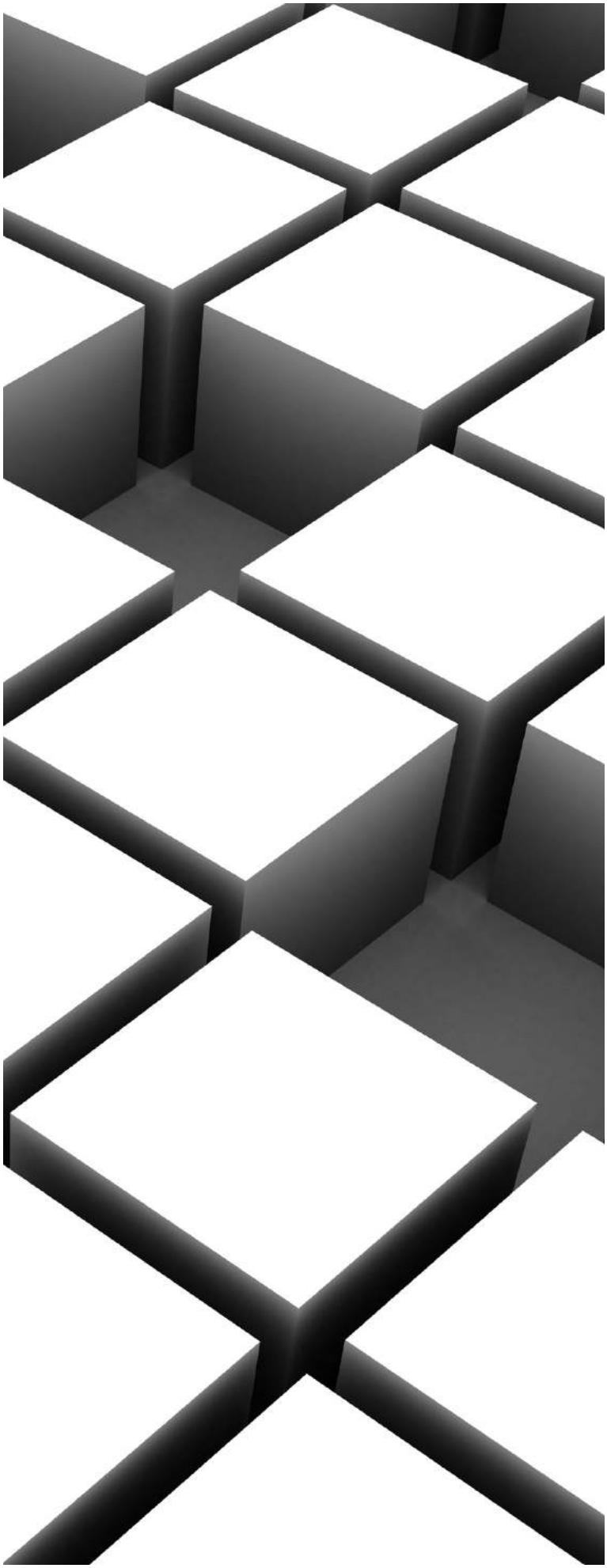


ENTERSOFT

Technical Documentation

Network Penetration Test

Prepared for:
ABC LTD

February 26, 2018

By:

Entersoft Security
162, Road No 72, Prashashan Nagar
Jubilee Hills, Hyderabad - 500033
Phone: +9140 23332299

Contents

Version Control

Version Date	Created/Modified by	Description/Pages Modified
26/02/2018	Mohan Gandhi	Author
26/02/2018	Sri Chakradhar	Review

1 Introduction

This report document hereby describes the results of an external network penetration test conducted against ABC Ltd external facing IP addresses between 9th February 2018 till 26th February 2018. The assessment was performed to incorporate the standards set forth by set forth by the OSSTMM and NIST.

1.1 Scope

The section defines the scope and boundaries of the project. The scope for the Penetration testing activity was restricted to:

1) *Testing Target IP addresses provided by ABC Ltd as mentioned in Section 1.1.2*

1.1.1 Constraints and Limitations

The assessment was performed without any prior knowledge whatsoever about the target company's IT infrastructure technical and architectural details but only the target IP address list.

The tests were conducted remotely and the result(s) / finding(s) made are highly subjective to target system(s) service(s) visibility (in terms of perimeter access rules) and availability at that given point of time.

1.1.2 Target IP Address List (total 40)

IP Addresses – Servers				
911.54.151.101	911.54.151.20	911.54.151.37	911.54.151.54	911.54.151.110
911.19.107.102	911.54.151.25	911.54.151.39	911.54.151.72	911.54.151.111
911.54.138.125	911.54.151.28	911.54.151.40	911.54.151.76	911.54.151.114
911.54.149.132	911.54.151.31	911.54.151.41	911.54.151.80	911.54.151.117
911.54.151.11	911.54.151.32	911.54.151.42	911.54.151.85	911.54.151.118
911.54.151.13	911.54.151.33	911.54.151.44	911.54.151.86	911.54.151.119
911.54.151.15	911.54.151.34	911.54.151.45	911.54.151.87	911.54.151.120
911.54.151.16	911.54.151.36	911.54.151.53	911.54.151.105	911.54.151.121

1.1.3 Test Attribute(s)

Starting Vector	External
Target Criticality	Production
Test Aggressiveness	Cautious & Calculated
Test Conspicuity	Clear
Proof of concept(s)	Attached wherever applicable

1.1.4 Test Type, Method, and Tools

The testing was done in a 'Black-Box' method, in which the tester's had no information or prior knowledge regarding the target systems(s) or the technology used to implement it. This type of test focuses on portraying a precise imitation of a real "hacker or attacker" attacking the system.

1.1.5 Risk Calculation and Classification

The final risk value of the vulnerability identified is arrived at by considering the likelihood of occurrence of an attack by exploiting the vulnerability and its impact on business.

Following is the risk classification:

CRITICAL	Vulnerabilities that can be exploited publicly, workaround or fix/ patch may not be available by vendor.
HIGH	Vulnerabilities that can be exploited publicly, workaround or fix/ patch available by vendor.
MEDIUM	Vulnerabilities may not have public exploit (code) available or cannot be exploited in the wild. Patch/ workaround not yet released.
LOW	Vulnerabilities may not have public exploit (code) available or cannot be exploited in the wild. Vulnerability observed may not have high rate of occurrence. Patch/ workaround released by vendor.
INFORMATIONAL	No direct threat to host/ individual user account. Sensitive information can be revealed to the adversary.

2 Executive Summary

The target(s) in the scope of assessment (stated in Section 1.1.2) were reviewed for the adequacy of the existing controls in accordance to industry known best practices. The summary below briefly documents the overall result of each test conducted.

	PENETRATION TEST OBJECTIVES	ABC LTD
1	IDENTIFIED CRITICAL / HIGH RISK VULNERABILITIES	✘
2	IDENTIFIED WEAK CIPHERS	✓
3	DNS AMPLIFICATION DOS ATTACK	✓
4	GAINED UNAUTHORIZED ACCESS TO NETWORK	✘
5	GAINED UNAUTHORIZED ACCESS TO SYSTEMS	✘
6	GAINED UNAUTHORIZED ACCESS TO DATA	✘
OVERALL SECURITY POSTURE		MEDIUM

Legend:

✘: Failed the test objective
✓: Passed the test objective.

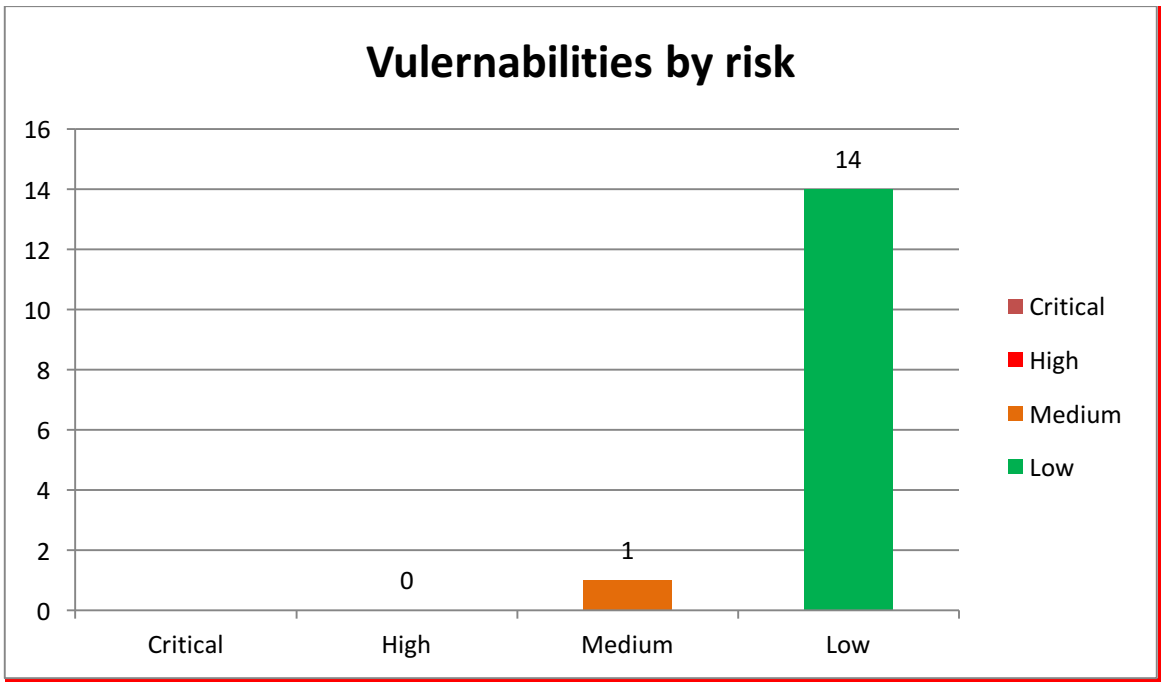
2.1 Graphical Representation of Vulnerabilities

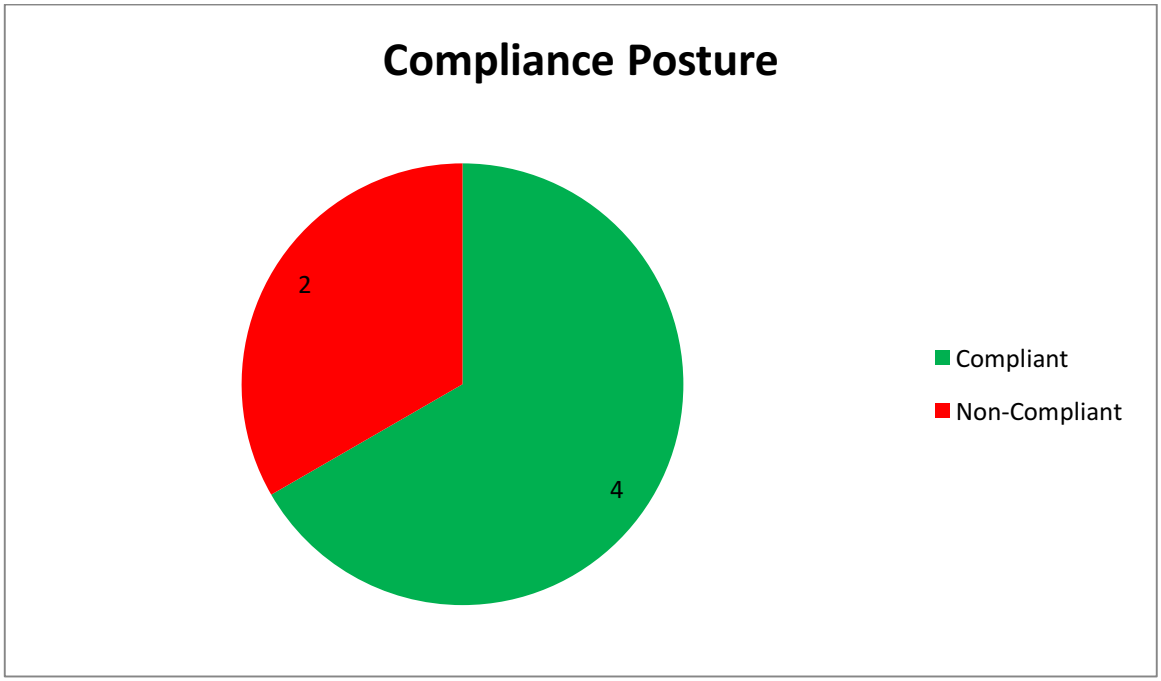
The following table is the summary of findings, which summarizes the overall risks identified during the penetration testing. For details, refer to section "Detailed Technical Summary".

Total of **15** security issues were identified during the test.

	CRITICAL	HIGH	MEDIUM	LOW	INFO
Summary	**00**	**00**	**01**	**14**	**00**

This section highlights the severity of the vulnerabilities discovered during the test.





3 Detailed Technical Summary

Listed below are the results corresponding to different scans and tests involved in assessment:

3.1 Scanning & Enumeration

These phases are conducted with a need to determine open TCP / UDP ports, protocols and services running on these open ports and their versions. The results below depict the port scan status for each IP tested.

Sr. No.	Live IP Address	Open Ports	Server
1	911.54.151.15	25, 80	Apache 2.2.17
2	911.54.151.20	25, 80, 443	Apache Tomcat/7.0.26
3	911.54.151.16	80	Microsoft IIS 8.5
4	911.54.151.13	80	
5	911.54.151.37	80, 443	Microsoft IIS 8.5
6	911.54.151.39	25	
7	911.54.151.36	443	Microsoft-HTTPAPI/2.0
8	911.54.151.32	25 80 443	Apache 2.2.19
9	911.54.151.33	25 80 143 443 587 993	Microsoft IIS 7.5
10	911.54.151.11	25	Apache 2.2.17
11	911.54.151.40	25, 443	RTC/5.0
12	911.54.151.25	25 80 443	Jetty 6.1.12
13	911.54.151.28	80, 443	GlassFish v2.1
14	911.54.151.31	25 80 443	Apache 2.2.19
15	911.54.151.34	25 80 443	
16	911.54.151.42	25, 443	
17	911.54.151.45	80, 443	Apache httpd 2.2.3
18	911.54.151.44	80,443	Apache httpd 2.2.3
19	911.54.151.53	25, 80, 443	Apache httpd 2.2.15
20	911.54.151.41	25, 443	
21	911.54.151.54	25,443	Apache 2.4.6
22	911.54.151.72	80,443	Apache 2.2.3
23	911.54.151.80	80,443	Microsoft ASP.NET IIS 8.0
24	911.54.151.76	80,443	Microsoft ASP.NET IIS 8.5
25	911.54.151.85	80,443	Microsoft ASP.NET IIS 7.5
26	911.54.151.86	25,80,443	Microsoft ASP.NET IIS 7.5
27	911.54.151.87	25,80,443	Microsoft ASP.NET IIS 7.5
28	911.54.151.110	443	Microsoft-IIS/8.0
29	911.54.151.114	25,80,443	Apache 2.4.6, PHP 7.0.23

30	911.54.151.105	25,80,443	Apache 2.4.6, PHP 5.4.16
31	911.54.151.111	80,443	Apache/2.2.15
32	911.54.151.120	21, 80	Apache/2.2.19
33	911.54.151.101	80, 443	
34	911.54.151.118	25,80,443	Microsoft-IIS 7.5
35	911.54.151.121	21,222	
	IPs		
36	911.19.107.202	25	Cisco SSL VPN
37	911.54.149.132	25, 443, 514	Cisco SSL VPN
	DNS		
38	911.54.151.117	53	
39	911.54.151.119	53	
40	911.54.138.125	53	

** Note: The enumerations listed above were derivative of various fingerprinting or scanning techniques and were derived on the best guess probability basis.*

3.2 Vulnerability Details and Remediation

3.2.1 DNS Amplification DoS Attack

Reference No:	**Vulnerability Rating:**
EXT_PT_01	**Medium**
Tools Used	**CVSS-3.0 Score**
Nessus	CVE-2006-0987
Vulnerability Description:	
The remote DNS server answers to any request. It is possible to query the name servers (NS) of the root zone ('.') and get an answer that is bigger than the original request. By spoofing the source IP address, a remote attacker can leverage this 'amplification' to launch a denial of service attack against a third-party host using the remote DNS server.	
Exploitation Summary	
Remote attacker can leverage this 'amplification' to launch a denial of service attack against a third party host using the remote DNS server.	
Vulnerability Identified By / How It Was Discovered	
Manual Analysis	
Vulnerable URLs / IP Address	

IP Address	**Port**
911.54.151.117	
911.54.151.119	
911.54.138.125	

Vulnerable Parameter(s)
DNS
Implications / Consequences of not Fixing the Issue
An adversary may identify known vulnerabilities in the installed version of the PHP and exploit those vulnerability further.
Suggested Countermeasures
Common ways to prevent or mitigate the impact of DNS amplification attacks include tightening DNS server security, blocking specific DNS servers or all open recursive relay servers, and rate limiting.
High-Level Category
Security Misconfiguration
References
NA

Proof of Concept:

