

Definitely Not Secure (DNS)



 <http://slides.dfirimmatt.com>

18th Annual
cybersecurity
symposium



About Me

I work for a big well-known organization...



As Vice President (VP) of Computer Security and Incident Response (IR). However, I have many years of hands-on technical experience, including Digital Forensics & Incident Response (DFIR).

I am also a Podcast Host for

ThreatReel

<https://threatreel.com>

Connect / Contact / Follow Matt:



<https://www.linkedin.com/in/mattscheurer>



<https://x.com/c3rkah>

Where I volunteer...

I am an Official



Advocate

<https://www.hackingisnotacrime.org>



Advisory Board: Information
Technology and Cybersecurity

<https://www.mywccc.org/>



Women's Security Alliance
(WomSA) Technical Mentor

<https://www.womsa.org>

Disclaimer!

Yes, I have a day job.
However...

Opinions expressed are based solely on my own independent security research and do not express or reflect the views or opinions of my employer.



Agenda

- **DNS** Essentials (Primer)
- **DNS** Tools (w/ Demos)
- **DNS** Attacks (w/ Demos)

Definition

D

N

S

Definition

Domain

Name

System

Definition

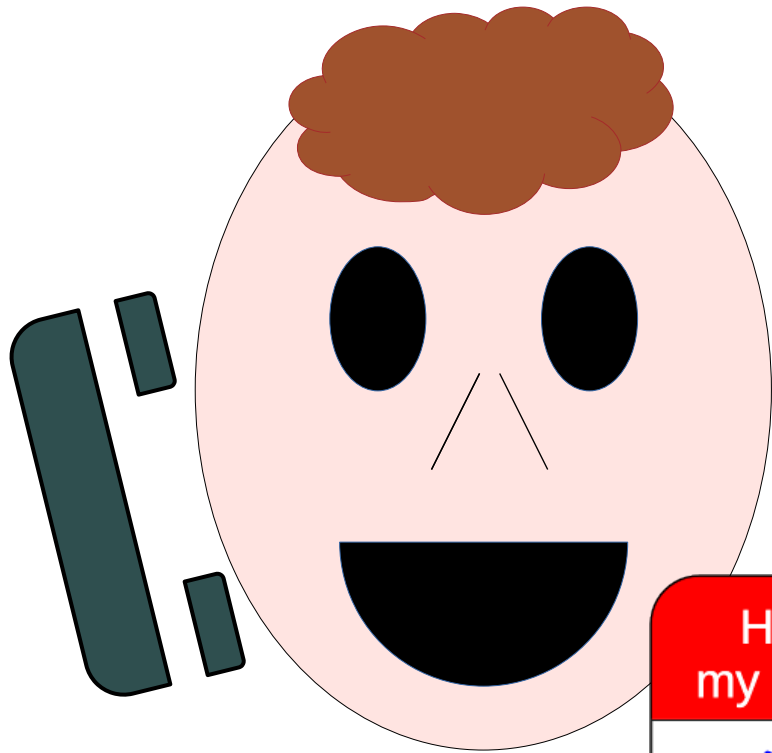
Domain
Name
System

NOTE: The 'S' does not stand for "Security"!

Purpose

The “**Domain Name System**” (DNS) is a vanity protocol making internet and network addressing human-friendly.

DNS gossips a lot!



*"And then CNAME
said to me, You
really need to go
and talk to..."*

HELLO
my name is

DNS

DNS in the OSI Model

Layer 7)	Application	DNS
Layer 6)	Presentation	
Layer 5)	Session	Port 53
Layer 4)	Transport	UDP, TCP
Layer 3)	Network	IP
Layer 2)	Data Link	
Layer 1)	Physical	

