Implementation of DNS Sinkholes in Next-Generation Firewalls

Christian Tsirlis, Brad Wilson
Advisor: Jorge Crichigno

Department of Integrated Information Technology
University of South Carolina

December 2nd, 2021

Agenda

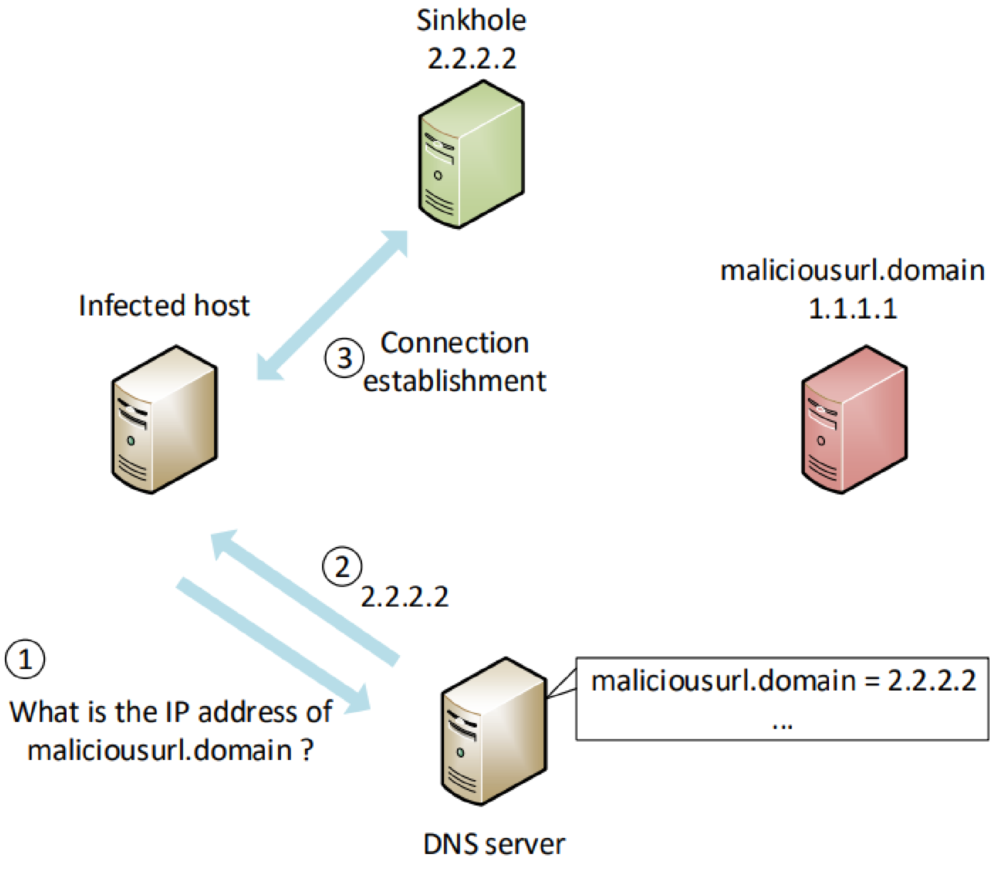
- Purpose
- Introduction
- Problem description
- Proposed solution and implementation
    - Anti-spyware profile
    - External dynamic list
- DNS Sinkhole Validation
    - Use of nslookup command
- Analyzing traffic logs
- Conclusion

Purpose

- Understand DNS Sinkholes
- Implement DNS Sinkholes in Security Policies
- Protect network from malicious attackers inside and outside of the network
- Analyze DNS and web browser traffic traversing the network
- Build stronger policies to minimize attacks

