisites

All candidates must bring their own laptop, capable of both Wi-Fi and Ethernet connections in order to connect to the training lab network. The laptop should have the ability to run two Virtual Machines, preferably on VMWare.

The student must have administrative rights over the laptop in order to install any software that may be required.

Laptop Hardware requirements:
- 8 GB RAM minimum
- Ethernet Adapter
- 50 GB of available HDD space

> "Offers excellent value for penetration testing consultants wanting to increase their knowledge and skill. It taught real-world effective simulated attack strategies, tools and techniques which I now use to conduct simulated attacks against our clients."
>
> Kai Stimpson - Principal Security Consultant

Day 1

Introduction
+ Cyber Kill Chain
+ MITRE Attack Framework
+ Tactics, Techniques and Procedures (TTPs)

Scoping & Pre-Engagement
+ Purpose of a red team
+ Understanding the scope and objectives
+ Attribution
+ Legal

Reconnaissance & OSINT
+ Threat Intelligence
+ Automation
+ Tips and tricks
+ Active vs passive reconnaissance

C2 Infrastructure
+ C2 architecture
+ C2 proxy servers and rewrite rules
+ Controlling traffic and user behavior
+ Security controls
+ Proxy labs
+ Purchasing collateral and staying Anonymous
+ Domain reputation
+ Domain fronting
+ HTTP versus HTTPS and building certificates
+ Phishing setup
+ Email security (SPF, DKIM, DMARC)
+ Information leakage
+ Burner phones
+ C2 communication
+ C2 safety
+ Operational security

Weaponisation
+ Introduction
+ Weaponisation handlers
+ Macro embedded office document (Auto_Run)
+ Macro embedded office document (Buttons)
+ OLE objects
+ HTA/MSHTA.exe
+ ClickOnce
+ Java applet
+ Document and application signing
+ PDF

Execution Methods
+ Bypassing whitelisting - living off the land
+ Certutil, MSbuild, Msiexec, Wmic, WScript, CScript, InstallUtil, etc.

Delivery
+ Perimeter controls
+ Phishing, social engineering, USB, network devices, physical
+ Tracking delivery
+ Live experiences and bypass techniques

NETTITUDE
A member of the Lloyd's Register group