Networking

Mostly UDP Port 53

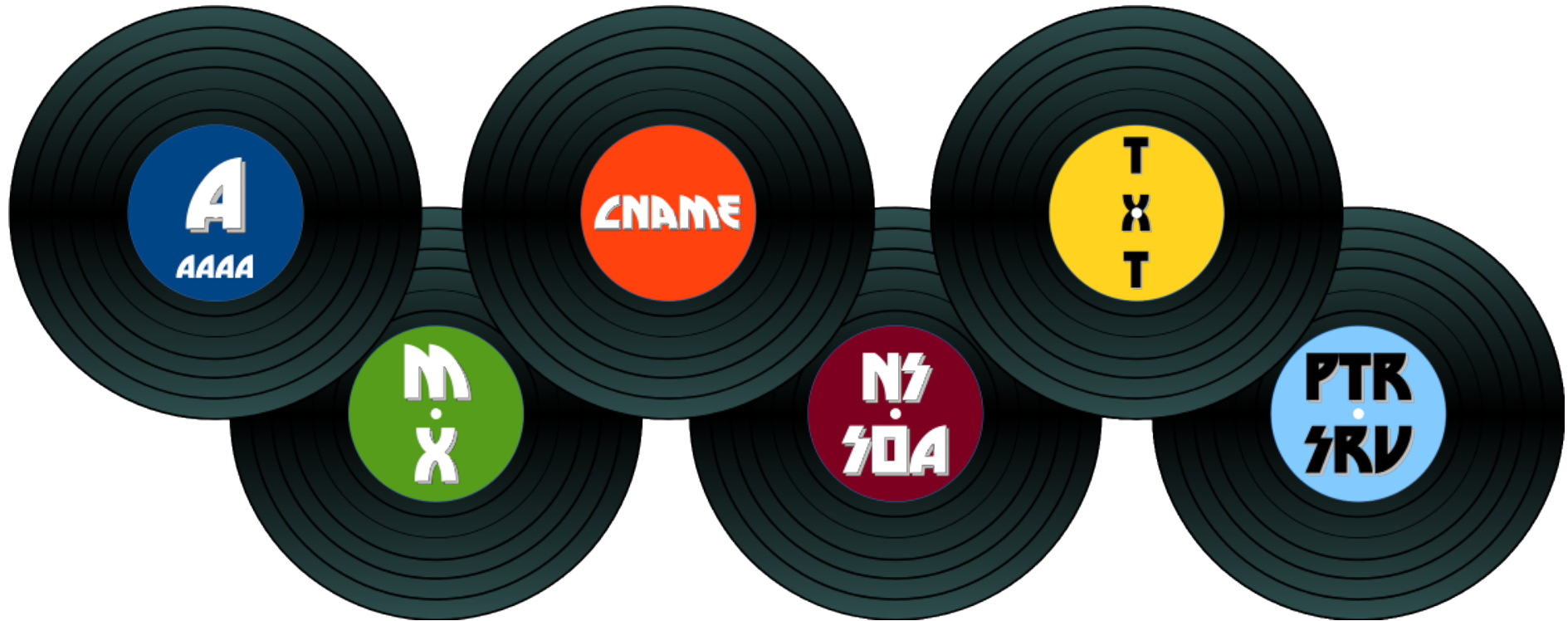
TCP Port 53

- > 512/4096 UDP byte limits
- DNSSEC
- Zone Transfers
 - Heavily restricted today

Other TCP Ports

- DNS over TLS (DoT)
 - TCP Port 853
- DNS over HTTPS (DoH)
 - TCP Port 443

Foundational DNS Records



More about “TXT”

