

# Protecting Backend Systems

I AM IN YOUR BASE, ROOTIN' YOUR SERVERS

**SECURITY**  
**dark READING**  
Protect The Business  Enable Access

# Presented by...

DARK READING – PROTECTING BACKEND SYSTEMS – 2014

## Bishop Fox



- Matt Bryant  
*Security Analyst*
  
- Joe DeMesy  
*Security Associate*

# Agenda

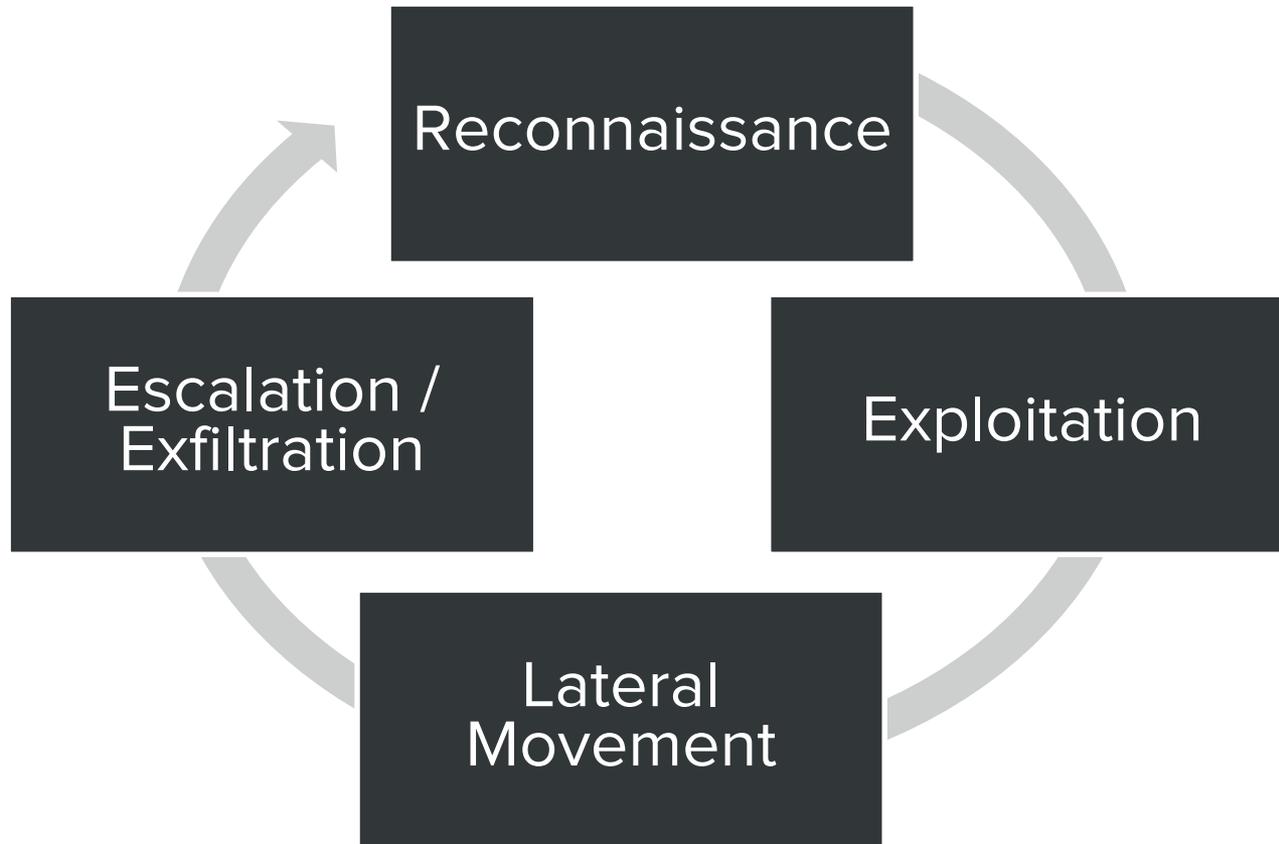
## TOPIC COVERAGE

### Backend Systems

- **Deny Footholds**
  - Web Servers
  - Databases
  - Domain Controllers
- **Deny Pivots**
  - Windows Networks
  - Linux Networks
  - “Cloud” Networks

