

Red Team: “Exploits Against a Corporate Network”

Noah Daugherty and Mike Gearhart

July 7, 2021

Hypothesis

“Let your plans be dark and impenetrable as night, and when you move, fall like a thunderbolt.” – **Sun Tzu**

Most corporate networks have enough vulnerabilities that will enough persistence an attacker will find a weakness.

“To know your Enemy, you must become your Enemy.” – **Sun Tzu**

Purpose of This Project

“To know your Enemy, you must become your Enemy.” –
Sun Tzu

We will simulate attacks on a theoretical network. The lessons learned will be applied to an actual small business network.

Gearhart's Cabinets
Corporation

Business Requirements

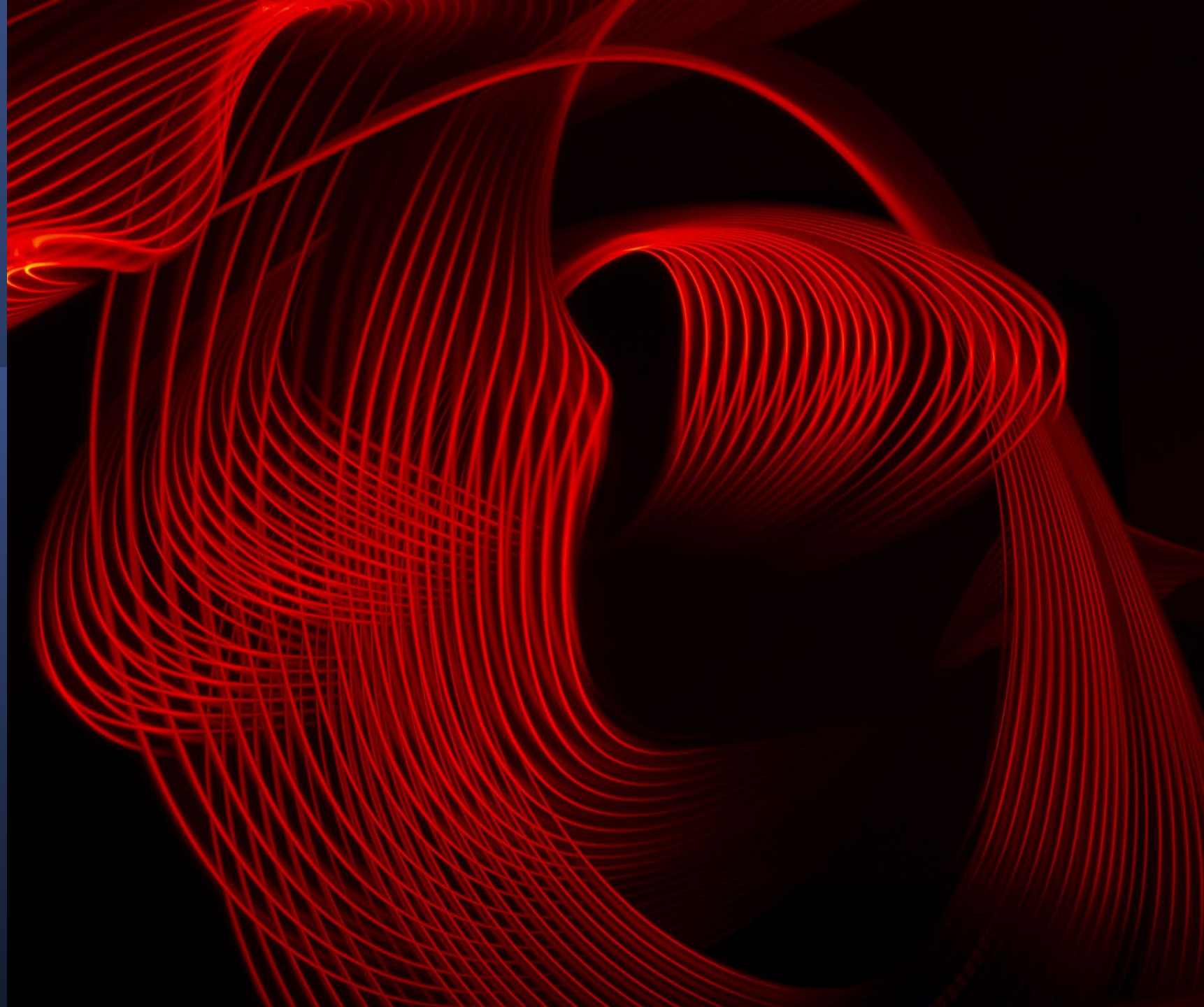


- A small office corporate ethernet network for a cabinetmaking business with 10 employees. No wireless to avoid distractions around dangerous machinery.
- One client for accounting using SaaS software, QuickBooks, but storing data locally. Remote access required to collaborate and work from home.
- One client for production, running CabinetVision on Microsoft Window Pro, storing and printing +250MB files

