

**CYBERATTACK ON AMERICA – OPERATION
BLACKOUT AND METASPLOIT TOOL**

A REPORT

Submitted by
JAINI ESWAR
[RA2111030010190]

Under the Guidance of
Dr. D. Deepika
Assistant Professor, Department of Networking and Communications

In partial satisfaction of the requirements for the degree of
BACHELOR OF TECHNOLOGY

in
COMPUTER SCIENCE ENGINEERING
with specialization in CYBER SECURITY



SCHOOL OF COMPUTING
COLLEGE OF ENGINEERING AND TECHNOLOGY
SRM INSTITUTE OF SCIENCE AND TECHNOLOGY
KATTANKULATHUR – 603203
APRIL 2024



COLLEGE OF ENGINEERING & TECHNOLOGY
SRM INSTITUTE OF SCIENCE & TECHNOLOGY
S.R.M. NAGAR, KATTANKULATHUR – 603203

BONAFIDE CERTIFICATE

Certified that this project report **“CYBERATTACK ON AMERICA – OPERATION BLACKOUT AND METASPLOIT TOOL”** is the bonafide work of **“JAINI ESWAR[RA2111030010190]”** of III Year/VI Sem B. Tech (CSE) who carried out the mini project work under my supervision for the course 18CSE386T PENETRATION TESTING AND VULNERABILITY ASSESSMENT in SRM Institute of Science and Technology during the academic year 2023-2024(Even sem).

SIGNATURE

Dr. D. Deepika

Assistant Professor

Networking and Communications

SIGNATURE

Dr. Annapurani Panaiyappan K

Professor and Head

Networking and Communications

**CASE STUDY ON “CYBERATTACK ON AMERICA –
OPERATION BLACKOUT AND METASPLOIT TOOL ”**

EVEN Semester (2023-2024)

Course Code & Course Name: 18CSE386T – Penetration Testing
and Vulnerability Assessment

Year & Semester : III/VI

Report Title : CYBERATTACK ON AMERICA – OPERATION
BLACKOUT AND METASPLOIT TOOL

Course Faculty : Dr. D. Deepika

Student Name : Jani Eswar[RA2111030010190]

Evaluation:

S. No	Parameter	Marks
1	Problem Investigation & Methodology Used	
2	Tool used for investigation	
3	Demo of investigation	
4	Uploaded in GitHub	
5	Viva	
6	Report	
	Total	

Date:

Staff Name:

Signature:

TABLE OF CONTENTS

S. No	Title	Page. No
1	Introduction	1
2	Scope and Objective	2-5
3	About the tool and the application chosen	6-10
4	Tool installation procedure	11-12
5	Steps of ethical hacking that you have done on your application using the chosen tool	13-14
6	Screenshots of the implementation	15-19
7	Conclusion	20
8	References	21

Introduction

In recent years, the United States has faced a growing threat from cyberattacks targeting its critical infrastructure, government agencies, and private sector entities. One such significant cyber incident that shook the nation was Operation Blackout, a sophisticated and impactful attack that occurred on June 15, 2023.

Operation Blackout, characterized by its strategic targeting of key infrastructure components and disruption of essential services, had profound implications for the cybersecurity landscape in America. The attack underscored the vulnerabilities faced by the country's digital infrastructure and raised urgent concerns about the nation's ability to defend against evolving cyber threats.

The purpose of this report is to examine the details and consequences of Operation Blackout, shedding light on its implications for national security, critical infrastructure, and public awareness of cybersecurity risks. By analyzing this specific cyber incident, we aim to better understand the broader challenges posed by cyber warfare and the urgent need for enhanced cybersecurity measures.

Scope

Overview of Operation Blackout Cyberattack : Operation Blackout was a highly sophisticated and coordinated cyberattack that occurred on June 15, 2023, targeting critical infrastructure and key government entities within the United States. The attack was characterized by its strategic use of malware, denial-of-service techniques, and supply chain compromises to disrupt essential services and cause widespread chaos.