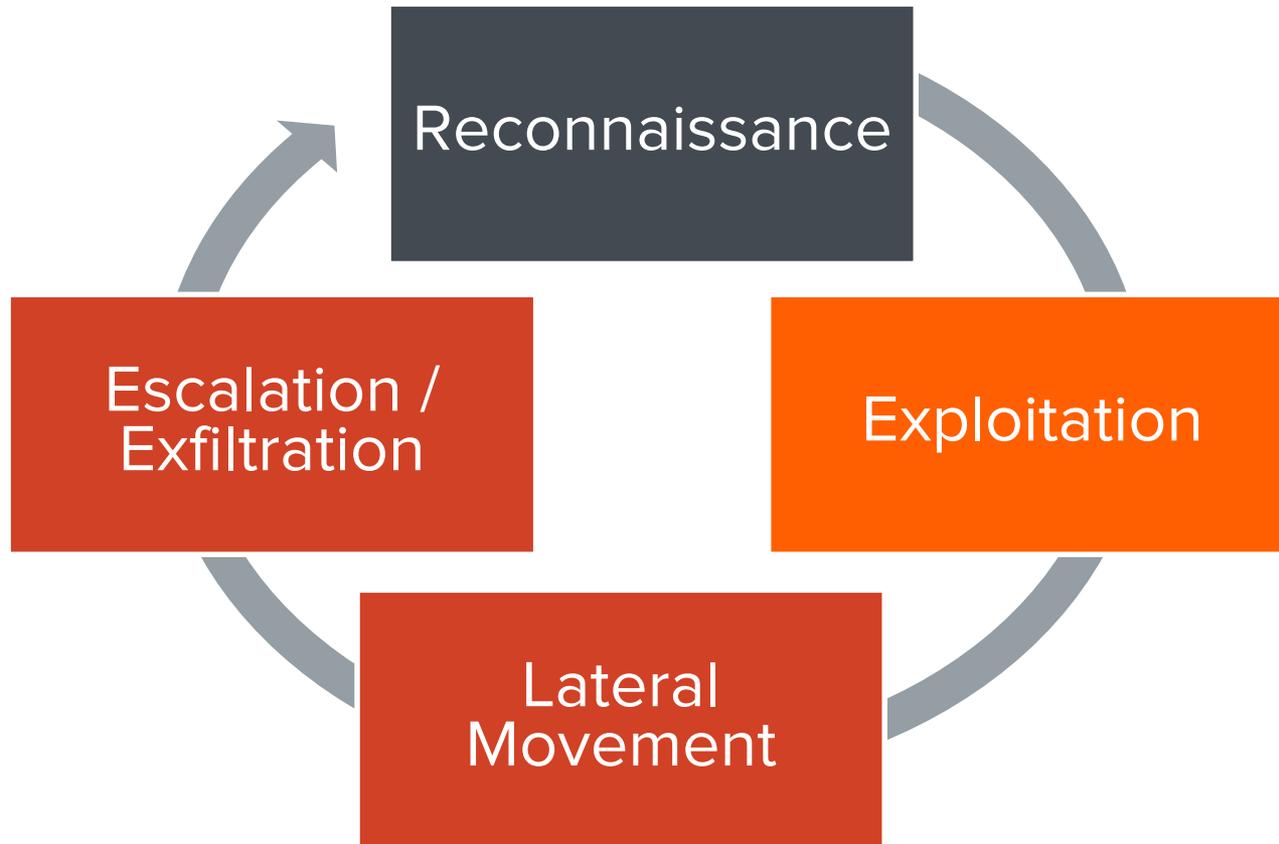
# Attacker Methodology

HACKING BY THE NUMBERS



# Attacker Methodology

HACKING BY THE NUMBERS



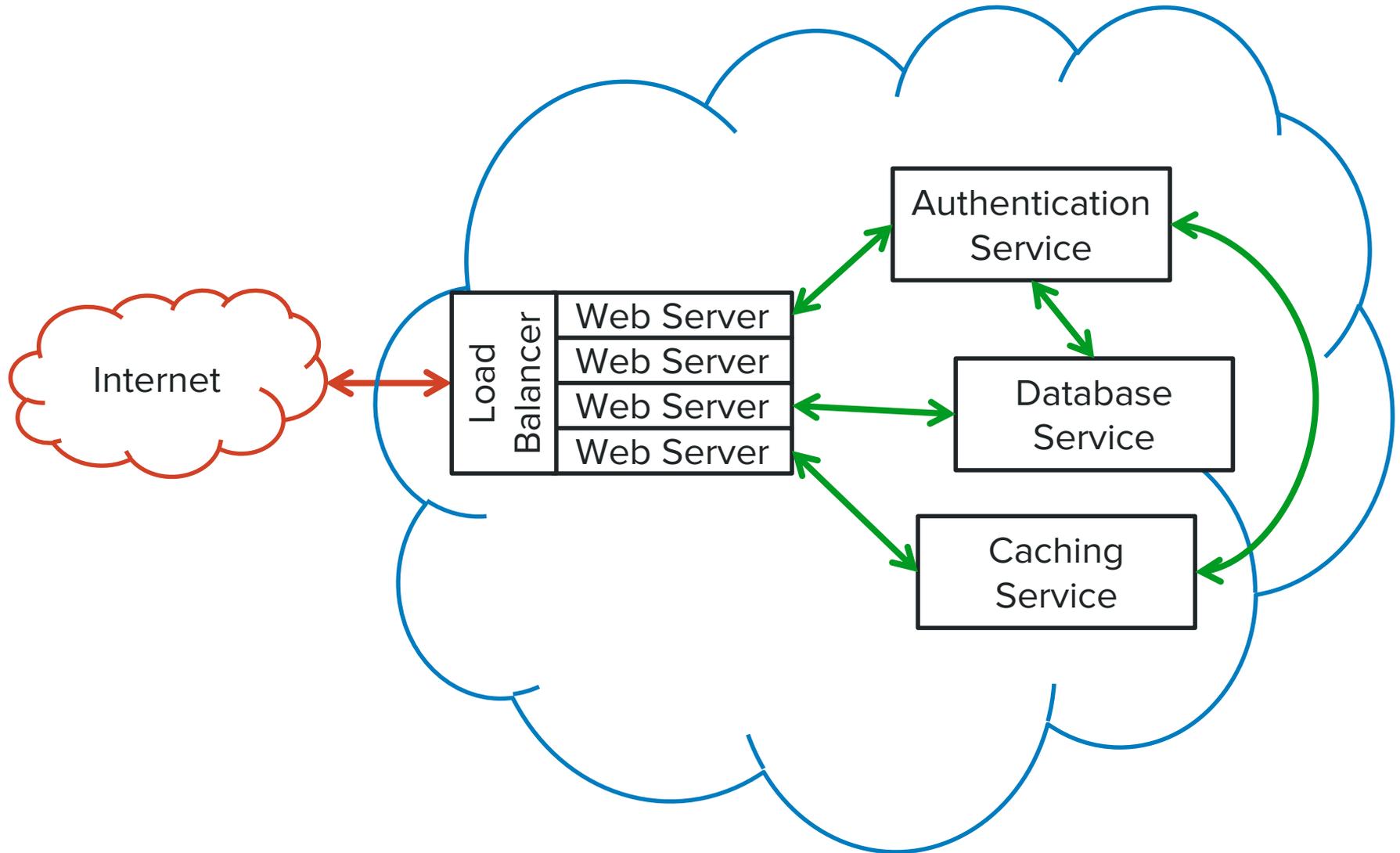
# Common Web Application

TRADITIONAL WEB APPLICATIONS



# Distributed Web Application

PRIVATE "CLOUD" MICRO-SERVICES ARCHITECTURE

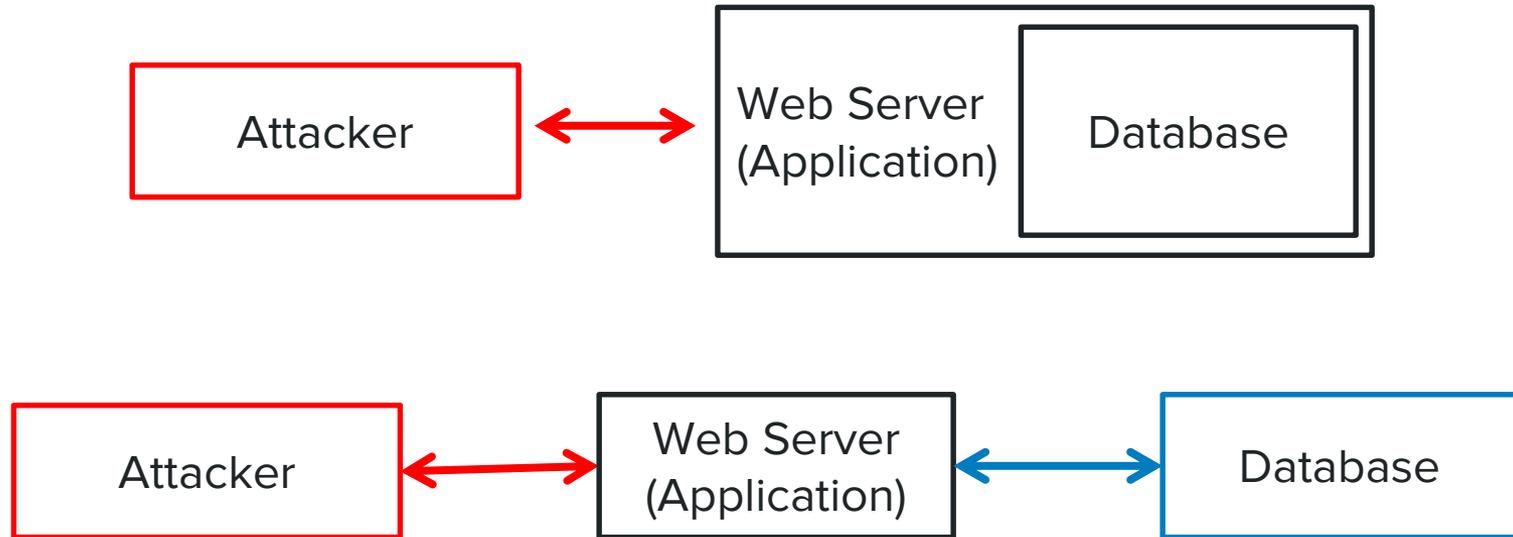


# FOOTHOLDS

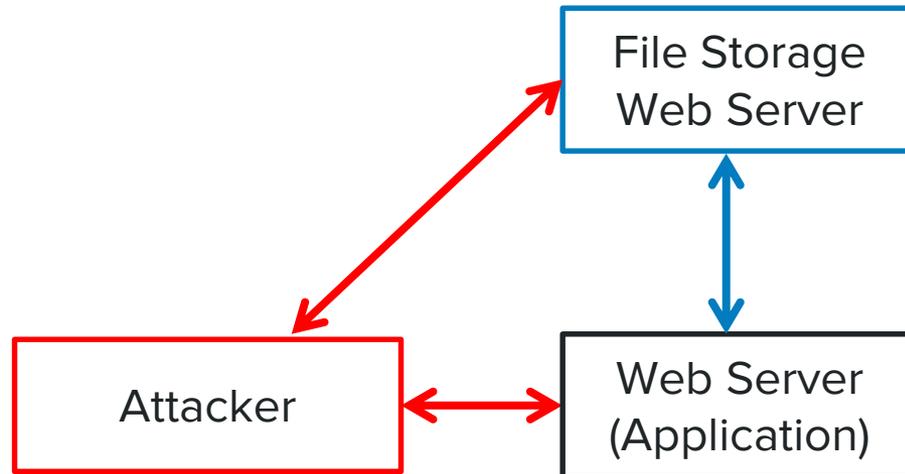
CRACKING THE PARAMETER