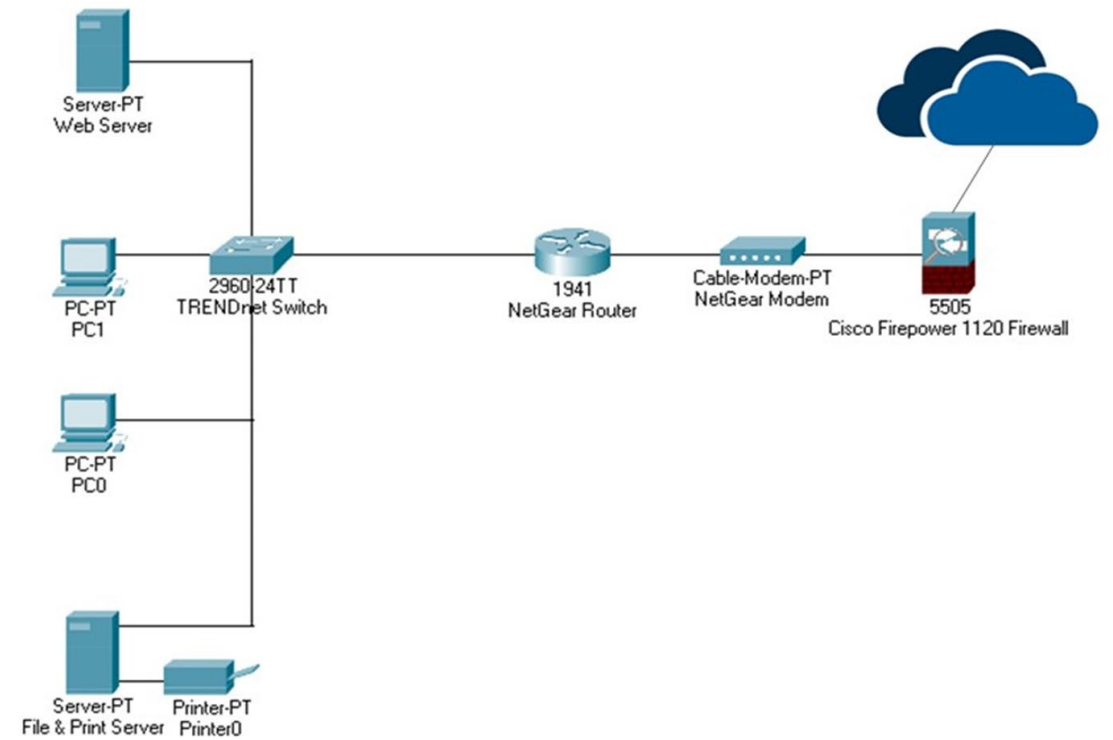
Proposed Hardware and Software

- Two servers that support Windows Server 2019, Ubuntu Server 20.04 LTS, and Red Hat® Enterprise Linux 8 : Dell Poweredge T140
- GbE switch, TRENDnet 24-Port Unmanaged Gigabit GREENnet Desktop Switch, Ethernet Network Switch
- Cat7 patch panel, Marketek, 24-port
- GbE router/modem, NETGEAR Cable Modem Wi-Fi Router Combo C6250
- Hardware firewall, Cisco Firepower 1120, 2.2Gps IPS throughput, 1.2Gbps VPN throughput, 400K concurrent sessions. Snort rules enabled.
- Printer: HP Color LaserJet Pro M454dw Wireless Laser Printer with Ethernet Connectivity
- Splashtop Business Access software, for remote access
- Two licenses of Windows 10 Pro
- Microsoft 365 Business Premium (2x)
- Two PCs - Dell Alienware Aurora R11 Desktop and Monitor compatible with Windows 10 Pro
- Cat 7 ethernet cable, 1000ft



Network Design




Network Architecture







Virtual Network Servers

Virtual Machine 1
Servers
Window Server 2019
Computer Name: WIN-A589T0T0725
Computer Description: File & Print Server
IP Address: 10.0.2.15
Mac Address: 08:00:27:8A:A1:F0
Subnet: 255.255.255.0
Last updated: July 5, 2021
Services
Firewall #2
DHCP Server
File & Print
 Gearharts Cabinests - Windows Server 2019 (May 30 2021)  Powered Off

