NGINX

Déployer un reverse proxy Nginx et un certificat Let's Encrypt pour Gophish

24/09/2024 Killian VAN RUYMBEKE 0 commentaire Gophish, Nginx, PfSense, Phishing

I. Présentation

Dans ce tutoriel, nous allons explorer la mise en place d'un reverse proxy Nginx pour un serveur de phishing Gophish. Cette démarche s'inscrit dans la continuité de notre série de tutoriels sur Gophish, où nous avons précédemment établi les fondations nécessaires pour le déploiement d'une campagne de phishing à des fins de sensibilisation.

Pour rappel, dans le premier tutoriel, nous avons configuré un domaine spécifique nommé "**kvrcybertechno.fr**" associé à une adresse IP publique (203.153.73.6) fournie par **OVHcloud**. Derrière cette adresse IP se cache un hyperviseur bare metal. Sur cet hyperviseur, nous trouvons une machine virtuelle (VM) dédiée à Gophish avec l'adresse IP "**192.168.1.17**" et une seconde VM qui accueillera notre serveur Nginx, dotée de l'adresse IP "**192.168.1.20**".

La lecture de l'article précédent est recommandée avant de lire celui-ci :

- Création d'une campagne de phishing avec Gophish et Microsoft 365

La gestion des noms de domaine est assurée par un pfSense configuré avec l'adresse IP publique "**96.122.153.201**". Ce pfSense est crucial puisqu'il intègre une règle de **port forwarding**, redirigeant les requêtes entrantes des ports HTTP (80) et HTTPS (443) vers notre serveur Nginx nouvellement configuré.

Nginx est un serveur web open source conçu pour offrir robustesse et flexibilité, éléments essentiels pour la mise en œuvre de nos objectifs de sécurité via un reverse proxy. Ce tutoriel vous guidera à travers les étapes détaillées de configuration, vous permettant ainsi de sécuriser et d'optimiser vos campagnes de phishing de manière efficace et contrôlée.

Remarque : le reverse proxy pourrait être hébergé directement sur le firewall pfSense, grâce à l'ajout du paquet HAProxy. Si cela vous intéresse, consultez cet article :

- Mettre en place un reverse proxy HAProxy sur pfSense

II. Créer et enregistrer les sous-domaines

Le but de créer des **sous-domaines** est de remplacer l'utilisation d'adresses IP dans notre campagne de phishing pour **induire en erreur vos utilisateurs** (le nom de domaine étant plus trompeur que l'adresse IP), ainsi que pour **faciliter l'accès** à votre CMS administrateur Gophish.

Depuis votre hébergeur (l'enregistrement pour OVHcloud se fait via cette URL), vous allez créer un nouvel enregistrement DNS pour votre "**phish_server**". Utilisez un champ de pointage de type **« A »** et un nom de sous-domaine crédible pour piéger vos utilisateurs ; ici, ce sera **« microsoft.kvrcybertechno.fr »**. Dans la section **« Cible »**, indiquez l'adresse de l'interface WAN de votre pfSense si vous en utilisez un, ou l'adresse IP du serveur hébergeant votre DNS forwarder, qui est **« 96.122.153.201 »**.

Le résultat final doit être comme suit :

Vous devrez **créer** de façon similaire depuis votre domaine légitime, ici **« kvrcybertechno.com »**, un enregistrement, cette fois pour votre "**admin_server**", qui vous permet d'accéder à l'interface de Gophish. Mon enregistrement se nommera **« gophish-admin.kvrcybertechno.com »**.

III. Configurer Pfsense pour une propagation DNS

Si vous n'utilisez pas **pfSense** ou **OPNsense** comme "**DNS Forwarder**", appliquez la même procédure avec votre solution alternative.

Accédez successivement aux sections suivantes dans votre pfSense :

- **Services** > **DNS Forwarder**
- **Services** > **DNS Resolver**

La configuration doit être identique pour les deux.

