Vulnerability Scanner

Acht verschillende scanners voor netwerk en platform op basis van Guardian360

IT-infrastructuur is tegenwoordig essentieel voor de bedrijfsvoering en de bescherming hiervan is van het grootste belang. 100% beveiliging bestaat echter niet, maar we kunnen je wel helpen om risico's te verkleinen, mogelijke bedreigingen op tijd te signaleren en snel te handelen als het toch fout gaat. Dat doen we op basis van de Vulnerability Scanner van onze partner Guardian360. Hiermee realiseren wij ongeëvenaard inzicht in de beveiliging en bescherming van alle applicaties en IT-infrastructuur.

Acht verschillende scanners

De Vulnerability Scanner bestaat uit acht verschillende netwerk- en platformscanners, die constant in en om jouw netwerk zoeken naar zwakke plekken of kwetsbaarheden in de netwerk- of webapplicatie-beveiliging. Mocht er ondanks alle vormen van beveiliging toch iemand het netwerk binnendringen dan wordt er een stil alarm geslagen. Het 24×7 opererende Security Operations Center (SOC) identificeert een eventuele indringer of hacker en kan direct vervolgstappen nemen om de inbraak te neutraliseren en/of de schade te beperken. De Vulnerability Scanner bestaat uit de volgende scanners:

Global Scanner

Deze scanner bekijkt jouw applicaties, infrastructuur en netwerk vanaf de buitenkant van jouw netwerk. Dat gebeurt door het netwerk te benaderen met technieken die een 'echte hacker' ook gebruikt om IT-omgevingen te infiltreren. Daardoor krijg je een goed beeld van de volgende bedreigingen:

- Is het netwerk bereikbaar van buitenaf?
- Is het netwerk kwetsbaar voor reflection/DDoS-aanvallen?
- Maken de servers of website maakt deel uit van een botnet?
- Zijn de servers kwetsbaar voor SSL/TLS-aanvallen of onjuist geconfigureerd?
- Zijn er veel voorkomende configuratiefouten gemaakt?

Poort Scanner

Deze scanner bekijkt vanaf de buitenkant van het netwerk of platform welke poorten open staan. Openstaande poorten bieden een aanvaller de mogelijkheid om verder in de infrastructuur door te dringen of om webapplicaties te kunnen aanvallen. Niet alleen wordt er gecontroleerd of de poort open staat, maar ook op wat er zich achter deze poort bevindt. Er wordt gescand op meer dan tachtig veel gebruikte en misbruikte poorten. Wij adviseren om deze scan dagelijks uit te voeren.

Amplification Scanner

De Amplification Scanner controleert servers op correcte configuratie en stelt vast of zij wel of niet vatbaar zijn voor diverse bedreigingen zoals bijvoorbeeld SSL- en TLS misconfiguratie en controleert op zogenaamde reflection attack mogelijkheden in het netwerk.

Netwerk Vulnerability Scanner

Deze scanner controleert op de aanwezigheid van onder andere oude applicaties die niet goed gepatcht zijn, maar ook op netwerk-toepassingen, complete besturingssystemen en webapplicaties. We kunnen zo meer dan 85.000 actuele bedreigingen herkennen en hierop alarmeren.

claranet

Meer informatie:
claranet.nl - twitter.com/claranet_nl
Voor het maken van een afspraak:
040 - 239 3300 - verkoop@claranet.nl

GUARDIAN 360°

Lokale Scanner
De Lokale Scanner is een fysieke of virtuele 'Probe' die op veilige en verantwoorde wijze in jouw interne netwerk wordt geplaatst, uiteraard in overleg met de IT-afdeling. Op deze Probe zijn Guardian360 scanners geïnstalleerd die het netwerk van binnenuit afspeuren op bedreigingen. Met behulp van een versleutelde verbinding worden resultaten en bevindingen naar een centrale database gestuurd, waar je de resultaten naast de externe scans kunt leggen.

Credential Scanner
Deze scanner speurt het netwerk af naar onversleutelde, niet-complexe of te korte wachtwoorden en probeert toegang te krijgen met behulp van de Guardian360 Cruncher. Dit is een password-kraker die inmiddels meer dan vier miljard wachtwoorden kent en in staat is om miljoenen wachtwoorden per seconde te testen.

Blacklist Scanner
De Blacklist Scanner zorgt ervoor dat je snel kunt ingrijpen als jouw domeinen of IP-adressen op een blacklist staan en scant onder andere op de volgende punten:

- Zijn jouw websites en/of IP-adressen bekend op pastebin?
- Staan jouw IP-adressen op een blacklist?
- Wordt er spam verstuurd vanaf jouw netwerk?
- Wordt er binnen het netwerk aan bitcoin-mining gedaan?
- Wordt jouw website gebruikt voor phishing?
- Zijn er virussen, malware of andere malicious activiteiten binnen het netwerk actief?
- Maakt jouw netwerk verbinding met "command and control" servers?
- Draait er een open Proxyserver in het netwerk waardoor je kwetsbaarder bent voor een botnet?
- Wordt jouw netwerk gebruikt om hack- of DDoS-aanvallen uit te voeren?
- Is er een TOR Exit node bekend binnen het netwerk?