Introduction

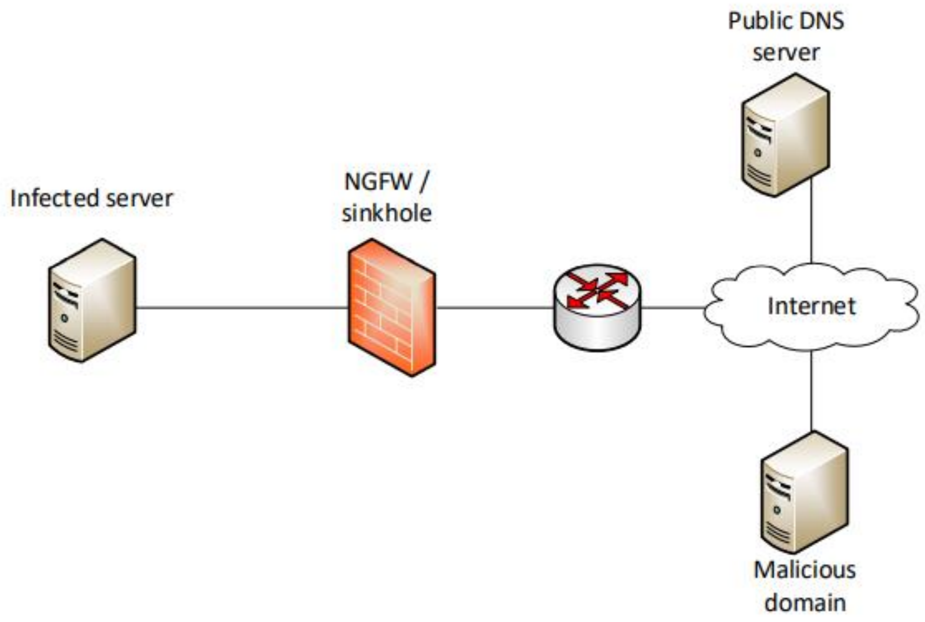
- A DNS sinkhole is a technique used to protect hosts from malicious domains.


Sinkhole
2.2.2.2
maliciousurl.domain
1.1.1.1
Infected host
3 Connection establishment
2 2.2.2.2
1 What is the IP address of maliciousurl.domain ?
maliciousurl.domain = 2.2.2.2
...
DNS server

With sinkhole

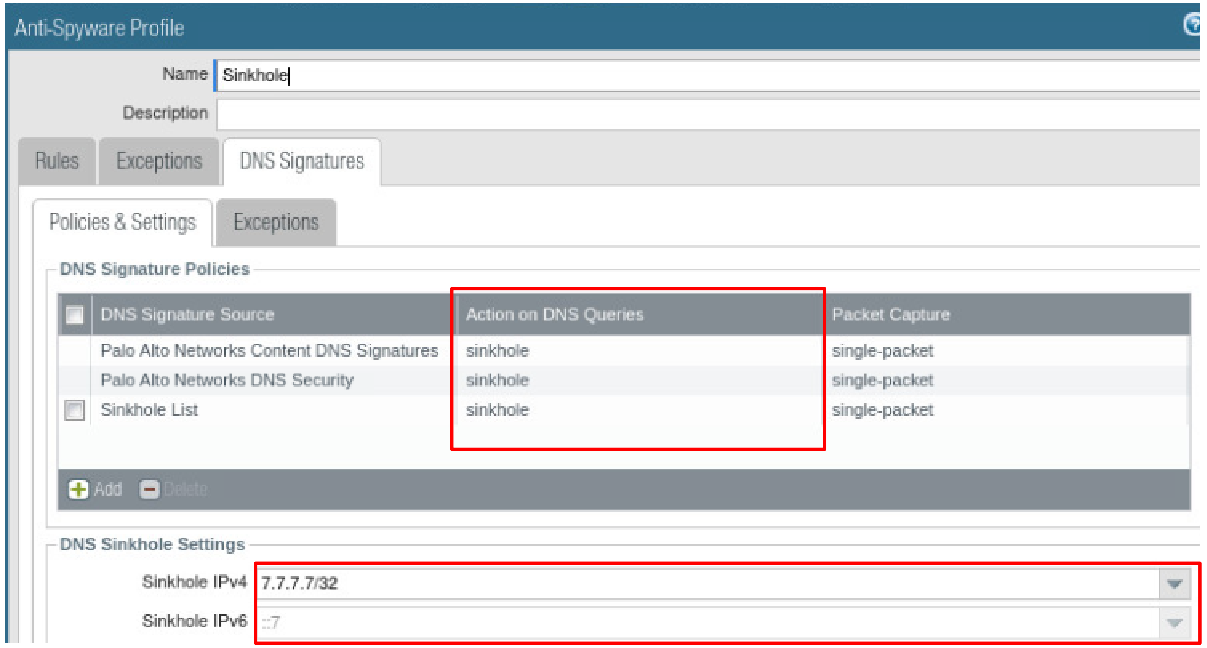
Problem Description

- Suspected malicious activity from internal network attempting to access malicious domains.
- Effectiveness of security policies using DNS sinkholes to protect internal network.



