

「Visual DNS Attack」を用いた DNSキャッシュポイズニングの仕組み

今井研究室 後藤祥仁

1

目次

- 用語解説
- DNS
- DNSキャッシュポイズニング
- デモについて

2

DNS(Domain Name System)

- ドメイン名とIPアドレスを相互変換するサービス(今回はドメイン名からIPアドレスについて述べる)
- IPアドレス → IPアドレスからドメイン名に逆変換したドメイン名を返すサービス(逆変換サービス)
- 例: `www.google.com` → `172.217.131.164`
- 權威サーバ(コンテナーサーバ)とDNSキャッシュサーバを使ってDNSサービスを実行している
- 權威サーバはドメイン名をIPアドレスに変換するサービス
- DNSキャッシュサーバは權威サーバに問い合わせる代わりにキャッシュ(記憶)されたドメイン名とIPアドレスの対応関係からIPアドレスを返すサービス



3

DNSキャッシュポイズニング

- キャッシュサーバが權威サーバに問い合わせし、權威サーバから返答が来る前に偽の情報をキャッシュサーバに送り込む攻撃
- 攻撃されると、同じドメイン名でも違うサイト(サーバ)に誘導されてしまう



4

例えば...

ドメイン名	IPアドレス
<code>www.google.com</code>	<code>172.217.131.164</code>
<code>www.yahoo.co.jp</code>	<code>182.22.25.124</code>

↓

ドメイン名	IPアドレス
<code>www.google.com</code>	<code>172.217.131.164</code>
<code>www.yahoo.co.jp</code>	<code>172.217.131.164</code>

5

とりえず覚えてほしいこと

- DNS
- ドメイン名のIPアドレスを覚えてくれる
- DNSキャッシュポイズニング
- 攻撃が成功すると、同じURLでも違うサイトに飛ばされる

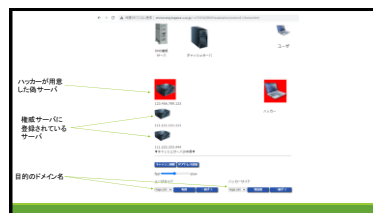
6

デモについて

- デモを行うこと
- DNSの動き
- DNSキャッシュポイズニングの動き
- ボタンを押すことでそれぞれ実行できる



7



8

デモに移ります

9