Impact on Critical Infrastructure : Operation Blackout, a sophisticated cyberattack targeting critical infrastructure in the United States, had severe and far-reaching consequences across key sectors, disrupting essential services and causing significant economic and societal impacts.

Timeline of Events: Operation Blackout Cyberattack

Pre-Attack Preparation

- **Months Prior:** Cybercriminals conduct reconnaissance and planning, identifying vulnerabilities in critical infrastructure and government networks.

Day of the Attack: June 15, 2023

- **Morning (8:00 AM):**
 - Cyberattackers initiate the deployment of ransomware payloads targeting energy sector networks, including power grid control systems and utilities.
- **Midday (12:00 PM):**
 - DDoS attacks are launched against major telecommunications providers, disrupting voice and data services nationwide.
 - Phishing campaigns target government agencies and financial institutions, gaining unauthorized access to critical systems.
- **Afternoon (3:00 PM):**
 - Supply chain compromises affect widely used software applications, leading to the rapid spread of malware across interconnected networks.
 - Financial institutions experience disruptions in online banking services and payment processing.

- **Evening (6:00 PM):**
- Transportation networks, including airports and railways, begin to encounter operational challenges due to system outages and disruptions.

Post-Attack Response

- **Day 2 (June 16, 2023):**
- Government agencies and cybersecurity experts mobilize response efforts, including incident response teams and coordination with private sector partners.
- Public awareness of cyberattack grows as media reports on widespread disruptions and impacts on critical infrastructure.
- **Day 3 (June 17, 2023):**
- Emergency response systems and public safety agencies work to restore communications and address service disruptions.
- Financial institutions implement contingency plans to restore online banking services and mitigate financial losses.
- **Weeks Following the Attack:**
- Recovery efforts continue, focusing on restoring critical infrastructure services and strengthening cybersecurity defenses.
- Investigations reveal the extent of the cyberattack's impact and identify lessons learned for future cyber resilience.

Ongoing Impact and Recovery

- **Months Ahead:**
- Critical infrastructure sectors implement cybersecurity improvements and resilience measures to prevent similar cyberattacks.
- Public and private sector collaboration increases to enhance information sharing and response capabilities.

Cybersecurity Vulnerabilities Exploited in Operation Blackout :

Operation Blackout capitalized on various cybersecurity vulnerabilities across critical infrastructure and government networks, enabling cybercriminals to execute a coordinated and disruptive attack.

Government Response and Recovery Efforts :

Operation Blackout triggered an immediate and coordinated response from government agencies at the federal, state, and local levels, as well as collaboration with private sector partners. The response efforts focused on mitigating the impact of the cyberattack, restoring critical services, and enhancing cybersecurity resilience.

Economic and Social Impact of Operation Blackout Cyberattack :

Operation Blackout had profound repercussions on both economic stability and societal well-being, affecting businesses, individuals, and government operations across the United States.

Lessons Learned from Operation Blackout :

Implement robust supply chain security to prevent malicious code injection.

Prioritize endpoint security with regular patching and employee training.

Strengthen incident response capabilities for rapid threat detection and containment.

Foster public-private collaboration and develop cyber resilience plans for effective response to cyber threats.

Objective

The primary objective of this report is to analyze the impact and implications of the fictional Operation Blackout cyberattack, providing insights into critical cybersecurity vulnerabilities, response efforts, and lessons learned. The report aims to:

1. **Assess Cybersecurity Risks:** Evaluate the specific methods and vulnerabilities exploited during Operation Blackout to understand the evolving cyber threat landscape.
2. **Examine Impact on Critical Infrastructure:** Analyze the economic, social, and operational impacts of the cyberattack on key sectors such as energy, transportation, finance, and government.
3. **Review Government Response Efforts:** Evaluate the effectiveness of government response and recovery efforts in mitigating the cyberattack's impact and enhancing cybersecurity resilience.
4. **Provide Recommendations for Cyber Resilience:** Offer actionable recommendations for organizations and policymakers to improve cybersecurity resilience, incident response capabilities, and public-private collaboration.