Proposed Solution and Implementation

- Sinkhole anti-spyware profile created.
  - Alerts network administrations and logs traffic.
  - Used in security policy to perform sinkhole action.



Name: Sinkhole

Description:

DNS Signature Policies

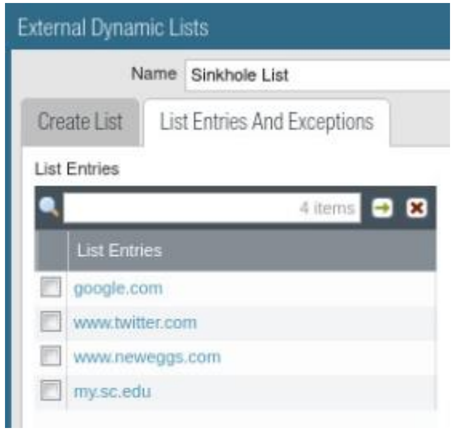
DNS Signature Source	Action on DNS Queries	Packet Capture
Palo Alto Networks Content DNS Signatures	sinkhole	single-packet
Palo Alto Networks DNS Security	sinkhole	single-packet
Sinkhole List	sinkhole	single-packet

DNS Sinkhole Settings

Sinkhole IPv4: 7.7.7.7/32

Sinkhole IPv6: ::7

- Sinkhole external dynamic list created.
  - Unique list to test sinkhole effectiveness.
  - Used in anti-spyware profile to filter DNS request.



