Training -
Defend Against Modern Targeted Attacks (DAMTA)

Een op maat gemaakte training voor je securityteam door Outflank in samenwerking met Cqure

Content

Defend Against Modern Targeted Attacks (DAMTA)

Maak je op voor een driedaagse kennisintensieve training die je leert hoe je je kunt verdedigen tegen de moderne aanvalstechnieken van red teams en gerichte aanvallers.

We zullen je niet lastigvallen met de standaard tools van pentesters. En we besteden geen aandacht aan de kant-en-klare regels in je SIEM die eindeloze false positives opleveren. We gaan je juist wel voeden met de nieuwste kennis en technieken van gerichte aanvallers, en geven je hulpmiddelen om je een betere verdediger te maken.

Gebaseerd op de vele jaren ervaring in het uitvoeren van Red Teaming operaties, en hands-on SOC- en incident response-ervaring, delen we de essentiële concepten en technieken met je om moderne aanvallen te begrijpen en ertegen te verdedigen. Hier geen Nmap, Nessus, exploits en Metasploit. Maar juist wel Pyramid of Pain, Course of Action Matrix, Cobalt Strike, Golden Tickets, Kerberoasting, Domain Fronting en andere zaken die er echt toe doen. We hebben ook een enorm online lab voorbereid dat een representatieve bedrijfsomgevingen is. Hierin besteed je grofweg de helft van de tijd aan het duiken in praktische opdrachten voor aanvallende en verdedigende acties.

Wie zou aanwezig moeten zijn?

De training is optimaal geschikt voor:

- Verdedigers (i.e. Blue Teamers, SOC-specialisten) die hun vaardigheden willen versterken, direct van ervaren Red Teamers willen leren en ervaring willen opdoen met aanvallende en verdedigende hulpmiddelen om zich beter te verdedigen tegen moderne offensieve methodieken, tools en technieken.Beveiligingsprofessionals die geïnteresseerd zijn in het uitbreiden van hun kennis van moderne aanvalstechnieken, Red Teaming en de verdediging hiertegen.
- Forensische professionals die de hele lijn van een aanvaller en aanvallende tactieken beter willen begrijpen.
- Penetratietesters en ethische hackers die de stap willen maken naar Red Teaming, of die hun klanten betere aanbevelingen willen kunnen geven over defensieve maatregelen.
- Technische auditors en security officers die hun praktische ervaring en technische vaardigheden willen vergroten.

We verwachten van deelnemers dat ze over een technische IT-achtergrond en een basisniveau van beveiligingskennis beschikken. Je wilt je waarschijnlijk niet aanmelden voor deze training als je bang bent van de command line of als je nog nooit hebt gehoord van Golden Ticket en Command en Control-verkeer. Maar de training is zodanig opgezet dat zowel beginners als gevorderden welkom zijn.

Belangrijkste trainingsdoelen

De training bevat de volgende belangrijkste doelen:

- Leer hoe moderne aanvallen werken en hoe je je hier beter tegen kunt verdedigen.
- Begrijpen en kunnen toepassen van belangrijke theoretische concepten zoals Kill Chain, Course of Action Matrix en Pyramid of Pain.
- Nieuwste en meest effectieve hack- en detectietechnieken.
- Praktisch leren gecombineerd met theoretische onderwerpen.
- Direct hands-on ervaring opdoen met verschillende aanvallende tools in combinatie met detectie- en onderzoekstools in een lab omgeving die groot en representatief is voor echte bedrijfsnetwerken.
- Lab-handleiding die de deelnemers helpt en die gemakkelijk te volgen is.
- Trainingsmateriaal vol met kennis om mee naar huis te nemen en opnieuw door te nemen.

Lab omgeving

Tijdens de training hebben de deelnemers toegang tot een lab omgeving die fungeert als speel- en leerterrein. Het hebben van een representatieve lab omgeving is een kernpunt voor deze training omdat wij geloven dat zo het leereffect wordt vergroot. Hier niet een kwetsbare webapplicatie, 2 Linux servers en een Windows werkstation. Nee deze persoonlijke(!) lab omgeving is bewust representatief met echte bedrijfsnetwerken. Verwacht dus een groot aantal Windows- en Linux-servers, Active Directory-domein met sub domeinen, Windows-desktops, meerdere services, gebruikersaccounts en service-accounts. Ook zijn er enkele vaak voorkomende zwakheden geconfigureerd.

Net zo belangrijk is de centrale monitoringomgevingen met open source en commerciële tools, o.a. Redline, sysmon, WEF en ELK-stack. Hier worden aanvallen opgespoord en geïnterpreteerd. Iedere student heeft ook de beschikking over een aanvallerslab, voor het uitvoeren van enkele offensieve acties. Dit aanvalsproces wordt vergemakkelijkt door het gebruik van de volwassen en gemakkelijk te gebruiken Cobalt Strike tooling.

Agenda en belangrijkste onderwerpen

Dag 1

- Introductie
- Theoretische kernbegrippen over aanvallen en verdedigen, 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: opzetten toegang naar offensieve en defensieve labs. Recon van je doelwit, en maken van een aanvalsplan.
- Theorie van aanvalsvectoren, e.g. watering hole, phishing, aanvalsmethoden met Microsoft Office.
- Lab 2: maken, editen en reviewen van malafide Office-documenten.
- Theorie infrastructuuropzet en -technieken van de moderne aanvaller, e.g. C2, redirectors, low and slow principle, beacon traffic, Domain Fronting, Cobalt Strike als platform.
- Lab 3: setup van je aanvallers infrastructuur, en deploy je malware.