# SQL Injection



# Arbitrary File Upload



# Command Injection

```
1 <?php
2     echo shell_exec('cat ' . $_GET['filename']);
3 ?>
```

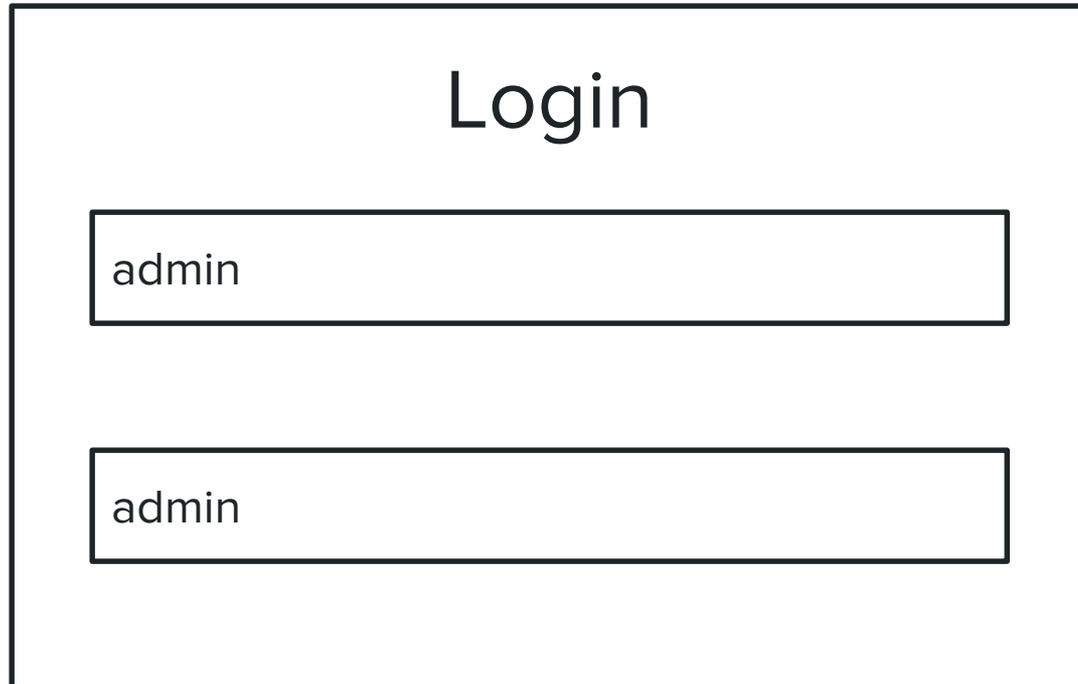
`http://www.example.com/view.php?filename=test.txt; rm -rf /`

# Weak & Default Passwords

Login

admin

admin

A diagram of a login form. It consists of a large rectangular box with a black border. Inside the box, the word "Login" is centered at the top. Below it, there are two horizontal rectangular input fields, also with black borders. The first input field contains the text "admin". The second input field, positioned directly below the first, also contains the text "admin".

# MOVING LATERALLY

THE CHEWY INSIDE



# WINDOWS

A PENTESTER FAVORITE



# Getting SYSTEM Privileges on Windows

- Windows XP has no user separation, all users are admin
- Admin to SYSTEM is easy with meterpreter  
`getsystem`
- Local privilege escalation vulnerabilities
- Find any cleartext credentials or sensitive files

# Admin to Domain Admin

- Mimikatz to extract LM and NTLM hashes
- Crack hashes to obtain cleartext passwords
- Extract Delegate & Impersonation tokens stored on the machine
- Incognito can be used to impersonate using these tokens
- These tokens can be used authenticate to other machines

