CompTIA

Starting Soon!

Ethical Hacking Using a Weaponized Operating System

Presented by Andrea Di Fabio

FREE Security Awareness Guide

Get 7 simple security hacks that you can use today.

bit.ly/SecurityAwarenessGuide

Ethical Hacking Using a Weaponized Operating System

1. Differences between threats and vulnerabilities
2. Pen testing do's and don'ts
3. Metasploit introduction through the Armitage GUI
4. Information gathering and scanning
5. Playing with auxiliary modules like ARP, DNS and DHCP attacks
6. Browser drive-by attack (application-based attack)
7. Remote exploit demo (application-based attack)
8. Payloads using the Meterpreter
9. Metasploit automation

Threat OR Vulnerability

End of life operating system

Threat OR Vulnerability

End of life operating system

Threat OR Vulnerability

Ransomware

End of life operating system

Threat

OR

Vulnerability

Ransomware

End of life operating system

Threat OR Vulnerability

End of life operating system

Ransomware

Unneeded running service

Threat OR Vulnerability

Ransomware

End of life operating system

Unneeded running service

Threat OR Vulnerability

Ransomware

End of life operating system

Unneeded running service

Hacker

Threat OR Vulnerability

Ransomware

Hacker

End of life operating system

Unneeded running service

Threat OR Vulnerability

End of life operating system

Ransomware

Unneeded running service

Hacker

Unlocked door

Threat OR Vulnerability

Ransomware

Hacker

End of life operating system

Unneeded running service

Unlocked door

Threat OR Vulnerability

Ransomware

Hacker

Untrained user

End of life operating system

Unneeded running service

Unlocked door

Threat	OR	Vulnerability
		End of life operating system
Ransomware		
		Unneeded running service
Hacker		
		Unlocked door
Untrained user		Untrained user

