



Behind Enemy Lines

Administrative Web
Application Attacks

Rafael Dominguez Vega

1001100100110100111011
001

DEEPSEC²⁰⁰⁸

Main Objectives

- Insecurities
- Impact
- Attack Techniques

A little about me ...



What this talk will cover

- Intro
- DHCP Script Injection Attack
- SSID Script Injection Attack
- Scanning for Webmin Servers Attack
- Recommendations, Summary & QA

Introduction

Administrative Web Interfaces

- Administer Systems and Networks
- Help Administrators
- Most Network Systems have One

Why should they be secured?

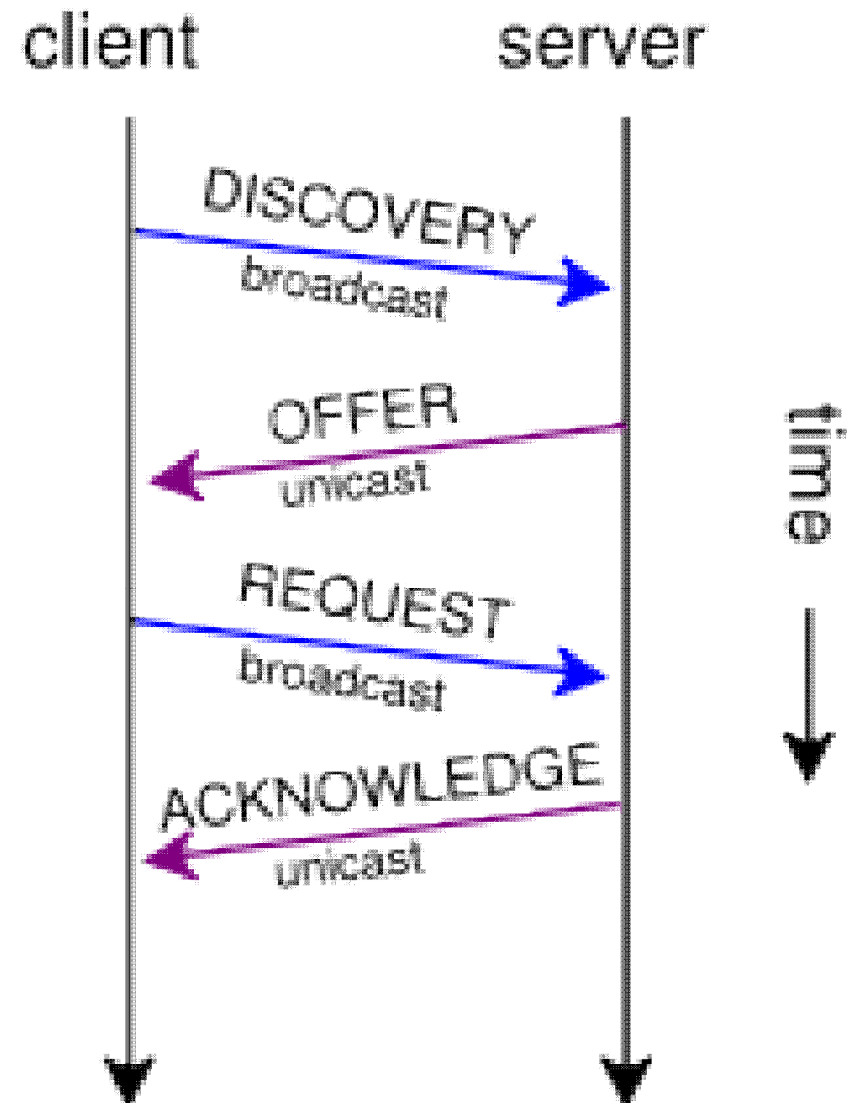
- Vulnerable as any other Web Application
- Highly Privileged Access
- Different Services, Systems and Protocols
- Used in “Trusted Environment”

Today's Web Application Attacks

- User Input Validation
- Security Best Practice
- Out of Band Channels

DHCP Script Injection Attack

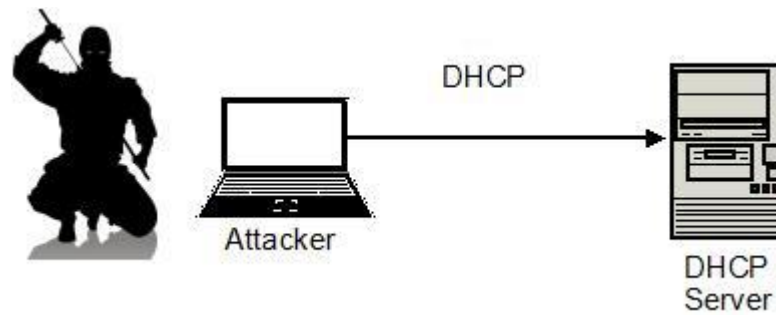
DHCP “HandShake”