# Move with cracked credentials



# Move with dumped tokens

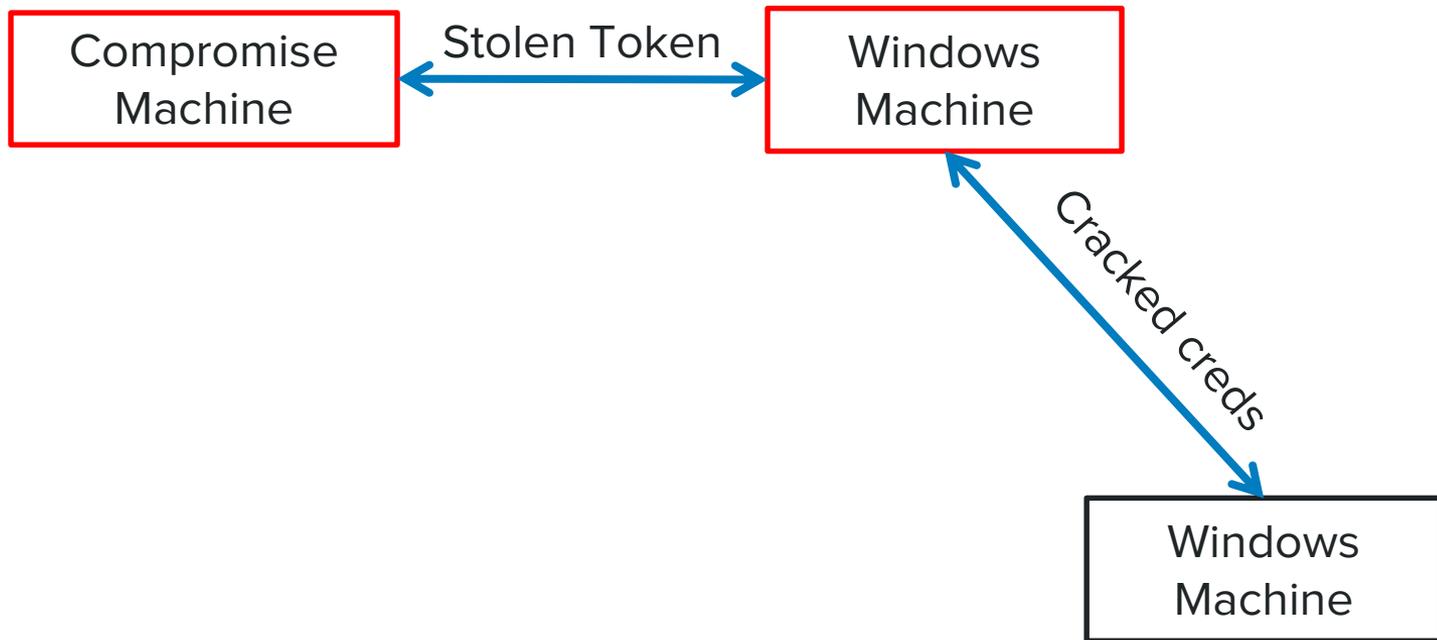


# SMBRelay



Source: <http://pen-testing.sans.org/blog/pen-testing/2013/04/25/smb-relay-demystified-and-ntlmv2-pwnage-with-python>

# Windows Domain Lateral Movement



**LINUX**

SLIGHTLY MORE COMPLEX



# Getting root on Linux

- Find all `setuid` binaries
- Check the Linux kernel version for known exploits (`Linux_Exploit_Suggester`)
- Check local services for known exploits
- Find any SSH keys stored on the Linux box
- Locate any sensitive files or cleartext credentials

# Pivoting using root

- Dump `/etc/shadow` and crack the password hashes
- Dump all SSH keys from all users on the system
- Use these keys and stolen credentials to move around the network

