DNS Tunneling dnscat2 Cheat Sheet ∞

CHEAT-SHEET 04 Jun 2021 Arr0way

What is DNS Tunneling

Table of Contents

DNS tunneling is used to evade egress firewall rules and/or IDS / proxy or other web filtering applicances by tunneling data over DNS.
DNS tunneling usually works as external DNS resolution is available on most networks, it should be noted that DNS tunneling is slow due to the low amounts of data that can be transfered.

What You Will Learn:

- What is DNS tunneling
- How to setup dnscat2
- How to tunnel data over dnscat2

You Will Need

1. A real world domain, NameSilo works well and has free WHOIS privacy.
2. A VPS to run DNSCAT2 - Linode is cheap and works for this and this link will give you a $100 voucher (see instructions below)

In order to tunnel data over DNS a real world domain must be used and the domains authoritivate name servers must be set to servers in your control.

Buying a Domain

NameSilo offers free domain WHOIS privacy, a lot of extensions and is well priced.

How to Change Name Servers On NameSilo

Login to NameSilo and follow these instructions to change the authoritative name servers:

1. Go to the Domain Manager page within your account
2. Click the applicable domain name (it will be underlined in black)
3. Click the "View/Manage Registered NameServers" link within the "NameServers" box

DNS Forwarding with Dnscat2

1. Install dsncat2 `apt-get install dnscat2 -y`
2. Run: `dnscat2-server yourdomain.com` on your VPS
3. From the client machine you will need to run the dnscat2 payload

All Blog
Cheat Sheets
Techniques
Security Hardening
WalkThroughs

CHEAT SHEETS

Reverse Shell Cheat Sheet: PHP, Python, Powershell, Bash, NC, JSP, Java, Perl
Nmap Cheat Sheet: Commands & Examples (2022)
DNS Tunneling dnscat2 Cheat Sheet
SSH Lateral Movement Cheat Sheet
Android Pen Testing Environment Setup
Password Reset Testing Cheat Sheet
SSRF Cheat Sheet & Bypass Techniques
Penetration Testing Tools Cheat Sheet
LFI Cheat Sheet
Vi Cheat Sheet
Systemd Cheat Sheet
nbtscan Cheat Sheet
Linux Commands Cheat Sheet
More »

WALKTHROUGHS

InsomniHack CTF Teaser - Smartcat2 Writeup
InsomniHack CTF Teaser - Smartcat1 Writeup
FristiLeaks 1.3 Walkthrough
SickOS 1.1 - Walkthrough
The Wall Boot2Root Walkthrough
More »

TECHNIQUES

SSH & Meterpreter Pivoting Techniques
More »

SECURITY HARDENING

Security Harden CentOS 7
More »

/DEV/URANDOM

MacBook - Post Install Config + Apps

4. If your domain's NS are configured correctly the session should be established
5. Enter `session -i` to spawn an interactive session
6. Launch a shell using `shell`

Dnscat2 Port Forwarding

Dnscat2 supports TCP forwarding allowing you to tunnel SSH or RDP connections over the established DNS tunnel.

```
command (client) 4> listen 127.0.0.1:22 target:22
```

Again this will slow but functional.

Enjoy.

More »

OTHER BLOG

Insecure Direct Object Reference (IDOR): Definition, Examples & How to Find
Encrypted Notes App Solution (iOS, Android, MacOS, Linux, Windows)
HowTo: Kali Linux Chromium Install for Web App Pen Testing
Jenkins RCE via Unauthenticated API
MacBook - Post Install Config + Apps
enum4linux Cheat Sheet
Linux Local Enumeration Script
HowTo Install Quassel on Ubuntu
HowTo Install KeepNote on OSX Mavericks