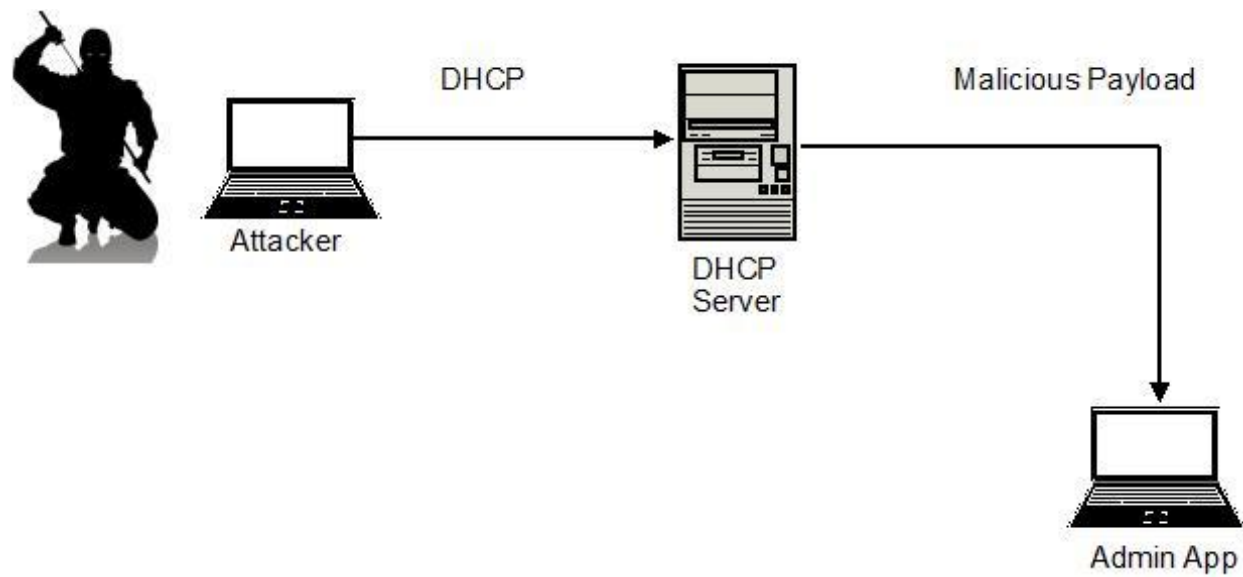
DHCP Script Injection Attack

- Active DHCP Leases List
- Attacker located in same LAN
- To Be Vulnerable

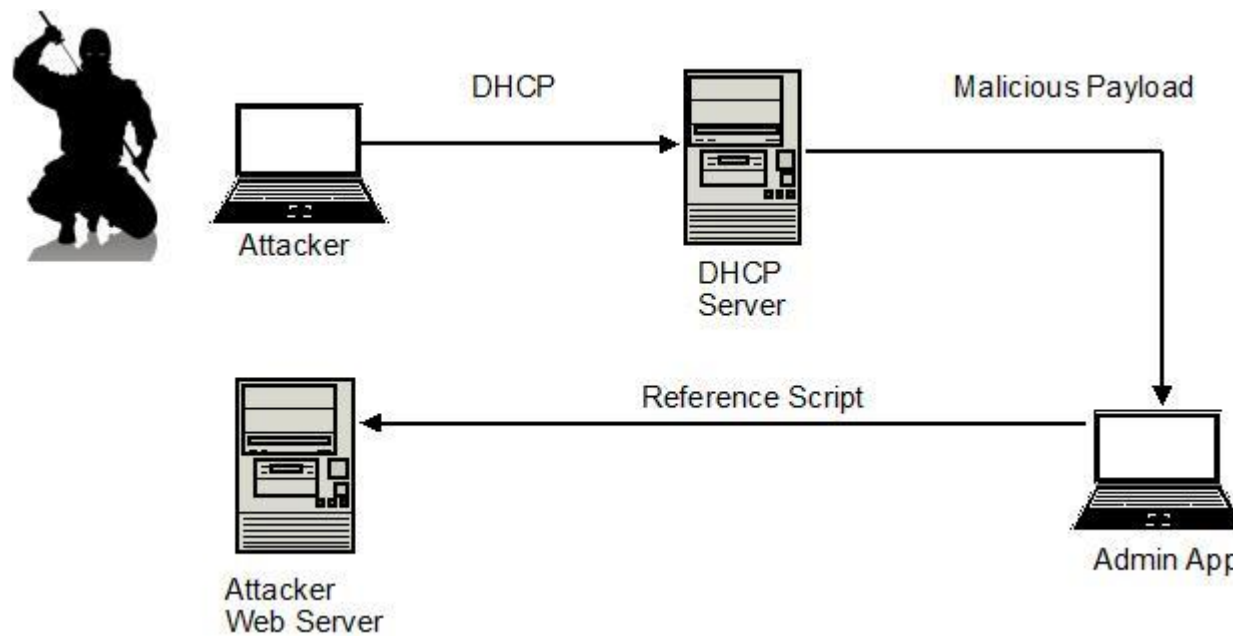
DHCP Script Injection Attack



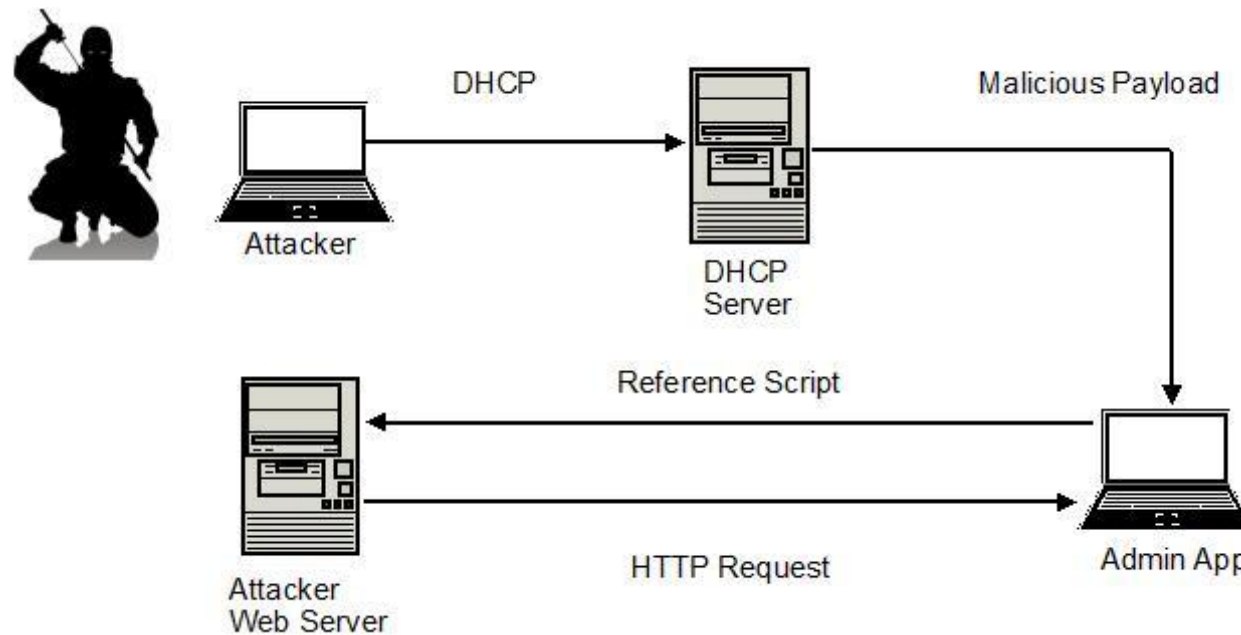
DHCP Script Injection Attack



DHCP Script Injection Attack



DHCP Script Injection Attack



DHCP Script Injection Attack - DEMO

- pfSense
- Tool
- Remote Command Execution

SSID Script Injection Attack

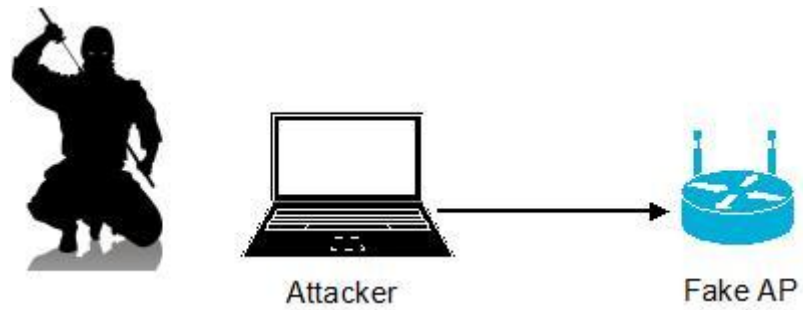
SSID Script Injection Attack

- 802.11 Protocol
- Management Beacon Frames
- Malicious Code in SSID

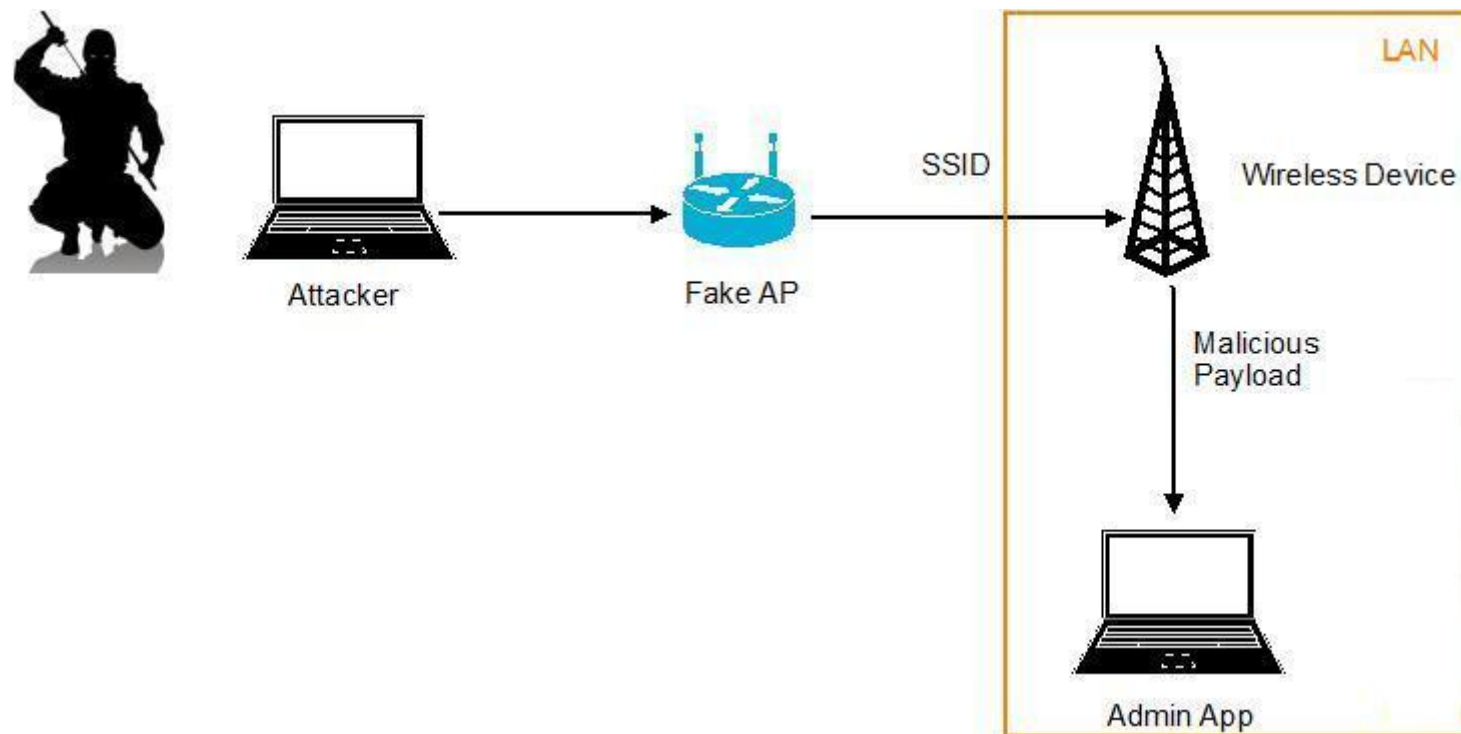
SSID Script Injection Attack

- “Scan for Neighbours AP” Functionality
- Attacker located in Wireless Range
- Max. SSID length = 32 Characters
- SSID1/** **/SSID2 = 64 Characters
- Access to Internet Attacker Server