# Moving with Linux



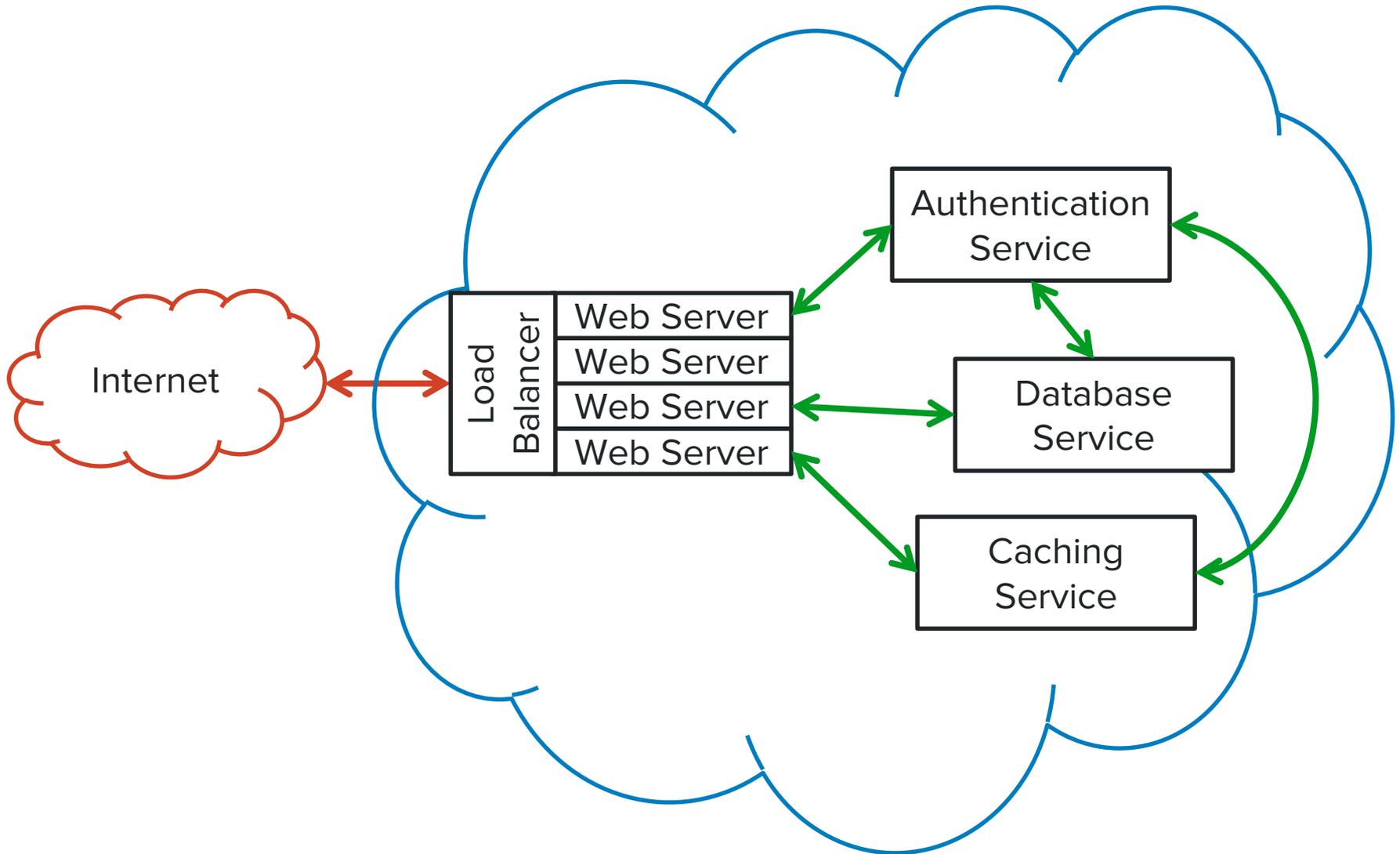
An abstract network diagram consisting of several interconnected nodes (small grey circles) and lines (thin grey lines) on a dark grey background. The nodes are arranged in a way that suggests a complex network structure, with some nodes connected to multiple other nodes. The lines are thin and grey, creating a subtle, technical aesthetic.