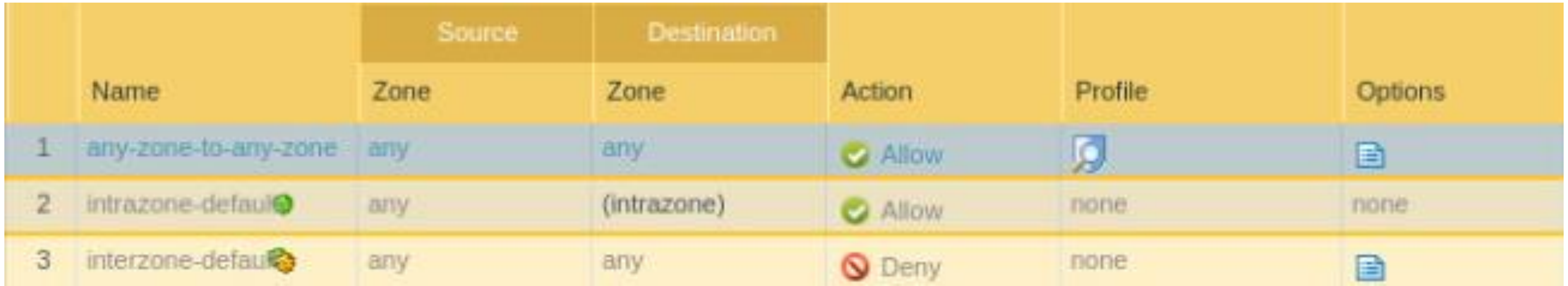
Name: Sinkhole List

List Entries

List Entries
google.com
www.twitter.com
www.neweggs.com
my.sc.edu

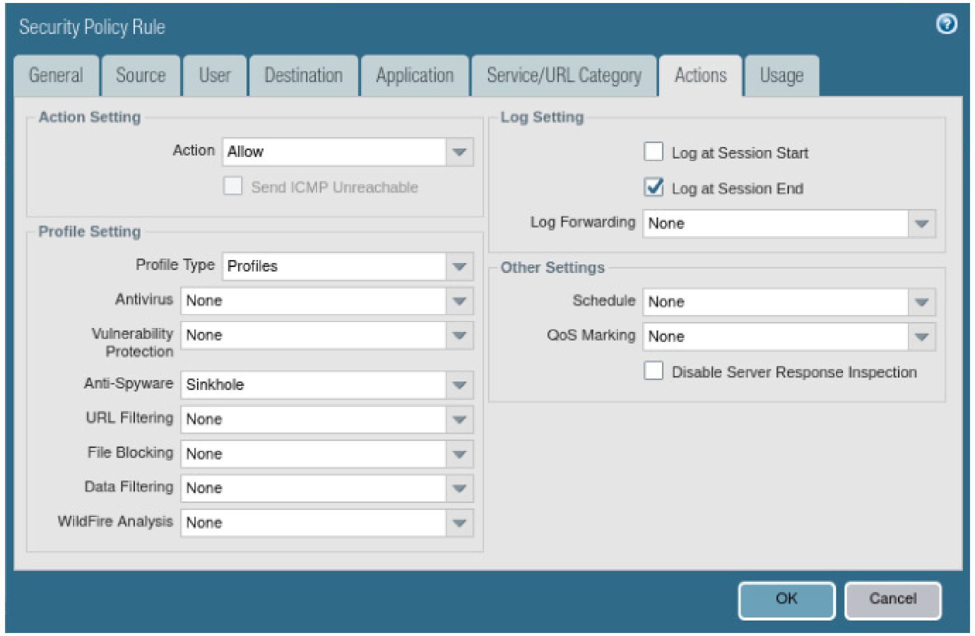
Proposed Solution and Implementation

- Security policy with anti-spyware profile attached.



		Source	Destination			
	Name	Zone	Zone	Action	Profile	Options
1	any-zone-to-any-zone	any	any	✓ Allow		
2	intrazone-default	any	(intrazone)	✓ Allow	none	none
3	interzone-default	any	any	⊘ Deny	none	

- Closer look at the security policy rule.
  - Focusing on the Actions tab.
  - Anti-spyware was added as a profile setting.