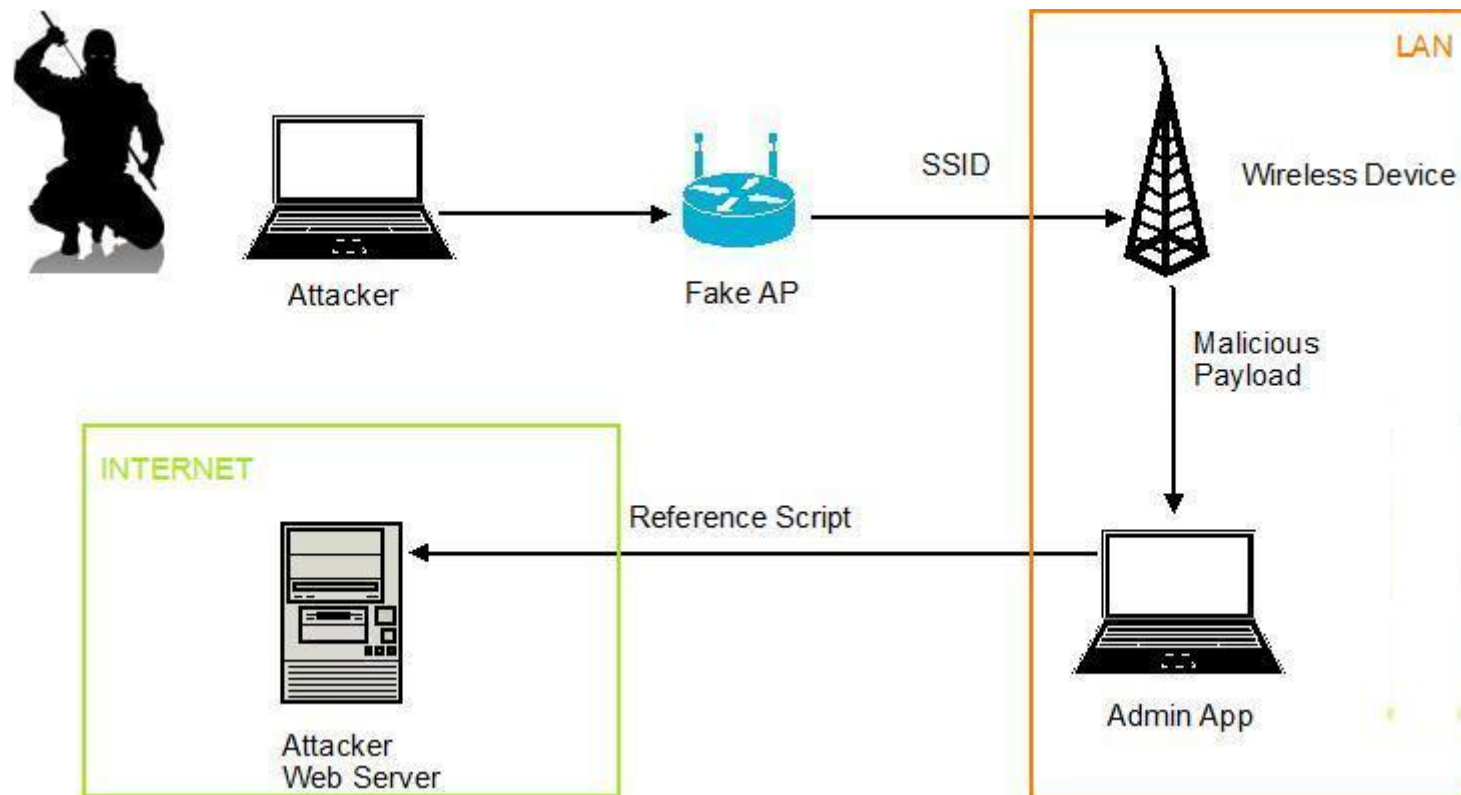
SSID Script Injection



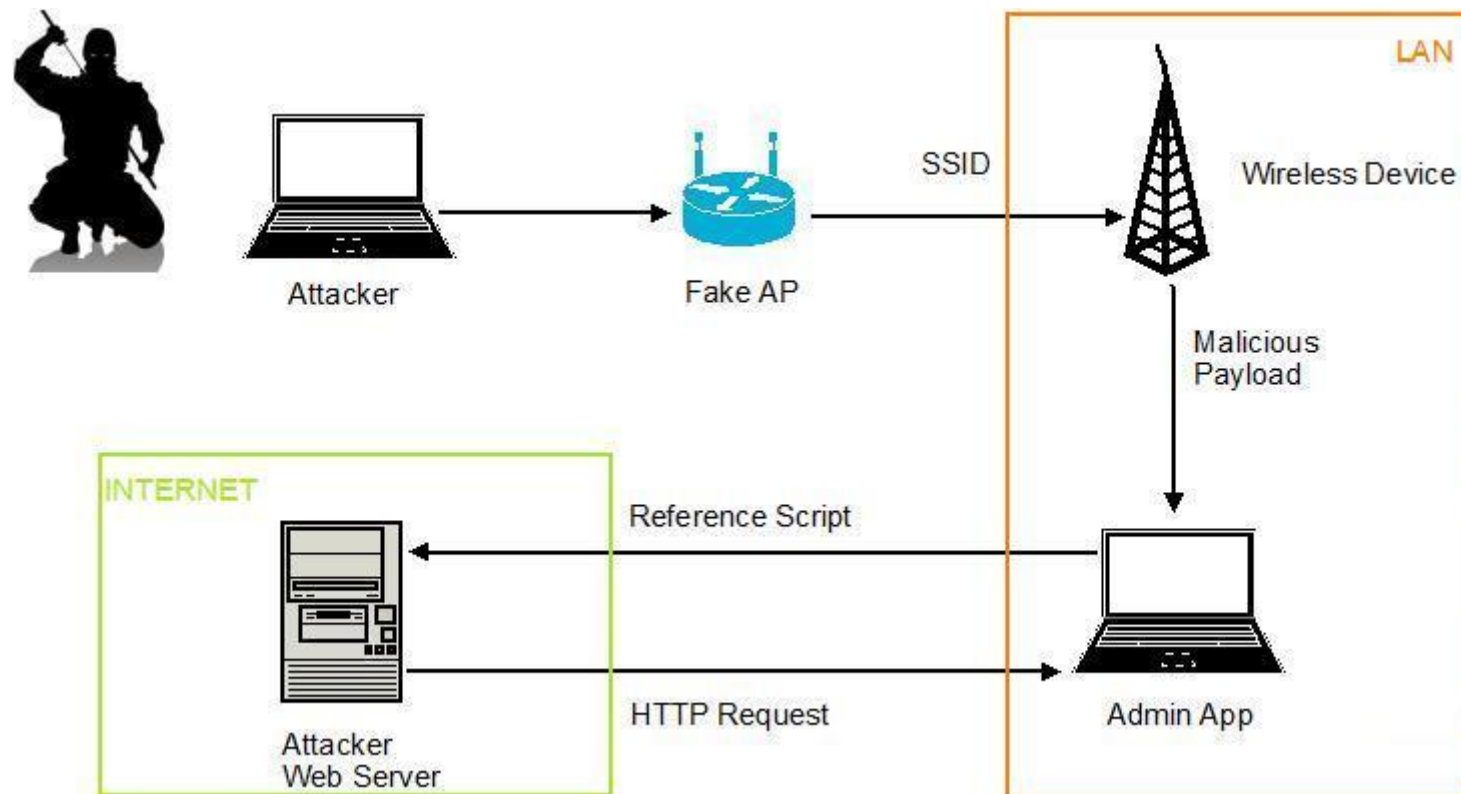
SSID Script Injection



SSID Script Injection



SSID Script Injection



SSID Attack - DEMO

- Linksys – DD-WRT firmware
- Tool
- Disable Wireless Encryption

Scanning for Webmin Servers Attack

Webmin



Scanning for Webmin Servers

Module Config

Webmin Servers

Select all. | Invert selection. | Register a new server.

<input type="checkbox"/>	 Unknown-00-02-3f-3e-1c-cd.config:10000 (edit)	<input type="checkbox"/>	 10.0.0.103:10000 (edit)
--------------------------	---	--------------------------	--

Select all. | Invert selection. | Register a new server.

Delete Selected Servers

Broadcast for servers

Click this button to automatically find any Webmin servers on your local network.

Scan for servers

Click this button to check every address on the network for Webmin servers.

Default login for servers

Default password

Webmin port

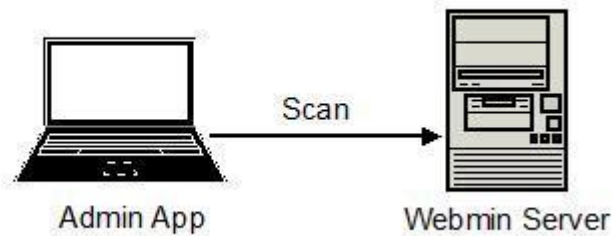
Automatically Find Servers

Click this button to setup the automatic periodic discovery of new Webmin servers on your network.

