Training -

Defend Against Modern Targeted Attacks (DAMTA)

A tailored training for your security team by Outflank in cooperation with Cqure

Content

Defend Against Modern Targeted Attacks (DAMTA) **3**

Who should attend? **3**

Key learning objectives **4**

Lab environment **4**

Agenda and key topics **5**

Day 1 5

Day 2 5

Day 3 5

Location, price, dates **6**

Location 6

Price and dates 6

Language 6

Participant references **6**

Your trainers **7**

Pieter Ceelen 7

Stan Hegt 7

Marc Smeets 7

Contact **8**

Defend Against Modern Targeted Attacks (DAMTA)

Get ready for a 3-day knowledge intensive training that teaches you how to defend against the modern offensive techniques that red teams and targeted attackers use.

We're not going to bother you with the default tools of penetration testers. And you should forget about the out-of-the-box rules in your SIEM that trigger endless false positives. But we are going to feed you with the latest knowledge, tools and techniques of modern targeted attacks that help you become a better defender.

Based on many years of Red Teaming and hands-on SOC/incident response experience, we share with the you the essential concepts and techniques to better understand and defend against modern attacks. In this training no Nmap, Nessus, exploits and Metasploit. Instead we focus on Pyramid of Pain, Course of Action Matrix, Cobalt Strike, Golden Tickets, Kerberoasting, Domain Fronting and other topics that really matter. We have also prepared a massive online lab that represents true corporate IT environments, in which you will spend about half of your time diving into hands-on assignments on offensive and defensive actions.

Who should attend?

The training is optimally suited for:

- Defenders (i.e. Blue Teamers, SOC-specialists) who want to strengthen their skillset, learn directly from Red Teaming specialists, and get hands on experience with offensive and defensive tools in order to better defend against modern offensive methodologies, tools, and techniques.
- Security professionals interested in expanding their knowledge of modern attack techniques, Red Teaming and defend against it.
- Forensic professionals who want to better understand the entire flow of an attacker and offensive tactics.
- Penetration testers and ethical hackers wanting to step into Red Teaming, or wanting to provide better recommendations to their clients on defensive measures.
- Technical auditors and security officers wanting to increase their hands-on experience and technical skills.

We do require participants to have a technical IT background and a basic level of security knowledge. So you probably do not want to subscribe to this training if you are afraid of the command line, or never ever heard of Golden Ticket and Command and Control traffic. But the training is setup in such a way that it can welcome both novices and veterans.

Key learning objectives

The training is focussed on several key elements:

- Learn how modern attacks work and how you can better defend against such attacks.
- Understanding and being able to use key theoretical concepts, e.g. Kill Chain, Course of Action Matrix and Pyramid of Pain.
- Latest and most effective hacking and detecting techniques.
- Hands-on learning combined with theory.
- Hands-on experience with various offensive tools combined with detection and investigation tools in a massive lab environment that resembles a true corporate network.
- Lab manual that helps the participants and makes it easy to follow.
- Knowledge packed training material for you to take home and revisit.

Lab environment

During the training, the participants have access to a personal lab environment that acts as a playground area. Having a lab is a key point of the training as we strongly believe it increases the ability to learn. The lab isn't just a vulnerable web app with a linux and windows server. No, this personal(!) environment is comparable to common enterprise networks. You can expect a large number of Windows and Linux servers, Active Directory domain with subdomains, Windows desktops, multiple services, user accounts and service accounts. Furthermore, common insecurities are configured on purpose.
Just as important is the central monitoring environments using open source and commercial tool, i.e. Redline, sysmon, WEF and ELK stack. You will use this to track and interpret attacks as they happen.
Every student also has a private offensive lab for the execution of several offensive actions. This process is supported by the using the mature and easy to use Cobalt Strike tooling.

Agenda and key topics

Day 1

- Introduction
- Core theoretical concepts, e.g. SIEM, SOC, Pyramid of Pain, TTPs, MITRE ATT&CK, Intruder's dilemma, attacker's playground, assume compromise, Kill Chain, lateral movement.
- Lab 1 - Setup: setup access to your defensive lab, setup access to your offensive infrastructure, recon your target and develop an attack scenario.
- Theory of attack vectors, e.g. watering hole, phishing, the Microsoft Office attack vectors.
- Lab 2- Attacker lab: Build, edit and review weaponized documents.
- Theory of the attacker's network infrastructure, e.g. C2, redirectors, low and slow principle, beacon traffic, Domain fronting, Cobalt Strike.
- Lab 3 – Attacker lab: Setup your attacking infrastructure and deploy malware.