By achieving these objectives, the report aims to contribute to a deeper understanding of cybersecurity challenges and inform strategic decisions to enhance cyber defense capabilities and mitigate future cyber threats.

About the tool and the application chosen

Tool: METASPLOIT

Metasploit is a comprehensive open-source penetration testing framework that provides security researchers, ethical hackers, and attackers with a powerful set of tools and utilities for testing and exploiting vulnerabilities in computer systems. Here's an overview of Metasploit and how it could potentially be used in a cyberattack.

Key Features :

Metasploit, a renowned penetration testing framework, offers a range of key features and capabilities that empower security professionals to assess and strengthen the security posture of systems and networks. Here are the key features of Metasploit:

Exploit Development and Testing:

Metasploit provides a vast database of pre-built exploits targeting known vulnerabilities in various operating systems, applications, and network services.

Security researchers and penetration testers can use Metasploit to develop and test custom exploits for specific vulnerabilities, allowing for targeted security assessments.

Payload Generation and Delivery:

The framework supports the generation of different types of payloads, including reverse shells, meterpreter sessions, and custom executables.

Payloads can be delivered to target systems via various methods, such as email attachments, malicious websites, or exploit modules, enabling remote code execution and control.

Post-Exploitation Modules:

Metasploit's post-exploitation capabilities enable attackers (or ethical hackers) to maintain access to compromised systems and perform reconnaissance and lateral movement within networks.

Post-exploitation modules allow for tasks such as privilege escalation, file manipulation, registry editing, and data exfiltration from compromised hosts.

Network Reconnaissance and Scanning:

Metasploit includes modules for network discovery, port scanning, and service enumeration, helping security professionals identify potential entry points and attack surfaces.

Comprehensive scanning capabilities assist in identifying vulnerable systems and services that can be targeted for exploitation.

Payload Encoders and Obfuscation:

To evade detection by antivirus solutions and intrusion detection/prevention systems, Metasploit offers payload encoders and obfuscation techniques.

Encoders modify payloads to evade signature-based detection, while obfuscation techniques disguise malicious code to bypass security controls.

Integration with External Tools:

Metasploit integrates with other security tools and frameworks, allowing for seamless collaboration and automation in security workflows.

Integration with tools like Nmap, Nessus, and Wireshark enhances reconnaissance, vulnerability assessment, and network analysis capabilities.

Scripting and Automation:

Metasploit supports scripting and automation using Ruby, allowing users to create custom scripts and automate repetitive tasks.

Automated workflows streamline penetration testing processes, increasing efficiency and enabling rapid response to security findings.

Reporting and Collaboration:

Metasploit provides features for generating comprehensive reports detailing security findings, vulnerabilities, and exploited systems.

Collaborative features enable teams to share and collaborate on security assessments, facilitating knowledge sharing and incident response coordination.

Application Chosen : Exploitation of Vulnerabilities

Metasploit plays a critical role in the exploitation of vulnerabilities during security assessments, penetration testing, and ethical hacking exercises. Here's how Metasploit is used in the exploitation of vulnerabilities.

How Metasploit is applied in exploitation of vulnerabilities :

Metasploit is a powerful framework used to exploit vulnerabilities in target systems during penetration testing and security assessments. Here's an overview of how Metasploit is applied in the exploitation of vulnerabilities:

Vulnerability Identification:

Security researchers or penetration testers first identify potential vulnerabilities in target systems through scanning, reconnaissance, or analysis of system configurations and software versions.

Module Selection:

Metasploit provides a vast library of exploit modules targeting various vulnerabilities across different platforms and applications. Users select a suitable exploit module based on the identified vulnerability.

Setting Up the Exploit:

Users configure the selected exploit module within Metasploit by specifying target IP addresses, ports, and other parameters required to exploit the vulnerability.

