SIGPwny

Purple Team FA2025 • 2025-09-18

Wireshark & Detecting Lateral Movement

Bryce Kurfman & Michael Khalaf

Announcements

- Cyber Range is back up and running, as the server has been placed at Siebel. Cyber Range is **NOT** accessible outside of IllinoisNet. If there is demand we will email engrit to open it up.

- DoE CyberForce registration is in progress. We are seeking approval to bring a second team in addition to the priority roster. If so…we will post an announcement and evaluate who is interested and ready.

- Hivestorm is cancelled this year (2025-26) and is expected (2026-27)

ctf.sigpwny.com

sigpwny{sniffin_packets}

Table of Contents

Network Forensics

The What

- Network forensics entails the monitoring and analysis of **computer network traffic** for the purposes of information gathering, legal evidence, or intrusion detection
- Traffic capturing is usually real-time.
- Forensics involves retroactively looking at the capture, discovering and mapping of adversarial presence in any infrastructure.
- The goal is to establish a timeline accounting for all actions taken by the adversary
  - This means pulling together digital “artifacts” to support the investigation and remediation
  - These findings are often reported to C suites.

The Why

- Investigating network traffic can help us identify **sus**picious activities and unauthorized intrusions **among us**
- This becomes especially important if logs and other artifacts from a compromised host are deleted
  - We can attempt to reconstruct events via externally saved network activity
- Understanding **sus**picious traffic pattern allows us to set up firewall rules to block them in the future, preventing similar incidents from happening again

The How

- Proactive Detection
  - **Continuously** surveil network data to find indicators of compromise as early as possible
  - Use spikes in data transfers, strange communication with external IPs, network threat signatures, etc. to locate malicious activity **as it occurs**
- Post-Incident Forensics
  - Review data collected from an incident to understand the situation and determine how best to respond
  - It often helps to correlate the stages of an attack with the **MITRE ATT&CK** framework to help deduce an attacker's actions and capabilities

Network Data Types

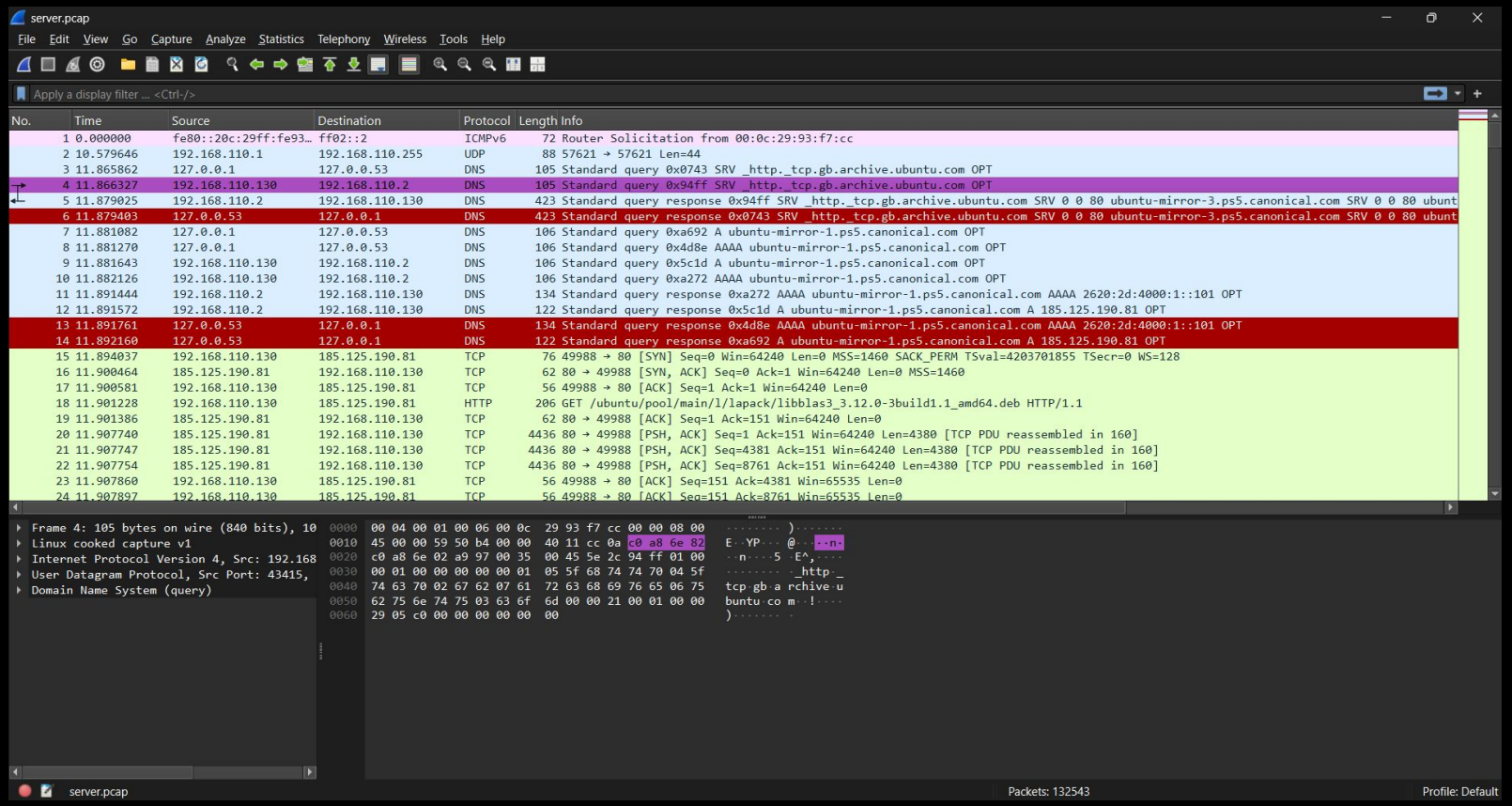
- Packet Capture (pcap)
  - Stores captured raw network packet data
  - Preserves all packet details like headers, payloads, and timestamps
  - Very resource intensive to collect and process at scale
- Next Generation pcap (pcapng)
  - Newer than pcap and supports advanced features like:
    - Ability to store packets with different link layer types, such as Ethernet and 802.11 WiFi packets
- Netflows
  - Only captures the metadata about IP traffic
    - Source and destination IP address, ports, protocol type, number of packets and bytes transferred, timestamps, etc.
  - More cost-effective and scalable

