PIG: Finding Truffles Without Leaving A Trace

Ryan Linn
DEFCON 19
Overview

- Introduction
- Why are we here?
- How will this help me?
- Talking is boring show me
- That’s neat, how does this work?
- Protocols and Plugins
- Remediation
Introduction

**Ryan Linn / Senior Security Consultant at Trustwave**

- Member of SpiderLabs team at Trustwave
- Contributor to Metasploit, BeEF, and other open source projects

**Interests:**

- Process streamlining through tool integration, sharing knowledge, Metasploit, making security knowledge accessible

- Twitter: @sussurro
- Web: [www.happypacket.net](http://www.happypacket.net)
Why are we here?

Passive Network Information Gathering
- Identify hosts/resources on a network
- Profile individuals/applications
- Determine network architecture
- Machine/domain/individual naming schemes

Completely Silent
- No IP address required
- No Man-In-The-Middle required
Why are we here?

- Understand what is on your network
- Deep Packet Parsing sounds like fun
- Make this information easier for everyone to access
- How to leverage this for pen tests
- Waiting here for the next talk..
How will this help me?

SysAdmin/User

• Know what traffic you are transmitting
• Are you tipping your hand by just being on the network?

Pen Tester

• Understand what information you can use to profile a network without anyone knowing you’re there

Everyone

• Make this process easier
• Use Metasploit Database to help process/manage data
• Organize and manage results with Dradis
• How to stay quiet on a network
Talking is boring, show me

Demo Time

- Demo 1 – Gathering Data
  - Use Metasploit PIG modules to parse traffic and save data to the database
- Demo 2 – Viewing data with Metasploit
  - Use Metasploit msfconsole to view collected data
- Demo 3 – Using Dradis to view information
  - Import Metasploit data into Dradis to view data
- Demo 4 – PWN Plug and PIG
That’s neat, how does this work

Metasploit framework plugin
  • Core auxiliary module that handles sniffing

Helper filters
  • Series of individual filters that handle protocol parsing
  • Each protocol sets sniffing parameters so that not everything goes to every filter

Let’s take a look
  • Demo time
    – Look at structure of building a simple parser
Dig Deeper

Currently supported filters

- CDP
- DHCP Inform
- Dropbox
- Groove
- MDNS
- SMB
- SSDP
Dig Deeper

**CDP / Cisco Discovery Protocol**
- OS Version
- IP address information
- VLAN Information
- Management Interface information
- VOIP vlans
- Can aid in VLAN Hopping
Dig Deeper

DHCP Inform

• Not completed yet, but
• Will pull out:
  – Mac address
  – Hostname
  – Vendor class
  – Request list
• Together can be used to guess OS and Service Pack
Dig Deeper

Dropbox

- Easily identify hosts using Dropbox
- Dropbox version
- Dropbox port
- Shared namespaces
Dig Deeper

Groove

• Online/Offline status
• Groove Port
• All addresses on the system
  – Can be used to identify boxes with VMs, link hosts together
• Groove Version
Dig Deeper

MDNS

- One of most interesting
- List open ports
- IP Addresses
- Peoples Names
- Active State of Machine
- Available Functionality
Dig Deeper

SMB

• Host OS Version
• Server/Client Status
• Hostname
• Domain Name
• SQL Server ?
Dig Deeper

SSDP / Simple Service Discovery Protocol (UPNP)
- AKA Network Plug and Play
- Printers
- Cameras
- Network Gateways
How do we fix it

Netbios
  • Disable Netbios over TCP

SSDP
  • Disable network plug and play

CDP
  • Enable it only where needed

DHCP
  • DHCP Helpers can limit where these packets go

Dropbox
  • Disable LAN Sync

Groove
  • Haven’t found a way

MDNS
  • Disable it when possible, may not always be an option
How to help

Need more data
  • Broadcast and Multicast traffic only

DHCP Host ID

More protocols
Future

Add functionality to Meterpreter
  • Meterpreter has sniffing capabilities, work on post module

More protocols
  • Collect data
  • ???
  • Profit

Better OS ID
  • Improve guessing with DHCP
Resources

Code
  • http://www.happypacket.net/Defcon2011.tgz

Metasploit
  • http://www.metasploit.org

Book
  • Coding for Pen Testers comes out in Oct!
Questions

Thanks for attending
Thanks to DEFCON staff
If you want to talk more head to follow-up room