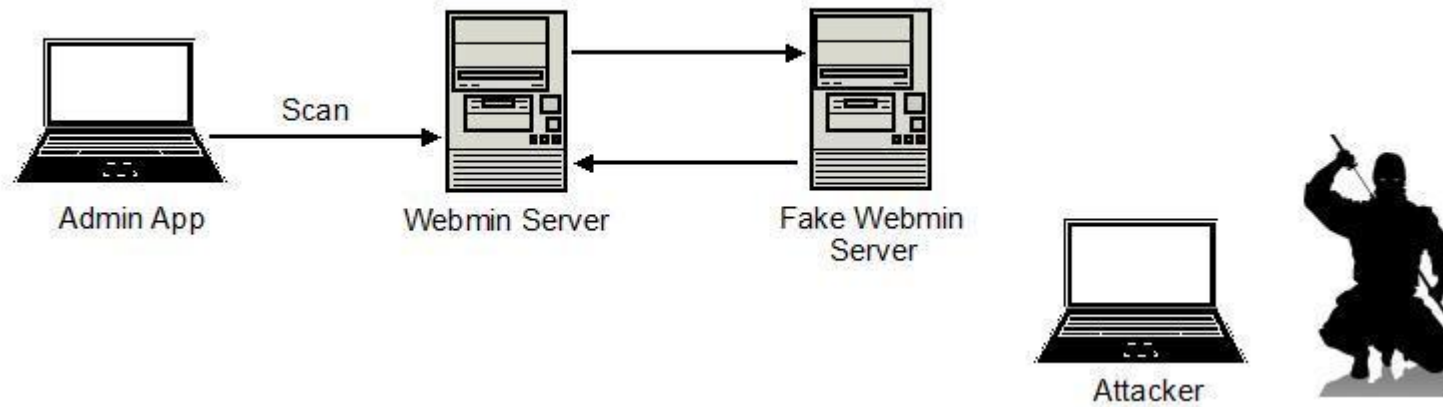
Scanning for Webmin Servers Attack

- Attacker located in same Network
- Redirect user to fake Webmin Server
- Obtain Administrator Credentials
- CSRF
 - Server Side Vulnerability - XSS
 - Client Side Vulnerability - Header Injection