RFC 1035

- 2.3.4 Size limits
 - 255 Characters



“Time to Live” (TTL) Values



Number of seconds DNS resolvers should cache records before refreshing

DNS Tools

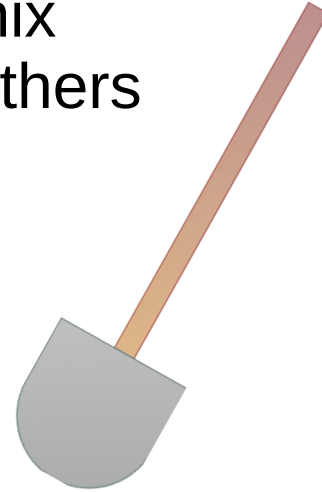


nslookup

- Windows
- *nix
- Mainframe
- Others

dig

- *nix
- Others



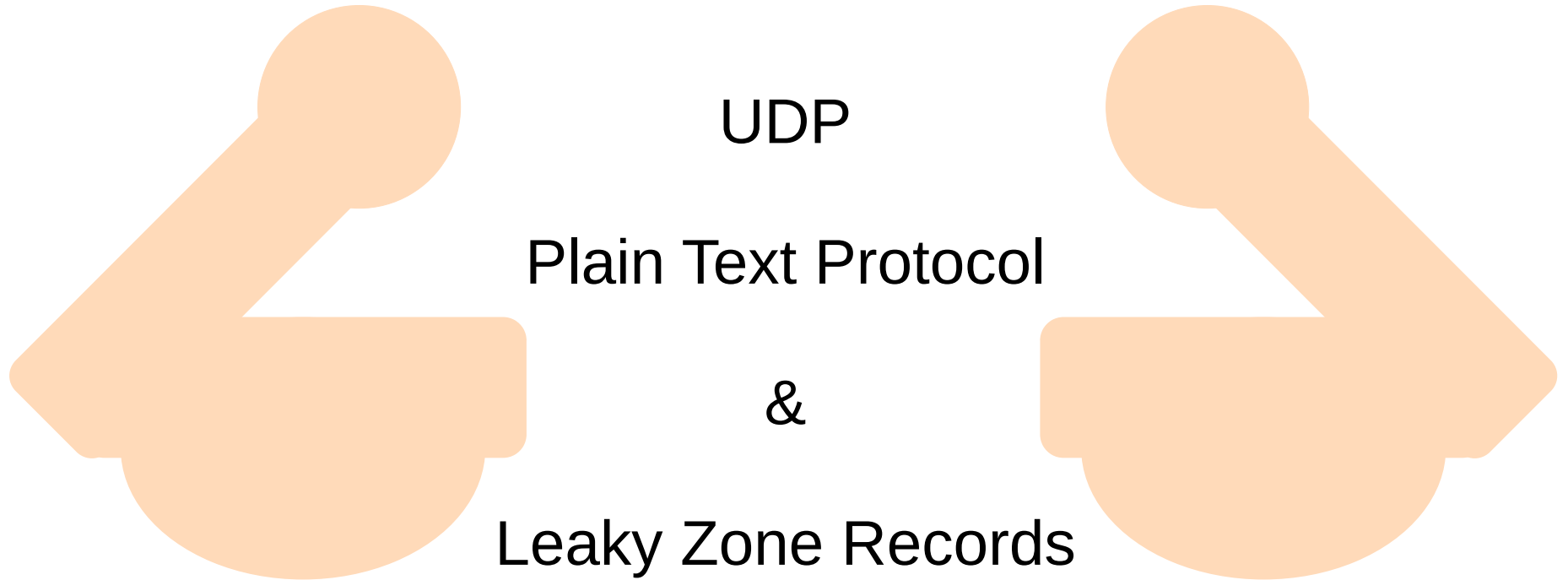
DNS tools demos

Live Demo

Early DNS Security Woes

- **RFC 1535**
 - A Security Problem and Proposed Correction With Widely Deployed DNS Software
 - <https://www.rfc-editor.org/info/rfc1535>
 - October, 1993