Wireshark

Wireshark

- Wireshark is a powerful, open-source network protocol analyzer that allows users to capture and interactively browse the traffic running on a computer network
- It has protocol dissectors for most all common protocols like HTTP, HTTPS, DNS, ARP, etc.
  - Also has capability to create user-defined dissectors for anything funky that comes up
- Wireshark allows you to visualize OSI components within each communication instance

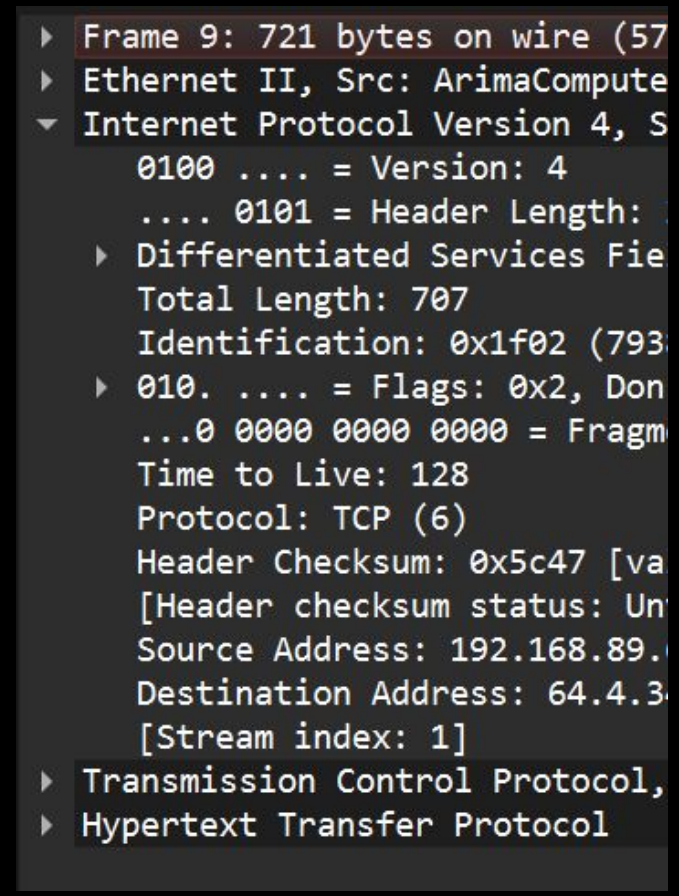
Interface



Wireshark Packet Capture

Protocol Hierarchy

- Provides a hierarchical breakdown of all the protocols present in a given network capture
  - Lower level protocols like Ethernet will be at the top
  - Higher-level protocols at the application layer like SMB will be sandwiched closer towards the bottom
- These protocols are presented in the form of various dropdown portions of the page
  - You can expand these to investigate each portion (headers, payload, footers, etc)