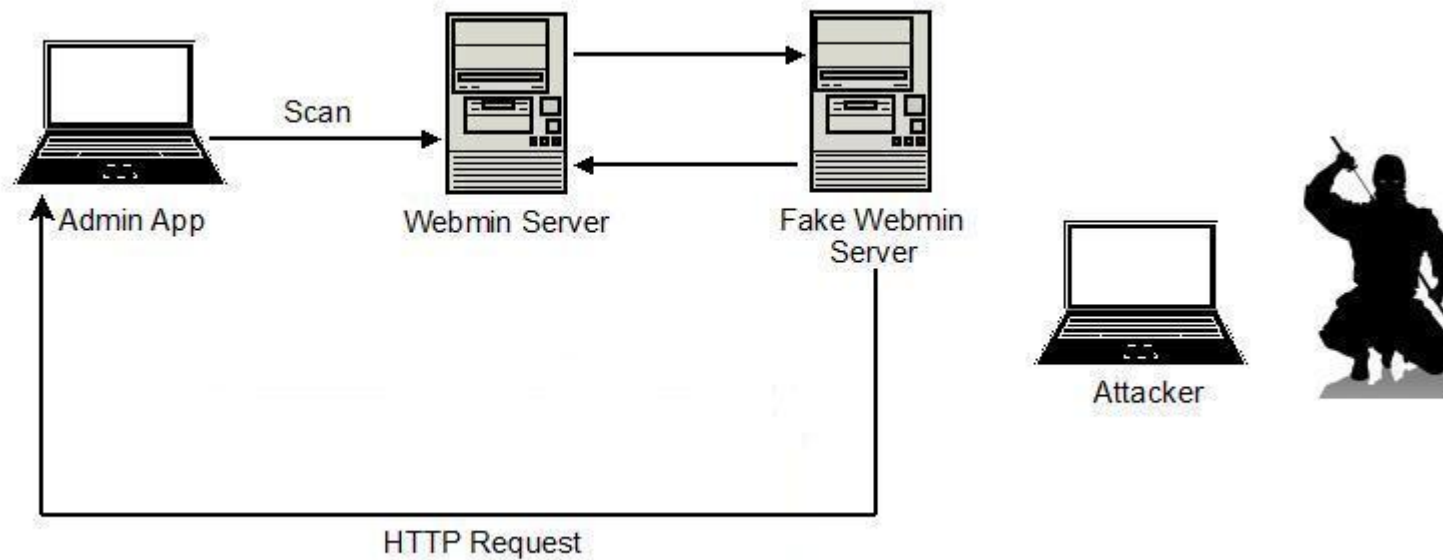
Scanning for Webmin Servers Attack



Scanning for Webmin Servers Attack



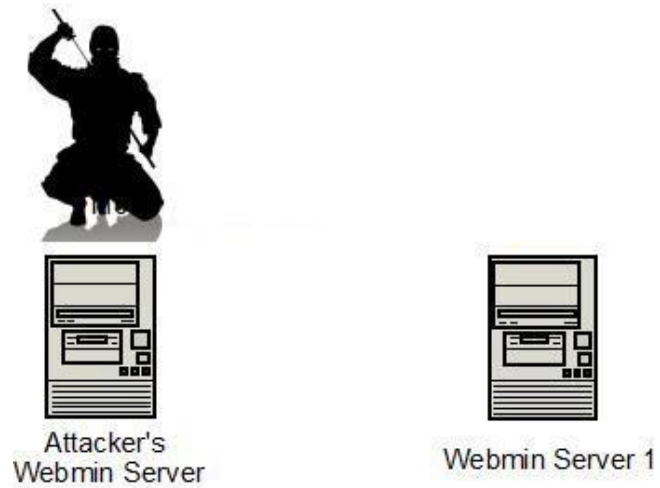
Scanning for Webmin Servers Attack



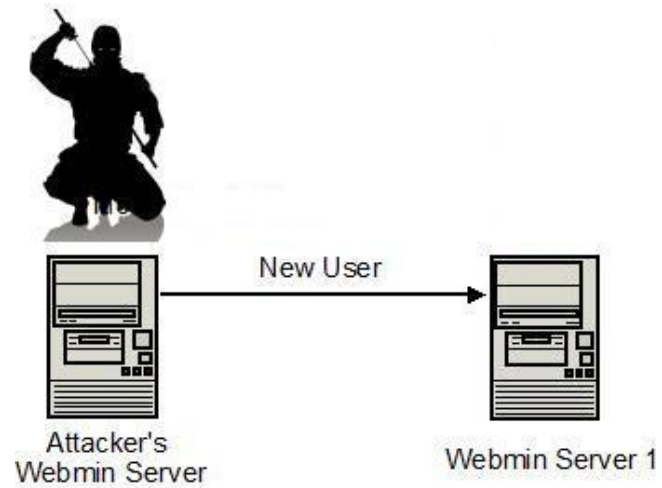
DEMO

Webmin Web Based Attack Propagation

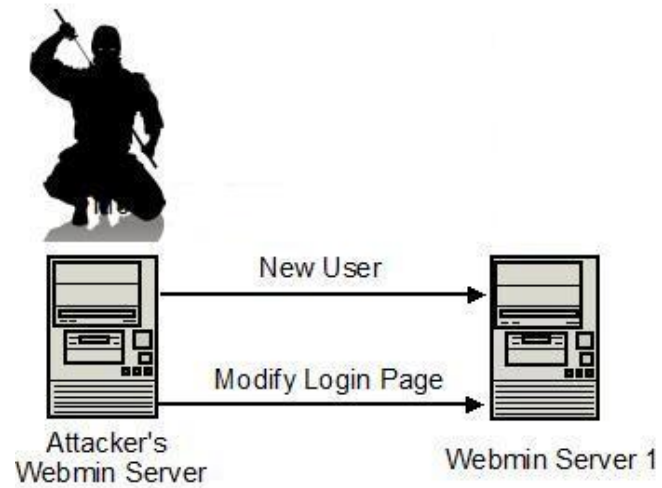
Webmin Web Based Attack Propagation



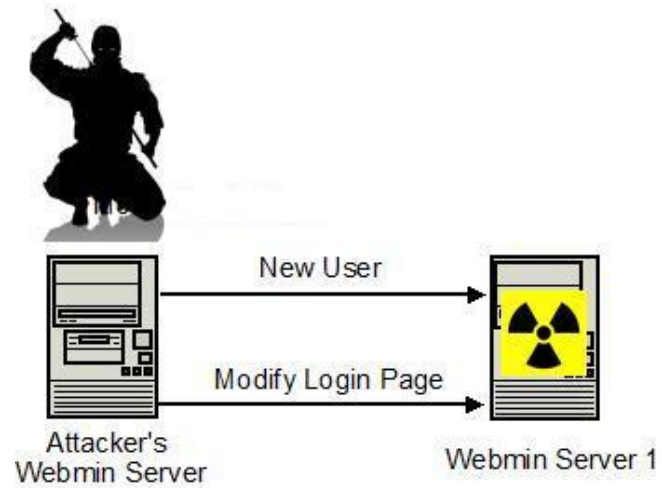
Webmin Web Based Attack Propagation



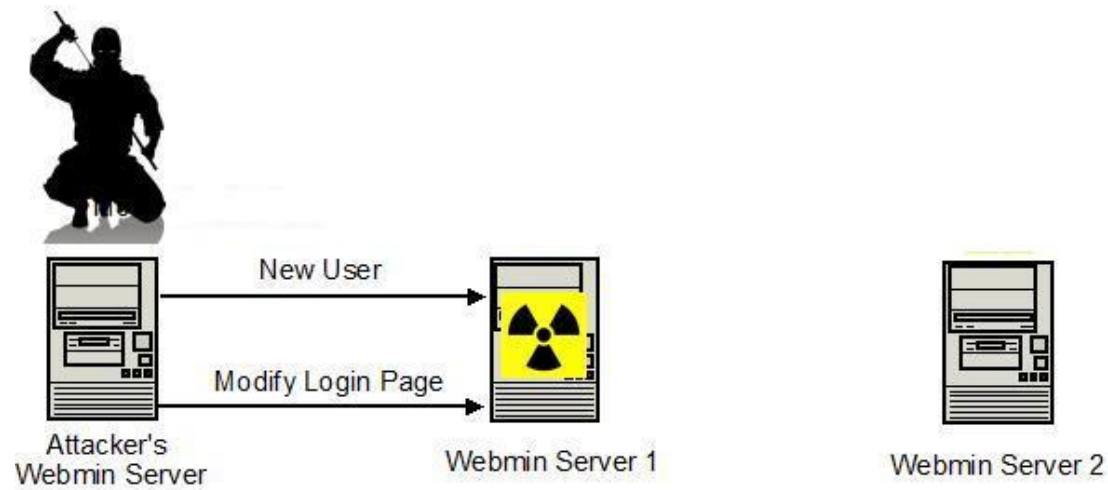
Webmin Web Based Attack Propagation



