RansomWare Aanval

Bert Van Itterbeeck

Ap Hogeschool Antwerpen

Ethical Hacking

Contents

[Vereisten: 2](#_Toc123670459)

[Virtual Machine (target): 2](#_Toc123670460)

[Python: 2](#_Toc123670461)

[Ransomware.py: 2](#_Toc123670462)

[Decrypt.py 2](#_Toc123670463)

[Sshconnect.py 2](#_Toc123670464)

[Dictionary: 2](#_Toc123670465)

[Instructies voor target: 2](#_Toc123670466)

[Opzet: 2](#_Toc123670467)

[Stap 1, Schrijven van de RansomeWare. 3](#_Toc123670468)

[Stap 2, Schrijven van de decryptie. 3](#_Toc123670469)

[Stap3, SSH connective. 3](#_Toc123670470)

[Safety first: 3](#_Toc123670471)

[De aanval zelf: 3](#_Toc123670472)

[Beschrijving: 3](#_Toc123670473)

[Screenshots: 4](#_Toc123670474)

[Beginsituatie Target: 4](#_Toc123670475)

[Commando op aanvaller: 4](#_Toc123670476)

[Script uitgevoerd op aanvaller: 5](#_Toc123670477)

[Situatie van Target na script: 5](#_Toc123670478)

[Bij foutief wachtwoord in Decrypt.py 8](#_Toc123670479)

[Bij juist wachtwoord in Decrypt.py 8](#_Toc123670480)

[Wat hiertegen doen? 9](#_Toc123670481)

# Vereisten:

Voor deze aanval zijn er enkele dingen nodig:

## Virtual Machine (target):

1. SSH moet geactiveerd zijn op de target machine en op poort 22.
2. Root moet kunnen in loggen met passwoord via SSH.
3. Deze aanval is geschreven om gebruikt te worden tegen een Linux machine.
4. Python is aanwezig op de target.
5. Uit veiligheid overweging valt dit script alleen de subdirectory test\_dir aan. Deze moet op de target worden aangemaakt in de home directory.

## Python:

Up to date python installatie met volgende modules geïnstalleerd per file:

### Ransomware.py:

* Os
* Sys
* From cryptography import Fernet

### Decrypt.py

* Os
* Sys
* From cryptogrphy import Fernet
* Base64

### Sshconnect.py

* Paramiko
* Socket

## Dictionary:

Deze kan zo groot of zo klein zijn als je wilt. Maar als het passwoord van je Virtual Machine er niet bij staat kan de aanval nooit slagen.

## Instructies voor target:

Omdat je zelf het script uitvoert moet je op 1 of andere manier je eisen kunnen doorgeven aan de target. Ik gebruik hiervoor een tekstbestand dat ik meestuur naar de target machine.

# Opzet:

Voor deze aanval heb ik een Debian 11, virtual Machine aangemaakt. Hierop heb ik SSH geactiveerd en geconfigureerd dat root kan inloggen met SSH en passwoord. Dit heb ik gedaan via /etc/ssh/sshd\_config.

## Stap 1, Schrijven van de RansomeWare.

Voor deze file heb ik inspiratie gehaald bij networkChuck en zijn YouTube video: <https://www.youtube.com/watch?v=UtMMjXOlRQc&t=1248s> . Extra heb ik ervoor gezorgd dat ook de subdirectory’s mee geëncrypteerd worden. En duidelijke zwakte is dat de key wordt opgeslagen in een aparte file.

## Stap 2, Schrijven van de decryptie.

Ook hier heb ik mijn inspiratie gehaald van dezelfde video. Hier heb ik buiten de inclusie van de subdirectory’s ook encryptie van een passwoord aan toegevoegd. De gebruiker moet een passwoord ingeven en slechts als dit overeenkomt met het passwoord in de file worden de files gedecrypteerd.

Ik besef heel goed dat deze file heel lek is en dat een geoefende informaticus hier op 2 seconden de files zo kan terughalen. Maar het gaat hier om een proof of concept. Bijvoorbeeld deze file hoeft eigenlijk helemaal niet mee gestuurd te worden.

## Stap3, SSH connective.

De aanval gaat via SSH, het bijgevoegde script controleert eerst dat poort 22 op de target open staat. Is dit niet het geval eindigt het script daar. Als dit wel het geval is Gaat het script proberen binnen te breken bij de target doormiddel van een dictionary attack. Ik heb een heel korte lijst van passwoorden meegegeven, maar deze kan uiterraard uitgebreid worden naar zoalang men maar wil.

Het script gaat alle passwoorden af en geeft de melding dat een paswoord niet juist is. Bij een juis paswoord krijg je echter het woord “Bingo!” te zien.

Automatisch gaat het script nu verder. We hebben nu root acces. Het script kopieert 3 files naar de target, het Ransomware script uit stap 1, het decryptie script uit stap 2 en een Readme met instructies naar de gebruiker.

Vervolgens wordt er getracht het ransomware script uit te voeren. Bij succes geeft het Ransomware script terug of het gelukt is, bij falen geeft het SSH-script terug dat het niet heeft gewerkt.

## Safety first:

Dit script valt enkel bestanden aan in een speciaal gemaakte test directory om beschadiging aan de VM of belangrijke persoonlijke bestanden te voorkomen!

# De aanval zelf:

## Beschrijving:

1. Zorg ervoor dat alle nodige bestanden in dezelfde directory staan.
2. In de file sshconnect.py vervang je het IP-adres met het IP-adres van je target.
3. Run het script sshconnect.py

Als je VM correct is ingesteld en je passwoord voorkomt in je dictionary zal je aanval automatisch verlopen.

## Screenshots:

### Beginsituatie Target:

Graphical user interface, application

Description automatically generated

### Commando op aanvaller:

Text

Description automatically generated

### Script uitgevoerd op aanvaller:

Text

Description automatically generated

### Situatie van Target na script:

Graphical user interface, application, Word

Description automatically generated

Graphical user interface, application, Word

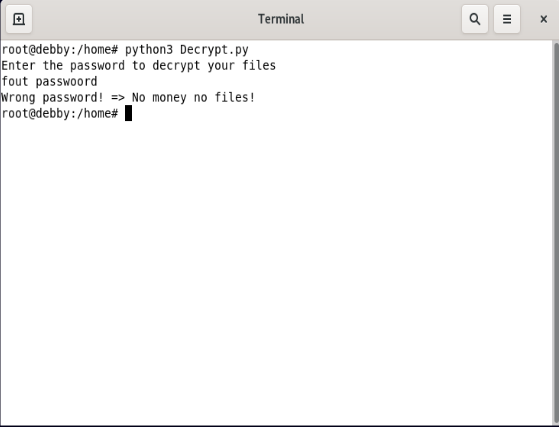
Description automatically generated

Graphical user interface, text, application, Word

Description automatically generated

(Enkel ter illustratie)

### Bij foutief wachtwoord in Decrypt.py



### Bij juist wachtwoord in Decrypt.py

Graphical user interface, text, application, email

Description automatically generated

# Wat hiertegen doen?

1. Geen Root acces toelaten op SSH, maakt niet uit hoe verleidelijk het is.
2. Gebruik maken van sleutels.
3. Gebruik maken van een sterk passwoord
4. Geen poorten laten openstaan.