Dans la section "**Host Overrides**", vous devez ajouter deux entrées. Voici l'exemple de configuration pour le "**phish_server**" :

- **Host :** microsoft
- **Domain :** kvrcybertechno.local
- **IP Address :** 192.168.1.20 (il faudra mettre l'adresse IP de votre Nginx)
- **Description :** gophish phish_server domain
- **Additional Names for this Hosts :** microsoft kvrcybertechno.fr

Et, voici ma configuration pour **l'admin_server** :

- **Host :** gophish-admin
- **Domain :** kvrcybertechno.local
- **IP Address :** 192.168.1.20 (il faudra mettre l'adresse IPde votre NGINX)
- **Description :** gophish admin_server domain
- **Additional Names for this Hosts :** gophish-admin kvrcybertechno.com

N'oubliez pas de faire de même pour votre **« DNS Resolver »**.

IV. Mise en place du reverse proxy Nginx

A. Installation Nginx sur Debian ou AlmaLinux

Vous allez maintenant installer **NGINX** après avoir mis à jour votre serveur, il sera utilisé comme **reverse proxy**.

```
# Debian
sudo apt -y update && sudo apt upgrade && sudo apt full-upgrade && sudo apt
autoclean && sudo apt clean
sudo apt install nginx -y
sudo systemctl start nginx
sudo systemctl enable nginx

# AlmaLinux
sudo dnf update -y && sudo dnf upgrade -y && sudo dnf autoremove -y && sudo dnf
```

```
sudo systemctl enable nginx
```

B. Création des fichiers de configuration Nginx

Maintenant que NGINX est installé, vous allez procéder à la création des fichiers de configuration pour vos deux reverse proxy. Commençons par le **phish_server** :

```
sudo nano /etc/nginx/conf.d/microsoft.conf
```

Vous pouvez copier la configuration initiale ci-dessous en modifiant les parties où **j'ai ajouté exprès des commentaires**. Voici la configuration pour le **phish_server** :

```
server {
    # remplacer par votre sous domaine
    server_name microsoft.kvrcybertechno.fr;
    keepalive_timeout 7200;
    proxy_connect_timeout 7200;
    proxy_send_timeout 7200;
    proxy_read_timeout 7200;
    send_timeout 3600;
    client_max_body_size 50m;

    location / {
        # remplacer par votre sous domaine, en laissant en http
        proxy_pass http://microsoft.kvrcybertechno.fr;
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header X-Forwarded-Proto $scheme;
        proxy_http_version 1.1;
        proxy_set_header Connection "upgrade";
    }

    location /.well-known/acme-challenge {
        root /var/www/letsencrypt;
    }

}
```

```
}
```

Maintenant, **créez** le fichier de configuration de **l'admin_server** :

```
  sudo nano /etc/nginx/conf.d/gophish.conf
```

Et, voici la configuration pour **l'admin_server** :

```
server {
    # remplacer par votre sous domaine
    server_name gophish-admin.kvrcybertechno.com;
    keepalive_timeout 7200;
    proxy_connect_timeout 7200;
    proxy_send_timeout 7200;
    proxy_read_timeout 7200;
    send_timeout 3600;
    client_max_body_size 50m;

    location / {
        # remplacer par votre sous domaine
        proxy_pass http://gophish-admin.kvrcybertechno.com;
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header X-Forwarded-Proto $scheme;
        proxy_http_version 1.1;
        proxy_set_header Connection "upgrade";
    }

    location /.well-known/acme-challenge {
        root /var/www/letsencrypt;
    }

}

upstream gophish-admin.kvrcybertechno.com {
    # remplacer par l'adresse ip de votre serveur Gophish sur le port 3333
    server 192.168.1.17:3333;
}
```

Vous allez pouvoir vérifier si vos fichiers sont bien configurés, et recharger NGINX :

C. Installer Certbot et générer les certificats

Vos fichiers de configuration NGINX étant créés, nous allons désormais pouvoir générer des **certificats Let's Encrypt** valides pour une durée de trois mois. Pour cela, nous allons utiliser l'outil Certbot. Tout d'abord, commencez par installer **Certbot** :

```
# Debian
sudo apt install certbot python3-certbot-nginx

# AlmaLinux
sudo yum install -y epel-release
sudo yum install -y certbot python3-certbot-nginx
```

