Hoe te werken met

Honeypots

Whitepaper door SecurityHive

SECURITYHIVE

Inhoudsopgave

Inleiding

Iedereen kent het concept van de lokfiets wel. De politie stalt fietsen op plaatsen waar ze veel gestolen worden. Op de lokfietsen zit een 'track-en-trace'-volgsysteem. Wanneer een fietsendief de fiets steelt kan de politie de verdachte opsporen. In de ICT-wereld worden Honeypots gebruikt om hackers en virusmakers te lokken. Dit is een systeem wat met opzet kwetsbaar is gemaakt voor aanvallen van hackers. De Honeypot vormt een bron van informatie over nieuwe virussen, kwetsbaarheden en bedreigingen. Dit is interessant voor de makers van beveiligings- en anti-spamsoftware. In deze Whitepaper laten wij van SecurityHive je zien hoe je kunt werken met de Honeypot.

1. Waarom is een Honeypot belangrijk?

Honeypots detecteren de indringer onmiddellijk, waardoor IT-experts de aanval kunnen stoppen en de schade kunnen beperken. Hierdoor dragen Honeypots bij aan de algehele beveiligingsstructuur van een organisatie.

In het boek 'Secrets and Lies' van Bruce Schneier wordt beveiliging in drie categorieën verdeeld: preventie, detectie en reactie. Een Honeypot voegt voornamelijk waarde toe aan de categorie van detectie en reactie.

- **Detectie**

Voor veel organisaties is het moeilijk om aanvallen te detecteren. Systeembeheerders krijgen een overvloed aan meldingen en kunnen deze lang niet allemaal beantwoorden. Honeypots kunnen het detectieproces vereenvoudigen. Honeypots hebben namelijk geen productieactiviteit, dus alle meldingen vanuit een Honeypot zijn per definitie verdacht. Dit betekent dan hoogst waarschijnlijk een ongeautoriseerde scan of aanval. Op deze manier kunnen beveiligers gemakkelijk de meldingen oppakken.

- **Reactie**

Daarnaast zijn Honeypots ook van toegevoegde waarde aan de reactie. Omdat er op systemen binnen een organisatie veel productieactiviteit plaatsvindt, is het moeilijk om te bepalen wat er gebeurd is waardoor er een kwetsbaarheid is ontstaan. Omdat er zoveel gebruikers op hetzelfde netwerk kunnen werken is het moeilijk om bewijs te verzamelen in deze omgeving. Daarnaast is er ook een andere uitdaging waar veel organisaties voor staan. Na een incident kunnen systemen vaak niet offline worden ingenomen. Dit zorgt ervoor dat het incidentresponsteam geen juiste forensische analyse kan doen.

Honeypots voegen waarde toe door deze beide uitdagingen op te lossen. Zo wordt er een systeem geboden met minder datavervuiling en een vervangbaar systeem dat offline kan worden gehaald na een incident.

2. Hoe werkt een Honeypot?

Misschien had je er nog nooit van gehoord, maar de Honeypots bestaan al tientallen jaren. Het principe hierachter is simpel: ga niet op zoek naar hackers, maar bereid iets voor dat hun interesse zou wekken. Cybercriminelen voelen zich aangetrokken tot Honeypots. Dit komt omdat zij denken dat de Honeypot een legitiem doelwit is. De hackers denken dat deze gegevens het echt waard is om te hacken. Het kan dan bijvoorbeeld gaan om een financieel systeem of internet of things (IoT)-apparaten. Deze systemen verschijnen als onderdeel van een netwerk, maar zijn geïsoleerd en worden nauwlettend gevolgd. Er is geen reden voor legitieme gebruikers om toegang te krijgen tot de Honeypot. Iedere poging tot communicatie wordt als vijandig beschouwd.

Het bekijken en loggen van activiteiten in de Honeypot geeft inzicht in het niveau van de bedreigingen waarmee de netwerkstructuur wordt geconfronteerd. Er worden bewust virtuele achterdeurtjes opengelaten. Dit zijn poorten waarmee een systeem gegevens verstuurt en binnenhaalt vanuit de buitenwereld. Hackers die proberen binnen te dringen in waardevolle systemen stuiten op deze open achterdeurtjes in de Honeypot. Dit terwijl de cyberaanvallers worden afgeleid van de systemen met echte waarde.