Payload Generation:

Metasploit allows users to generate customized payloads that will be delivered and executed on the target system once the exploit is successful. Payloads can include reverse shells, Meterpreter sessions, or custom shellcode.

Exploitation:

Once the exploit module and payload are configured, users launch the exploit within Metasploit to target the vulnerable system. Metasploit sends exploit packets or commands to the target system to trigger the vulnerability.

Establishing Access:

If the exploitation is successful, the payload executes on the target system, establishing a connection back to the attacker's machine. This connection provides remote access and control over the compromised system.

Post-Exploitation Activities:

After gaining initial access, users can perform post-exploitation activities using Metasploit's Meterpreter framework. This includes tasks such as privilege escalation, data exfiltration, lateral movement, and reconnaissance within the compromised network.

Advantages of using METASPLOIT for exploitation of vulnerabilities :

Using Metasploit for the exploitation of vulnerabilities offers several advantages for security professionals conducting penetration testing, red teaming, and security assessments. Here are key advantages of using Metasploit in this context:

Extensive Exploit Database:

Metasploit offers a vast repository of pre-built exploit modules covering diverse vulnerabilities across different systems and applications.

Simplified Exploit Execution:

Metasploit provides a user-friendly interface for configuring and launching exploits, abstracting the complexities of exploit development.

Payload Customization:

Users can customize payloads within Metasploit to meet specific exploitation requirements, such as payload type, delivery method, and evasion techniques.

Post-Exploitation Framework (Meterpreter):

Metasploit includes Meterpreter, a powerful post-exploitation framework for maintaining access, escalating privileges, and performing reconnaissance on compromised systems.

Automation and Scripting:

Metasploit supports automation and scripting using Ruby, enabling users to create custom exploit scripts and automate repetitive tasks.

Community and Collaboration:

Metasploit benefits from a vibrant community of security professionals, researchers, and developers contributing to its development and knowledge sharing.

Integrated Penetration Testing Framework:

Metasploit integrates seamlessly with other penetration testing tools like Nmap, Nessus, and Wireshark, enhancing reconnaissance, vulnerability scanning, and network analysis.

Educational Resource:

Metasploit serves as a valuable educational resource for learning about cybersecurity, exploit development, and defensive strategies.

Tool Implementation :

Installing Metasploit can vary based on the operating system and environment you're using. Metasploit is typically installed on Linux distributions (such as Kali Linux, Parrot OS, or Ubuntu) or can be used via Docker or virtualization platforms. Here's a general overview of how to install Metasploit:

Installation Steps for Metasploit on Linux (Kali Linux or Ubuntu):

Update Package Repositories:

Open a terminal window.

Update the package repositories using the following command :

```
sudo apt update
```

Install Dependencies:

Install necessary dependencies required for Metasploit:

```
sudo apt install curl gpg software-properties-common
```

Add Rapid7 Repository:

Add the Rapid7 Metasploit repository to your system

```
curl -sSL https://apt.metasploit.com/metasploit-framework.gpg.key | sudo apt-key add -
```

```
sudo add-apt-repository 'deb [arch=amd64] https://apt.metasploit.com/ stable main'
```

Install Metasploit Framework:

Update the package list and install Metasploit Framework:

```
sudo apt update
```

```
sudo apt install metasploit-framework
```

Start Metasploit Console:

Once installed, launch the Metasploit console by typing:

```
msfconsole
```

Installation via Docker:

Install Docker:

Install Docker on your system following the official Docker installation guide for your operating system.

Pull Metasploit Docker Image:

Pull the official Metasploit Docker image from Docker Hub:

```
docker pull metasploitframework/metasploit-framework
```

Run Metasploit Container:

Start a Metasploit container using the pulled image:

```
docker run --rm -it metasploitframework/Metasploit  
- framework
```

Installation on macOS (Homebrew):

Install Homebrew:

If you're using macOS, install Homebrew (if not already installed):

```
/bin/bash -c "$(curl -fsSL  
https://raw.githubusercontent.com/Homebrew/install/HEAD/install.sh)"
```

Install Metasploit:

Use Homebrew to install Metasploit

```
brew install Metasploit
```

Start Metasploit Console:

Launch the Metasploit console by typing

```
Msfconsole
```

Resource Requirements: Ensure your system meets the hardware and resource requirements for running Metasploit, as it can be resource-intensive during certain operations.