Dag 2

- Theorie en effectiviteit van 'Malware prevention and investigation', e.g. antivirus, anti-spam evasion, C2 basics, drive-by downloads, HTA, Java and Jscript, application whitelisting, End-Point Detection & Response.
- Lab 4 - Forensics: onderzoek van een gecompromitteerd werkstation d.m.v. Endpoint Detection and Response tooling, malware sandboxes en Yara.
- Theorie van 'Privilege Escalation and Lateral Movement'.
- Windows en Active Directory vanuit het perspectief van de aanvaller en de verdediger. Aandacht voor kernonderwerpen zoals Wdigest, NETNTLM vs. NTLM hashing, Sharphound, WMI, Psexec, Remote PowerShell, Golden and Silver Tickets, SPNs, Kerberos, LLMNR, etc.
- Lab 5 - Offensief: gebruik de eerder verkregen toegang tot je target om verdere toegang in het netwerk te krijgen. Gebruik de zojuist geleerde technieken, en een aantal bekende tools zoals Cobalt Strike, PowerView en Mimikatz en een aantal minder bekende tools gaandeweg.

Dag 3

- Theorie van 'Detection & Incident Response', e.g. centrale logging d.m.v. Windows Event Forwarding, Sysmon, shim caches, NetFlow, belang en details van templates bij incident response, methodes voor containment.
- Lab 6: Detection, Hunting and Investigation. Gebruik de SIEM van het lab om een complexe aanval te analyseren.
- Theorie 'Mitigation & Improvment': ASD Top 35, voorname papers en defensieve concepten van Microsoft (LAPS, AppLocker, Privileged Access Management) en anderen.

- Lab 7: verrassings-lab

Locatie, prijs en data

Locatie

BCN Utrecht CS
Catharijnesingel 48
3511 GC Utrecht

BCN Utrecht CS ligt op loopafstand van het treinstation. Bij reizen met de auto raden wij het gebruik van Parkeergarage Hoog Catharijne (P1 en P2) aan, welke zich bevindt tegenover BCN Utrecht CS. Deze parkeergarage is betaald parkeren. NB: Toets bij het gebruik van navigatieapparatuur de naam 'Spoorstraat' (willekeurig) in, in plaats van Catharijnesingel.

Prijs en data

De training duurt drie volledige dagen en staat gepland op 16, 17 en 18 april 2019, tussen 09:00 uur en 17:00 uur. Gedurende deze dagen wordt drinken en lunch geserveerd. Aan het eind van de eerste dag kan er, indien gewenst, deelgenomen worden aan een diner. Aan het einde van de training ontvang je een certificaat van deelname. Dit alles samen kost je € 1950, - exclusief BTW per persoon.

Benodigdheden

Het cursusmateriaal is in het Engels. Tijdens de training spreken de trainers in principe Nederlands, maar op verzoek van de deelnemers kan tijdens de cursus ook in het Engels gesproken worden.

Je dient een eigen laptop mee te brengen naar de training waarop een RDP gedraaid kan worden. Dit is mogelijk op Windows, MacOS of Linux.

Deelnemersreferenties

Een selectie van reacties van vorige deelnemers:

- “Excellent training, excellent and complementary skill sets brought to the table by the trainers!”
- “Very refreshing to learn from an offensive point of view. Thanks so much!”
- “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!”

- “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!”

Jouw trainers

De training wordt gegeven door 3 trainers: Pieter Ceelen, Stan Hegt en Marc Smeets. Allen werkzaam bij Outflank, richten ze zich op Red Teaming-operaties en geavanceerde penetratietests. De training is gemaakt op basis van hun jarenlange ervaring met offensieve operaties en het adviseren van hun klanten. Ze hebben elk hun eigen expertise in deze training.

Pieter Ceelen

Pieter is een ervaren technisch beveiligingsanalist met meer dan 8 jaar ervaring. Hij heeft ervaring met technische beveiligingsbeoordelingen/ -advies, penetratietesten, respons op incidenten en dreigingsbeheer. De laatste jaren richtte hij zich specifiek op preventie, detectie en reactie op gerichte aanvallen/ APT's en andere cybercriminaliteit. Naast zijn technische kennis is hij een adviseur met een bredere kennis op het gebied van informatiebeveiliging, auditing en IT-processen. Meer informatie op https://outflank.nl/pieter

Stan Hegt

Stan is een digitale beveiligingsspecialist en een professionele hacker. Hij heeft meer dan een decennium aan ervaring op dit gebied en heeft een Master of Science-graad in Information Security Technology. Begonnen als een computer hacker op 10-jarige leeftijd, heeft Stan diepe technologische kennis verworven die hij combineert met sterke professionele vaardigheden. Zijn expertise ligt bij red teaming, complexe penetratietesten, malware-analyse, dreigingsbeheer en security awareness training. Meer informatie op https://outflank.nl/stan

Marc Smeets

Marc is een ervaren professionele hacker en red teamer. Met 10+ jaar ervaring in IT security en 3 jaar als systeem- en netwerkengineer weet hij hoe in te breken en ook hoe te verdedigen. Zijn specifieke expertise ligt op de onderliggende technische lagen: infrastructuren, netwerk protocollen, core routing protocollen, Active Directory en operating systems. Hij combineert sterke inhoudelijke technische kennis met de mogelijkheid om beveiliging te zien in de grotere context van organisaties. Meer informatie op https://outflank.nl/marc

Contact

We hopen je voldoende te hebben geïnformeerd, maar als er vragen zijn, als je meer informatie wilt of als je een interne training voor jouw bedrijf wilt plannen, helpen we je graag. Je kunt Dennis Nuijens van Cqure bereiken voor vragen en verdere informatie. Zijn contactgegevens zijn +31 (0) 6 588 12 977 of dennis.nuijens@cqure.nl