Best Practices Ansible Configuration Management

Onderzoeksvoorstel Bachelorproef

Pieter Van Wambeke[1]*

Samenvatting
Ik heb besloten om de best practices van Ansible Configuration Management te gaan onderzoeken met de nadruk op veiligheid. Dit onderzoek is nodig omdat de beveiliging van netwerken steeds belangrijker wordt in een wereld met almaar meer mensen die de zwakke punten in een netwerk willen uitbuiten. Ik ga de huidige best practices die bekend zijn testen op waarom ze er zijn en ik hoop tijdens mijn onderzoek nieuwe best practices tegen te komen. Ik verwacht dat ik door te testen begrijp waarom er bepaalde best practices zijn en hoop nieuwe best practices tegen te komen. Security zal altijd een belangrijke rol spelen, dus dit is een werk dat zeker zijn meerwaarde zal hebben voor de toekomst.

Sleutelwoorden
Systeem- en netwerkbeheer. Ansible — Security — Best practices

[1]Student Toegepaste Informatica, Valentyn Vaerwyckweg 1, 9000 Gent
*__Contact__: pieter.vanwambeke.u8838@student.hogent.be

Inhoudsopgave

1. Introductie

Ik ga de best practices van Ansible Configuration Management onderzoeken. Ik wil dit onderzoeken omdat dit een belangrijk punt is op vlak van beveiliging en omdat dit een veelgebruikte automatiseringstool is in de IT-wereld. Ik wil de huidige best practices toetsen en eventueel nieuwe best practices opstellen als ik deze vind tijdens mijn onderzoek. De onderzoeksvraag luidt: Wat zijn de best practices op vlak van security voor Ansible Configuration Management?

2. State-of-the-art

Er zijn al gelijkaardige onderzoeken uitgevoerd naar best practices rond Ansible. Zo is er de bachelorproef van Jurgen¨ Van Meerhaeghe (Meerhaeghe, 2015), maar die ging niet dieper in op security. Daarin wordt SELinux vermeld, maar daar blijft het dan ook bij. Vooral het boek Ansible for DevOps (Geer-ling, 2017) geeft al een goede inkijk in best practices wat betreft security. De auteur van dit boek raadt net als Jurgen¨ Van Meerhaeghe aan om SELinux te gebruiken, maar gaat dieper in op zaken als poorten en ongebruikte software. Zo zet je best enkel de benodigde poorten open en verwijder je best ongebruikte software. Als conclusie kan je stellen dat het vooral gaat om het verhinderen van ongeautoriseerde toegang tot je netwerk.

Je mag gerust gebruik maken van subsecties in dit onder-deel.

3. Methodologie

Ik ben van plan om de huidige best practices te toetsen in enkele testmachines. Hiervoor ga ik enkele CentOS machines opzetten aan de hand van Ansible. Ik ga nagaan op welke manieren ik kan inbreken wanneer er bepaalde best practices niet in acht genomen worden. Dit kunnen banale dingen zijn zoals een te simpel wachtwoord, maar ook het gebruik van een standaard telnetpoort.

4. Verwachte resultaten

Ik verwacht dat bij het niet naleven van de huidige best prac-tices op vlak van security ik in staat zal zijn om in te breken in de CentOS machines. Ik verwacht dus dat de huidige best practices nodig zijn om een door Ansible opgezet netwerk veilig te houden. Ik verwacht ook dat ik enkele nieuwe best practices op vlak van security zal tegenkomen tijdens het testen.

5. Verwachte conclusies

Ik verwacht als conclusie dat de huidige best practices moeten nageleefd worden omdat ik naar alle waarschijnlijkheid zal kunnen inbreken in een netwerk waarbij deze best practices niet zijn toegepast. Ik hoop dat ik ook een conclusie ga hebben waarin ik kan zeggen dat ik nieuwe best practices gevonden

heb en waarbij ik kan verklaren dat deze nodig zijn voor een netwerk nog veiliger te maken.

Referenties

Geerling, J. (2017). Ansible for DevOps (Leanpub, Red.). Leanpub.

Meerhaeghe, J. V. (2015). Best practices voor Test Driven Infrastructure met het Ansible Configuration Management-systeem (masterscriptie, Hogeschool Gent).