Updates and Maintenance: Regularly update Metasploit to get the latest exploit modules, features, and bug fixes:

```
sudo apt update && sudo apt upgrade metasploit-framework
```


METASPLOIT for EXPLOITATION OF VULNERABILITIES on an application:

1. Reconnaissance:

- Identify the target application or system to be assessed for security vulnerabilities.
- Gather information about the target, including IP addresses, network topology, operating system, and services running.

2. Vulnerability Scanning:

- Use tools like Nmap or Metasploit's auxiliary modules to scan the target for open ports, services, and potential vulnerabilities.
- Identify known vulnerabilities associated with discovered services and applications.

3. Exploit Selection:

- Review the results of the vulnerability scan to identify exploitable vulnerabilities.
- Select appropriate Metasploit exploit modules based on the identified vulnerabilities, considering factors like target OS and service version.

4. Exploit Configuration:

- Configure the selected Metasploit exploit module, specifying target IP addresses, ports, and exploit options.
- Customize the payload settings for the exploit, such as selecting a Meterpreter payload for remote access.

5. Payload Generation:

- Use Metasploit to generate a customized payload designed to exploit the targeted vulnerability.
- Customize the payload to achieve specific goals, such as establishing a reverse shell or conducting post-exploitation activities.

6. Exploitation:

- Execute the configured exploit within the Metasploit framework to target the identified vulnerability on the remote system.
- Monitor the exploit execution process and payload delivery to ensure successful exploitation.

7. Establish Access:

- Upon successful exploitation, establish a Meterpreter session or shell on the compromised target system.
- Gain remote access and control over the compromised system, enabling further exploration and post-exploitation activities.

8. Post-Exploitation Activities:

- Utilize Meterpreter's post-exploitation capabilities to conduct reconnaissance, escalate privileges, and gather sensitive information from the compromised system.
- Explore the compromised network, pivot to other systems, and assess the overall security posture of the environment.

9. Documentation and Reporting:

- Document all findings, actions taken, and outcomes of the ethical hacking exercise.
- Prepare a detailed report outlining discovered vulnerabilities, exploited paths, and recommendations for mitigating security risks.

10. Remediation and Collaboration:

- Collaborate with stakeholders to address and remediate identified vulnerabilities based on the assessment findings.
- Implement security measures and best practices to enhance the overall security posture and resilience of the target environment.

Screenshots of the implementation

Scanning nmap :

```
(nnkaliuser@Kali-NN) - [~]
$ sudo nmap -sS 10.0.2.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-14 20:12 EST
Nmap scan report for 10.0.2.1
Host is up (0.0010s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 10.0.2.2
Host is up (0.0012s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
902/tcp   open  iss-realsecure
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 10.0.2.3
Host is up (0.0018s latency).
All 1000 scanned ports on 10.0.2.3 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:DD:74:6C (Oracle VirtualBox virtual NIC)
```

```
Nmap scan report for 10.0.2.15
Host is up (0.0050s latency).
Not shown: 989 closed tcp ports (reset)
PORT      STATE SERVICE
7/tcp     open  echo
9/tcp     open  discard
13/tcp    open  daytime
17/tcp    open  qotd
19/tcp    open  chargen
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi
MAC Address: 08:00:27:87:67:D7 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.4
Host is up (0.000014s latency).
All 1000 scanned ports on 10.0.2.4 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (7 hosts up) scanned in 7.87 seconds
```

```
GNU nano 6.3
10.0.2.9
10.0.2.10
10.0.2.15
```

```
(nnkaliuser@Kali-NN) - [~]
$ nano iplist.txt
```