Protocol Hierarchy

Protocol	Percent Packets	Packets
Frame	100.0	40294
Ethernet	100.0	40294
Internet Protocol Version 4	100.0	40294
User Datagram Protocol	0.1	48
NetBIOS Datagram Service	0.0	5
SMB (Server Message Block Protocol)	0.0	5
SMB MailSlot Protocol	0.0	5
Microsoft Windows Browser Protocol	0.0	5
Link-local Multicast Name Resolution	0.0	1
eXtensible Markup Language	0.0	14
Dynamic Host Configuration Protocol	0.0	1
Data	0.1	27
Transmission Control Protocol	99.9	40239
NetBIOS Session Service	93.5	37688
SMB2 (Server Message Block Protocol version 2)	93.5	37686
Data	45.7	18408
SMB (Server Message Block Protocol)	0.0	2
Distributed Computing Environment / Remote Procedure Call (DCE/RPC)	0.4	177
Service Control	0.4	142
DCE/RPC Endpoint Mapper	0.0	10
Data	0.0	5
Internet Group Management Protocol	0.0	7

Establishing Baselines

- Before we get too deep in the weeds, we need to attain a general idea of what is going on to find deviations easier
- Determine:
  - Top Talking IP Address
    - Statistics > Endpoints
  - Device-to-Device Communication
    - Statistics > Conversations
  - Used Protocols
    - Statistics > Protocol Hierarchy
- This helps us find any stark anomalies off the bat, for example if x.x.x.x IP is sending 200GB of data to a Russia IP over DNS

Finding IoCs Basics

- Different protocols, **different artifacts**
  - HTTP/HTTPS: Suspicious domains, unusual URIs, odd User-Agents, web forms/login attempts
  - DNS: Excessive lookups, queries for known malicious domains
  - SMTP/Email: Malicious attachments, spoofed headers, unusual sending patterns
  - SMB/FTP/SSH: Unauthorized file transfers, brute-force attempts, odd access times
- Each protocol has its own "normal" behavior—knowing the baseline helps spot anomalies
- Many adversaries would use automated tools for data transfer - this means it’s broken down into packets of same size and set interval.

Nmap

What is Nmap?

-Network Mapper (Nmap) is an open source security auditing tool that sends especially crafted packets to target systems over a network

-These packets help return information about target systems: OS, running services, and open ports

-You then use information about these services and ports to determine any points of entry into a network

-As a defensive measure, you can use nmap to conduct assessment of vulnerabilities

Nmap: TCP & UDP Scans

- We’re primarily interested in two different scan types Nmap allows us to do: TCP and UDP scan
- The TCP scan is a SYN scan. To execute this scan, nmap will utilize the 3-way handshake to initiate via a SYN flag and await for SYN/ACK flags as a response from target IPs

- As for a UDP scan, nmap will utilize this broadcast protocol to identify open/closed ports
- We see PORT, STATE, SERVICE in the output

Why Nmap?

-When you conduct an assessment of the IPs on a network's ports and services, you must ask the following questions:

  -Is this service essential for my business/organization?

  -"Just how open is my network?"

-Adversaries start here to find information about a network topology to decide later where to eventually pivot

-What can you a do?