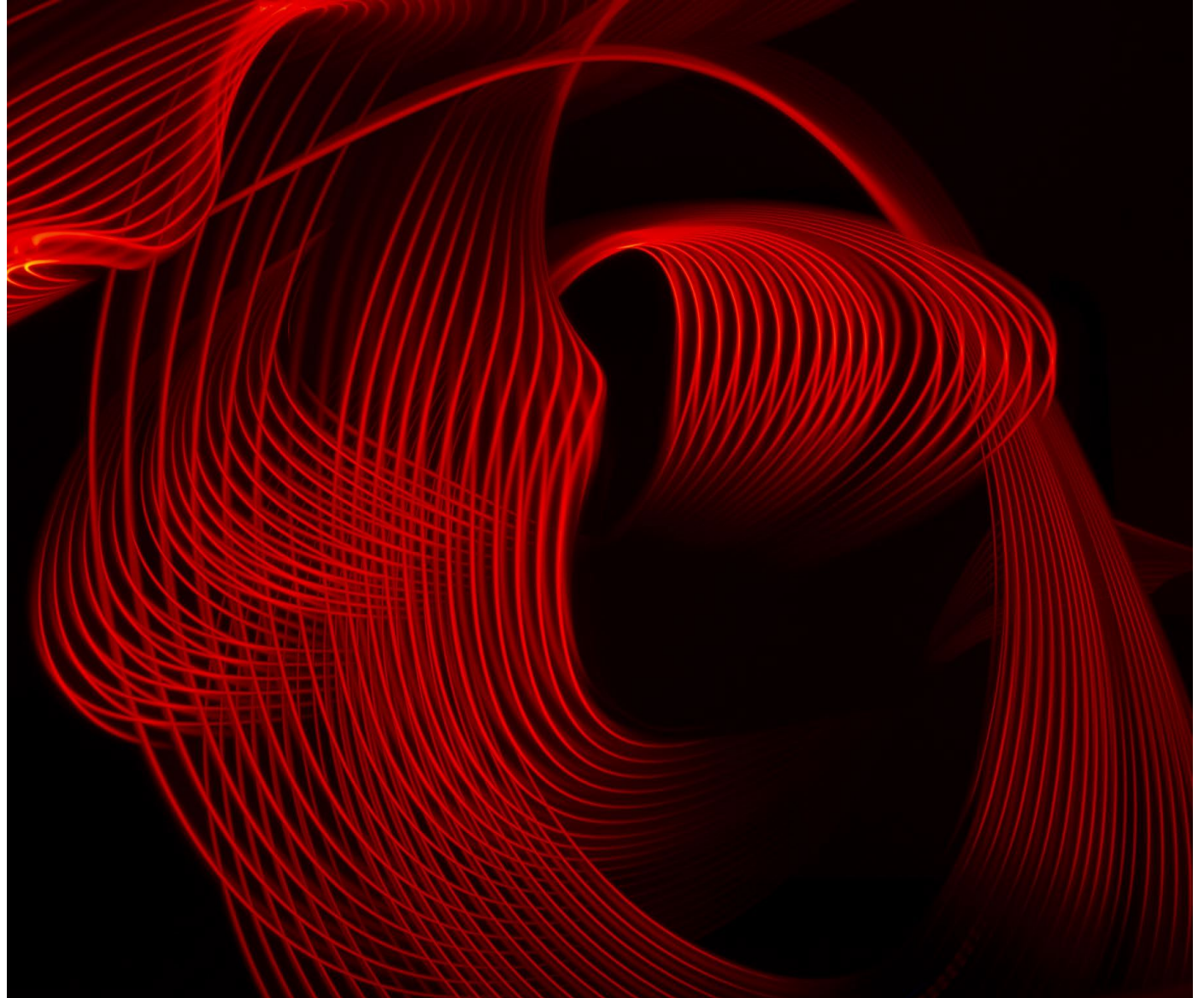
Virtual Machine 2
Servers
RedHat 8.4 Linux with Apache HTTP Server Apache 2.4.6
Computer Name:
Computer Description: Web Server
Static IP Address:
Mac Address:
Subnet: 255.255.255.0
Last updated: July 5, 2021
Services
Web server
SSH
 RedHat 8.4  Powered Off

Virtual Network Clients

Virtual Machine 3
Workstations
Windows 10
Computer Name: fullstack-cyber
Computer Description: Production
IP Address: 192.168.56.110
Mac Address: 08:00:27:36:dd-5D
Subnet: 255.255.255.0
Last updated: July 5, 2021
 Gearharts Cabinets - Production - Windows 10  Powered Off