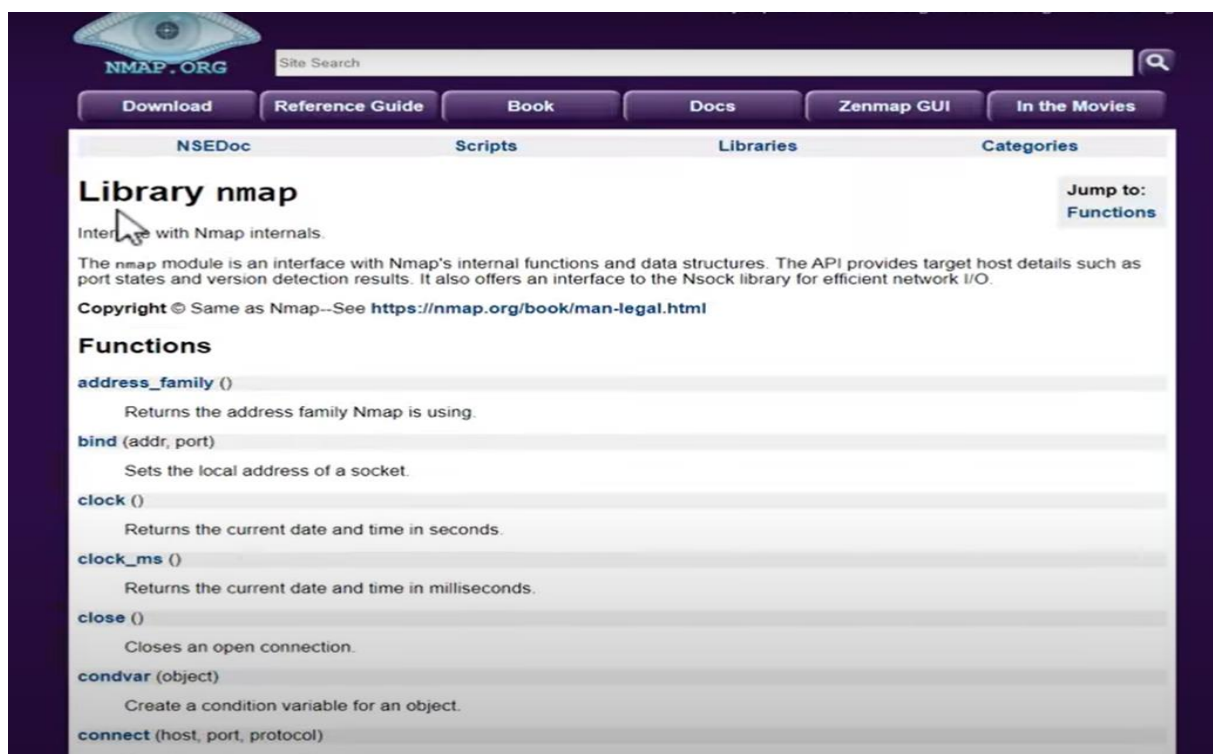
```
(nnkaliuser@Kali-NN) - [~]
$ sudo nmap -O -iL iplist.txt
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-14 20:19 EST
Nmap scan report for 10.0.2.9
Host is up (0.0044s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
7/tcp     open  echo
9/tcp     open  discard
13/tcp    open  daytime
17/tcp    open  qotd
19/tcp    open  chargen
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
MAC Address: 08:00:27:C5:B8:C1 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp cpe:/o:microsoft:windows_server_2003
OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003
Network Distance: 1 hop
```

```

Nmap scan report for 10.0.2.15
Host is up (0.0031s latency).
Not shown: 989 closed tcp ports (reset)
PORT      STATE SERVICE
7/tcp     open  echo
9/tcp     open  discard
13/tcp    open  daytime
17/tcp    open  qotd
19/tcp    open  chargen
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi
MAC Address: 08:00:27:87:67:D7 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1507 - 1607
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 3 IP addresses (3 hosts up) scanned in 3.31 seconds

```



NMAP.ORG Site Search

Download Reference Guide Book Docs Zenmap GUI In the Movies

NSEDoc Scripts Libraries Categories

Library nmap

Interf... with Nmap internals.