DNS Weaknesses



DNS packet capture

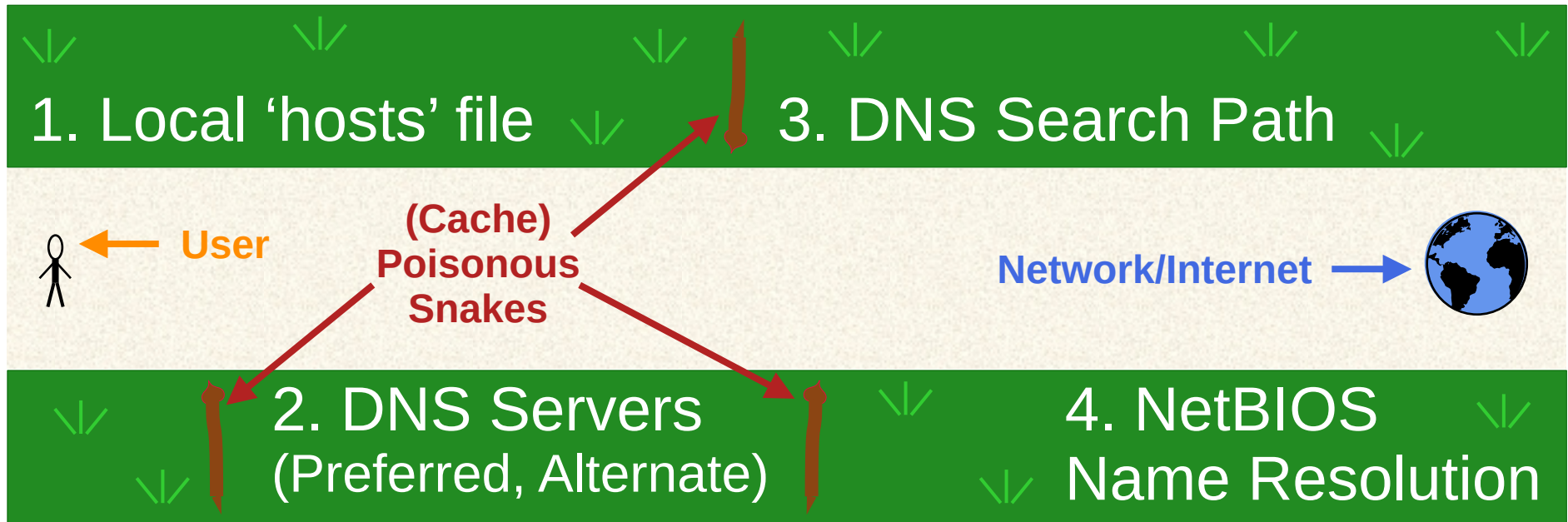
Live Demo

Leaky DNS Zones

Live Demo

DNS Hijacking

Abuse along the DNS Default Search Order trail



DNSSEC to the rescue?

The text 'DNSSEC' is rendered in a large, bold, green 3D font. The letters have a thick black outline and a slight shadow, giving them a three-dimensional appearance. The font style is a sans-serif, blocky typeface.

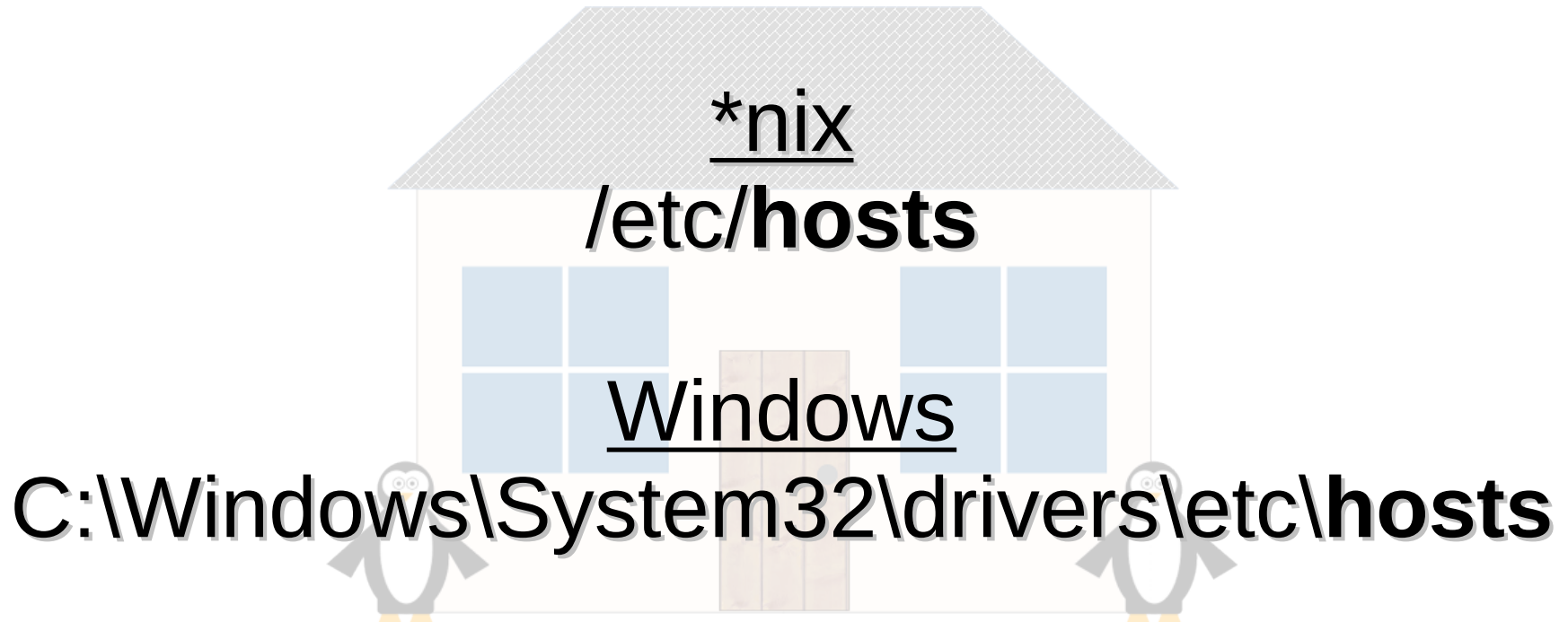
DNSSEC provides a cryptographic “Chain of Trust” to prevent DNS spoofing and DNS Cache Poisoning