Une fois Certbot installé, générez les certificats en utilisant la commande suivante :

```
  sudo certbot --nginx -d gophish-admin.kvrcybertechno.com -d
microsoft.kvrcybertechno.fr
```

Cette commande fera **plusieurs choses** :

- **Certbot va vérifier** si le domaine pointe bien vers le serveur actuel, en utilisant un challenge DNS ou HTTP.
- **Il générera les certificats SSL/TLS** via Let's Encrypt.
- **Il mettra à jour vos fichiers de configuration NGINX** pour intégrer ces nouveaux certificats.
- **Il testera automatiquement la configuration NGINX** et rechargera le service pour appliquer les modifications.

Les certificats étant générés et les fichiers de configuration ayant été mis à jour par Certbot, ils devraient maintenant ressembler à cela :

```
server {
    server_name gophish-admin.kvrcybertechno.com;
    keepalive_timeout 7200;
    proxy_connect_timeout 7200;
    proxy_send_timeout 7200;
    proxy_read_timeout 7200;
    send_timeout 3600;
    client_max_body_size 50m;

    location / {
        proxy_pass http://gophish-admin.kvrcybertechno.com;
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header X-Forwarded-Proto $scheme;
        proxy_http_version 1.1;
        proxy_set_header Connection "upgrade";
    }

    location /.well-known/acme-challenge {
        root /var/www/letsencrypt;
    }

    listen 443 ssl; # managed by Certbot
    ssl_certificate /etc/letsencrypt/live/gophish-
admin.kvrcybertechno.com/fullchain.pem; # managed by Certbot
    ssl_certificate_key /etc/letsencrypt/live/gophish-
admin.kvrcybertechno.com/privkey.pem; # managed by Certbot
    include /etc/letsencrypt/options-ssl-nginx.conf; # managed by Certbot
    ssl_dhparam /etc/letsencrypt/ssl-dhparams.pem; # managed by Certbot


}

upstream gophish-admin.kvrcybertechno.com {
    server 192.168.1.17:3333;
}

server {
    if ($host = gophish-admin.kvrcybertechno.com) {
        return 301 https://$host$request_uri;
    } # managed by Certbot

    server_name gophish-admin.kvrcybertechno.com;

    listen 80;
```

V. Modifier le fichier de configuration de Gophish

Maintenant que vous êtes censé avoir un reverse proxy fonctionnel, **rendez-vous sur votre serveur Gophish** et modifiez son fichier de configurations :

```
sudo nano /opt/gophish/config.json
```

Vous allez devoir modifier vos adresses IP pour **changer l'écoute** de toutes vos interfaces à **l'adresse IP de votre interface principale**. Ensuite, ajoutez une ligne pour **préciser chaque sous-domaine** :

```
{
        "admin_server": {
                "listen_url": "192.168.1.17:3333",
                "use_tls": false,
                "cert_path": "gophish_admin.crt",
                "key_path": "gophish_admin.key",
                "trusted_origins": ["gophish-admin.kvrcybertechno.com"]
        },
         "phish_server": {
         "listen_url": "192.168.1.17:80",
         "use_tls": false,
         "cert_path": "gophish_phish.crt",
        "key_path": "gophish_phish.key",
        "trusted_origins": ["microsoft.kvrcybertechno.fr"]
    },
    "db_name": "mysql",
    "db_path": "gophiser:MotdepasseFort!12345@(localhost:3306)/gophish?
charset=utf8&parseTime=True&loc=UTC",
    "migrations_prefix": "db/db_",
    "contact_address": "",
    "logging": {
        "filename": "",
        "level": ""
    }
}
```

Redémarrez le démon et relancez Gophish :

```
sudo systemctl daemon-reload
sudo systemctl restart gophish
```

VI. Première campagne Gophish avec un reverse proxy

Vous pouvez normalement accéder sans problème à votre **Gophish** depuis **le sous-domaine configuré**. Cependant, pour **tirer pleinement profit** de ce tutoriel, vous allez créer une **nouvelle campagne** en modifiant **l'adresse IP** habituellement utilisée par votre **sous-domaine piège**.