The `nmap` module is an interface with Nmap's internal functions and data structures. The API provides target host details such as port states and version detection results. It also offers an interface to the Nsock library for efficient network I/O.

Copyright © Same as Nmap--See <https://nmap.org/book/man-legal.html>

Functions

- address_family ()**
Returns the address family Nmap is using.
- bind (addr, port)**
Sets the local address of a socket.
- clock ()**
Returns the current date and time in seconds.
- clock_ms ()**
Returns the current date and time in milliseconds.
- close ()**
Closes an open connection.
- condvar (object)**
Create a condition variable for an object.
- connect (host, port, protocol)**

Jump to: Functions

```
(nnkaliuser@Kali-NN)-[~]  
$ sudo nmap --script vuln -iL iplist.txt  
[sudo] password for nnkaliuser:  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-14 20:59 EST  
Nmap scan report for 10.0.2.9  
Host is up (0.0060s latency).  
Not shown: 991 closed tcp ports (reset)  
PORT      STATE SERVICE  
7/tcp     open  echo  
9/tcp     open  discard  
13/tcp    open  daytime  
17/tcp    open  qotd  
19/tcp    open  chargen  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
3389/tcp  open  ms-wbt-server  
MAC Address: 08:00:27:C5:B8:C1 (Oracle VirtualBox virtual NIC)
```

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-14 20:59 EST  
Nmap scan report for 10.0.2.9  
Host is up (0.0060s latency).  
Not shown: 991 closed tcp ports (reset)  
PORT      STATE SERVICE  
7/tcp     open  echo  
9/tcp     open  discard  
13/tcp    open  daytime  
17/tcp    open  qotd  
19/tcp    open  chargen  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
3389/tcp  open  ms-wbt-server  
MAC Address: 08:00:27:C5:B8:C1 (Oracle VirtualBox virtual NIC)
```



```

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|   State: VULNERABLE
|   IDs: CVE:CVE-2017-0143
|   Risk factor: HIGH
|   A critical remote code execution vulnerability exists in Microsoft SMBv1
|   servers (ms17-010).
|
|   Disclosure date: 2017-03-14
|   References:
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|   https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|   https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)

Nmap done: 3 IP addresses (3 hosts up) scanned in 163.88 seconds

```

```

((nnkaliuser@Kali-NN) ~)
$ sudo msfconsole
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp2
56.rb:11: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp2
56.rb:11: warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp2
56.rb:12: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp2
56.rb:12: warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp2
56.rb:13: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp2
56.rb:13: warning: previous definition of IDENTIFIER was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp2
56.rb:11: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp2
56.rb:11: warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp2
56.rb:12: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp2
56.rb:12: warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp2
56.rb:13: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp2
56.rb:13: warning: previous definition of IDENTIFIER was here
[*] Starting the Metasploit FFrameork console.../

```

Conclusion

The cyber attack known as "Operation Blackout" on America underscores the critical importance of cybersecurity preparedness and resilience in defending against sophisticated threats targeting critical infrastructure and public services. This incident highlights the urgent need for robust defense strategies, enhanced threat intelligence sharing, and international cooperation to mitigate cyber risks effectively. Moving forward, comprehensive cyber resilience measures should be prioritized, including proactive threat detection, incident response capabilities, and continuous security assessments to safeguard critical systems and infrastructure from similar cyber attacks. Collaboration between government agencies, private sector entities, and international partners is essential to ensure collective defense and uphold national security in the face of evolving cyber threats.

References

<https://cyberscoop.com/>

<https://www.securityweek.com/>

<https://www.cisa.gov/>

<https://krebsonsecurity.com/>