# CLOUD NETWORKS

IT'S ALL ABOUT THE IMPLEMENTATION

# Moving in the Cloud

PRIVATE "CLOUD" MICRO-SERVICES ARCHITECTURE

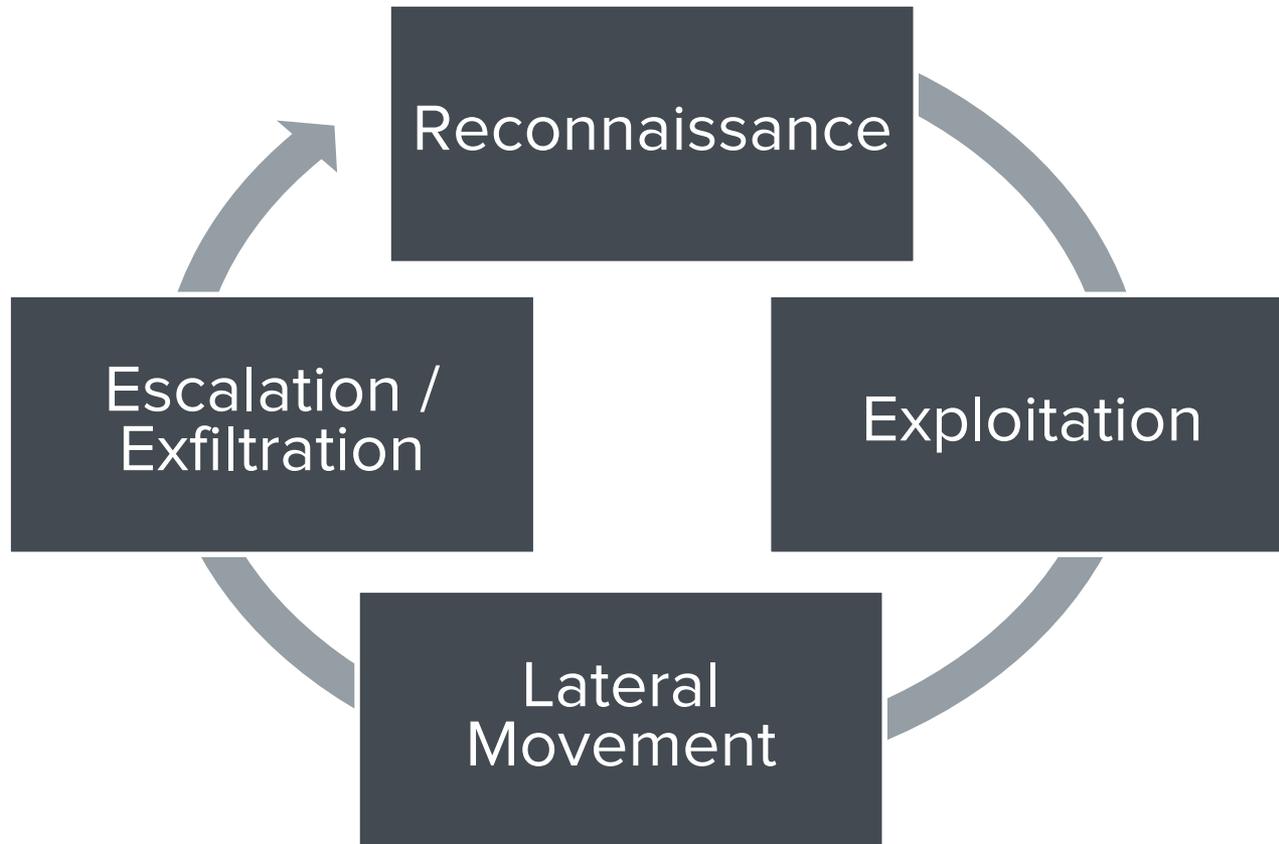


# OS Agnostic Tactics

- Use stolen credentials to authenticate to other services (FTP, SSH, RDP, etc.)
- Brute-force new services using common passwords
- Use default credentials for services

# Attacker Methodology

HACKING BY THE NUMBERS



# Contact Us

[bishopfox.com](http://bishopfox.com)

[contact@bishopfox.com](mailto:contact@bishopfox.com)

[@bishopfox](#)

[facebook.com/bishopfoxconsulting](https://facebook.com/bishopfoxconsulting)

[linkedin.com/company/bishopfox](https://linkedin.com/company/bishopfox)

[google.com/+bishopfox](https://google.com/+bishopfox)

# Thank You

**SECURITY**  
**dark READING**  
Protect The Business  Enable Access

**BISHOP FOX**<sup>®</sup>