Security Policy Rule

Action Setting

Action: Allow

□ Send ICMP Unreachable

Profile Setting

Profile Type: Profiles

Antivirus: None

Vulnerability Protection: None

Anti-Spyware: Sinkhole

URL Filtering: None

File Blocking: None

Data Filtering: None

WildFire Analysis: None

Log Setting

□ Log at Session Start

☑ Log at Session End

Log Forwarding: None

Other Settings

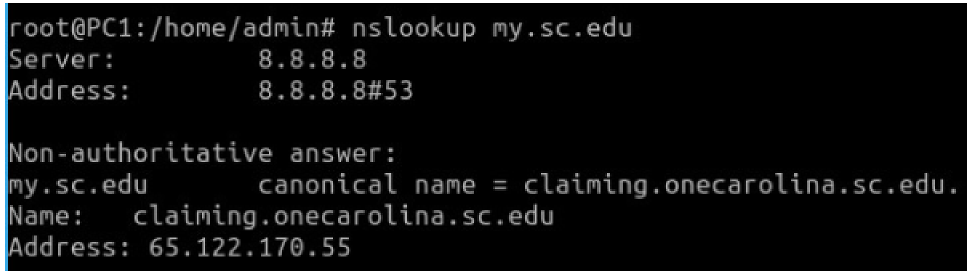
Schedule: None

QoS Marking: None

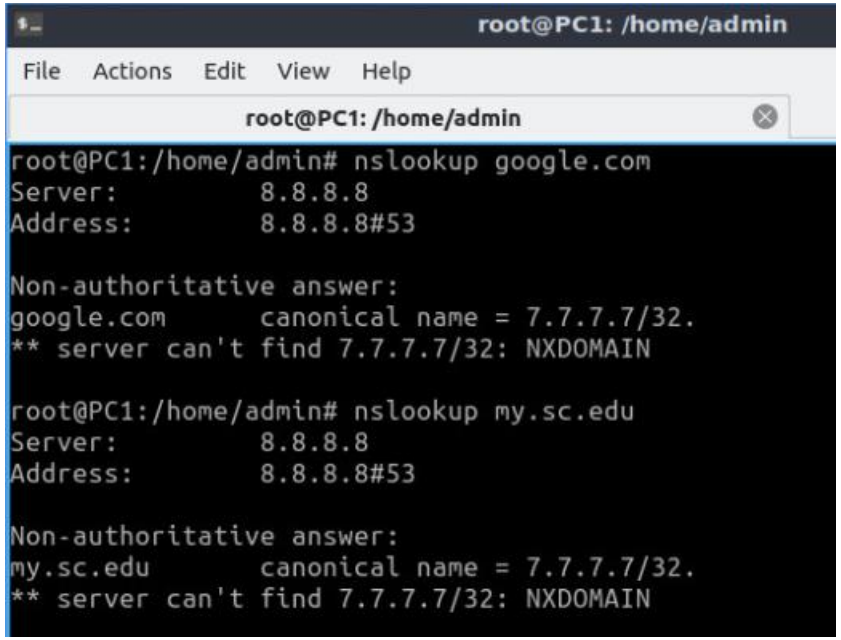
□ Disable Server Response Inspection

DNS Sinkhole Validation

- How to verify?
  - nslookup returns the ip address of the requested domain.
  - We used the nslookup command to confirm if the sinkhole was working.
- Results
  - DNS Sinkhole works with nslookup.
  - Web browser can evade DNS sinkhole using encrypted web browser traffic.



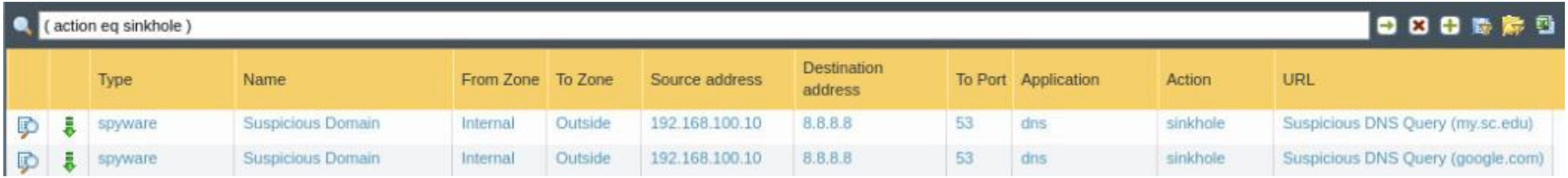
```
root@PC1:/home/admin# nslookup my.sc.edu
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
my.sc.edu       canonical name = claiming.onecarolina.sc.edu.
Name:   claiming.onecarolina.sc.edu
Address: 65.122.170.55
```



```
root@PC1:/home/admin# nslookup google.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
google.com      canonical name = 7.7.7.7/32.
** server can't find 7.7.7.7/32: NXDOMAIN

root@PC1:/home/admin# nslookup my.sc.edu
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
my.sc.edu       canonical name = 7.7.7.7/32.
** server can't find 7.7.7.7/32: NXDOMAIN
```

Analyzing Traffic Logs

- Search traffic logs by “sinkhole” action.
  - Ability to know the source address of DNS request.
  - Provides the URL requested by client.



```
( action eq sinkhole )
```

		Type	Name	From Zone	To Zone	Source address	Destination address	To Port	Application	Action	URL
		spyware	Suspicious Domain	Internal	Outside	192.168.100.10	8.8.8.8	53	dns	sinkhole	Suspicious DNS Query (my.sc.edu)
		spyware	Suspicious Domain	Internal	Outside	192.168.100.10	8.8.8.8	53	dns	sinkhole	Suspicious DNS Query (google.com)

Conclusion

- Why is this work important?
  - Our test highlights, that there are some weaknesses in DNS sinkholes and how web browsers can encrypt data, which makes the domain request impossible to see.
- Future work includes deeper packet analysis
- Use of URL filtering with DNS sinkhole is effective
- Questions?
- Thank you for listening and watching