الفصل العشرين
ثغرة ال Subdomain Takeover

المؤلف
د.م/ أحمد هاشم الفقي
استشارى أمن المعلومات و التحول الرقمي
Ahmed.Hashem.ElFiky@outlook.com

ثغرة ال Subdomain Takeover

- ال CNAME هو DNS Record وهو أختصار (Canonical Name) وهو يعتبر أسم مستعار (Alias) للأسم الحقيقي, أي بمعنى أدق عندما يكون مثلا لدينا null.test.comال CNAME Record الخاص به هو iamtest123.herokuapp.com اي يعني أن null.test.com هو subdomain يشير إلى iamtest123.herokuapp.com فمثلا عندما تعدل على شيء في iamtest123.herokuapp.com او مثلا رفعت ملف سوف يتعدل وييكون مرفوع ايضا في null.test.com
- كيفية استخراج CNAMEالخاص في Subdomain
- للويندوز تستطيع عن طريق أمر nslookup

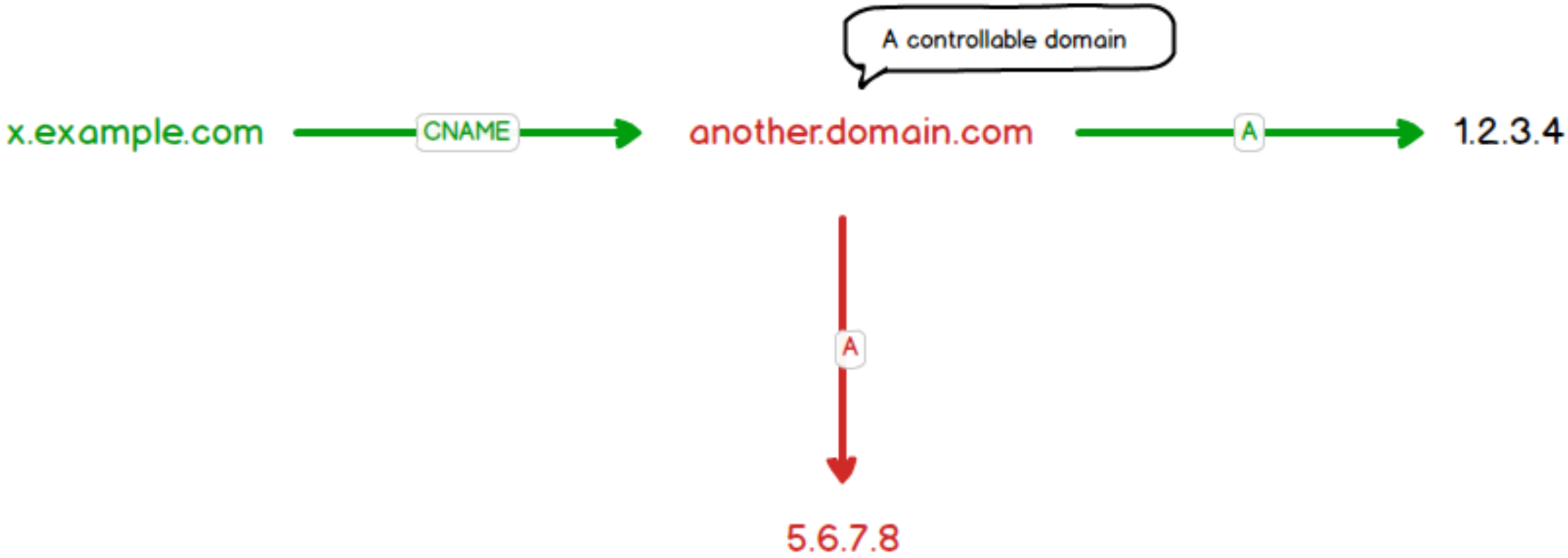
```
nslookup syed.subdomain-takeover.tk
```

ثغرة ال Subdomain Takeover (تكمله...)

```
dig @8.8.8.8 syed.subdomain-takeover.tk CNAME
```

- للينكس تستطيع عن طريق أمر dig
- ماهي ثغرة Subdomain Takeover
- هي ثغرة من نوع misconfiguration لل CNAME DNS Record
- غير واضح ؟ دعني أعطيك سيناريو شرح أفضل, مثلا هناك شركة ما انشأت subdomain وال CNAME DNS Record يشير الى أحد الخدمات السحابية المقدمة منه AWS او Heroku الخ.. لكن مع مرور الوقت أتحذف هذا CNAME او انتهت صلاحيته لكن المصيبة هي عندما ينسى المسؤول تغييره او تجديده ! فيقوم المهاجم بتسجيل حساب جديد في AWS او Heroku (يجب ان يكون نفس external service فمثلا لو كان AWS تسجل في AWS لو كان heroku تسجل في heroku لو كان Github تسجل في Github) وعندما يسجل المهاجم يذهب لتسجيل الأسم المنتهي او المحذوف كأنه أسم جديد وهنا يستطيع التحكم بال subdomain الذي انشأته الشركة وهذه تسمى Subdomain Takeover

ثغرة ال Subdomain Takeover (تكمله...)



Sub-domain takeover

ثغرة ال Subdomain Takeover (تكمله...)

- كيف تتجنب Subdomain Takeover
- تخلص من CNAME DNS Records الغير مستخدمه او المنتهيه الصلاحية او المحذوفة .

تم بحمد الله انتهاء الفصل العشرين