-As an organization, maybe you can only allow specific folks within to run these commands so that there isn't a public capability to perform scans on your network. You can set up alerts when scans are being performed

Demonstration

-When you pair this with Wireshark (perform a scan while capturing live), you can see some of the traffic nmap will send to X systems

-Make note of Nmap's command page

→ *man nmap* ←

→ *nmap -h* ←

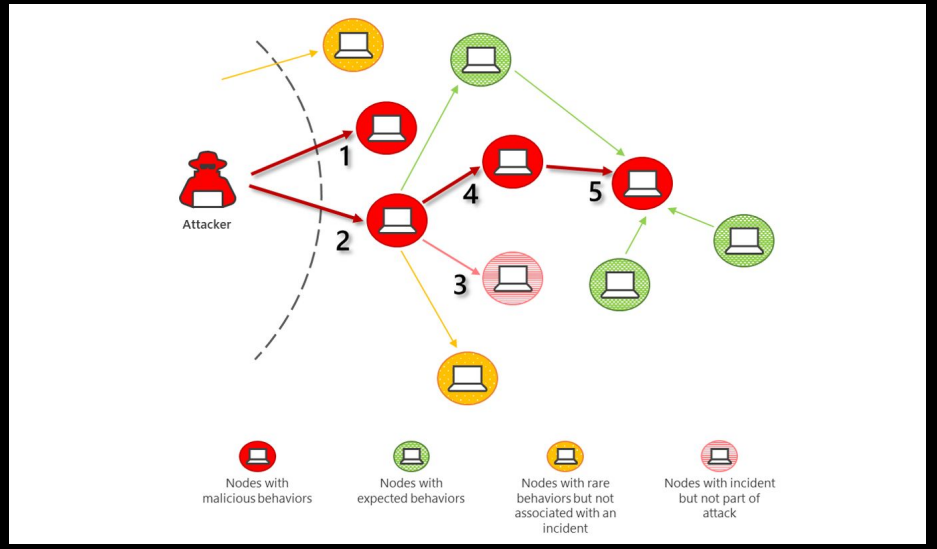
Lateral Movement

What is Lateral Movement

- add stuff here TODO
- TLDR: lateral movement is when an attacker logins to another computer with stolen creds
- e.g. SSH, VNC, RDP, etc.
- Depending on a target's network segmentation, generally an adversary wants to know which devices to pivot to. Their success at doing so is known as *lateral movement*.
- We will cover PSexec today, which is a way to login through windows SMB services.

What is Lateral Movement (TA008)

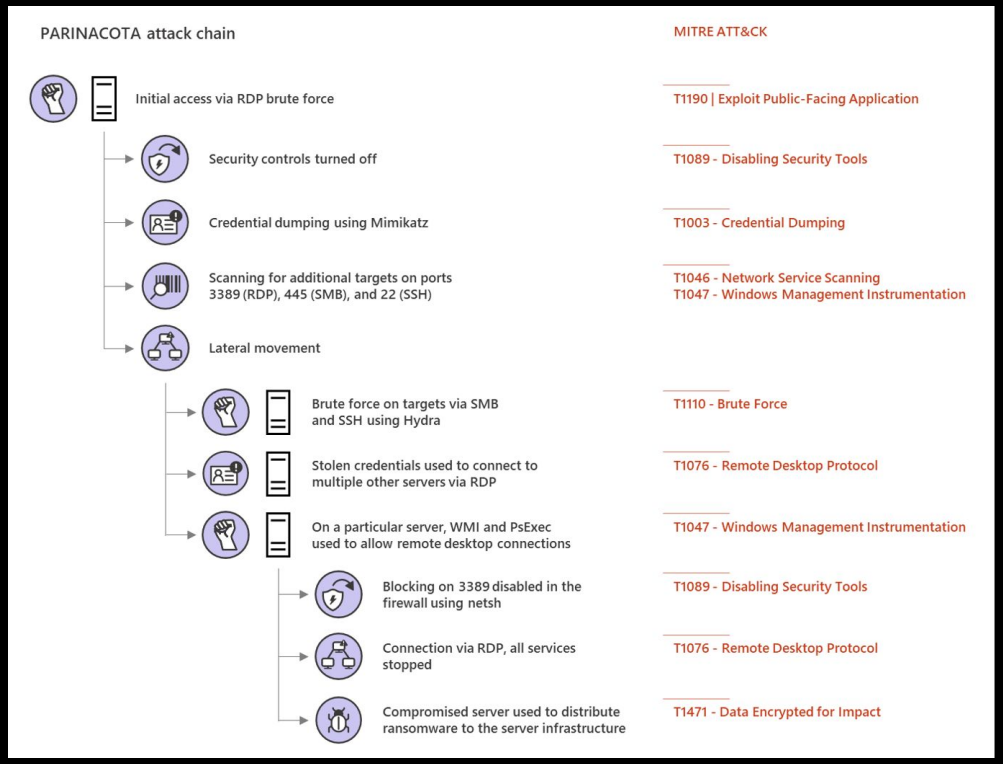
- Lateral movement is the process where attackers spread from an entry point to other parts of the network
  - This often occurs with previously stolen credentials over valid services that are already running in an environment, e.g. SSH, VNC, RDP, etc. (T1210)
  - We will cover PsExec today, which is a way to login through Windows SMB services.