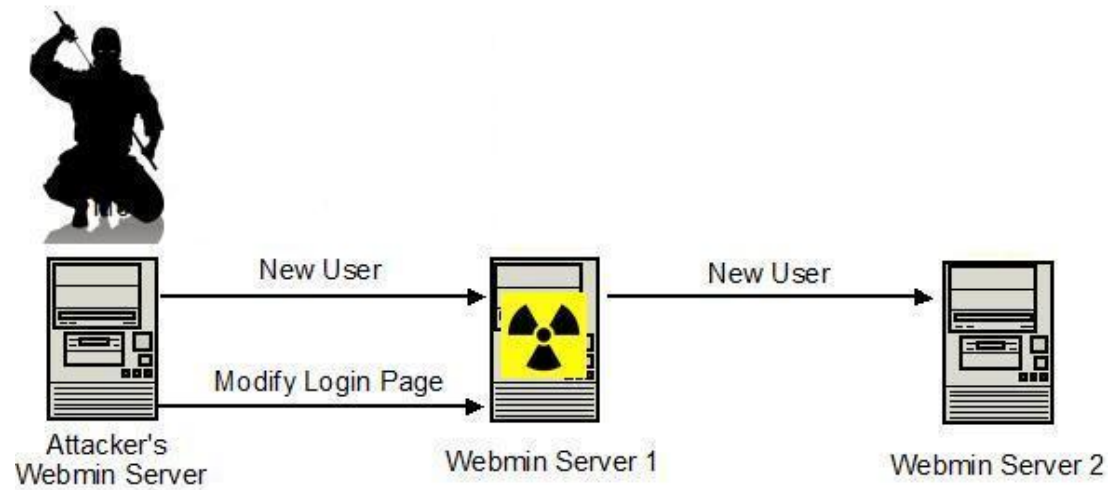
Webmin Web Based Attack Propagation



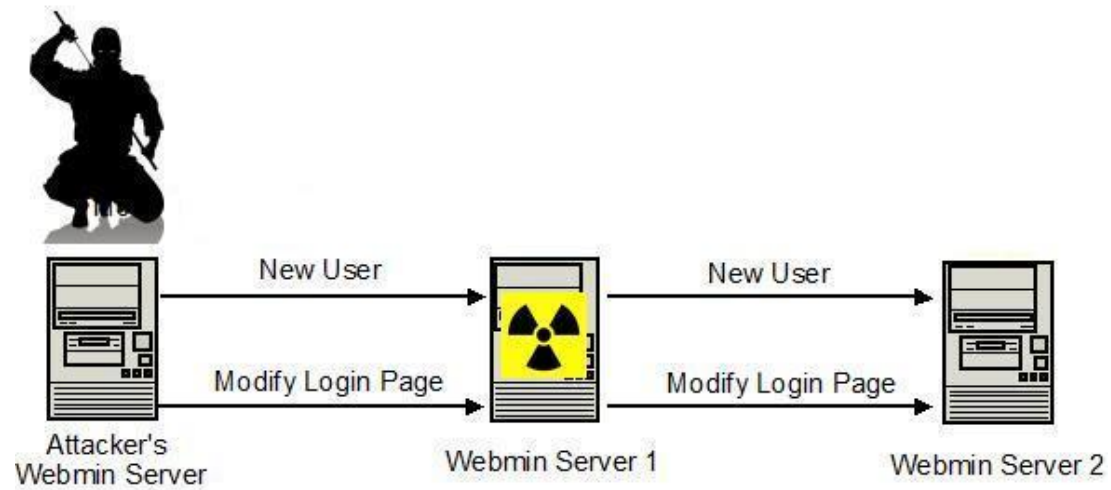
Webmin Web Based Attack Propagation



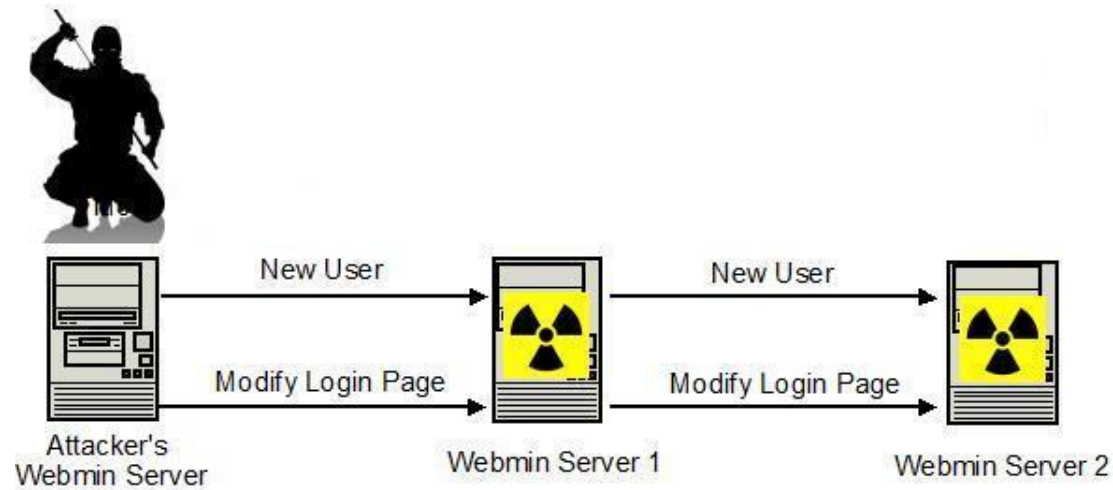
Webmin Web Based Attack Propagation



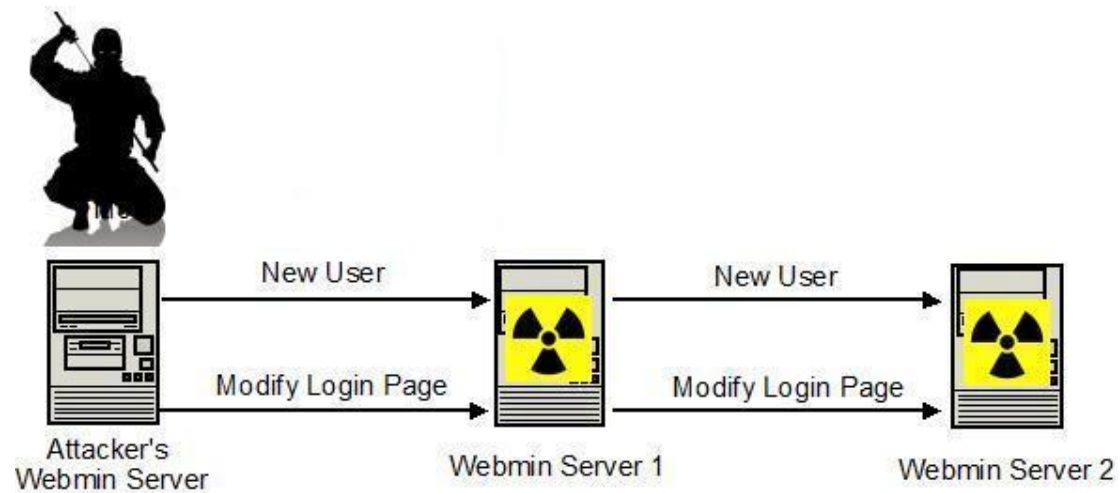
Webmin Web Based Attack Propagation



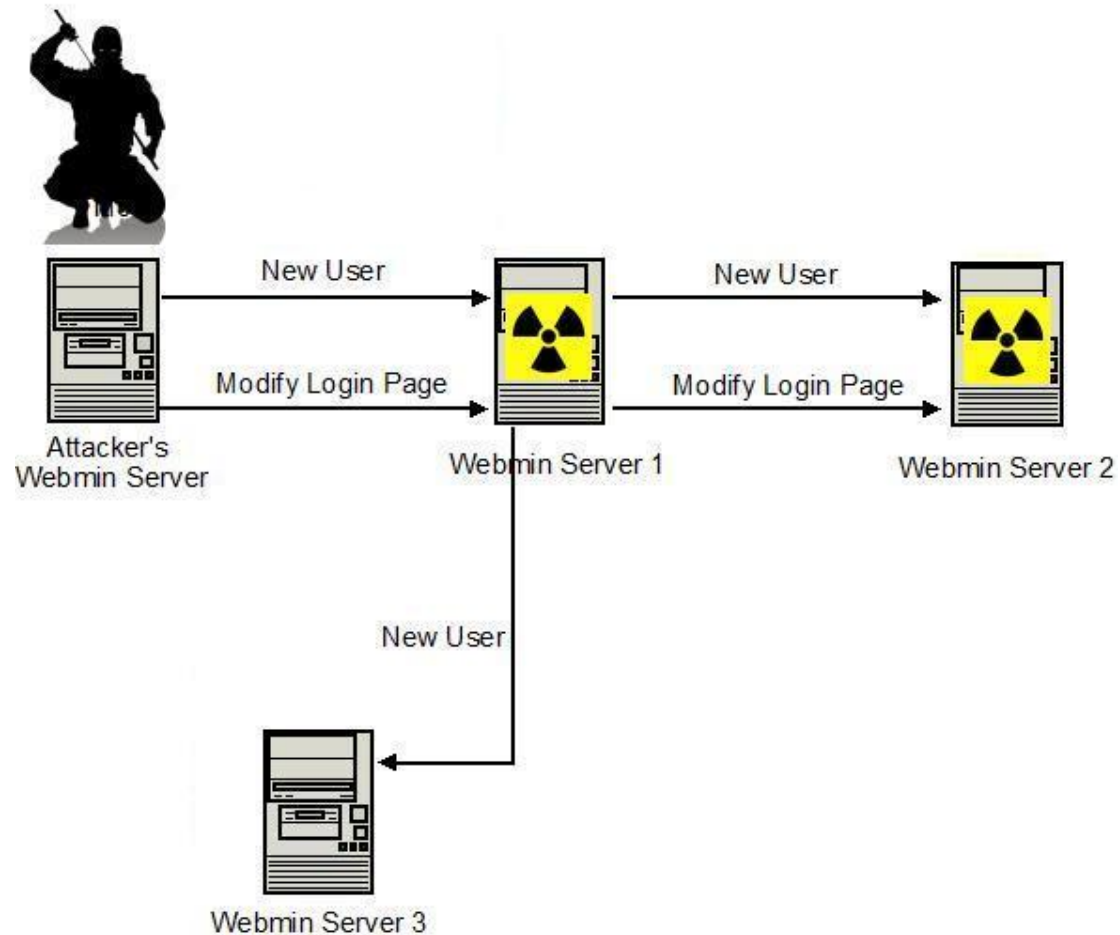
Webmin Web Based Attack Propagation



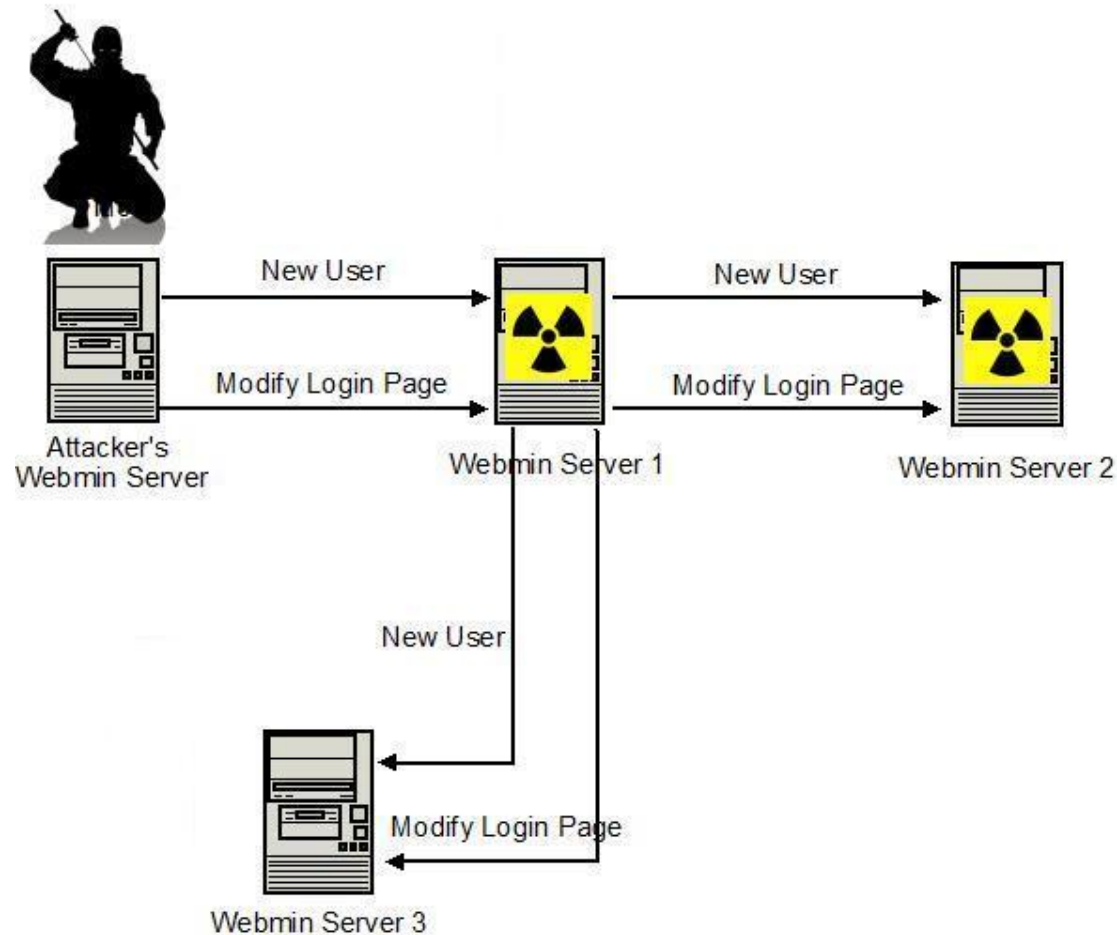
Webmin Web Based Attack Propagation



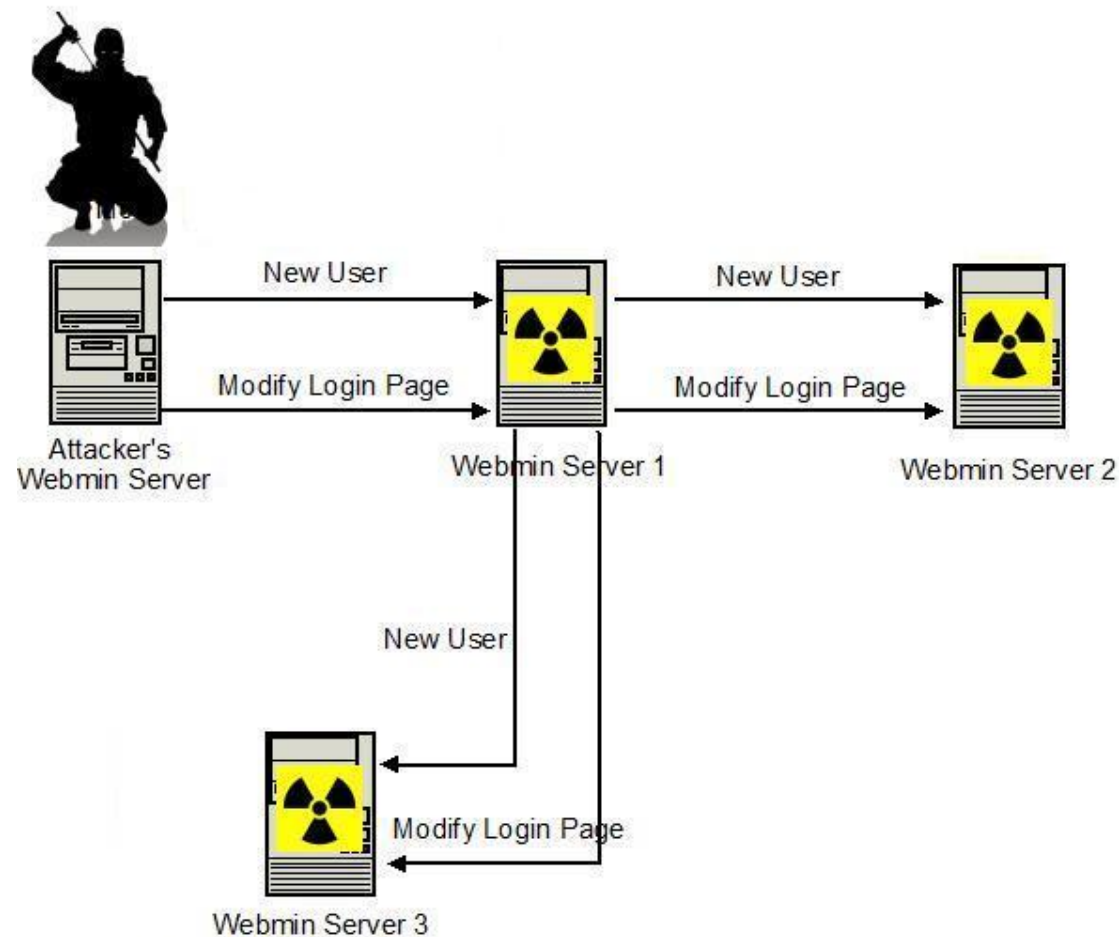
Webmin Web Based Attack Propagation