Virtual Machine 4
Workstation
Windows 10
Computer Name:
Computer Description: Accounting
IP Address:
Mac Address:
Subnet: 255.255.255.0
Last updated: July 5, 2021
 Gearharts Cabinets - Accounting - Windows 10  Powered Off

Active & Passive Recon



Tools for Testing the Network

recon-ng

- Purpose: Web reconnaissance

nmap

- Purpose: Host discovery, port scanning, version detection

Nikto

- Purpose: Scan web servers for dangerous files/CGIs, outdated server software and other problems

enum4linux

- Purpose: Password policies on a target. The operating system of a remote target.

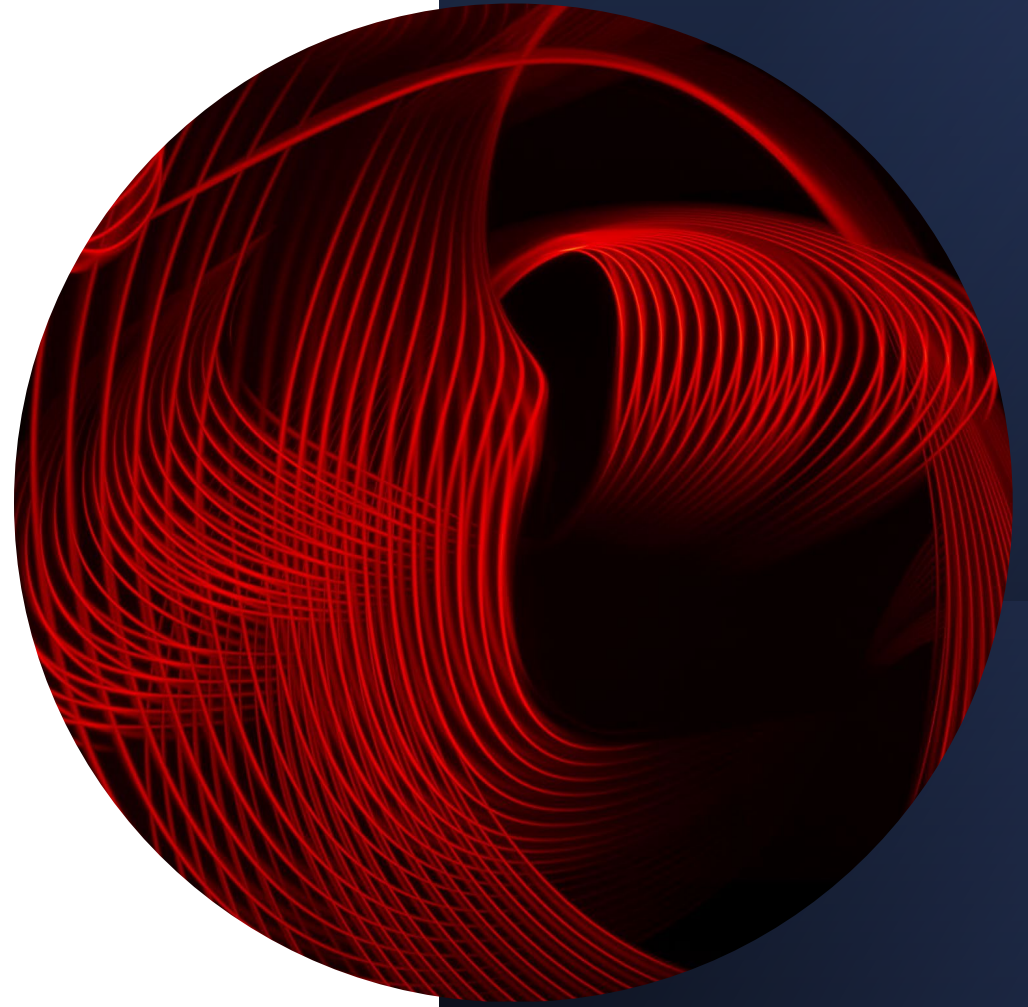
curl

- Purpose: Use to transfer data to and from a server. At the most fundamental, cURL lets you talk to a server by specifying the location (in the form of a URL) and the data you want to send