3. Wat zijn de voordelen van een Honeypot?

• Honeypots doorbreken de keten van aanvallen en vertragen de hackers
Terwijl hackers zich door je netwerkomgeving heen verplaatsen gebeurt er veel. Ze voeren verkenningen uit, scannen je netwerk en zoeken naar een kwetsbaar apparaat. In dit stadium zullen de Honeypots de aanvallers laten struikelen en worden de hackers omgeleid naar een nutteloos systeem. Ook wordt de organisatie gewaarschuwd om de toegang van de aanvallers te beperken. Honeypots zorgen er dus voor dat er op tijd gereageerd kan worden voordat een aanvaller de kans krijgt om met succes toegang te krijgen tot de gegevens.

• Ze zijn eenvoudig om mee te werken
Moderne Honeypots zijn eenvoudig te downloaden en te installeren. Daarnaast geven ze ook nauwkeurige waarschuwingen over gevaarlijke configuraties en aanvallersgedrag. Hierdoor weet het beveiligingsteam precies wat er moet gebeuren. In tegenstelling tot inbraakdetectiesystemen hebben Honeypots geen nieuwe bedreigingsinformatie nodig om bruikbaar te kunnen zijn in een organisatie.

• Honeypots helpen bij het testen van incidentresponsprocessen
Honeypots zijn een goedkope manier om een bedrijf te helpen bij het vergroten van de beveiligingsvolwassenheid. Dit kunnen ze doen door te testen of het beveiligingsteam weet wat ze moeten doen als de Honeypot een onverwachte activiteit onthuld. Weet het team hoe de waarschuwing onderzocht kan worden en welke maatregelen passend zijn? Een Honeypot moet niet de volledige strategie voor het detecteren van bedreigingen zijn, maar kan wel een nuttig onderdeel zijn. Het is een van de weinige methoden die gebruikt kan worden om cyberaanvallen in de echte wereld te onderzoeken en om interne netwerklekken op te sporen.

4. Waar worden Honeypots voor gebruikt?

Het doel is niet om hackers in de val te lokken of op heterdaad te betrappen, maar om informatie over deze aanvallers vast te leggen. Beveiligingsteams zetten deze lokkers in als onderdeel van hun netwerkverdedigingsstrategie. Ook worden de Honeypots gebruikt om het gedrag van cyberaanvallers en de interactie met netwerken te onderzoeken. Het is als het ware een muizenval.

Er kan online bijvoorbeeld een e-mailadres worden achtergelaten waar spambots op stuiten. Of een IT-beveiliger van een bank kan een bestand maken met de persoonlijke creditcard gegevens van klanten. Allemaal lokkers die de interesse van internetcriminelen kunnen wekken. Honeypots zijn dus interessant om informatie te verzamelen over op welke manier systemen en data gesaboteerd kan worden.

5. Welke soorten Honeypots bestaan er?

Op basis van ontwerp zijn er twee typen Honeypots: productie en onderzoek.

1. De onderzoek Honeypots
De onderzoek Honeypots voeren een nauwkeurige analyse uit van de activiteit van hackers. Ze hebben het doel te ontdekken hoe een cyberaanval zich ontwikkelt, om zo te leren hoe het systeem beter beschermd kan worden. Analisten kunnen de gegevens uit de Honeypot ook gebruiken om ze op te sporen wanneer deze gegevens worden gestolen. Hiermee kunnen verbindingen tussen verschillende cybercriminelen bij een aanval geïdentificeerd worden.

2. De productie Honeypots
Productie Honeypots worden veelal ingezet binnen de productienetwerken van productieservers. De Honeypot fungeert hier als een lokaas om zo indringers weg te trekken van het productienetwerk. Een productie Honeypot is ontworpen om als een echt onderdeel binnen het netwerk te verschijnen. De Honeypot bevat interessante informatie om hackers aan te trekken en hun tijd vervolgens te bezetten. Deze aanpak geeft de IT-beheerders uiteindelijk genoeg tijd om het dreigingsniveau te beoordelen en de kwetsbaarheden in hun daadwerkelijke systeem te verminderen.

Onderzoek Honeypots

Productie Honeypots

5. Welke soorten Honeypots bestaan er?

De complexiteit van de onderzoeks- en productie Honeypots variëren.

1. Pure Honeypot
Dit is een volledig productiesysteem dat nagebootst wordt en op verschillende servers draait. Het bevat 'vertrouwelijke' data en gebruikersinformatie. Dit soort Honeypot is complex en moeilijk te onderhouden, maar de informatie die de systemen te bieden hebben zijn van onschatbare waarde.