[Microsoft]

What is Lateral Movement (TA008)

- Depending on a target's network segmentation, generally an adversary wants to know which devices to pivot to
  - Requires additional network recon from **inside** the target network
  - The end goal is to gain access to valuable systems and data



[Microsoft]

Intro to PsExec

What is PsExec

- **PsExec** is a lightweight telnet replacement that lets users execute processes and launch interactive command prompts on other systems over SMB without having to manually install client software
- Is a legitimate tool for system administrators to remotely:
  - Deploy and update software
  - Modify system configurations
  - Execute diagnostic tools and access event logs
  - etc.
- Because it is so powerful, **attackers also use it** to execute commands and run malicious payloads using stolen credentials
  - This helps attackers blend in with legitimate admin activities as well

How PsExec Works

- PsExec establishes an Server Message Block (SMB) connection to a target host over TCP port **445** with the appropriate admin credentials
  - PsExec -s \\MACHINE-NAME -u USERNAME -p PASSWORD COMMAND
- After successful authentication, PsExec temporarily places a process called **PsExeSvc.exe** to the target's **ADMIN$** share
  - This service acts as an intermediary to facilitate remote code execution
  - It needs admin privileges otherwise PsExec can't install/register the service

How PsExec Works

- **PsExeSvc.exe** is then launched and establishes named pipes stdin, stdout, stderr between the initiating and target system
  - It uses the SMB file sharing and named pipe mechanisms to establish channels to send commands and receive responses
  - Pipes are in the form: \\<IP>\pip\PSEXESVC…
  - These pipes are **critical** in identifying renamed versions of PsExec or clones with the same functionality like RemCom, PAExec, or CSExec who have similar named pipe conventions
- Note that PsExec's first run on a system prompts acceptance of the PsExec EULA that leaves a permanent trace in the sending host
  - *\\PsExec\\EulaAccepted*

How PsExec Works

- After installing the service, PsExec relies on a second authentication step for when the **PsExeSvc.exe** *service* attempts to logon to the target system using the provided credentials with the provided credentials that hopefully have the “Log on as a service” right
- If the **PsExeSvc.exe** service starts successfully, all is well
  - However, if an account lacks required privileges or security policies block this, execution fails
  - **PsExeSvc.exe** and the named pipes already created may still remain on the target system
- After successfully executing commands, **PsExeSvc.exe** removes the named pipes

PsExec Abuse Detection

Detecting PsExec Abuse

- Monitor the creation of **PsExeSvc.exe** and associated End User License Agreement (EULA) registry keys
- Track abnormally high volume SMB traffic, or between unusual hosts
- Alert on admin share access like **ADMIN$** or **IPC$** by non-standard accounts
- Document NTLM usernames to identify compromised accounts
- There are also a multitude of ways to investigate PsExec activity on given endpoints but that is not today's topic
  - If anyone is interested in more, reach out to after this finishes

PsExec Detection Lab

Scenario

- An alert from the Intrusion Detection System (IDS) flagged suspicious lateral movement activity involving PsExec. This indicates potential unauthorized access and movement across the network. As a SOC Analyst, your task is to investigate the provided PCAP file to trace the attacker's activities. Identify their entry point, the machines targeted, the extent of the breach, and any critical indicators that reveal their tactics and objectives within the compromised environment.
- Link to the source here

Let’s a Go!

- Work through the provided packet capture, trying to understand what is going on and answering the questions as you go

Next Meetings

2025-09-23 • **Next Tuesday**

- Web Hacking For Red Teamers
- Learn practical web hacking

2025-09-25 • **Next Thursday**

- Web Defense
- Secure web interfaces

2025-09-30 • **Next Tuesday**

- Linux & Linux Privilege Escalation
- Linux OS and ways to exploit it

ctf.sigpwny.com

`sigpwny{sniffin_packets}`

Meeting content can be found at sigpwny.com/meetings.

SIGPwny