Securing DNS

Betty DuBois
PACKET DETECTIVE

@PacketDetective www.bettydubois.com

Module Goals

Prevent Common Attacks

Filter DNS

Suhani

GLOBOTICKET
A Globomantics Company

- Suhani - Security Analyst

DNS Attacks

DNS Amplification

Attacker uses open DNS servers as pawns to flood victim with DNS responses

DDoS Attack

Malicious bots send high amounts of requests to a DNS server until it cannot resolve legitimate requests

Spoofing

Attacker makes DNS server "think" they are the true client

Filter DNS at the Server

Microsoft – DNS Policy

Client Subnet
Transport Protocol
Internet Protocol
Server Interface IP address
FQDN
Query Type
Time of Day

BIND – DNS Filtering/Blocking

Query Type
Subdomain
Domain
Top Level Domain

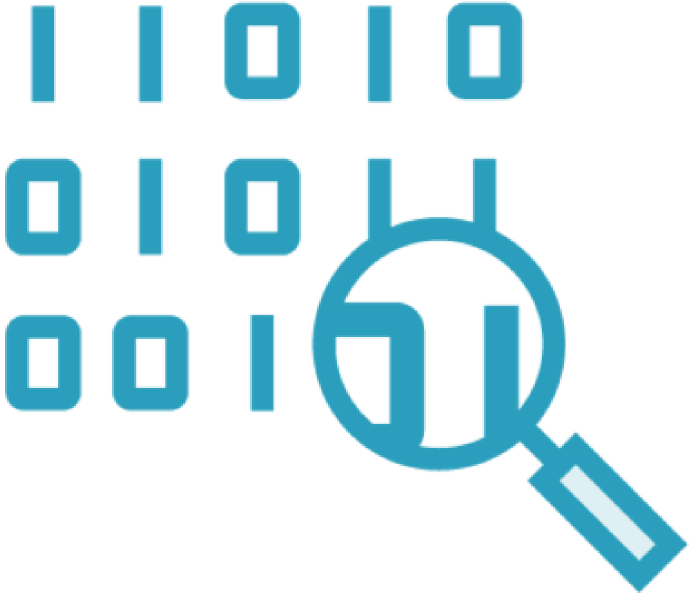
Demo

Configure DNS Policy to block query type

Summary

Prevent common attacks

Filter DNS



Thank you!