DNSSEC shortcomings

DNSSEC

- Lack of adoption
- Configuration woes
- 'hosts' file bypass
- AitM / MitM
- Typosquatting

Where the “hosts” file lives

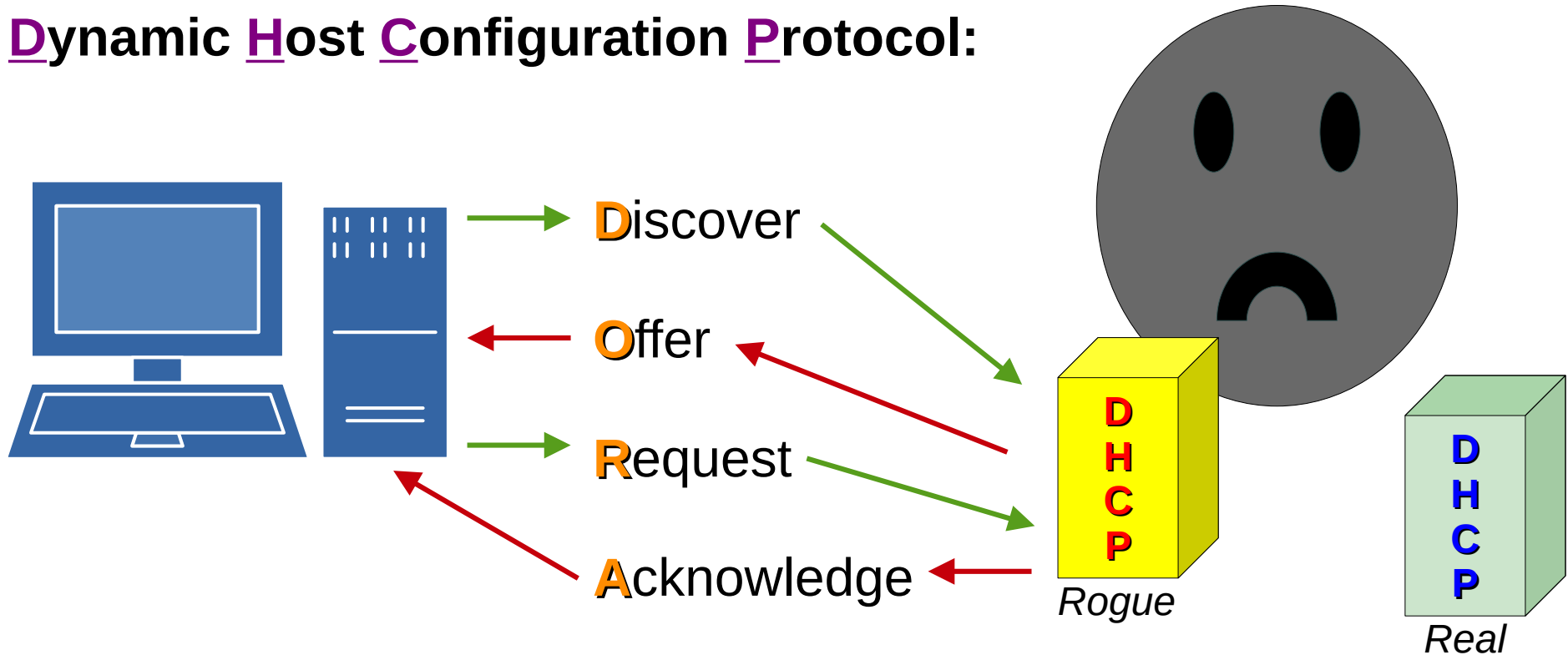


Injecting the “hosts” file

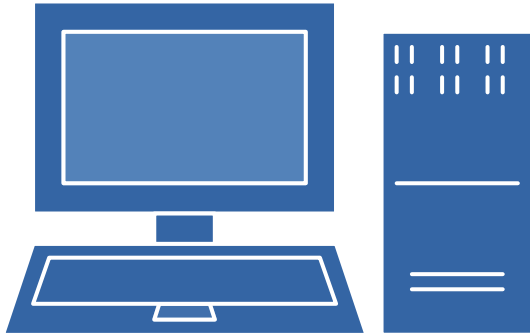
Live Demo

Rogue DHCP

Dynamic Host Configuration Protocol:



DHCP Network Settings



IP Address

Subnet Mask

Default Gateway

DNS Servers

Other (WINS for NetBIOS, etc.)

NOTES: NetBIOS = Network Basic Input/Output System, WINS = Windows Internet Name Service

DNS Tunneling



C2



Exfil

C2 & Data Exfiltration

Live Demo

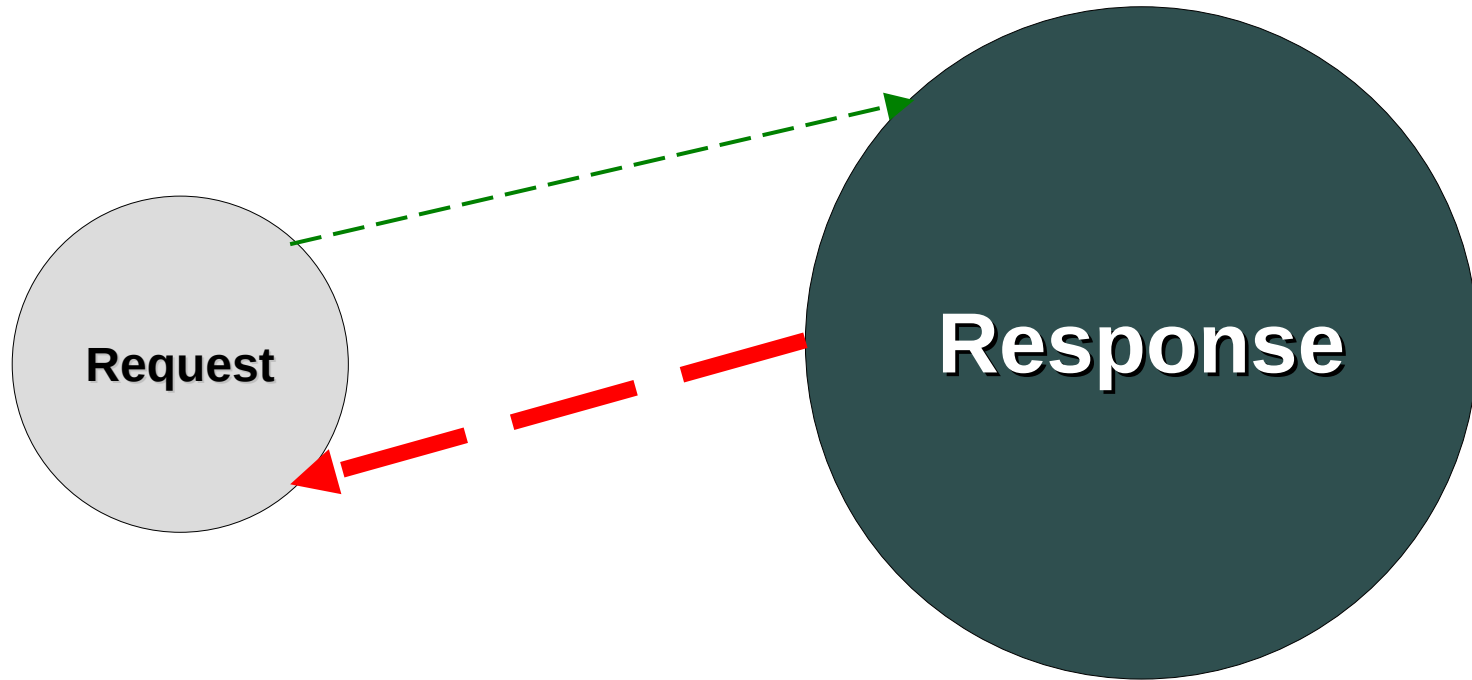
Other DNS Spoofing

**ARP
Poisoning**

**DNS
Server
Record
Changes**

**Domain
Registration