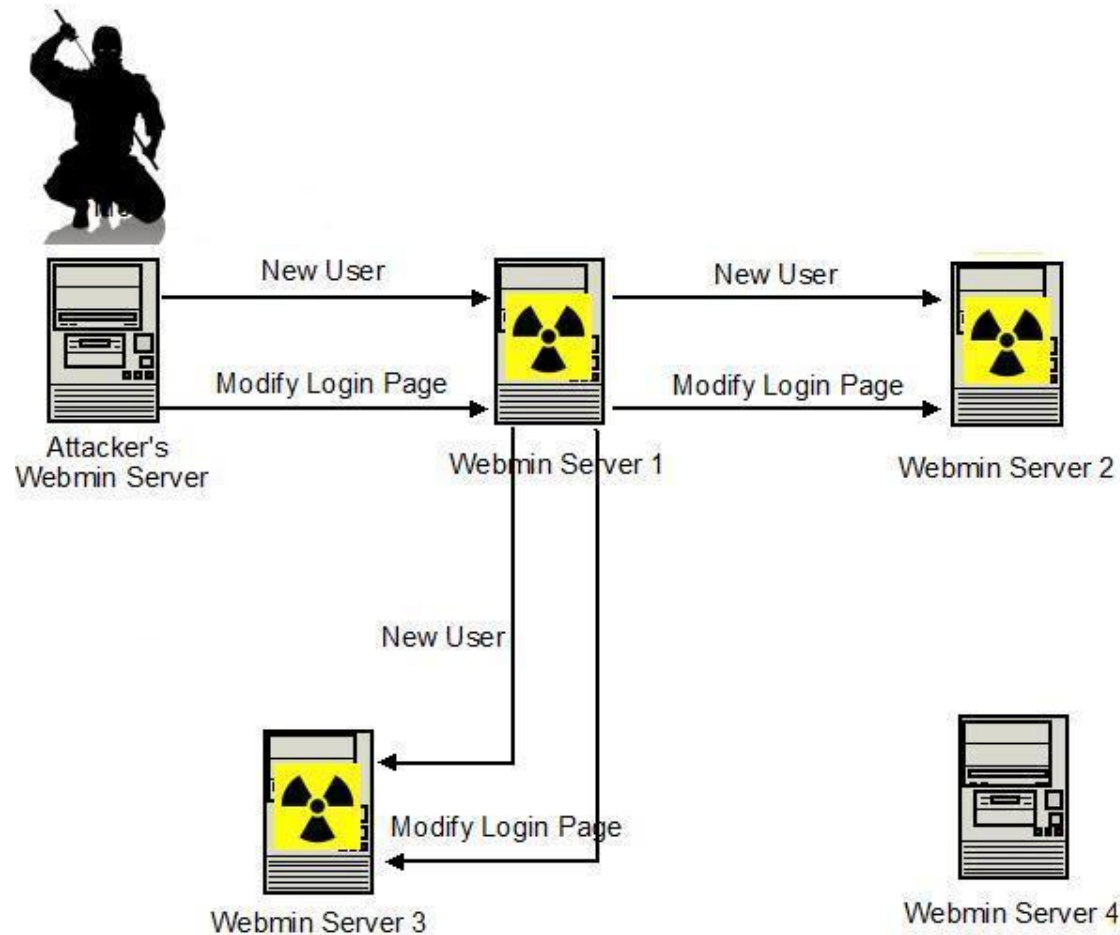
Webmin Web Based Attack Propagation



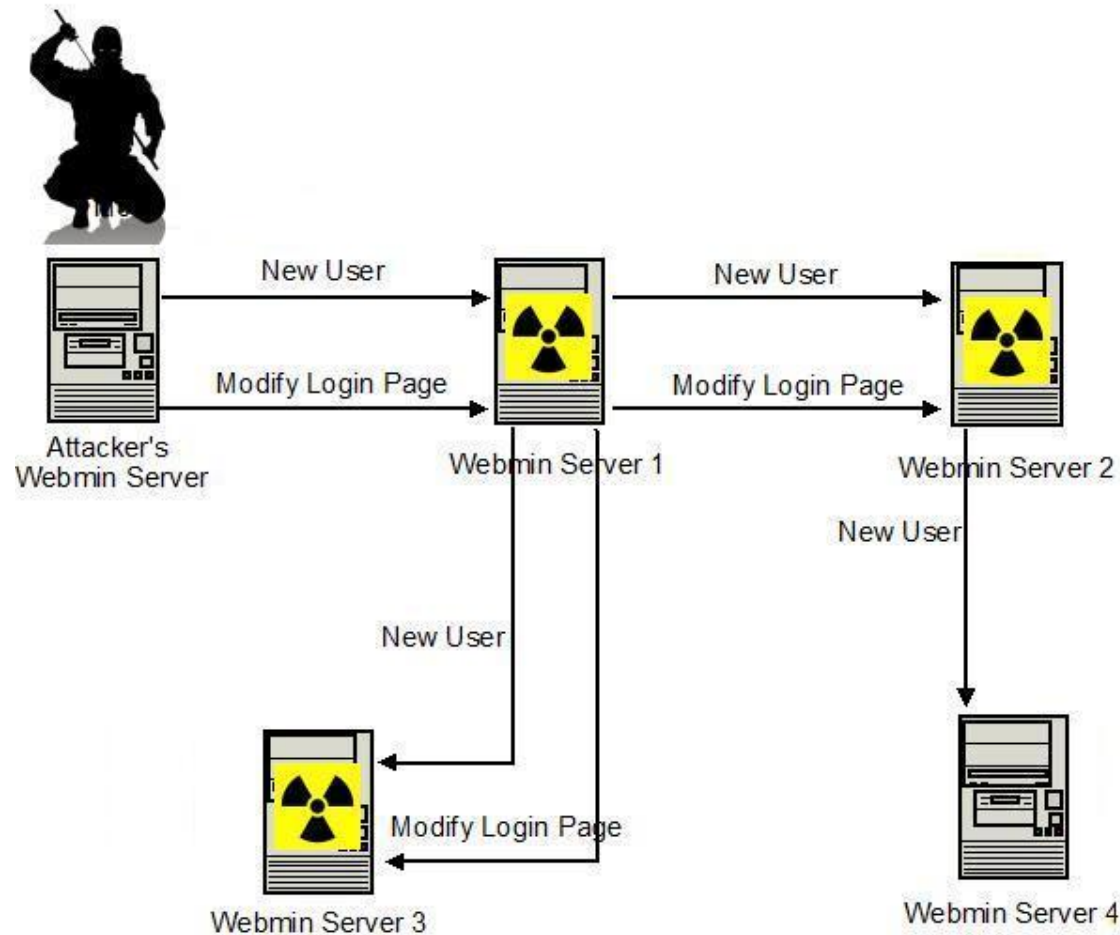
Webmin Web Based Attack Propagation



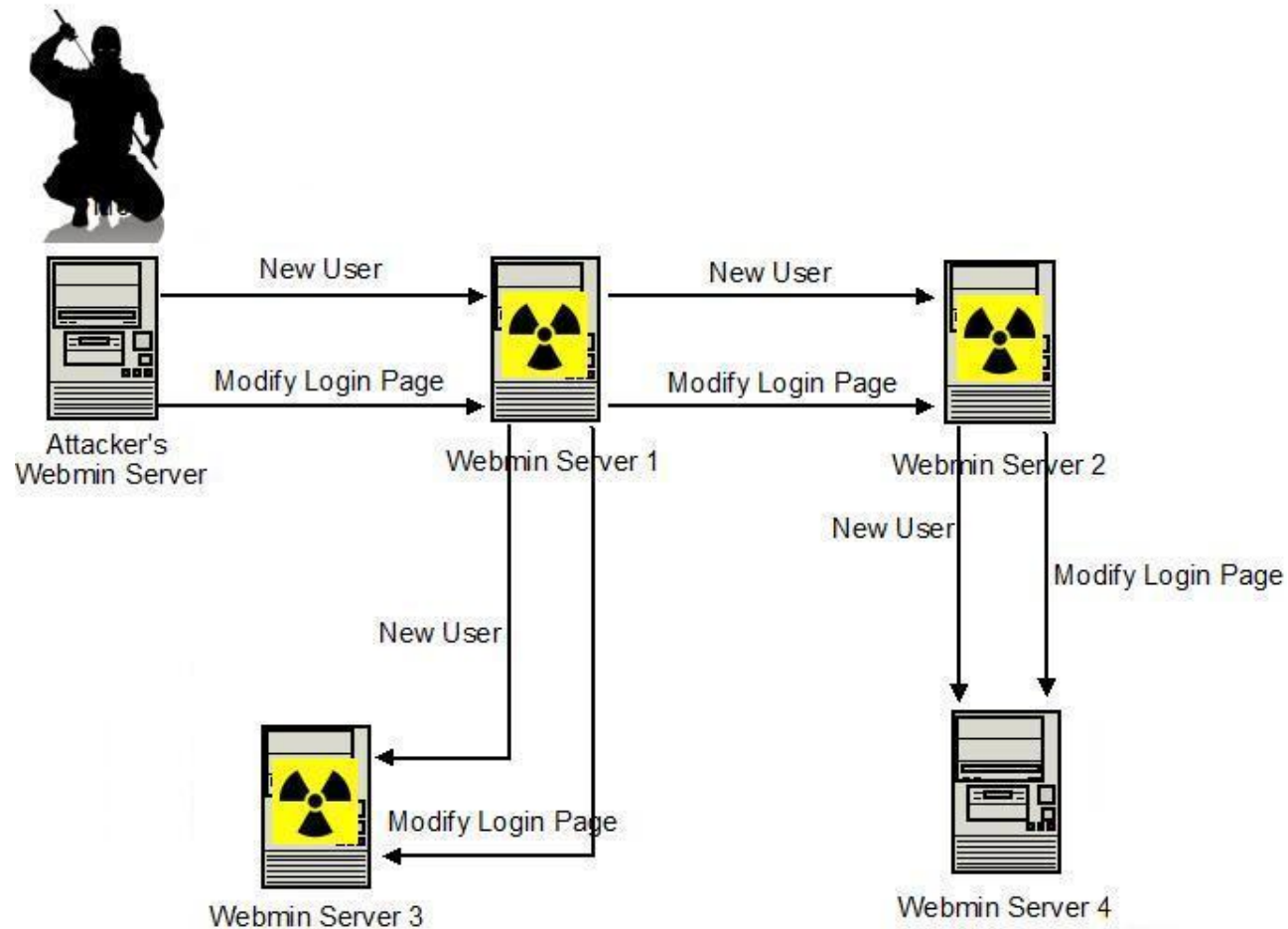
Webmin Web Based Attack Propagation



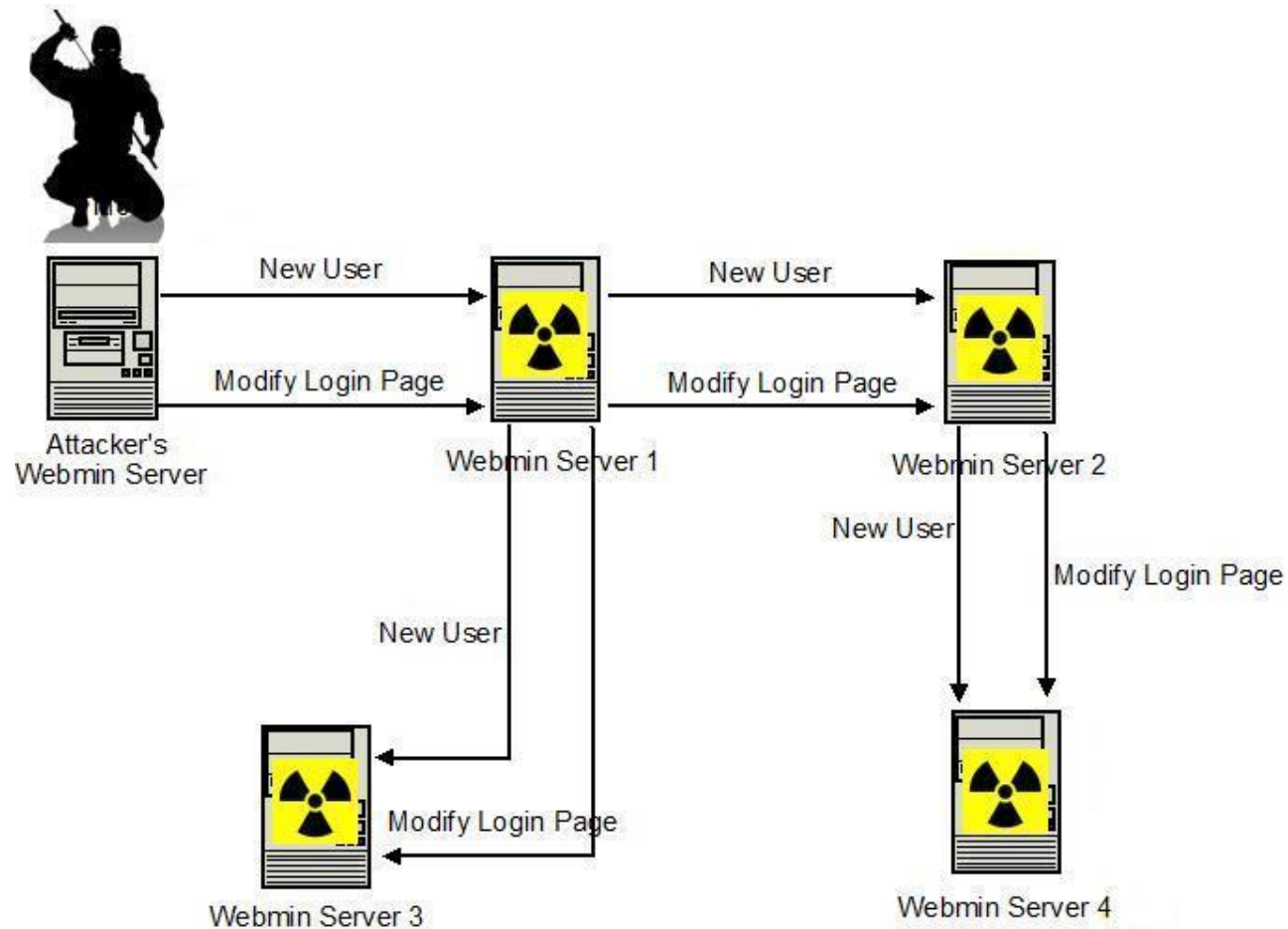
Webmin Web Based Attack Propagation



Webmin Web Based Attack Propagation



Webmin Web Based Attack Propagation



Recommendations

Recommendations



Recommendations

- Assess Deployment
- Do not Trust your Internal Network
- Penetration Testing
- Strict Security Policy
- Risk Management

Summary

- Vulnerable as any other Web Application
- Additional Attack Vectors
- “Scanning”, “Detecting “ , “Finding” Functionality
- Risks Increased
- Used in “Trusted Environment”

References & Further Reading



Project Web Site:

<http://labs.mwrinfosecurity.com/>

usefulfor.com/security

<http://usefulfor.com/security/2008/08/04/dhcp-script-injection/>

<http://usefulfor.com/security/2008/08/04/ssid-script-injection/>

Contact Me

rafael.dominguez-vega()mwrinfosecurity!com