Defense Scanner
De Defense Scanner zoekt in plaats van directe kwetsbaarheden naar het ontbreken van defense-in-dept maatregelen. Dit soort maatregelen helpen jouw (web)applicaties en netwerk preventief te beschermen tegen mogelijke toekomstige aanvallen of bij het preventief verhelpen en voorkomen van nog onbekende kwetsbaarheden. Wij controleren o.a. op de volgende soorten defense-in-depth maatregelen:

- Maken jouw webapplicaties gebruik van extra beschermingslagen zoals "headers"?
- Zijn er standaard paden of instellingen actief op jouw webapplicaties die informatie kunnen lekken aan kwaadwillenden?
- Zijn jouw applicaties/netwerk voldoende voorzien van configuratie hardening?
- Hebben de domeinen spam/phishing/spoofing preventie?
- Zijn de DNS-servers van jouw website domein(en) beschermd tegen Man-in-the-Middle aanvallen?
- Lekt jouw netwerk data die misbruikt kan worden om credentials van werknemers of andere gevoelige data te achterhalen?
- Kan een kwaadwillende eenvoudig data uit jouw interne netwerk halen en op welke manier(en)?
- Werken aanwezige Intrusion Prevention System maatregelen naar behoren?

Garanties en voordelen:

100% Nederlandse organisatie
Onafhankelijke rapportage
Bescherming van (persoons)gegevens en intellectueel eigendom
360 graden blik op het totale IT-landschap
Vermindert de kans op datalekken
Ondersteunt compliancy binnen de organisaties
Continue scanning en awareness

Binnenkort verwacht: Adversary Simulation

Deze test gebruikt een door Guardian360 ontwikkelde intelligentie om jouw netwerk actief geautomatiseerd aan te vallen. Hierbij zal gebruik gemaakt worden van zowel kwetsbaarheden als misconfiguraties. Het systeem is zo ontwikkeld dat dit geen impact heeft op de werking van het platform en maakt gebruik van bekende door hackers gebruikte methodes. Een kwaadwillende wil zo min mogelijk opvallen en zal daardoor alleen methodes gebruiken waar hij zelf bekend mee is. De aanvallen die deze test onder andere zal gebruiken, zijn:

- Inloggen op applicaties of systemen met credentials die zijn gevonden met de Credential Scanner om zo toegang te krijgen tot achterliggende systemen en/of om nog meer wachtwoorden te achterhalen;
- Toegang verkrijgen tot systemen door het misbruiken van ontbrekende beschermingsmaatregelen;
- Toegang verkrijgen tot systemen door misconfiguraties die zijn gevonden door de Defense Scanner;
- Indien toegang tot een systeem is verkregen, poging tot escaleren van privileges op systeem om mogelijk nog meer credentials te achterhalen met bijvoorbeeld domein privileges;
- "Lateral movent"; pogingen tot bewegen door het netwerk met gevonden credentials en kwetsbaarheden op systemen.

Overzichtelijk dashboard

Naast het volledig automatisch proberen te achterhalen van mogelijke kwetsbaarheden, geeft Guardian360 ook de mogelijkheid om geldige netwerk credentials van bijvoorbeeld een Active Directory domein op te geven. Op deze manier kan een situatie nagebootst worden om te zien waar een kwaadwillende bij kan, mocht hij in het bezit komen van een geldige gebruikersnaam/wachtwoordcombinatie (bijvoorbeeld via malware via een phishing e-mail). Bovenstaande simulatie geeft een uniek inzicht in jouw netwerk en geeft je de mogelijkheid om jouw bescherming voor het netwerk te verbeteren. Het dashboard zal grafisch inzichtelijk maken welke kwetsbaarheid en/of misconfiguratie op welk systeem is misbruikt, op welke manier en tot welk niveau er is doorgedrongen binnen het netwerk.

Over Guardian360

Guardian360 is een Nederlandse securityspecialist, gevestigd in Rotterdam. Het Guardian360-team bestaat uit specialisten die jarenlange ervaring hebben binnen de informatiebeveiliging en webapplicatieontwikkeling. Naast de voor de hand liggende certificeringen bezitten een aantal van de medewerkers de gerenommeerde OSCP-certificering.

claranet

Meer informatie:
claranet.nl - twitter.com/claranet_nl
Voor het maken van een afspraak:
040 - 239 3300 - verkoop@claranet.nl

GUARDIAN 360°