2. Honeypot met hoge interactie
Deze Honeypot is vergelijkbaar met de pure Honeypot als het gaat om het uitvoeren van de vele services. Het verschil is wel dat deze niet zo complex is en niet zoveel gegevens bevat als de pure Honeypot. De Honeypots met hoge interactie zijn niet bedoeld om een volledig productiesysteem na te bootsen. In plaats daarvan draaien ze alle services die een productiesysteem zou uitvoeren. Dit type Honeypot kan ingezet worden door bedrijven die het gedrag en de technieken van de aanvallers willen onderzoeken.

3. Mid-interaction Honeypot
Dit soort Honeypot heeft aspecten van de applicatie laag, maar in tegenstelling tot de Honeypot met een hoge interactie heeft dit type geen eigen besturingssysteem. Ze werken om aanvallers af te schrikken en te verwarren, zodat de organisatie meer tijd heeft om uit te zoeken hoe ze op de juiste manier op deze cyberaanval kunnen reageren en kwetsbaarheden kunnen oplossen.

4. Honeypot met weinig interactie
Dit type Honeypot wordt het meeste gebruikt in een productieomgeving. De Honeypots met weinig interactie voeren een handvol services uit en geven een vroegtijdige waarschuwing bij een cyberaanval. Ze zijn eenvoudig te implementeren en te onderhouden. In de tabel hieronder is het verschil te zien tussen een Honeypot met een lage interactie, een hoge interactie en de Honeypot van SecurityHive. In de laatste worden de voordelen van beide soorten Honeypots gecombineerd.

	Lage interactie	Hoge interactie	SecurityHive Honeypot
Installatie	Makkelijk	Moeilijker	Makkelijk
Onderhoud	Makkelijk	Tijdsintensief	Automatisch
Opererend systeem	Nee	Ja	Ja
Data verzamelen	Gelimiteerd	Uitgebreid	Zeer uitgebreid
Interactie	Geëmuleerd	Volledige controle	Geëmuleerd

5. Welke soorten Honeypots bestaan er?

Daarnaast zijn er ook nog verschillende soorten Honeypot technologieën die gebruikt worden. Deze zijn onder meer:

Malware Honeypots
Deze Honeypots werken als replicatievectoren om malware te detecteren. Een voorbeeld daarvan is een Honeypot die vertoond wordt als een USB-opslagapparaat. Als er dan een aanval is die zich via USB verspreidt, dan zal de Honeypot de malware misleiden om het apparaat te infecteren.

Spam Honeypots
Bij dit soort Honeypots worden open mailrelays en open proxy's nageboot-st. Spammers testen de open mail relay door eerst zelf een e-mail te sturen. Als dit lukt, dan worden er grote hoeveelheden spam verstuurd. De spam Honeypot kan deze test detecteren en herkennen. Daarna volgt het systeem met succes de enorme hoeveelheid spam en blokkeert deze spam.

Database Honeypots
Sommige activiteiten kunnen vaak onopgemerkt blijven door firewalls. Een voorbeeld daarvan is een SQL-injectie. Dit is een kwetsbaarheid in de web beveiliging waardoor een aanvaller zich kan bemoeien met de vragen die een toepassing aan zijn database stelt. Een database-Honeypot kan onder-steuning bieden om een lokdatabases te maken voor de database-firewall.

Klanten Honeypots
De meeste Honeypots zijn servers die naar verbindingen luisteren. Honey-pots van klanten gaan actief opzoek naar kwaadaardige servers die klanten aanvallen en controleren op verdachte en onverwachte wijzigingen aan de Honeypot. Deze systemen hebben over het algemeen een strategie om het risico voor het onderzoeksteam van de klant te minimaliseren.

Honeynet
In plaats van een enkel systeem, is een honeynet een netwerk dat uit meer-dere Honeypots kan bestaan. Een honeynet is bedoeld om de methoden en motieven van een cyberaanvaller strategisch te volgen en tegelijkertijd al het inkomende en uitgaande verkeer kan controleren.

OVER SECURITYHIVE

"Iemand heeft een slechte bijlage geopend"
mag nooit de reden zijn waarom het hele bedrijf niet kan werken.

SecurityHive - opgericht in 2017 door Nederlandse techneuten - ontwikkelt oplossingen om cybersecurity maximaal eenvoudig te maken. Het is ons doel om bedrijven een veilige toekomst te bieden en zo ongestoord te groeien. Het resultaat van onze visie is dat cybersecurity toepasbaar en begrijpelijk is voor iedereen. Wereldwijd vertrouwen partners en organisaties op de technologie van SecurityHive. Samen met het beste netwerk aan partners, beschermen wij grote en kleine bedrijven in elke sector.

Kom in contact met SecurityHive-experts voor meer informatie.

Securityhive.nl | LinkedIn.com/SecurityHive

SECURITYHIVE