Takeover**

DNS Amplification Attacks

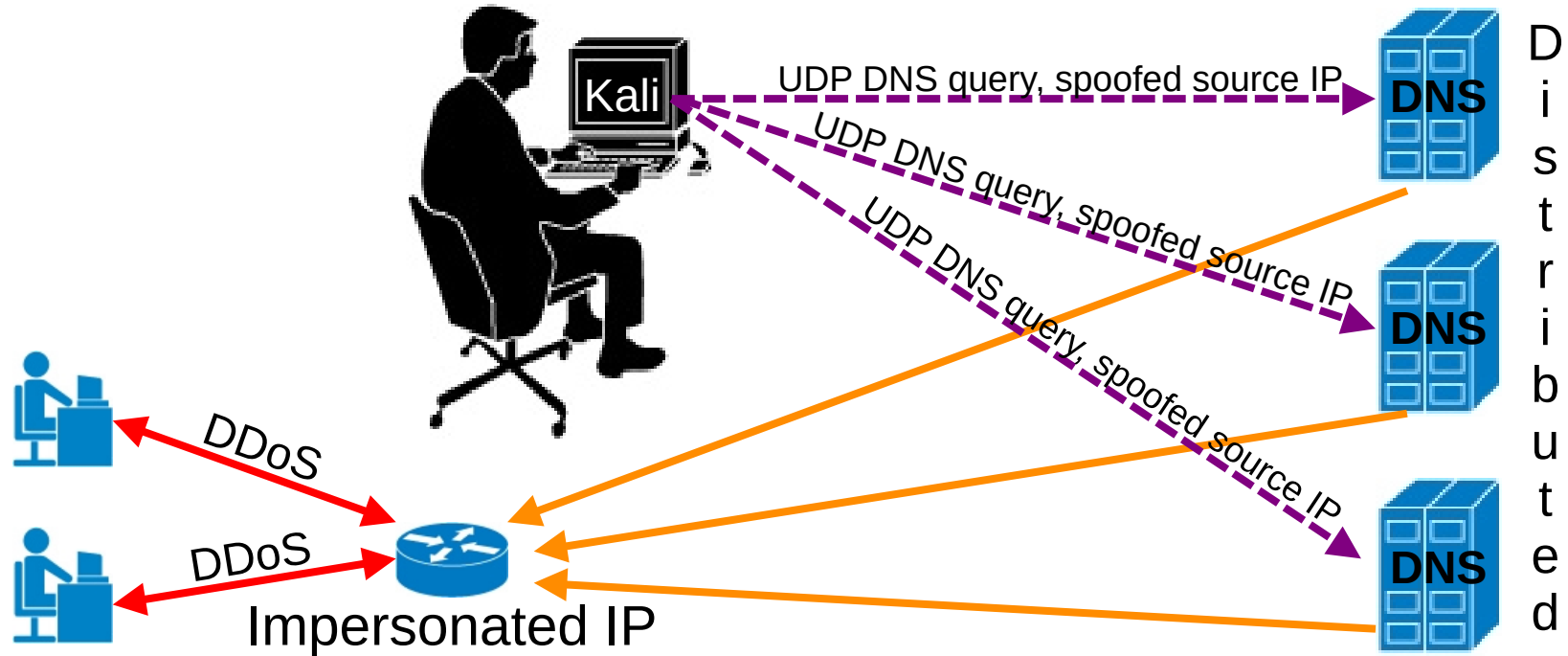


Too many large responses: Denial of Service (DoS)

DNS Reflection



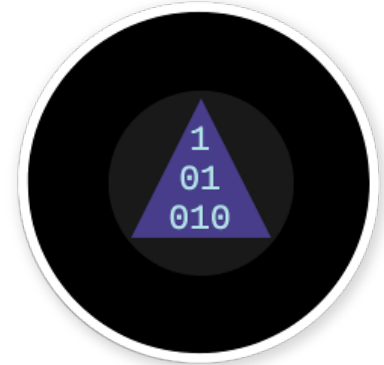
How Reflection Attacks Work



Questions



Who?
What?
When?
Where?
Why?
How?



Definitely Not Secure (DNS)



 <http://slides.dfirimmatt.com>

18th Annual
cybersecurity
symposium



Matt Scheurer