dirbuster

- Purpose: Crack passwords

Exploiting the Network



Tools and Type of Exploits



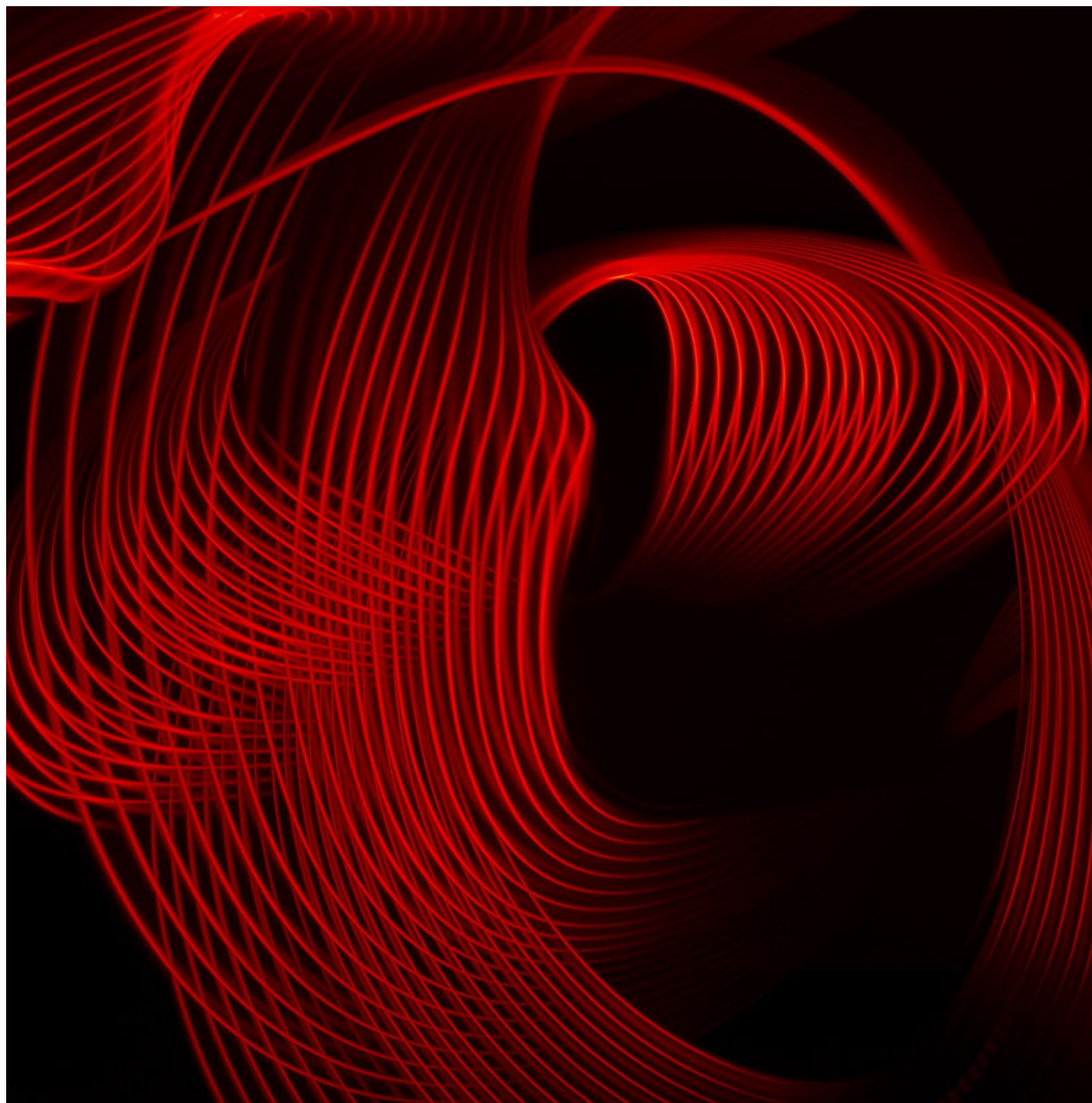
Microsoft Windows Server 2019 & Windows 10 Client Tests

- Reverse Powershell
- Event Tracing for Windows Information
- Scripting Engine Memory Corruption
- Windows Filter Manager Elevation of Privilege
- Windows Portmapping Information
- Other tests

RedHat Linux 8.4 Server with HTTP Apache Tests

- DoS due using oversized files
- Cross Site tracing to steal cookie information
- Directory traversal
- Gain user information
- Gain Privileges
- Secured ports 80(HTTP) and 443(HTTPS)
- Other tests

Test Results



Exploits

Results



To be published by 7/25/2021 after the simulation is completed.

Practice Defense in Depth

“Victorious warriors win first and then go to war,
while defeated warriors go to war first and then seek
to win.” – **Sun Tzu**