Day 2

- Theory of malware prevention and investigation, e.g. anti-virus, anti-spam evasion, C2 basics, drive-by downloads, HTA, Java and Jscript, application whitelisting, End-Point Detection & Response.
- Lab 4 – Defender lab: Forensics, investigation of a compromised workstation and malicious using Endpoint detection and response tooling, malware sandboxes, YARA.
- Theory of Privilege escalation & Lateral movement.
- Windows and Active Directory internals from the attacker's and defender's point of view. Key topics like Wdigest, NETNTLM vs NTLM hashing, Sharphound, WMI, Psexec, Remote PowerShell, Golden and Silver Tickets, SPNs, etc.
- Lab 5 - Attacker lab: Leverage initial access on workstation further into the lab. Use Cobalt Strike, PowerView, Mimikatz and several lesser known tools.

Day 3

- Theory of Detection & Incident Response, e.g. log collection using Windows Event Forwarding, SIEM, shim caches, netflow, structure and templates for incident reporting, containment methods.
- Lab 6 – Defender lab: Detection, hunting and investigation. Using the lab's SIEM environment to unravel complex attacks.
- Theory Mitigation & Improvement: ASD top 35, important papers and defensive concepts from Microsoft, LAPS, AppLocker and non-Windows solutions.
- Lab 7 - Final technical deep dive – surprise topic.

Location, price, dates

Location

BCN Utrecht CS
Catharijnesingel 48
3511 GC Utrecht

BCN Utrecht CS is located at a walking distance of train station Utrecht CS. If you want to travel with car, we recommend usage of Parking garage Hoog Catharijne (P1 en P2), which is located across of BCN Utrecht CS. This parking garage provides paid parking only. Note: Navigate to 'Spoorstraat' (any number) instead of Catharijnesingel, when you use your navigation system.

Price and dates

The training will be covering three full days and is scheduled April 16, 17 and 18 of this year, between 09:00 and 17:00 hours. During these days you will be served drinks and lunch. At the end of the training you will receive a certificate of participation. All this together will cost you € 1950,- excluding tax per person.

Necessities

The course material is written in English. The training will be given in Dutch unless request by (one or more of) the attendees to the trainers to talk in English. If one more attendees make this request, the training will be full in English.

You need to bring your own laptop to the training which is capable of running an RDP. This is possible on either Windows, MacOS or Linux.

Participant references

A selection of reactions from previous participants:

- “Excellent training, excellent and complementary skill sets brought to the table by the
- trainers!”
- “Leuk team, goede presentaties, presentatoren beheersen duidelijk de materie.”
- “Goede verbeterplannen voor eigen organisatie, zowel korte als langere termijn”
- “Veel bruikbare informatie over incident lifecycle management bij security incidenten!”
- “Very refreshing to learn from an offensive point of view. Thanks so much!”
- “Simply superb!! An excellent exercise to see things from the perspective of an attacker and use the methods and tools. Also, to attack not a single server but to gain entrance to a complex network, this made it much more real and rewarding!”

Your trainers

There will be 3 trainers: Pieter Ceelen, Stan Hegt and Marc Smeets. Working at Outflank, they focus on Red Teaming operations and advanced penetration tests. The training is created based on their years of experience with offensive operations and advising their. They each bring their own unique expertise to this training.

Pieter Ceelen

Pieter is an experienced technical security analyst with over 8 years of experience. He has experience in technical security assessments/advice, penetration testing, incident response and threat management. In recent years he specifically focused on prevention, detection and response on targeted attacks/APTs and other cyber crime. Besides his technical knowledge he is an advisor with broader knowledge in the area of information security, auditing and IT processes. More info at https://outflank.nl/pieter

Stan Hegt

Stan is a digital security specialist and professional hacker. He has more than a decade of experience in this area and holds a Master of Science degree in Information Security Technology. Starting as a computer hacker at the age of 10, Stan has acquired deep technology knowledge that he combines with strong professional skills. His areas of expertise included Red teaming, attack simulation and complex penetration tests, malware analysis, threat management and security awareness training. More info at https://outflank.nl/stan

Marc Smeets

Marc Smeets is a senior ethical hacker and red teamer. With over 10+ year experience in IT security and 3 years in IT operations he knows how to ‘make’ and ‘break’. His specific areas of expertise are in the underlying layers: infrastructures, network protocol, core routing protocols, Active Directory, operating systems, etc. He combines his in-depth technical knowledge with the ability to see IT security in greater context of organizations. More information at https://outflank.nl/marc

Contact

We hope to have informed you sufficiently, but if any questions arise, if you want further information or if you want to plan an in-house training for your company, we are happy to help. You can reach Dennis Nuijens of Cqure for questions and further informations. His contact details are +31 (0) 6 588 12 977 or dennis.nuijens@cqure.nl