Puis, rendez-vous sur **l'URL piège** contenu dans **l'e-mail envoyé** par Gophish :

Si vous accédez, comme moi, à votre page de destination piège, c'est que votre configuration fonctionne parfaitement !

VII. Conclusion

En suivant ce tutoriel, vous avez appris à déployer et à configurer un **reverse proxy Nginx** pour un serveur de phishing Gophish. Dans le cadre de vos opérations de sensibilisation, cette configuration va rendre encore plus réaliste vos campagnes de phishing.

L'intégration d'un reverse proxy Nginx est une étape importante pour **masquer les détails internes** de votre réseau tout en fournissant un point d'accès sécurisé et contrôlé pour vos simulations. Cela contribue non seulement à **la crédibilité de vos campagnes,** mais renforce également la protection contre les accès indésirables.

Si vous rencontrez des difficultés lors de la mise en place de Nginx ou de Gophish, n'hésitez pas à poser vos questions ou à partager vos expériences en commentant cet article. Vous pouvez aussi vous connecter sur le Discord IT-Connect. Nous sommes là pour vous aider.

Ingénieur Cybersécurité M1 en alternance, j'ai une forte appétence pour tous les domaines technologiques. Dans un esprit d'entraide, j'essaie de partager les connaissances que j'ai pu acquérir à travers mes articles.
See Full Bio >

Partagez cet article

TELEGRAM PARTAGERA L'ADRESSE IP ET LE NUMÉRO DE TÉLÉPHONE DES UTILISATEURS EN CAS D'AFFAIRE CRI MINELLE

COMMENT CRÉER UNE CLÉ USB CHIF FRÉE VIA LUKS AVEC CRYPTSETUP ?

Vous pourrez aussi aimer

Gérer le log level sous Nginx

Laisser un commentaire

Votre adresse e-mail ne sera pas publiée. Les champs obligatoires sont indiqués avec *

Commentaire *

Nom *

E-mail *

Site web

Enregistrer mon nom, mon e-mail et mon site dans le navigateur pour mon prochain commentaire.

Laisser un commentaire

Newsletter : 1 e-mail par semaine !

S'abonner

A la une

POWERSHELL STRATÉGIE DE GROUPE

30/09/2024 Florian BURNEL 0 commentaire

Apprenez à exécuter des scripts PowerShell en tant que tâches planifiées immédiates, et donc sans redémarrage de Windows, à l'aide d'une GPO (Preferences).

Perplexity.ai : le moteur de recherche boosté à l'intelligence artificielle

29/09/2024 0 commentaire

Stirling PDF : comment ajouter une signature numérique à un PDF ?

28/09/2024 1 commentaire

Windows 11 : Recall peut être désinstallé et il est plus sécurisé !

27/09/2024 0 commentaire

Windows 11 KB5043145 : que contient cette mise à jour ? Il ne s'agit pas de Windows 11 24H2 !

27/09/2024 2 commentaires

Microsoft va bloquer l'application Teams sur les anciennes versions de Windows 10 et Windows 11 !

27/09/2024 5 commentaires

Nos derniers cours gratuits

13 chapitres

★★★★★

Maîtrisez Cisco IOS : les bases indispensables

Florian Duchemin

26 chapitres

★★★★★

Débuter avec Hyper-V – La virtualisation sur Windows Server 2022

Vous cherchez quelque chose ?

Recherche

Découvrir IT-Connect

A propos

Comment contribuer sur IT-Connect ?

Contact

Espace annonceurs

L'Équipe

Offres d'emploi

Politique de confidentialité

Puis-je réutiliser le contenu publié sur IT-Connect ?

Soutenir IT-Connect

Espace personnel

Inscription

Connexion

Flux des publications

Recommandations

Blogmotion

Délibérata