Threat

OR

Vulnerability

Ransomware

Hacker

Untrained user

Actor

End of life operating system

Unneeded running service

Unlocked door

Untrained user

Flaw or Gap

Pen testing

Do's

Don'ts

Get WRITTEN authorization

Pen testing

Do's

Get WRITTEN authorization

Get contact information

Don'ts

Pen testing

Do's

Get WRITTEN authorization

Get contact information

Define the Scope and timing

Don'ts

Pen testing

Do's

Don'ts

Get WRITTEN authorization

Get contact information

Define the Scope and timing

Review Threats and Vulnerabilities

Pen testing

Do's

Get WRITTEN authorization

Get contact information

Define the Scope and timing

Review Threats and Vulnerabilities

Don'ts

Test public cloud environments

Pen testing

Do's

Get WRITTEN authorization

Get contact information

Define the Scope and timing

Review Threats and Vulnerabilities

Don'ts

Test public cloud environments

Use payloads that cause damage

Pen testing

Do's

Get WRITTEN authorization

Get contact information

Define the Scope and timing

Review Threats and Vulnerabilities

Don'ts

Test public cloud environments

Use payloads that cause damage

Change configurations

Pen testing

Do's

Get WRITTEN authorization

Get contact information

Define the Scope and timing

Review Threats and Vulnerabilities

Don'ts

Test public cloud environments

Use payloads that cause damage

Change configurations

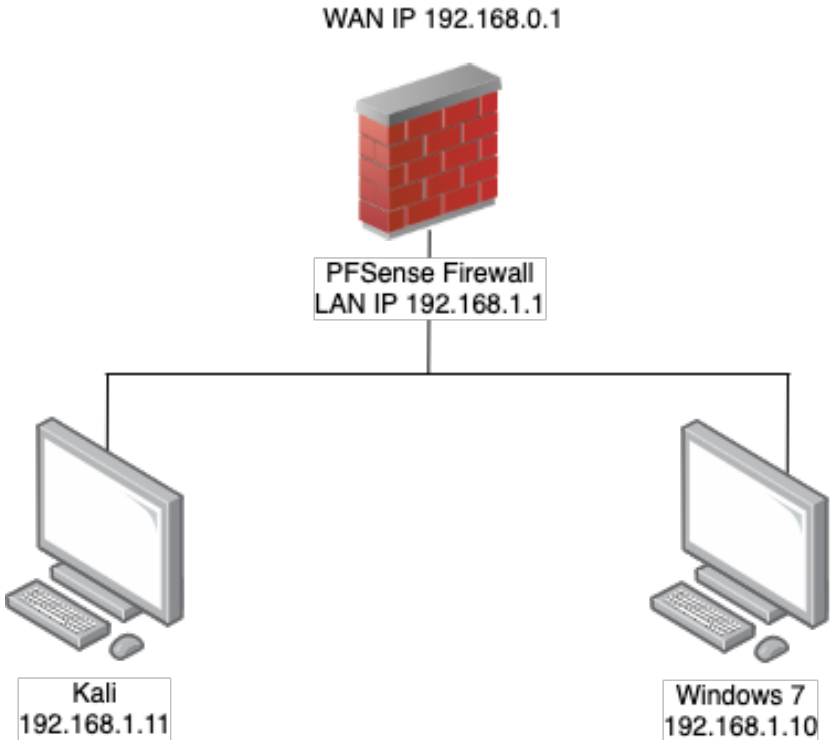
Practice in production

WARNING

Don’t test anyone’s network unless you
Get WRITTEN authorization!

Everything you see here has an IDS signature
and will trigger an alert!

Environment

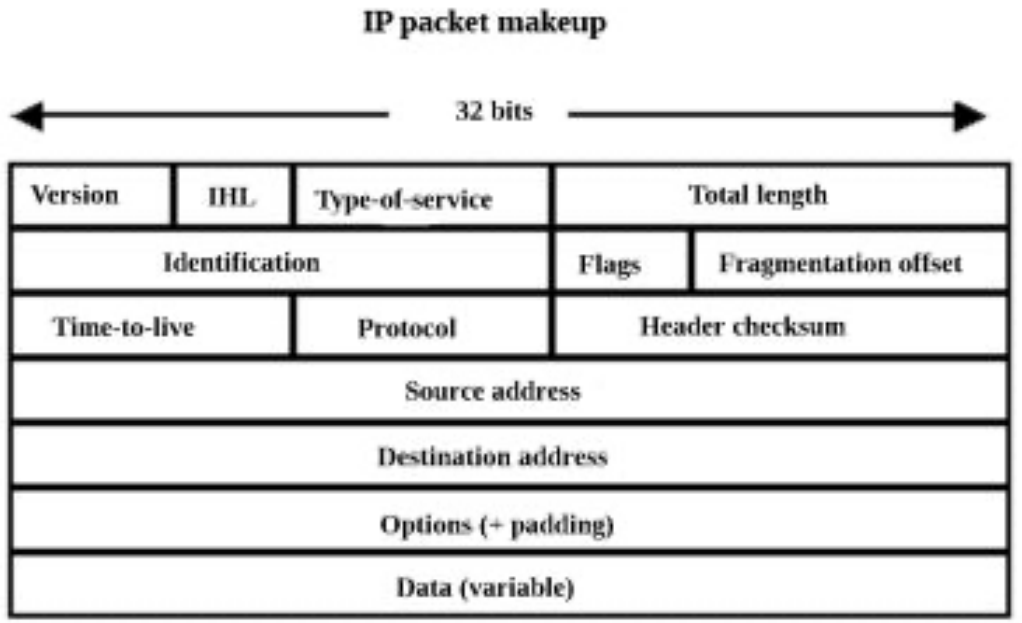


Armitage

- Live GUI Review

Information Gathering

- NMAP Again? Nah
- Let's learn Info Gathering through protocols and HPING3
  - TTLs
  - Packet ID



EternalBlue

- Leaked by Shadow Brokers April 2017. Fixed by Microsoft in May
- The vulnerability is tracked by CVE-2017-0144
- The exploit targets the Microsoft Server Message Block (SMB) protocol
- Used by WannaCry
- Let's play with it!
  - I become the threat

ARP

- Address Resolution Protocol (ARP)
- RFC 826 from 1982 https://tools.ietf.org/html/rfc826
- Layer 2 of the OSI
- Used to find the hardware address or Media Access Control (MAC) address
- ARP cache
- MAC looks like 11-22-33-44-55-66
  - First 3 octets are the OUI
- Mitigation: Dynamic ARP inspection
  - On supported cisco devices: IP ARP INSPECTION VLAN 100

DHCP

- Dynamic Host Configuration Protocol (DHCP)
- First implemented in the Bootstrap Protocol BOOTP in 1985 RFC 951
- Last updated in 1997 with RFC 2131 https://tools.ietf.org/html/rfc2131
- Layer 7 of the OSI
- Uses Broadcast
- DHCP Relays turn broadcast into unicast to remote DHCP servers
- Mitigation: DHCP Snooping
  - On supported cisco devices: DHCP SNOOPING VLAN 100

DNS

- Domain Name System (DNS)
- First implemented in RFC 882 in 1983
- Last updated in 1997 with RFC 2181 https://tools.ietf.org/html/rfc2181
- Layer 7 of the OSI
- Hierarchical and decentralized

Question & Answer

Ask your questions in the Q&A chat box!

See You Next Time!