Fig 1: 911.54.151.117

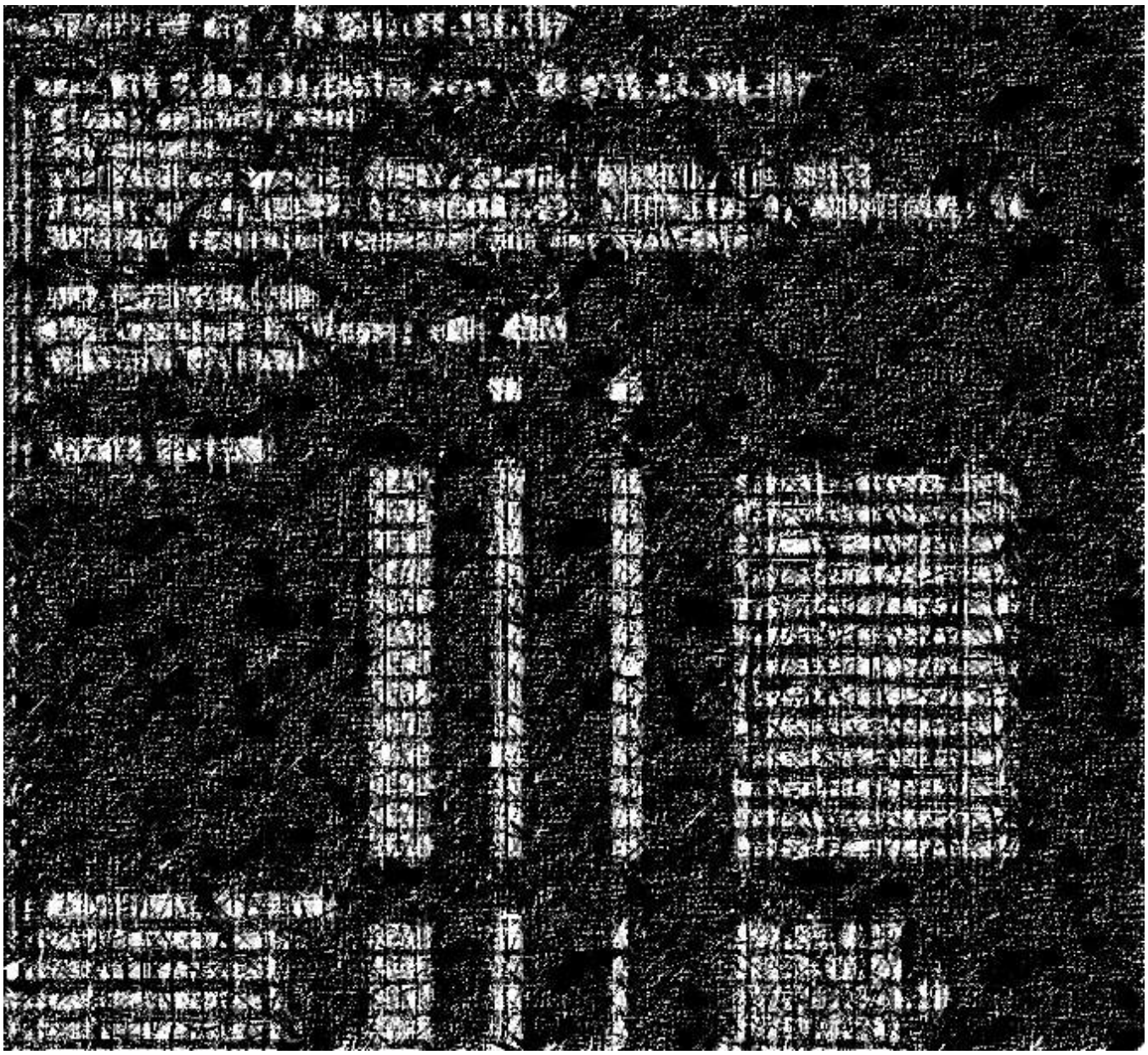


Fig 2: 911.54.151.119

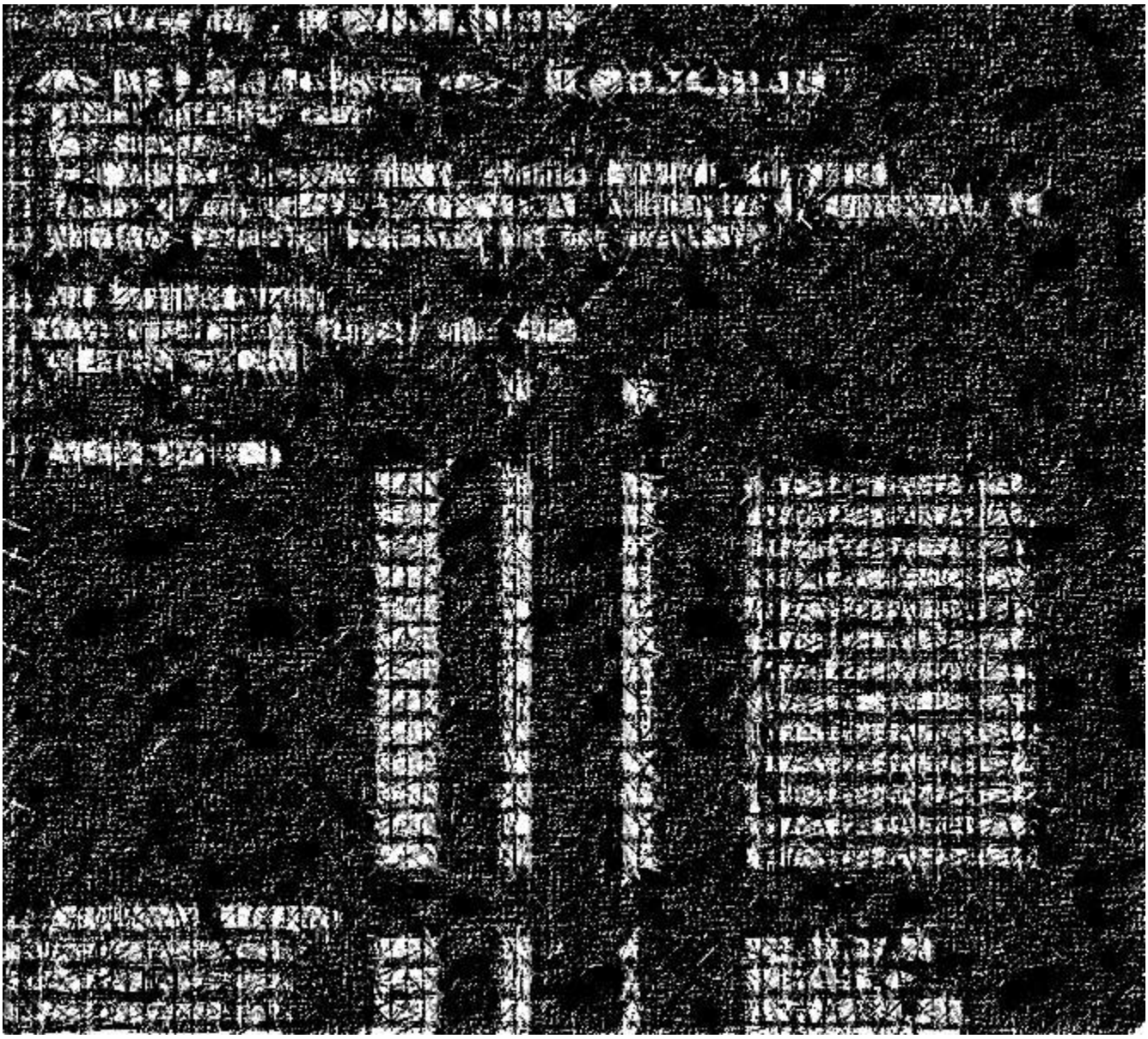


Fig 3: 911.54.138.125

3.2.2 Web Server Version Disclosure

Reference No:	**Vulnerability Rating:**
EXT_PT_02	**Low**
Tools Used	**CVSS-3.0 Score**
Manual assessment	CVE-2006-0987

Vulnerability Description:

Server shouldn't disclose version information. Attacker can further exploit if version is disclosed.

Exploitation Summary

If the version of your web server is known to be vulnerable to a specific exploit, the hacker would just need to use the exploit as part of his attack on your server.

Vulnerability Identified By / How It Was Discovered

Manual Analysis

Vulnerable URLs / IP Address

IP Address	Port
911.54.151.15	
911.54.151.20	
911.54.151.37	
911.54.151.36	
911.54.151.31	
911.54.151.45	
911.54.151.53	
911.54.151.54	
911.54.151.33	
911.54.151.118	
911.54.151.28	
911.54.151.44	
911.54.151.85	

Vulnerable Parameter(s)

Server version

Implications / Consequences of not Fixing the Issue

Chance of exploitation is easy if version is disclosed

Suggested Countermeasures

Configure your web server to prevent information leakage from the SERVER header of its HTTP response.

High-Level Category

Security Misconfiguration

References

NA

Proof of Concept:

Fig 1: 911.54.151.15

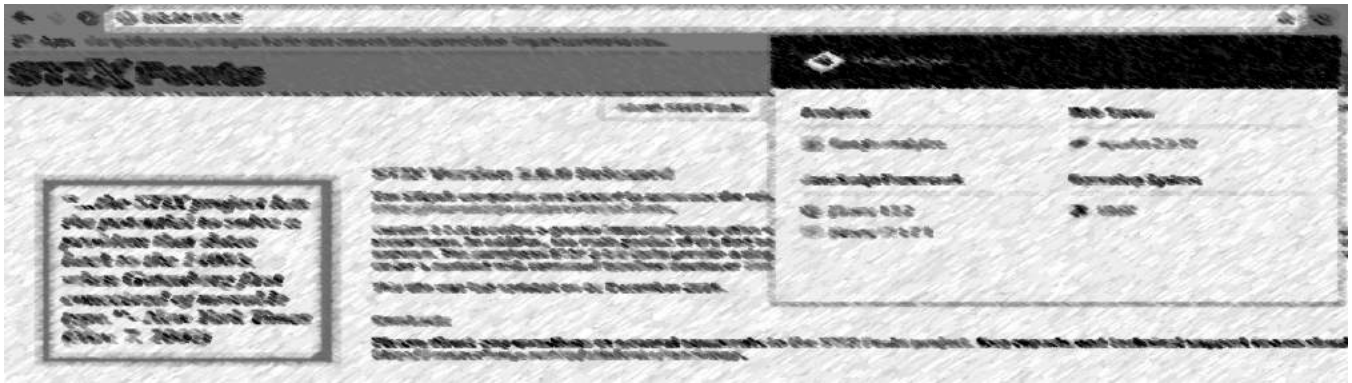


Fig 2: 911.54.151.20

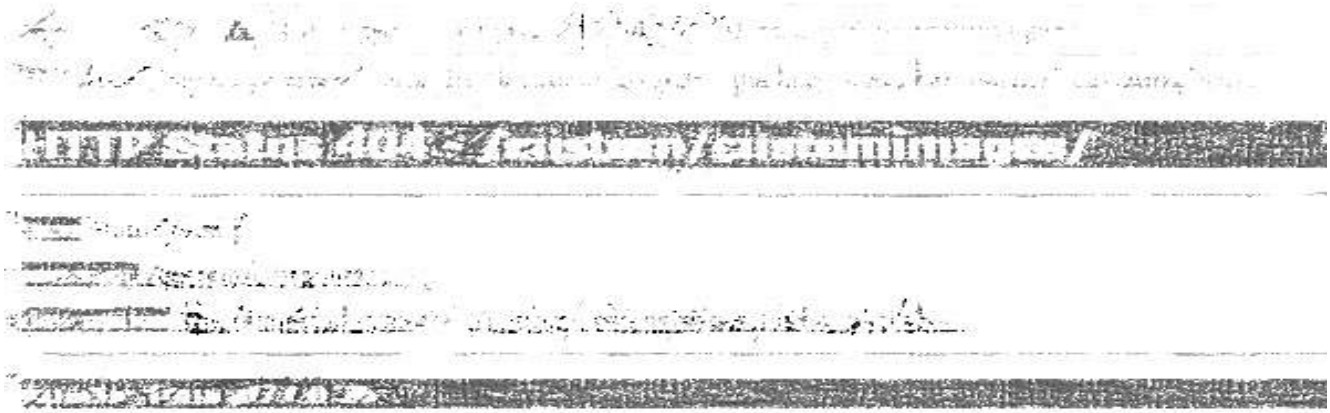


Fig 3: 911.54.151.28

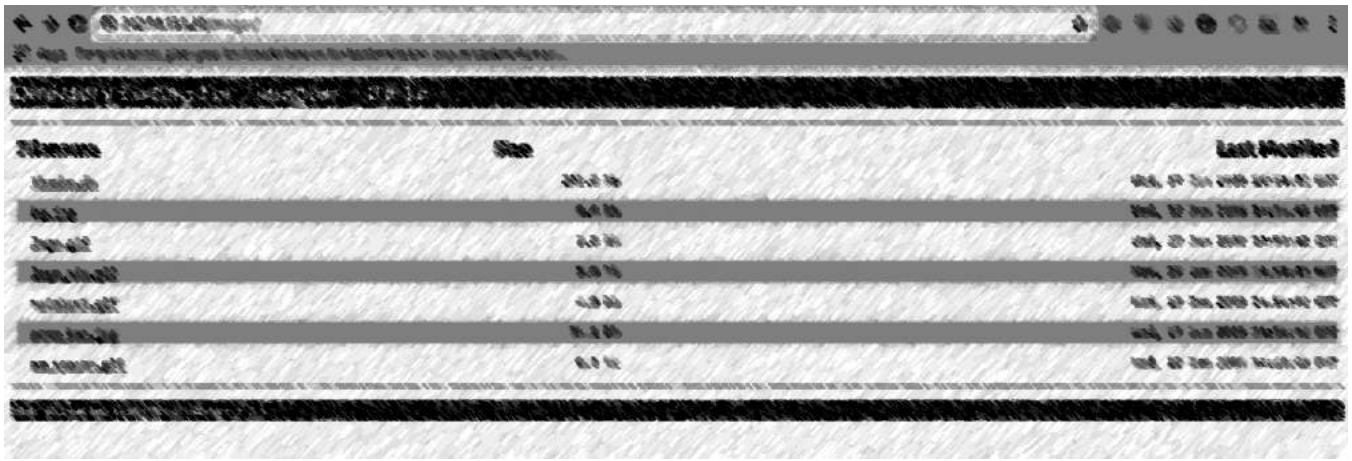


Fig 4: 911.54.151.31

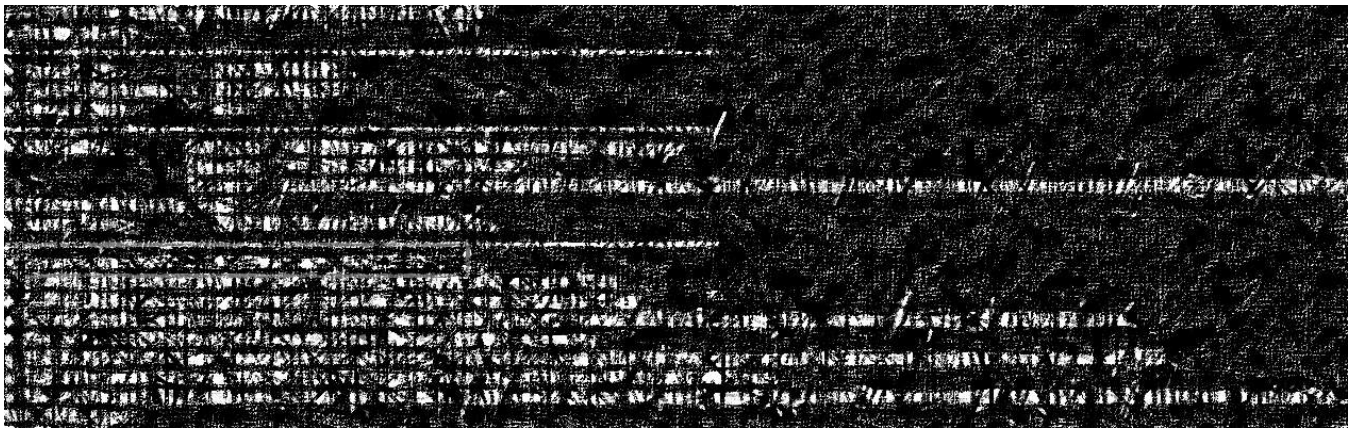


Fig 5: 911.54.151.33

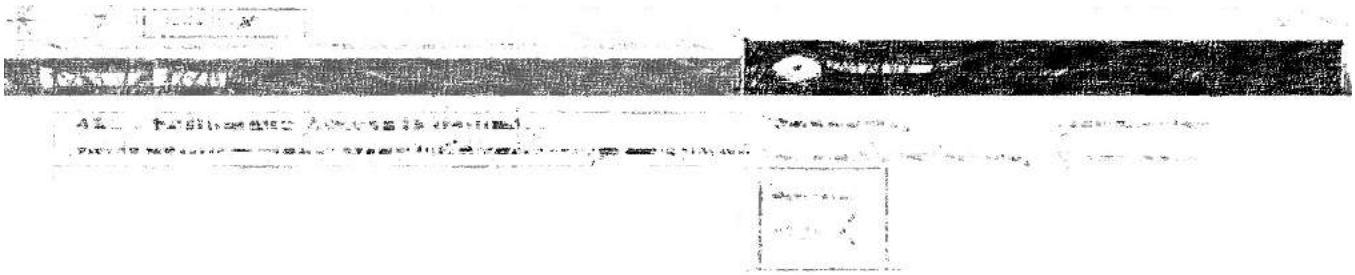


Fig 6: 911.54.151.36

Fig 7: 911.54.151.37

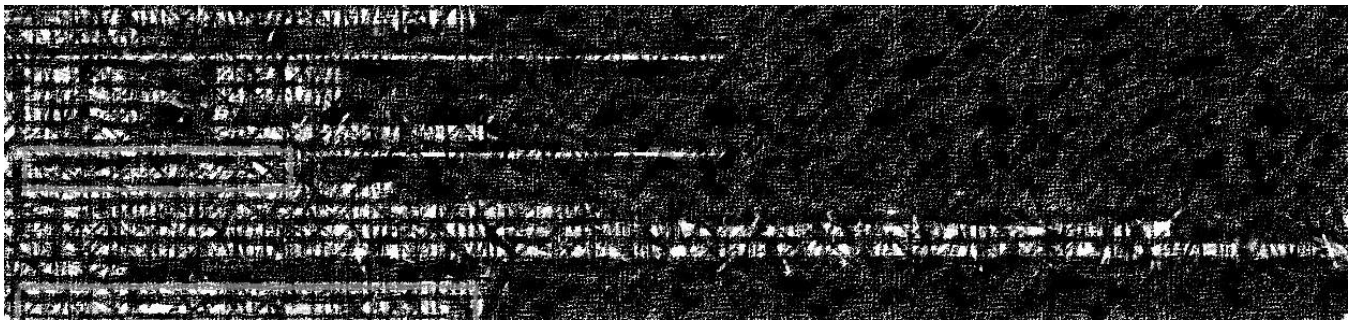


Fig 8: 911.54.151.44

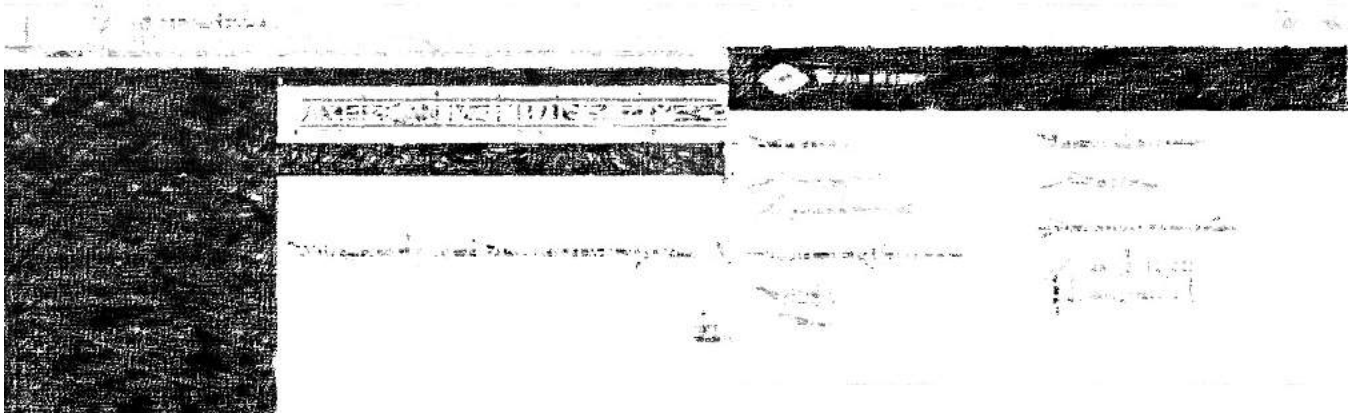


Fig 9: 911.54.151.45

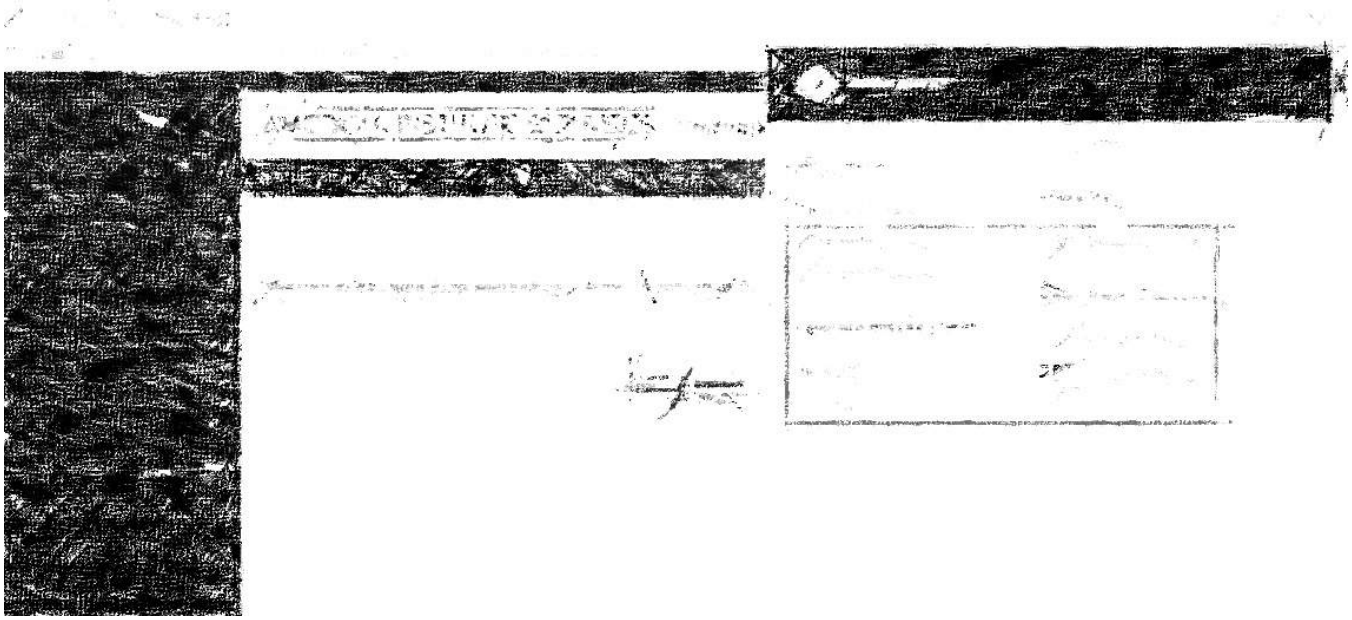


Fig 10: 911.54.151.53

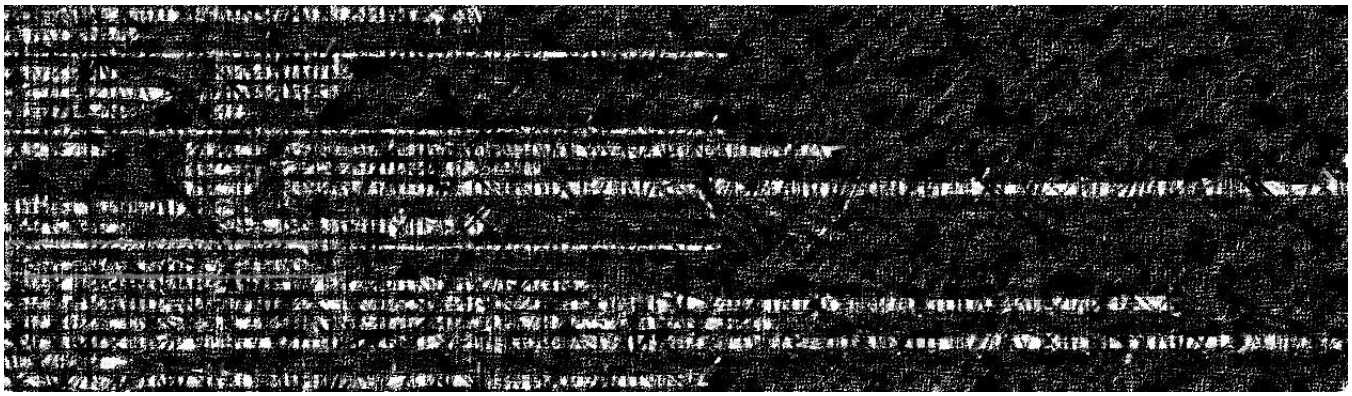


Fig 11: 911.54.151.54

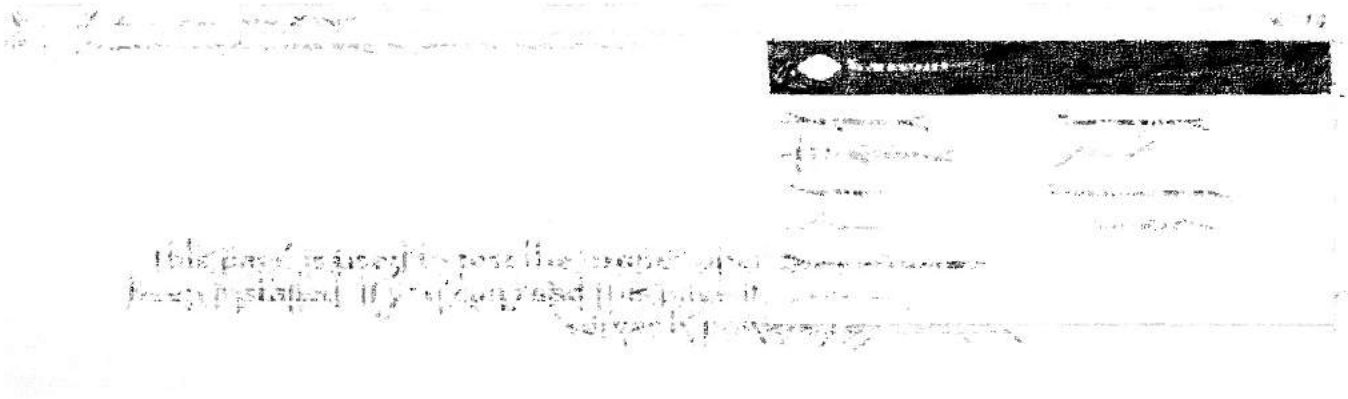


Fig 12: 911.54.151.85

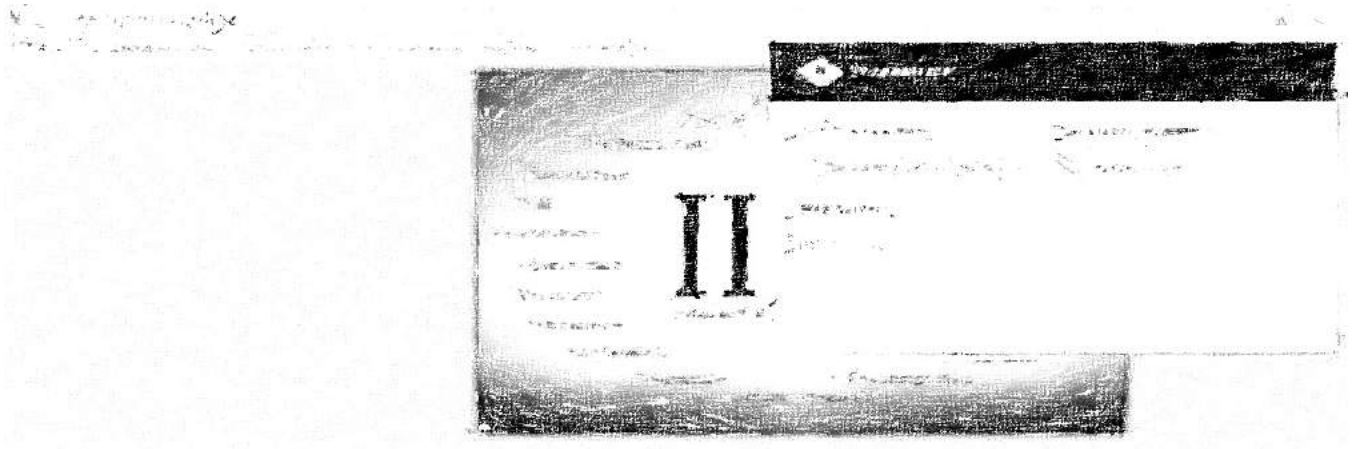
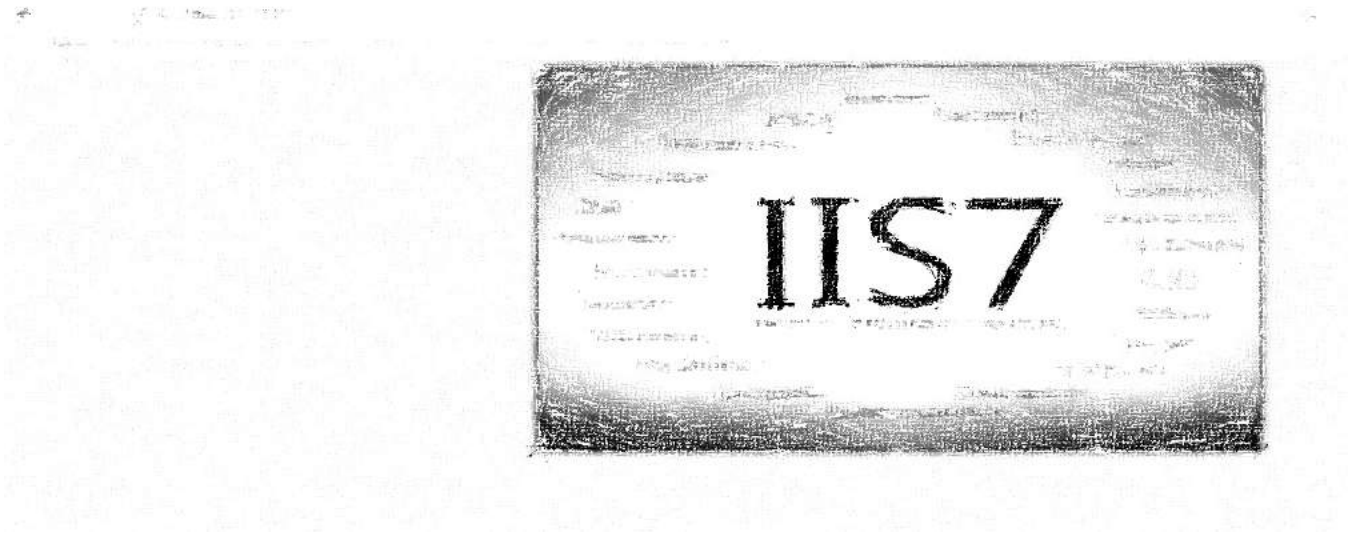


Fig 13: 911.54.151.118



3.2.3 Clickjacking

Reference No:	Vulnerability Rating:
EXT_PT_03	**Low**
Tools Used	**CVSS-3.0 Score**
Browser based manual attack	CVE-2016-1941

Vulnerability Description:

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

Exploitation Summary

It might be possible for a web page controlled by an attacker to load the content of this response within an iframe on the attacker's page. This may enable a "clickjacking" attack, in which the attacker's page overlays the target application's interface with a different interface provided by the attacker. By inducing victim users to perform actions such as mouse clicks and keystrokes, the attacker can cause them to unwittingly carry out actions within the application that is being targeted. This technique allows the attacker to circumvent defenses against cross-site request forgery, and may result in unauthorized actions.

Vulnerability Identified By / How It Was Discovered

Manual Analysis

Vulnerable URLs / IP Address

IP Address	Port
911.54.151.15	
911.54.151.20	
911.54.151.54	
911.54.151.105	

Vulnerable Parameter(s)

Entire site

Implications / Consequences of not Fixing the Issue

It might be possible for a web page controlled by an attacker

Suggested Countermeasures

To effectively prevent framing attacks, the application should return a response header with the name X-Frame-Options and the value DENY to prevent framing altogether, or the value SAMEORIGIN to allow framing only by pages on the same origin as the response itself.

High-Level Category

Security Misconfiguration

References

NA

Proof of Concept:

Fig 1: 911.54.151.15

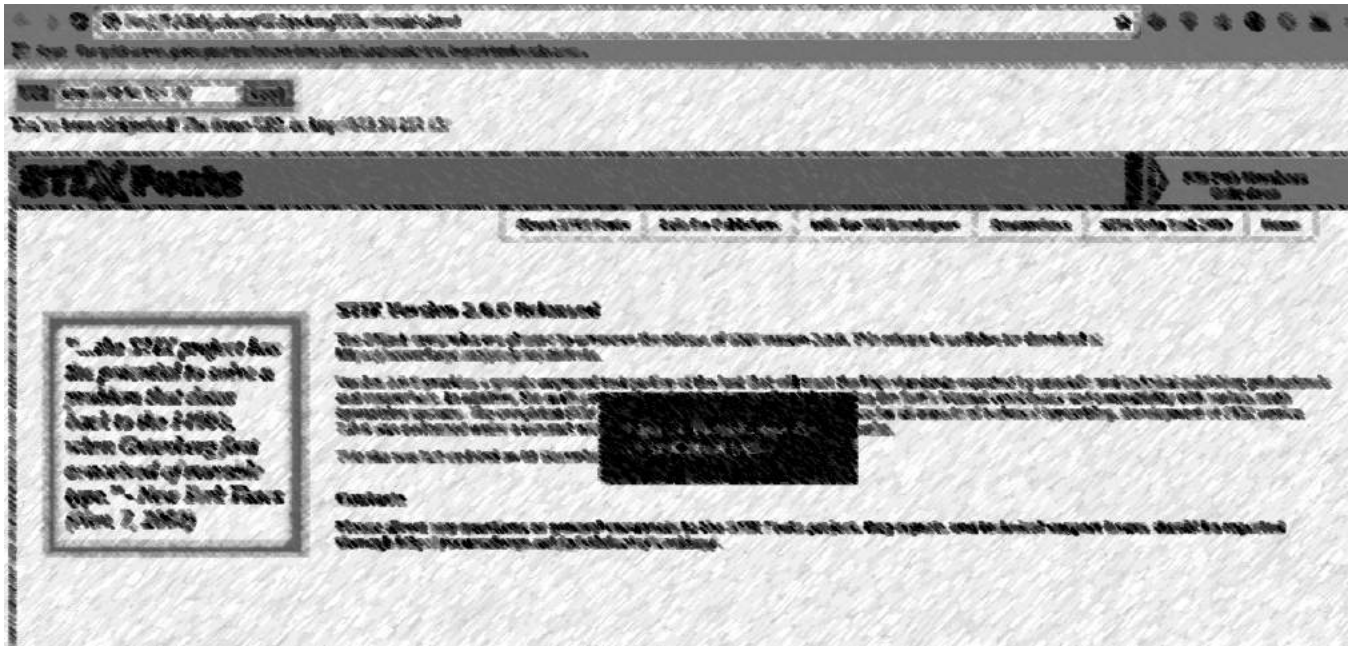


Fig 2: 911.54.151.20

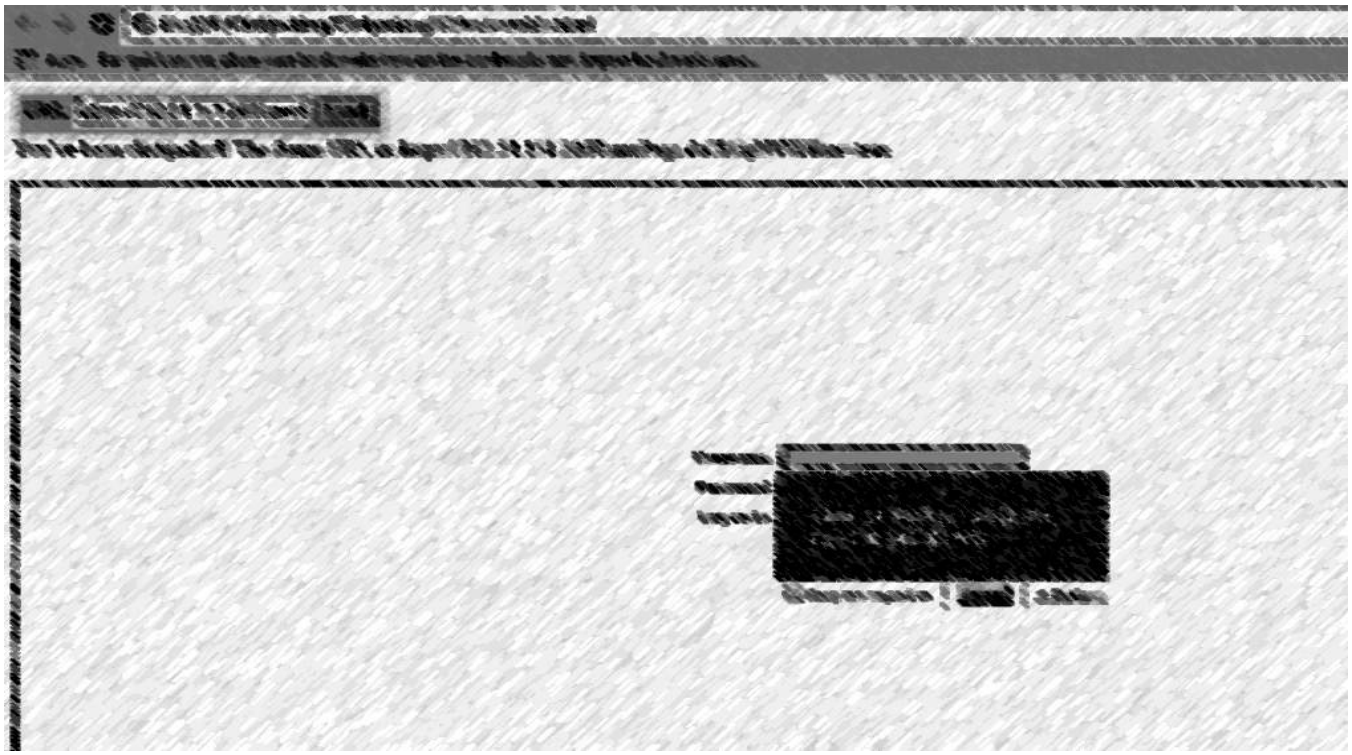


Fig 3: 911.54.151.54

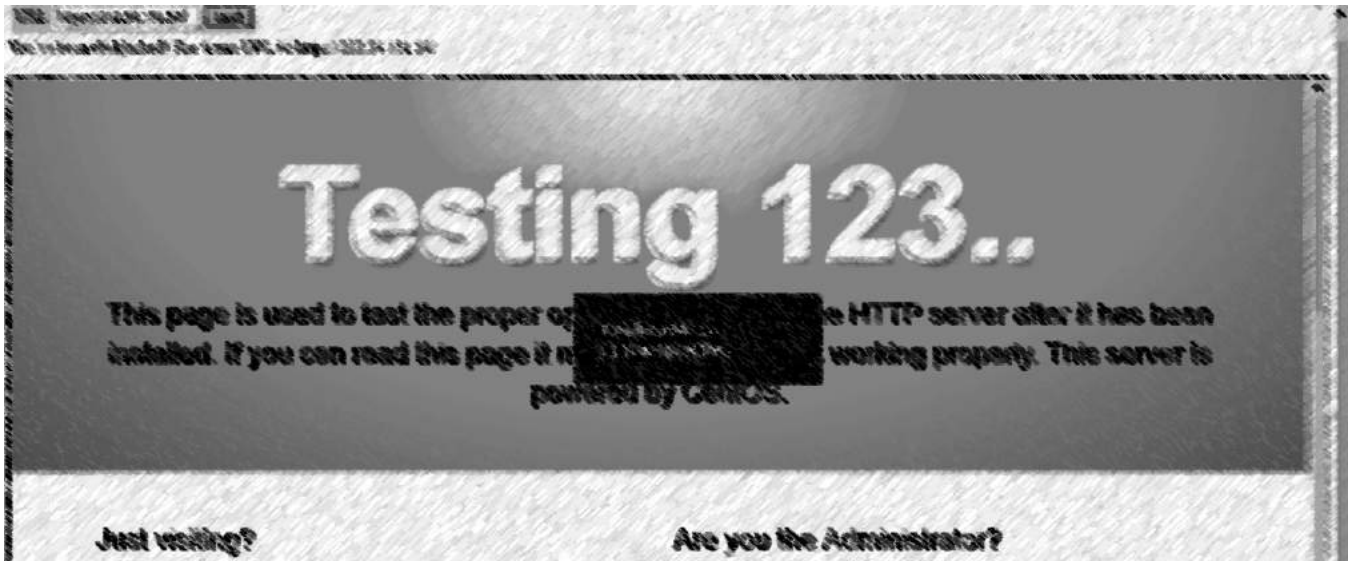
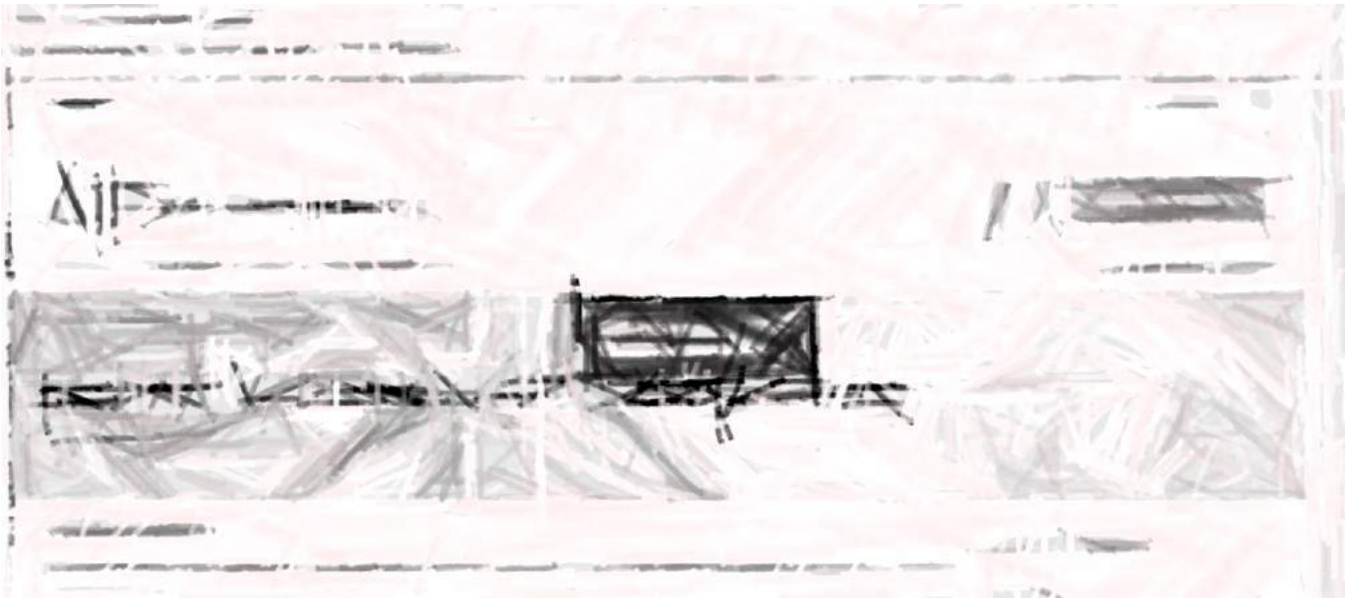


Fig 4: 911.54.151.105



3.2.4 SSL 64-bit Block Size Cipher Suites Supported (SWEET 32)

Reference No:	Vulnerability Rating:
EXT_PT_04	**Low**
Tools Used	**CVSS-3.0 Score**
Nessus & Nmap	NA

Vulnerability Description:

Legacy block ciphers having block size of 64 bits are affected by a vulnerability, known as SWEET32.A man-in-the-middle attacker who has sufficient resources can exploit this vulnerability via birthdayattack
By misusing the SWEET32 vulnerability, an attacker can send in large volume of dummy data, and get blocks of cipher text that matches that of a customer.

Attack Process:
1. The attacker sniffs all data sent to your customer.
2. Attacker sends dummy data to your server until a key used for a customer matches the attacker's session key.
3. Once there's a match, sensitive data can be decrypted by determining how the key was chosen.

Exploitation Summary

1. The attacker sniffs all data sent to your customer.
2. Attacker sends dummy data to your server until a key used for a customer matches the attacker's session key.
3. Once there's a match, sensitive data can be decrypted by determining how the key was chosen.

Vulnerability Identified By / How It Was Discovered

Automated & Manual analysis

Vulnerable URLs / IP Address

IP Address	Port
911.54.151.36	
911.54.151.33	
911.54.151.54	
911.54.151.72	
911.54.151.80	
911.54.151.76	
911.54.151.85	
911.54.151.86	
911.54.151.110	
911.54.151.32	
911.54.151.118	
911.54.151.101	
911.54.151.28	
911.54.151.31	
911.54.151.44	

911.54.151.41	
Vulnerable Parameter(s)	
3DES Ciphers	
Implications / Consequences of not Fixing the Issue	
An attacker can send in large volume of dummy data, and get blocks of cipher text that matches that of a customer.	
Suggested Countermeasures	
The obvious way to avoid these attacks is to stop using legacy 64-bit block ciphers. Alternatively, the attack can be mitigated by rekeying the session frequently.	
High-Level Category	
Using Weak Ciphers	
References	
https://sweet32.info https://www.openssl.org/blog/blog/2016/08/24/sweet32/	

Proof of Concept:

Fig 1: 911.54.151.28

Fig 2: 911.54.151.31

Fig 3: 911.54.151.32

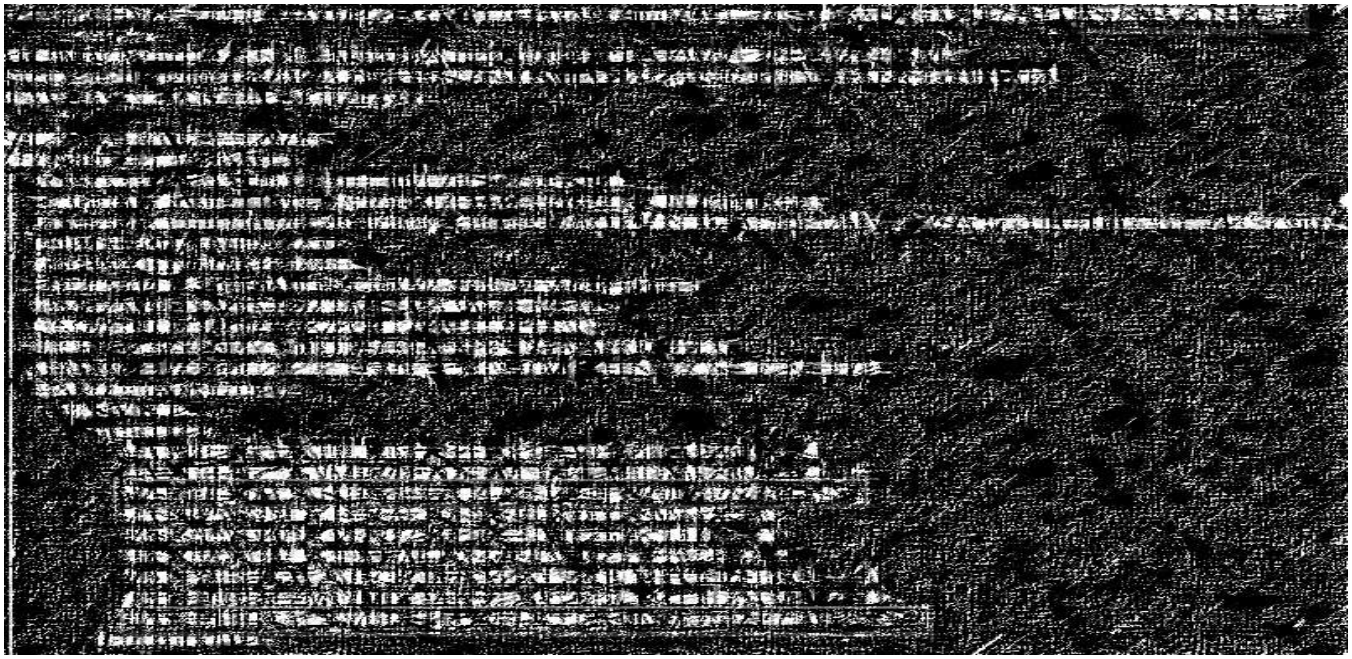


Fig 4: 911.54.151.33

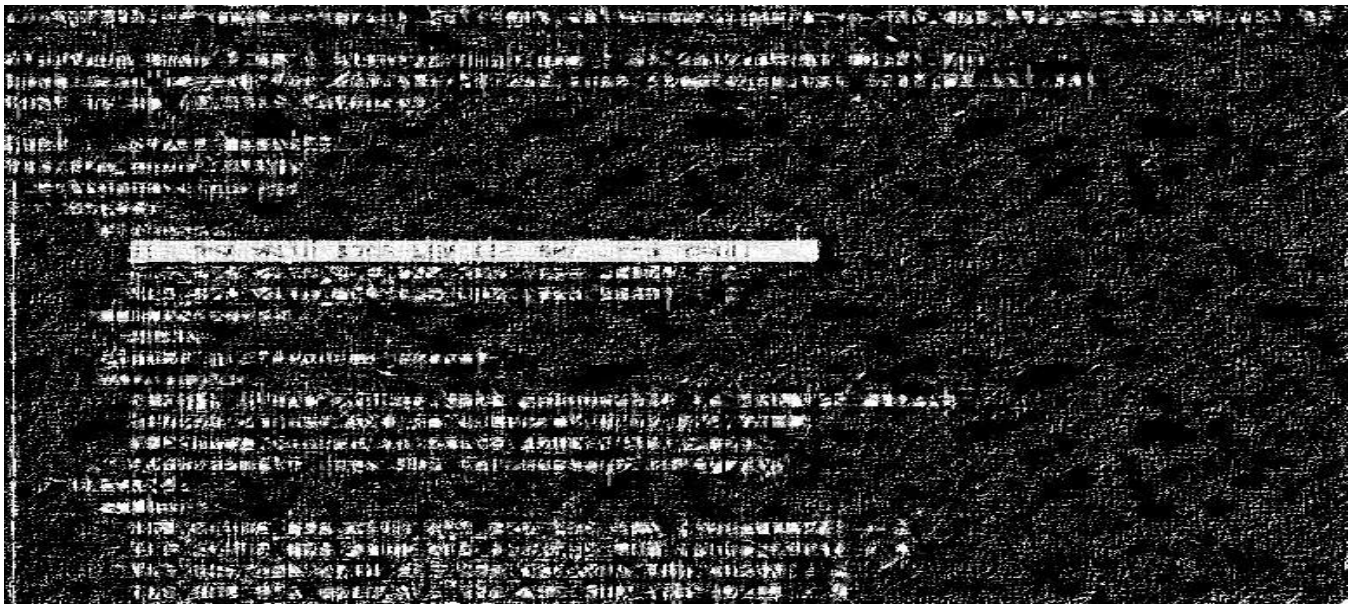


Fig 5: 911.54.151.36

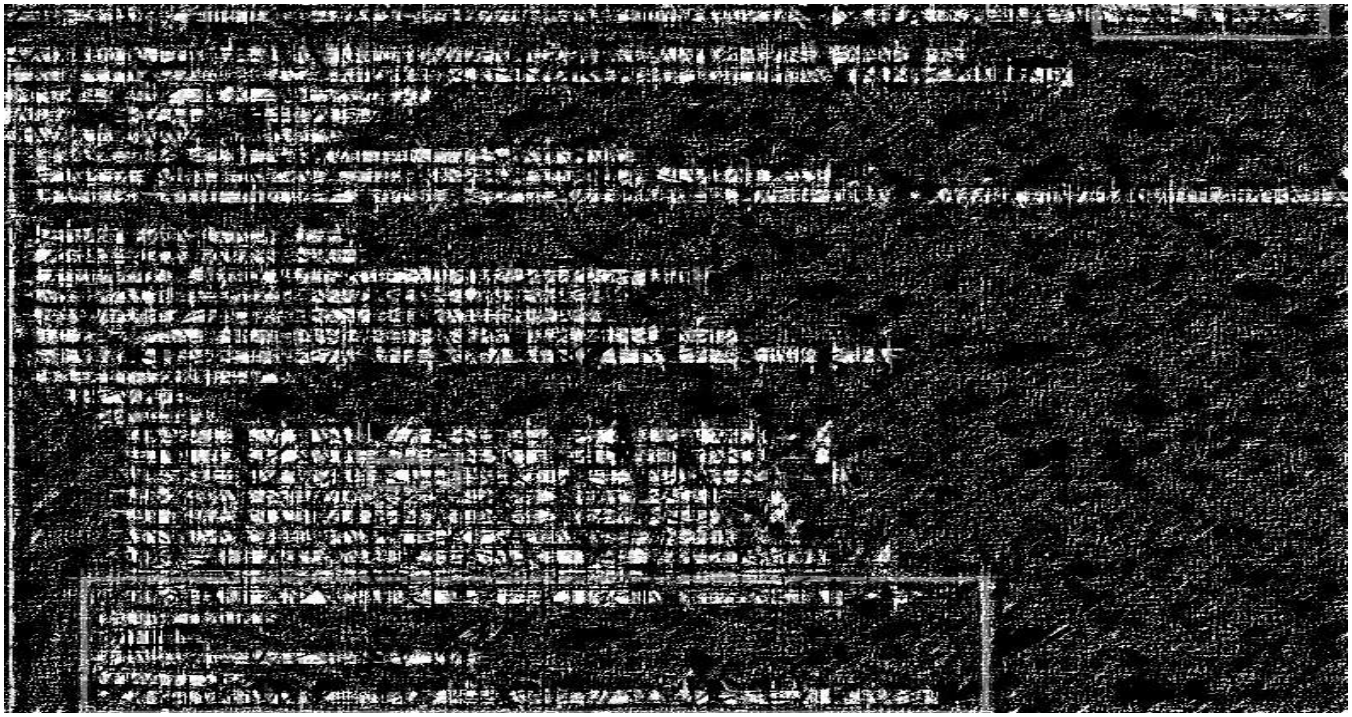


Fig 6: 911.54.151.41

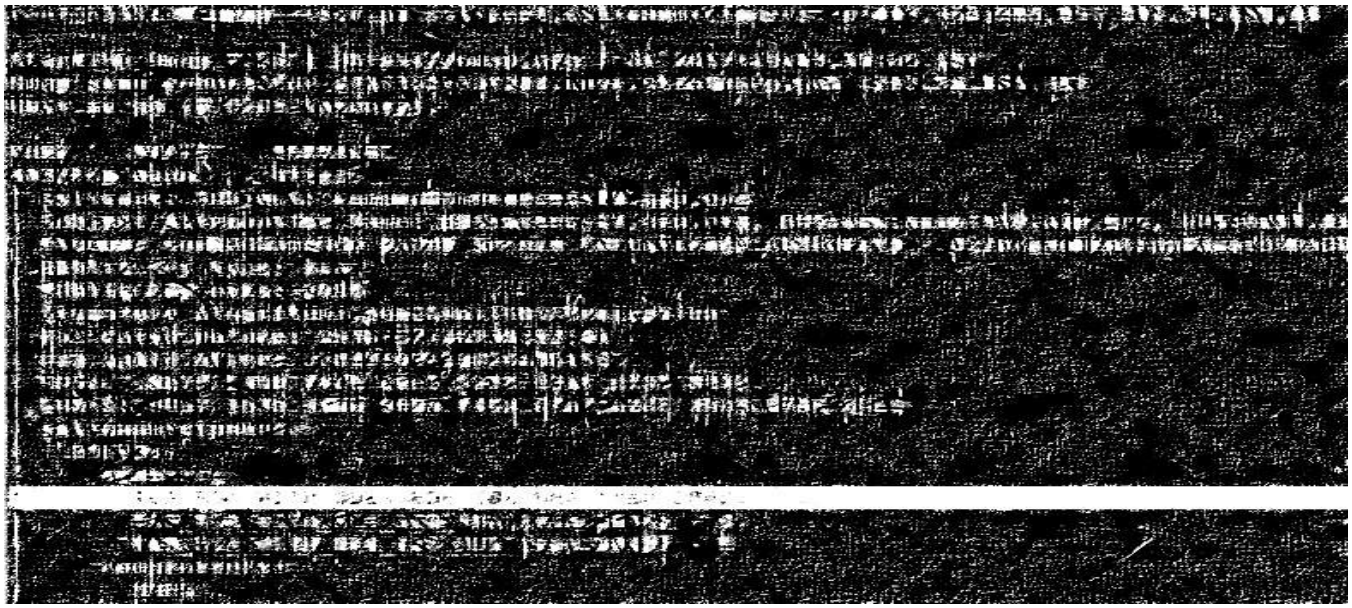


Fig 7: 911.54.151.44

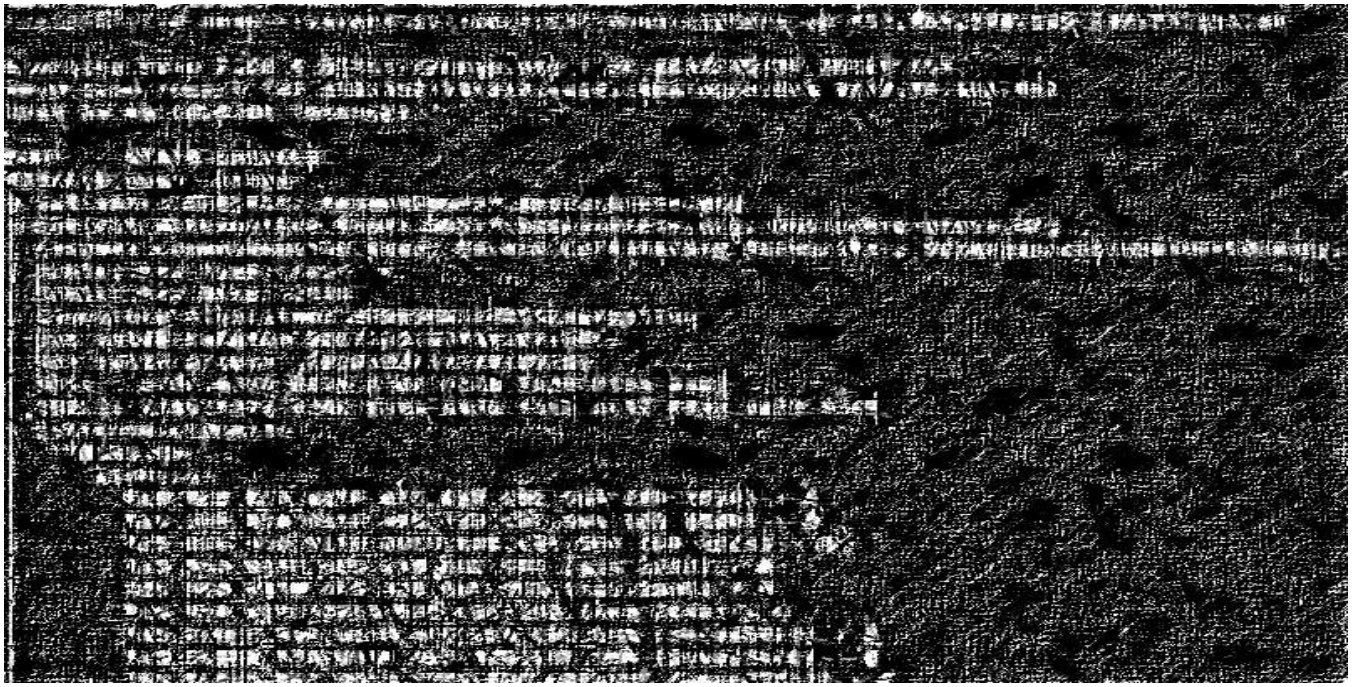


Fig 8: 911.54.151.54

Fig 9: 911.54.151.72

Fig 10: 911.54.151.76

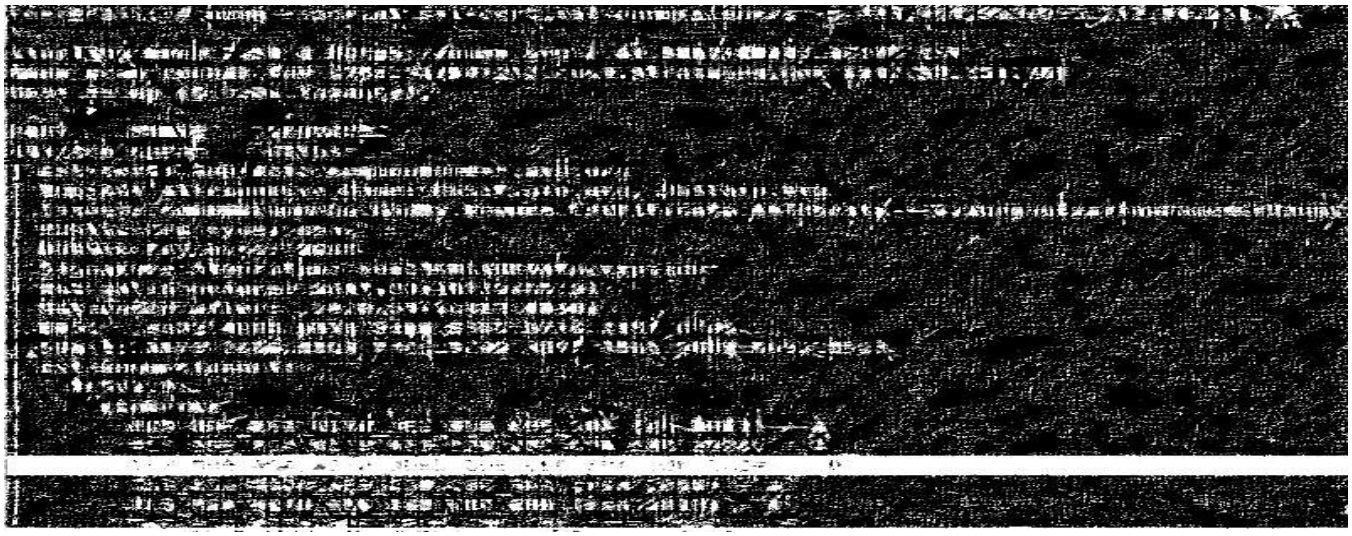


Fig 11: 911.54.151.80

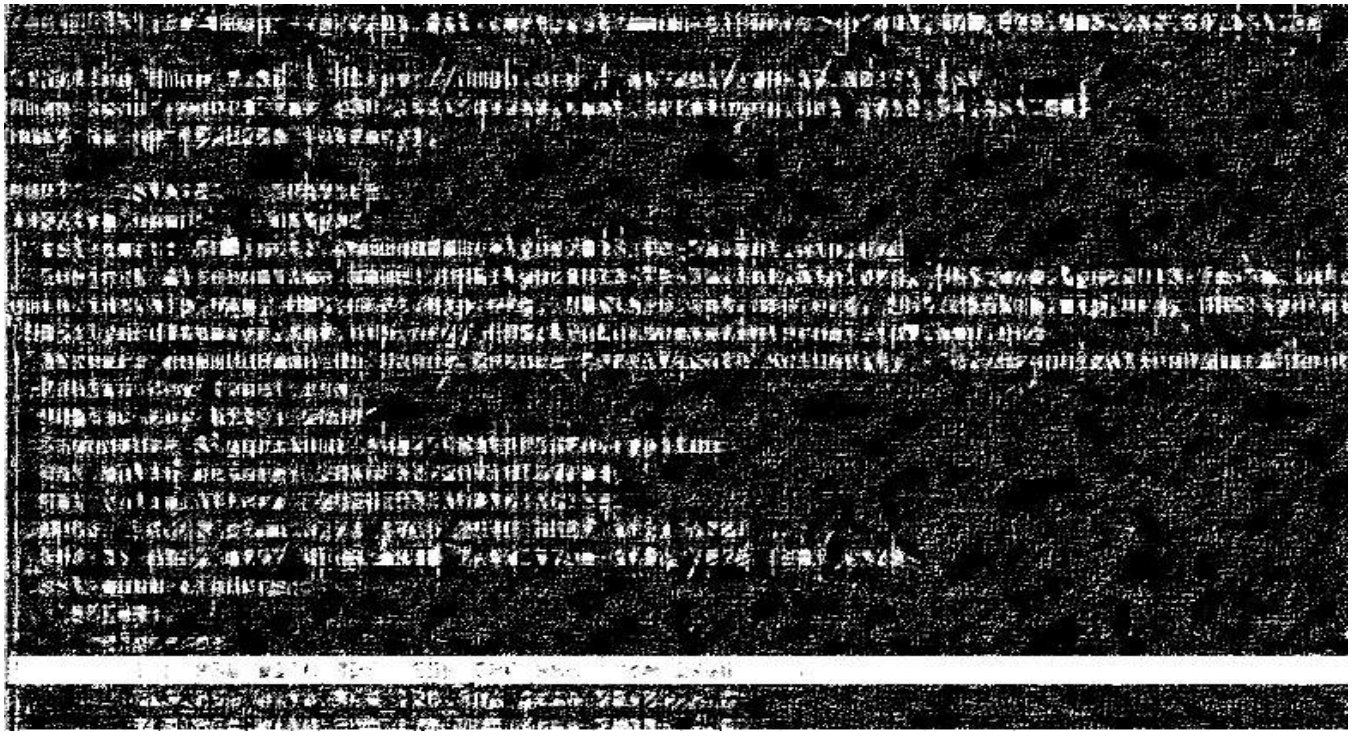


Fig 12: 911.54.151.85

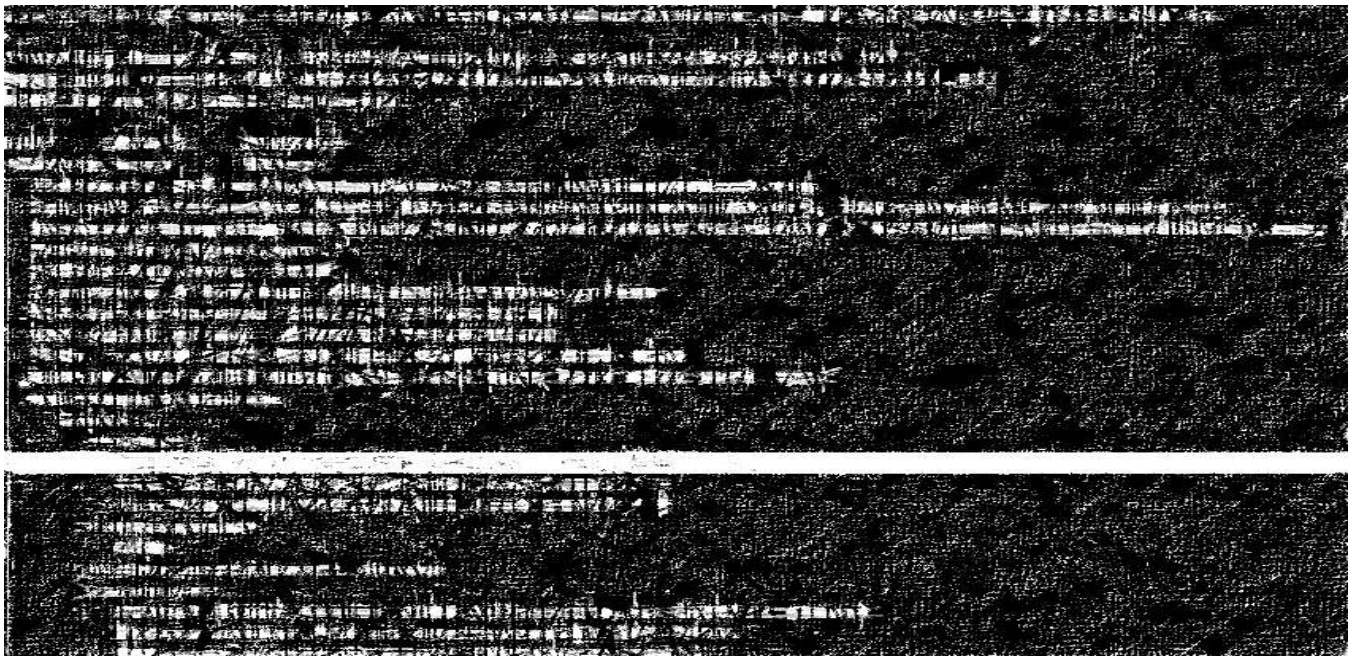


Fig 13: 911.54.151.86

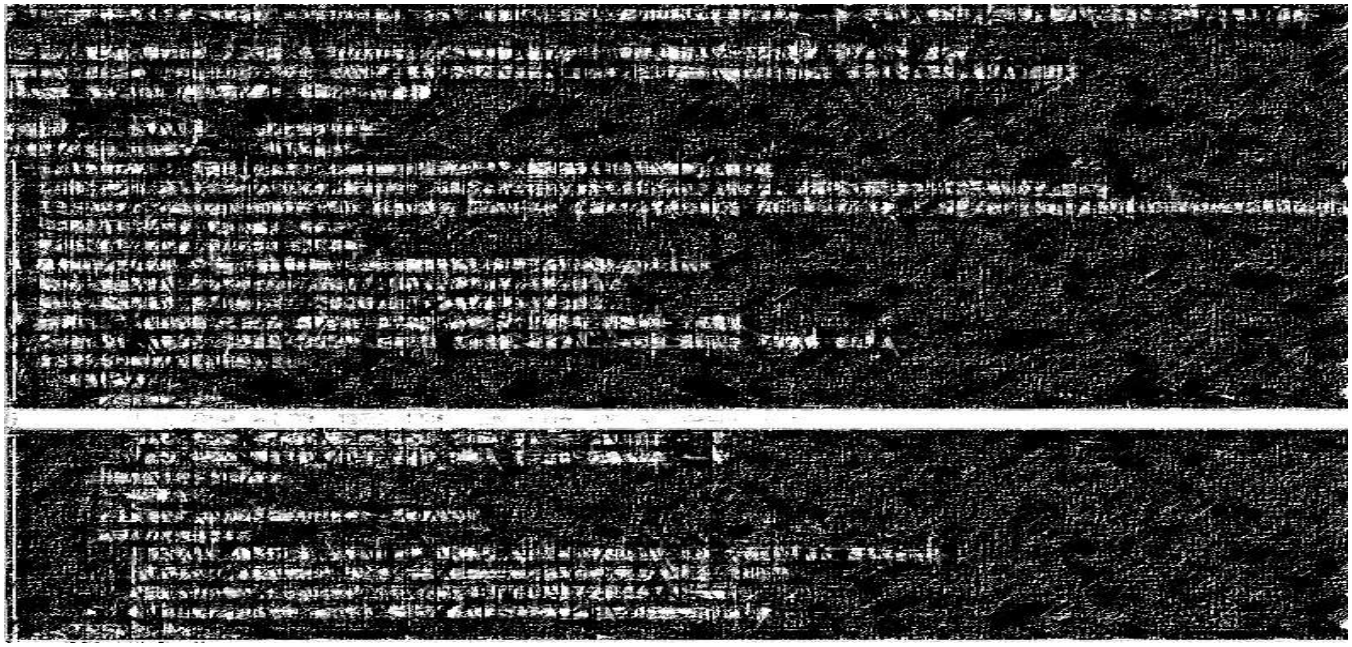


Fig 14: 911.54.151.101

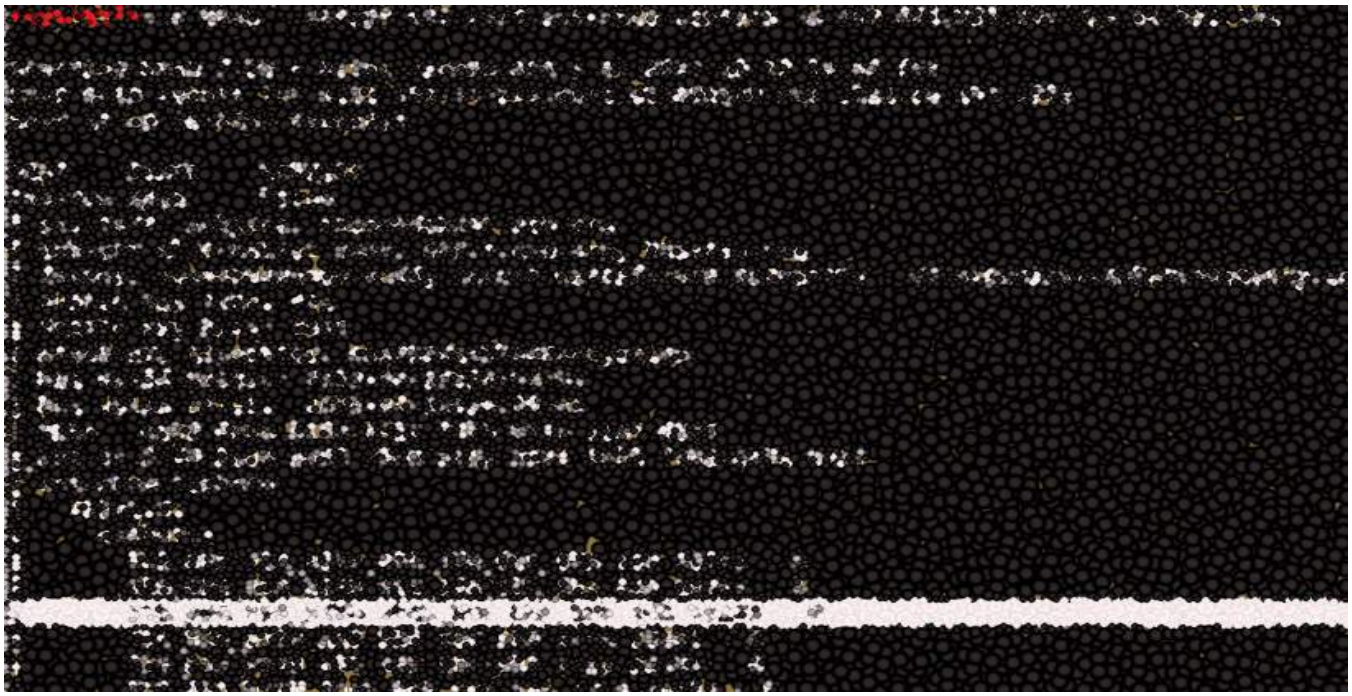


Fig 15: 911.54.151.110

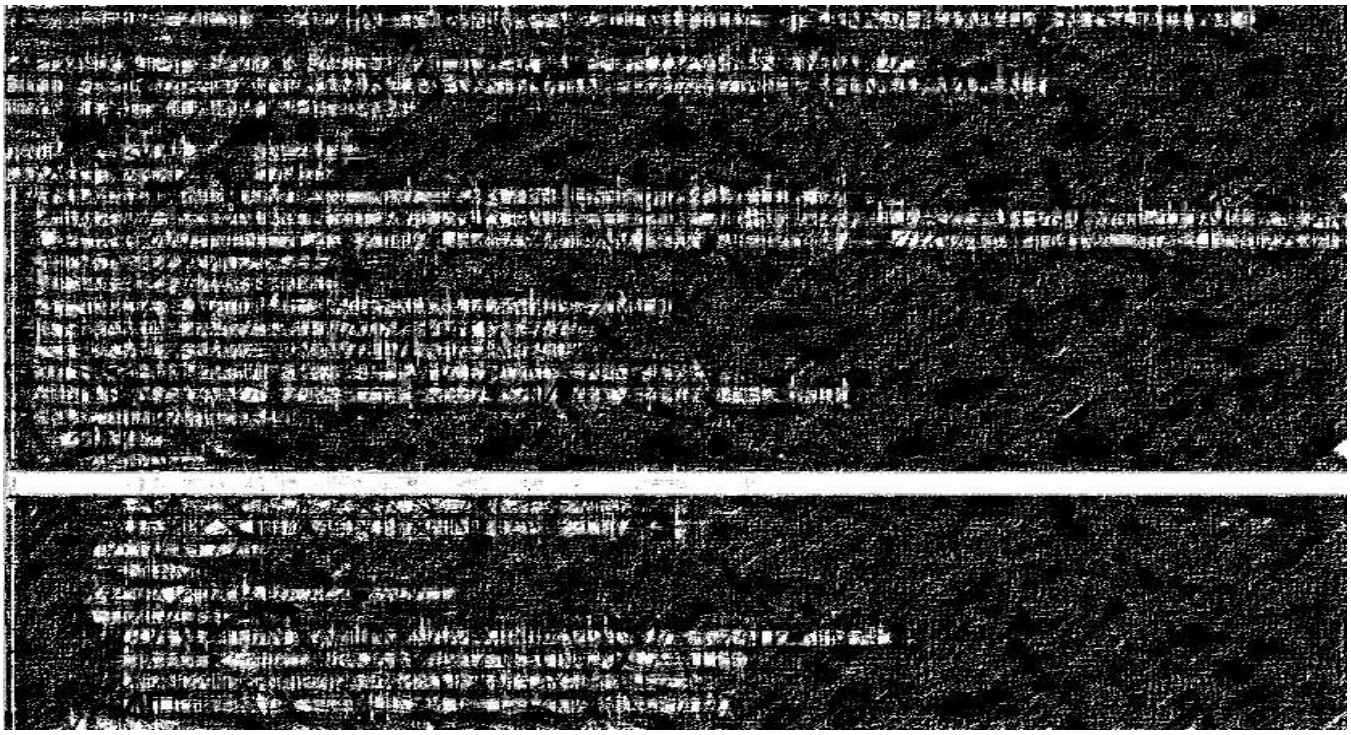
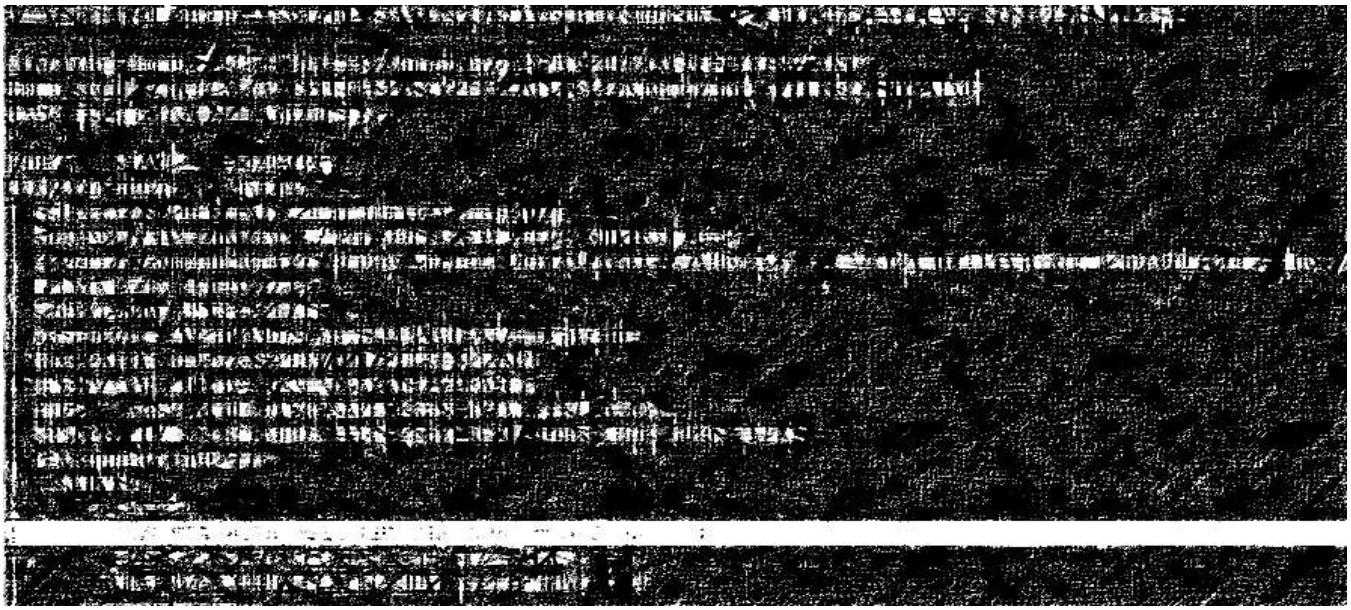


Fig 16: 911.54.151.118



3.2.5 SSL RC4 Cipher Suites Supported

Reference No:	Vulnerability Rating:
EXT_PT_05	**Low**
Tools Used	**CVSS-3.0 Score**
Nessus & Nmap	CVE-2013-2566

Vulnerability Description:

The remote host supports the use of RC4 in one or more cipher suites. The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

Exploitation Summary

The attacker intercepts a large number of SSL/TLS connections that use RC4, and waits until a weak key is found. The weak key can then be used to recover partial plain text data. Researchers have determined that one out of every 16 million RC4 keys is weak.

Vulnerability Identified By / How It Was Discovered

Automated & Manual Analysis

Vulnerable URLs / IP Address

IP Address	Port
911.54.151.33	
911.54.149.132	
911.54.151.40	
911.54.151.42	
911.54.151.41	
911.54.151.54	
911.54.151.80	
911.54.151.85	
911.54.151.110	

Vulnerable Parameter(s)

RC4 Ciphers

Implications / Consequences of not Fixing the Issue

An adversary may identify known vulnerabilities in the installed version of the PHP and exploit those vulnerability further.

Suggested Countermeasures

Reconfigure the affected application. If possible, avoid the use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

High-Level Category

Using Weak Ciphers

References

NA

Proof of Concept:

Fig 1: 911.54.151.33

Fig 2: 911.54.151.40

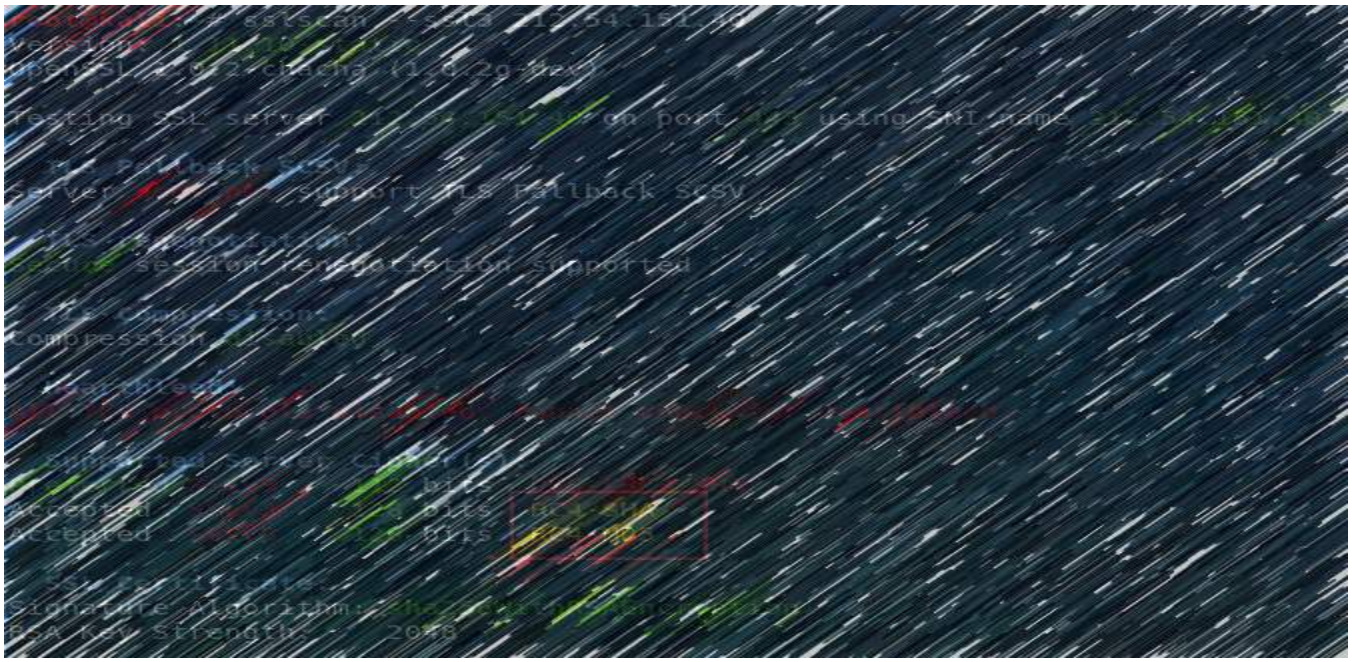


Fig 3: 911.54.151.41

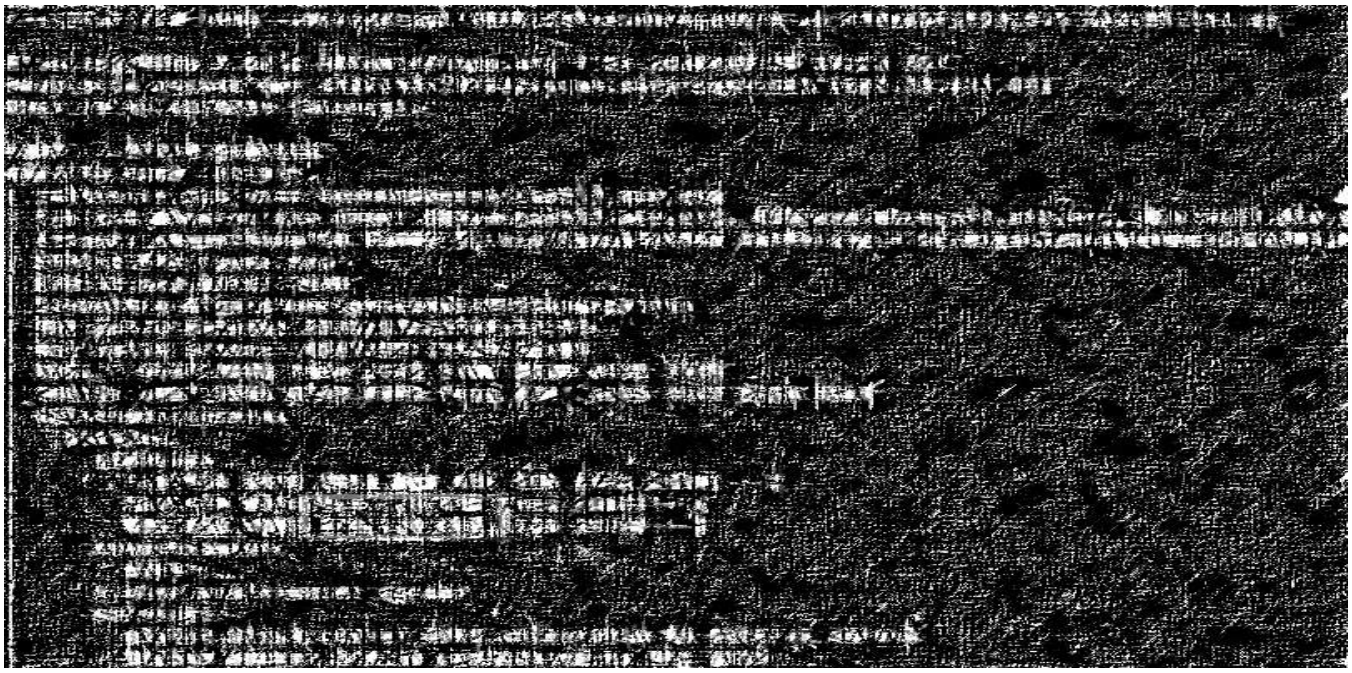


Fig 4: 911.54.151.42

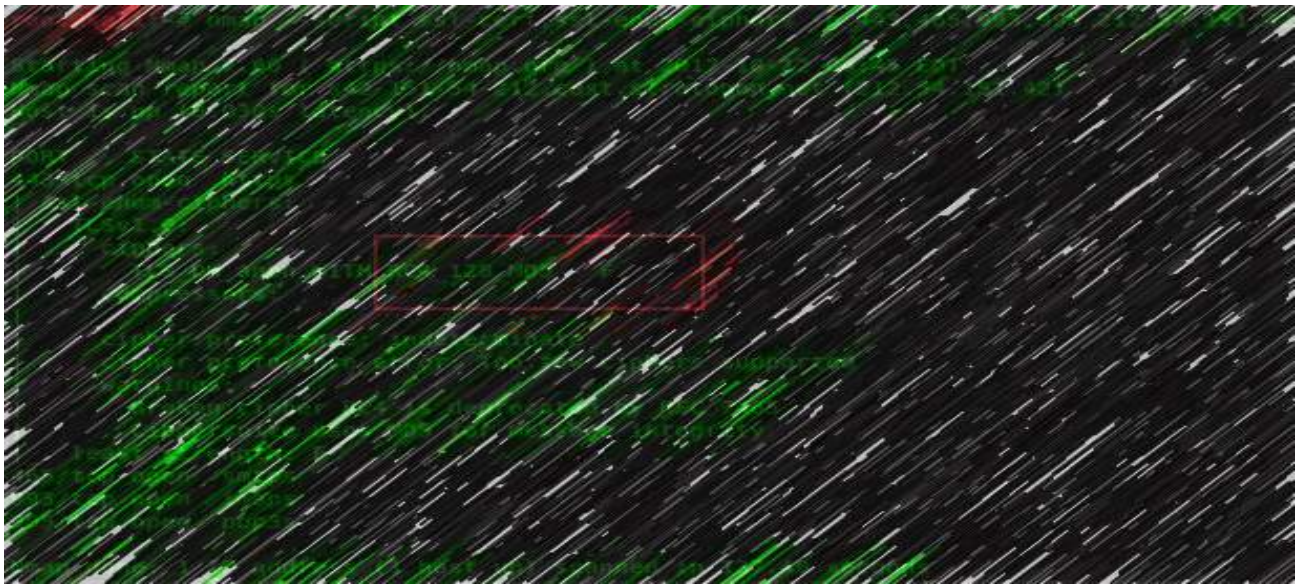


Fig 5: 911.54.151.54

Fig 6: 911.54.151.80

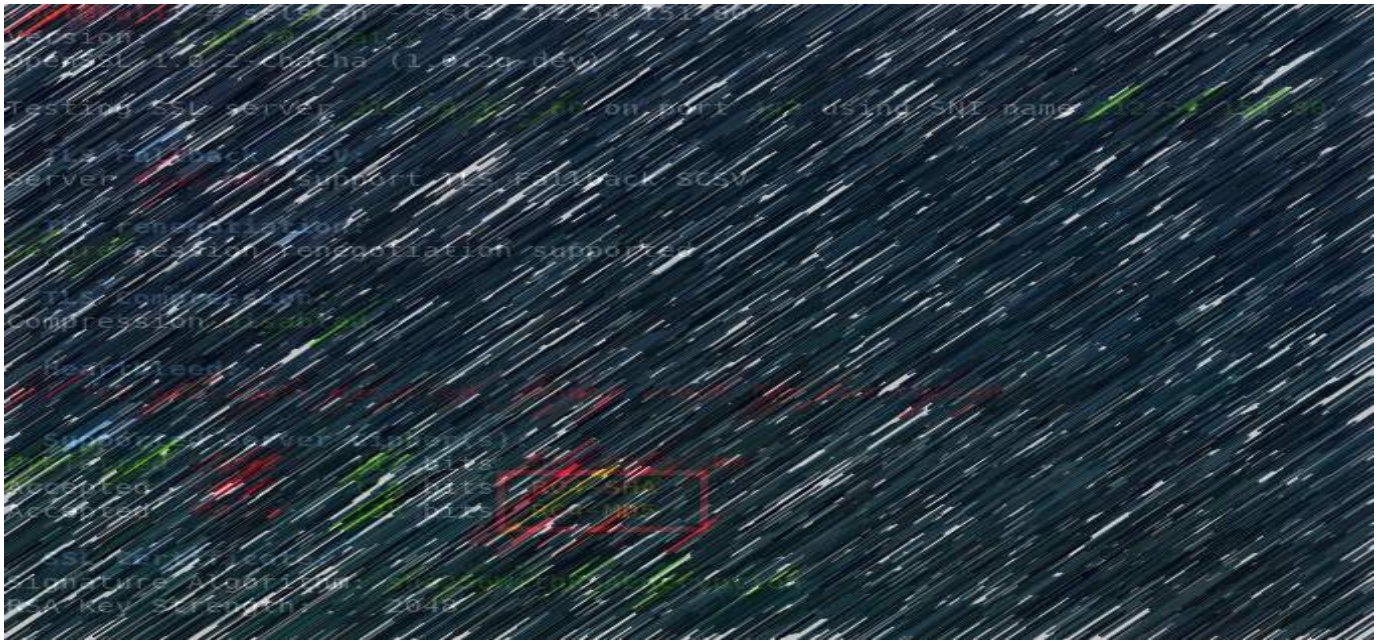


Fig 7: 911.54.151.85

Fig 8: 911.54.151.110

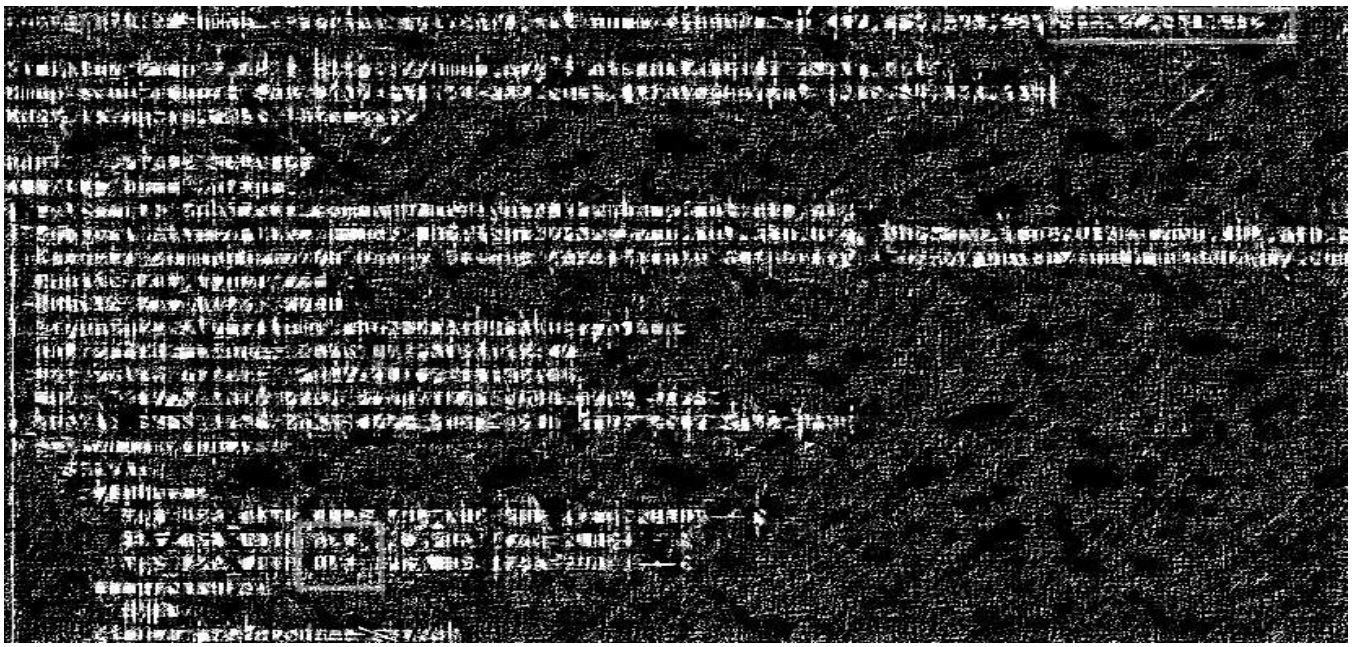
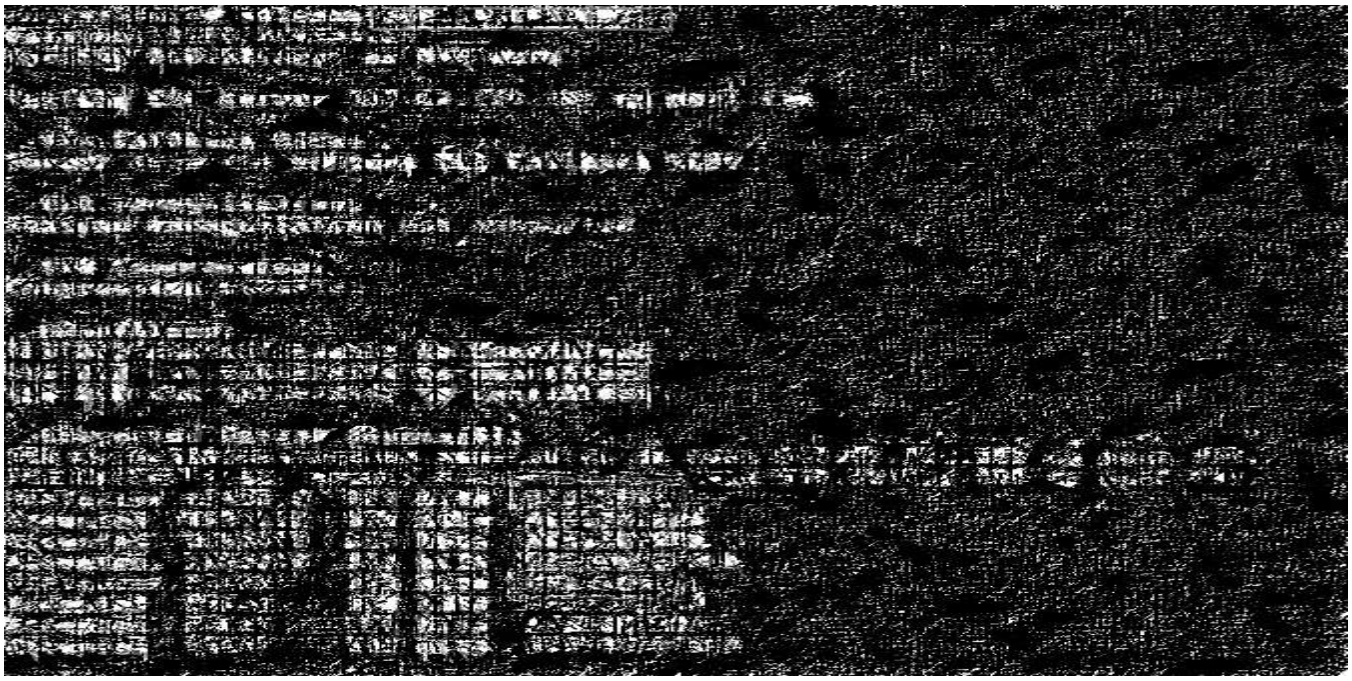


Fig 9: 911.54.149.132



3.2.6 SSLv3 Padding Oracle on Downgraded Legacy Encryption Vulnerability

Reference No:	**Vulnerability Rating:**
EXT_PT_06	Low
Tools Used	**CVSS-3.0 Score**
SSL Scan	CVE-2014-3566

Vulnerability Description:

If Poodle SSLv3 on any website, then it is vulnerable to poodlebleed attack. The remote service accepts connections encrypted using SSL 3.0. These versions of SSL reportedly suffer from several cryptographic flaws.

Exploitation Summary

A typical attack scenario is that a victim has visited a web server and her web browser now contains a cookie that an attacker wishes to steal. For a successful attack, the attacker must be able to modify network traffic between the victim and this web server, and both victim and system must be willing to use SSL 3.0 for encryption

An Attacker can exploit the vulnerability to decrypt and pull information from within an encrypted transaction.

Vulnerability Identified By / How It Was Discovered

Automated & Manual Analysis

Vulnerable URLs / IP Address

IP Address	Port
911.54.151.33	
911.54.151.54	
911.54.151.80	
911.54.151.85	
911.54.151.86	
911.54.151.110	
911.54.151.118	
911.54.151.40	
911.54.151.41	

Vulnerable Parameter(s)

SSLv3 Protocol

Implications / Consequences of not Fixing the Issue

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC'S definition of strong cryptography

Use the TLS 1.1 or more

Suggested Countermeasures

Common ways to prevent or mitigate the impact of DNS amplification attacks include tightening DNS server security, blocking specific DNS servers or all open recursive relay servers, and rate limiting.

High-Level Category

Using SSLV3 Which is no longer used for secure communication

References
NA

Proof of Concept:

Fig 1: 911.54.151.33

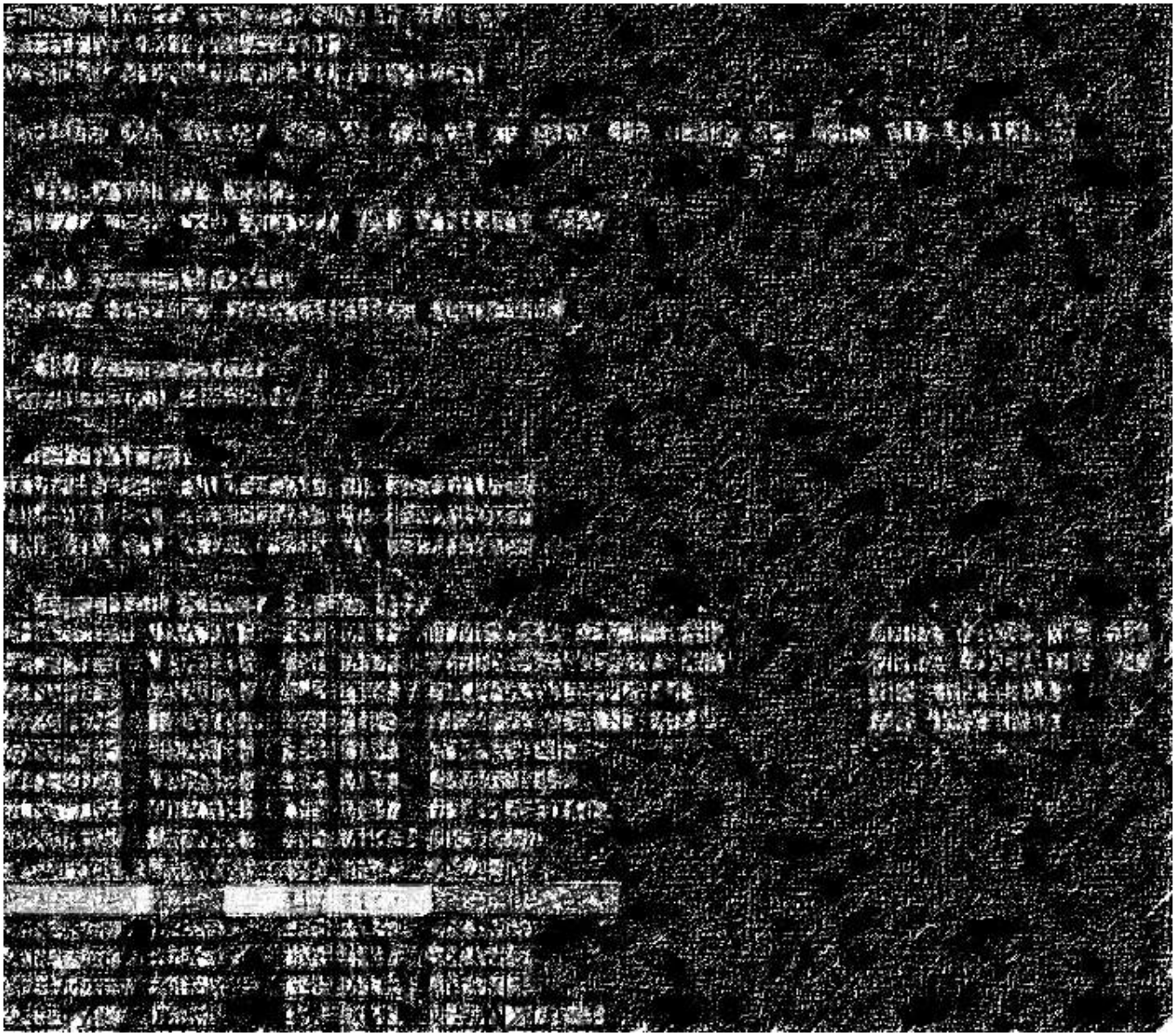


Fig 2: 911.54.151.40

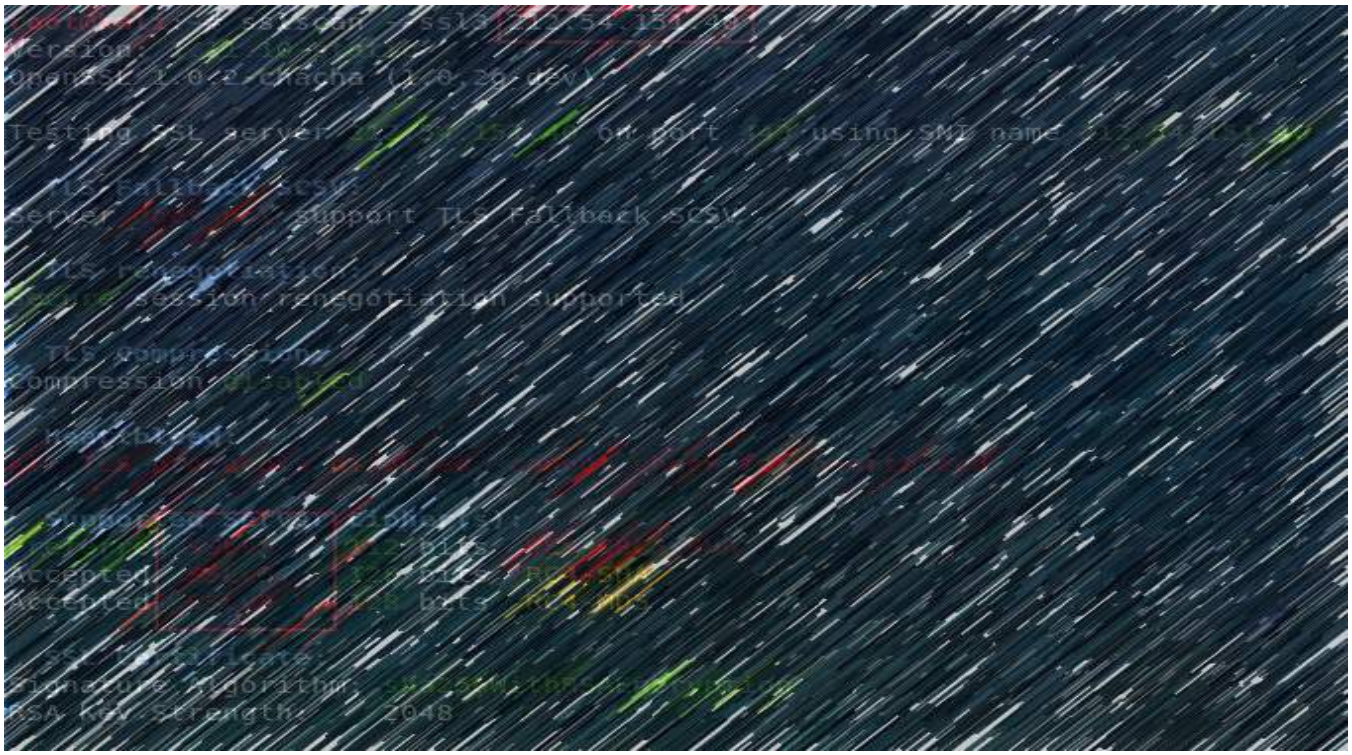


Fig 3: 911.54.151.41

Fig 4: 911.54.151.54

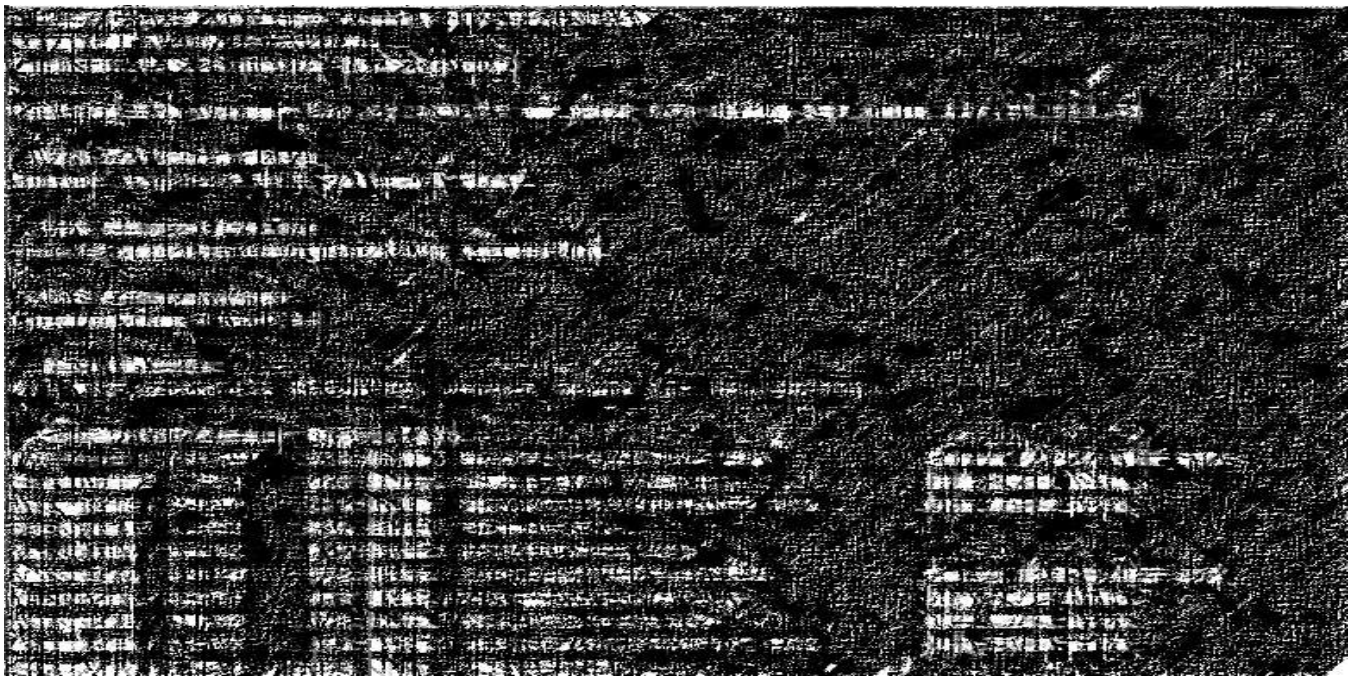


Fig 5: 911.54.151.80

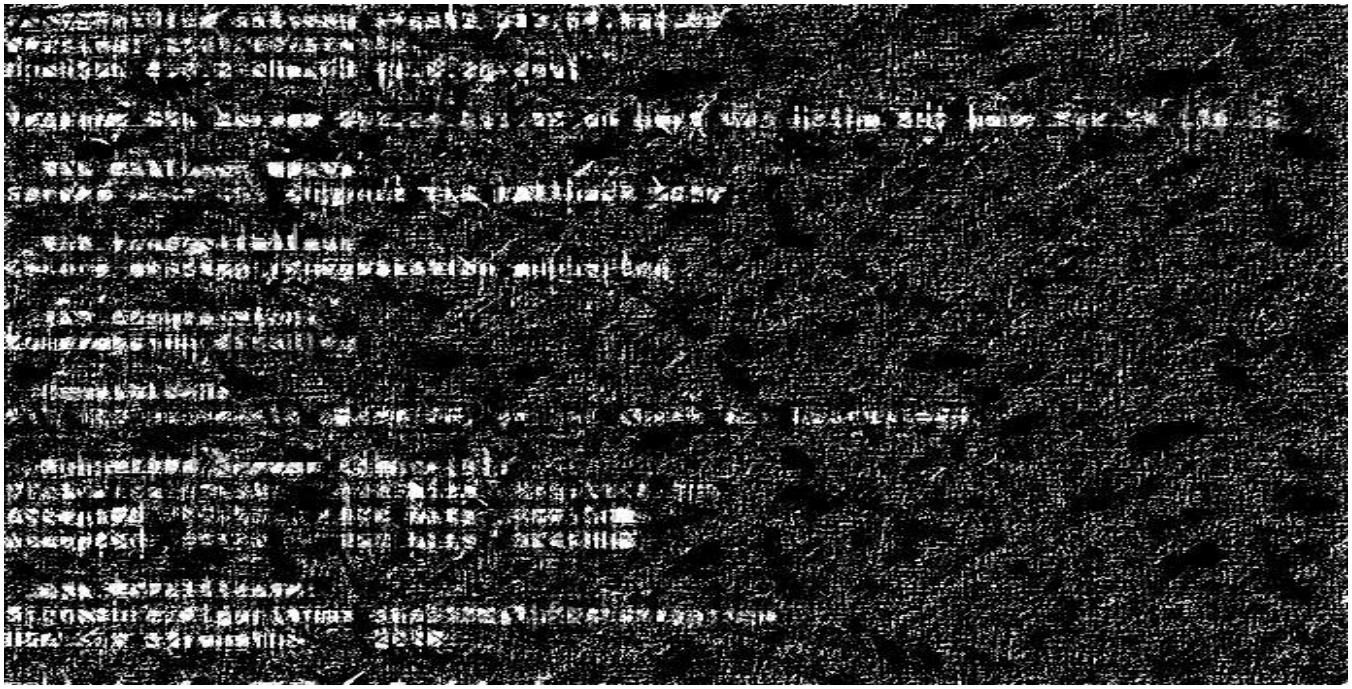


Fig 6: 911.54.151.85

Fig 7: 911.54.151.86

Fig 8: 911.54.151.110

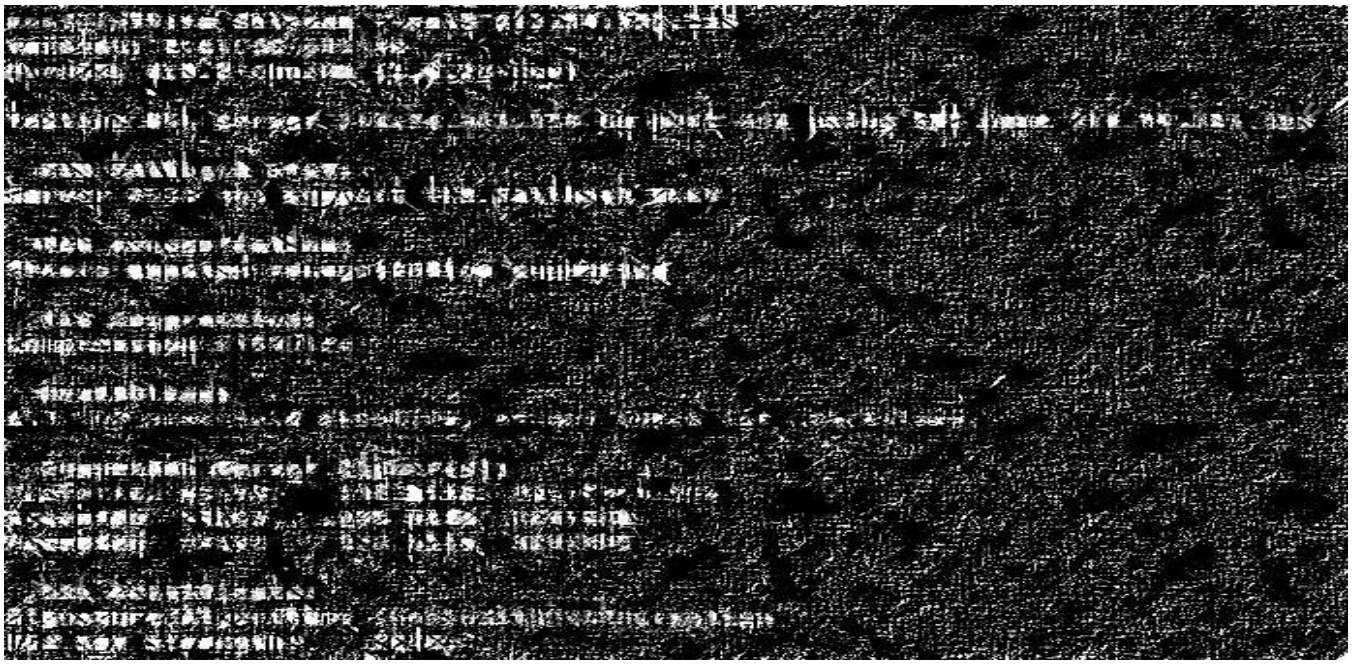
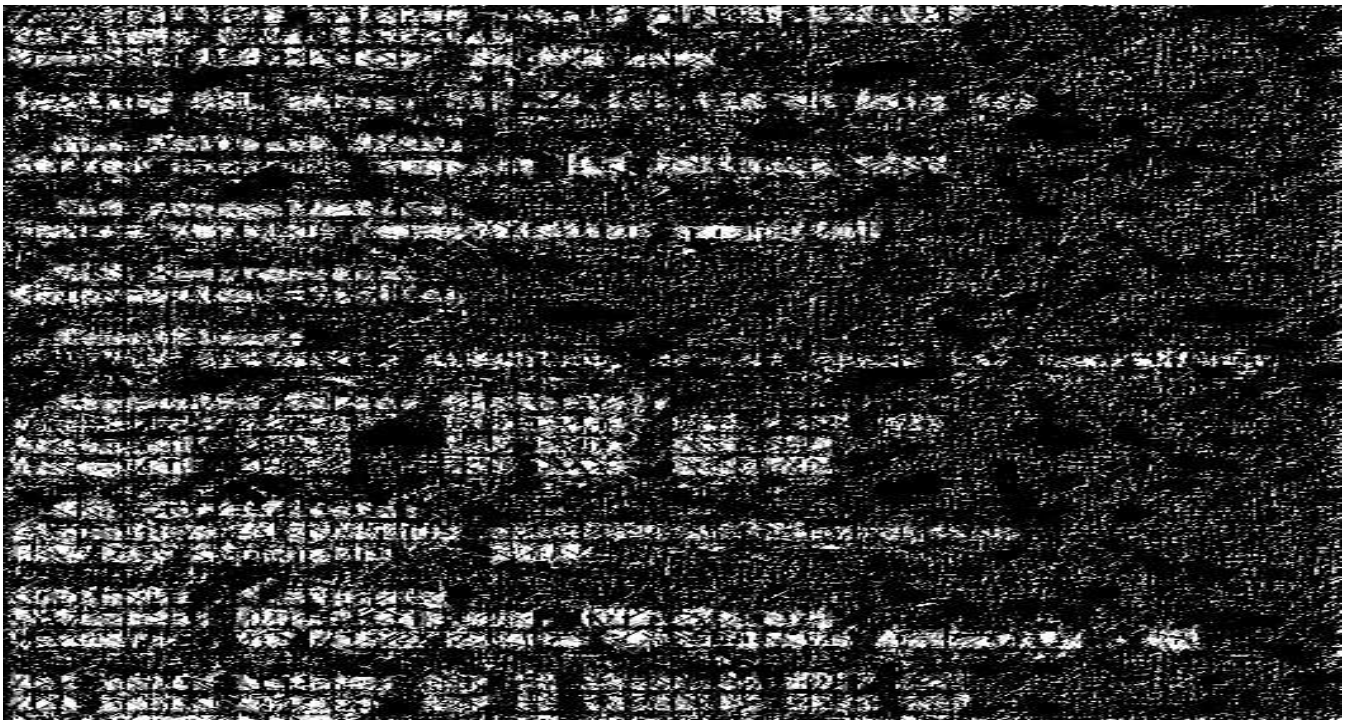


Fig 9: 911.54.151.118



3.2.7 SSL Drown Attack Vulnerability

Reference No:	Vulnerability Rating:
EXT_PT_07	**Low**
Tools Used	**CVSS-3.0 Score**
SSL Scan	CVE-2016-0800

Vulnerability Description:

DROWN stands for Decrypting RSA with Obsolete and Weakened encryption.
DROWN is a serious vulnerability that affects HTTPS and other services that rely on SSL and TLS, some of the essential cryptographic protocols for Internet security. These protocols allow everyone on the Internet to browse the web, use email, shop online, and send instant messages without third-parties being able to read the communication.

Exploitation Summary

DROWN allows attackers to break the encryption and read or steal sensitive communications, including passwords, credit card numbers, trade secrets, or financial data. Our measurements indicate 33% of all HTTPS servers are vulnerable to the attack

Vulnerability Identified By / How It Was Discovered

Automated & Manual Analysis

Vulnerable URLs / IP Address

IP Address	Port
911.54.151.33	
911.54.151.118	
911.54.151.85	
911.54.151.86	

Vulnerable Parameter(s)

SSLv2 Protocol

Implications / Consequences of not Fixing the Issue

An adversary may identify known vulnerabilities in the installed version of the PHP and exploit those vulnerability further.

Suggested Countermeasures

As per the industry best practices SSLv2 protocol should be disabled.

High-Level Category

SSLv2 is enabled

References

NA

Proof of Concept:

Fig 1: 911.54.151.33

Fig 2: 911.54.151.85

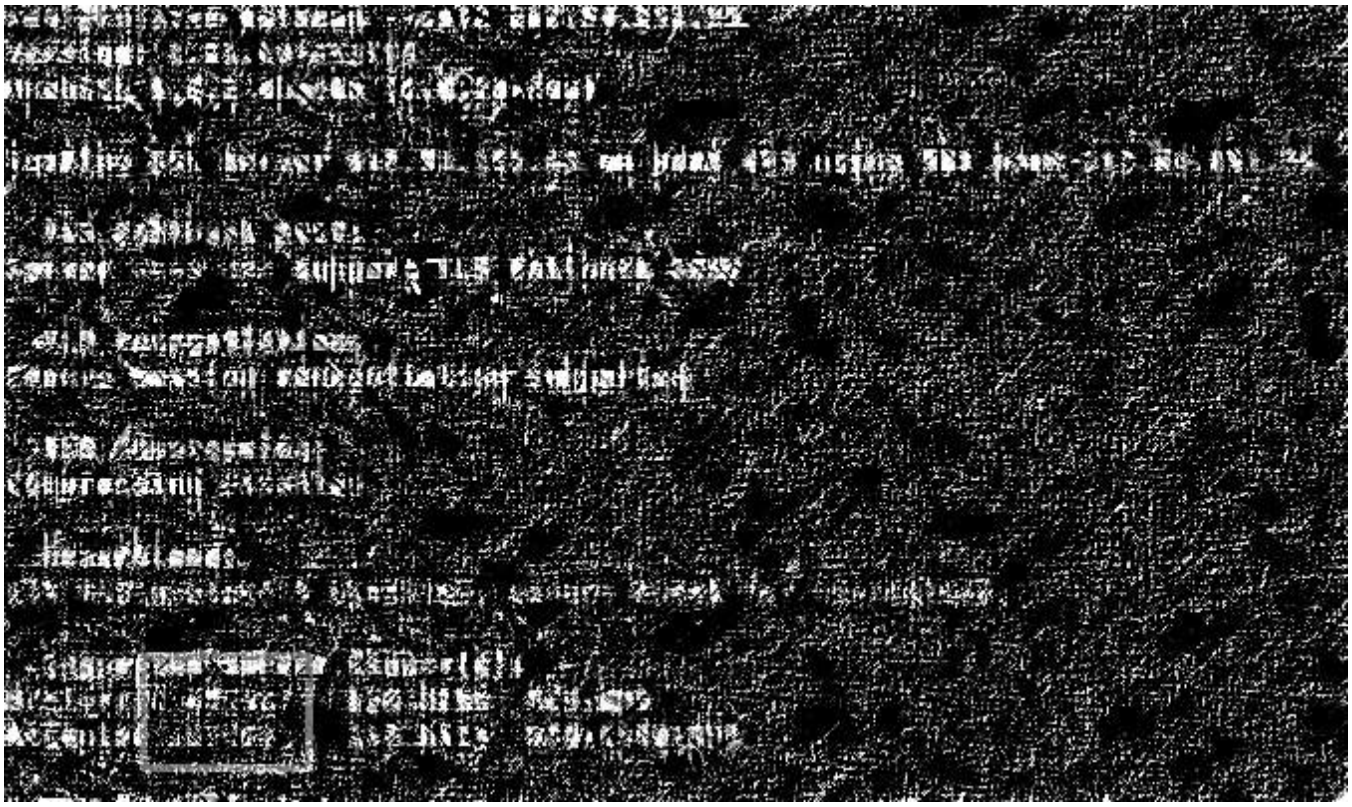


Fig 3: 911.54.151.86

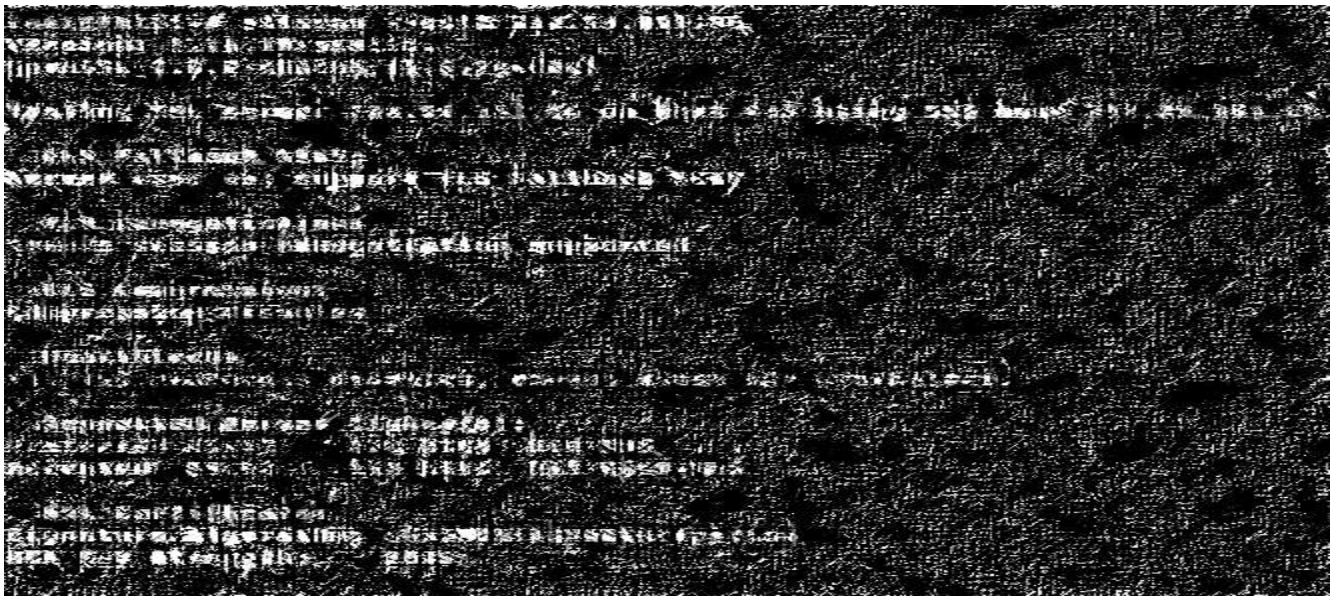
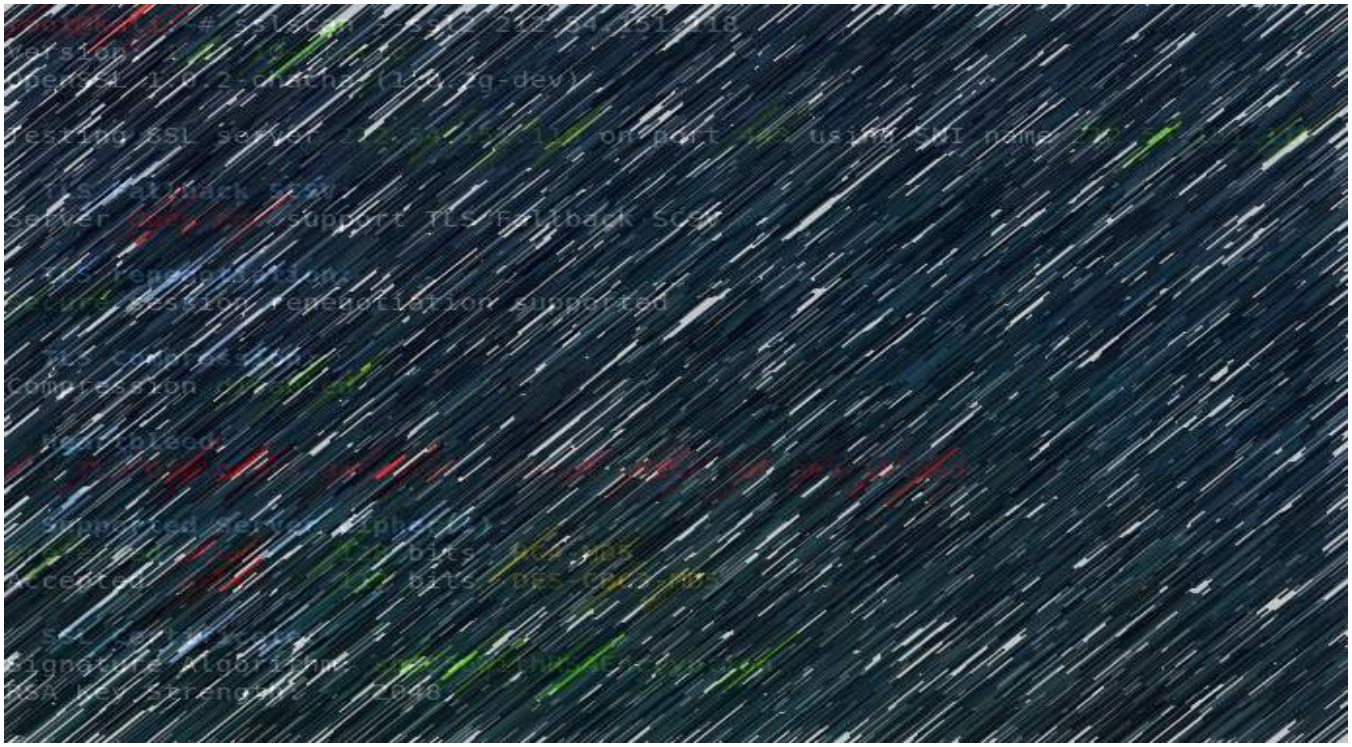


Fig 4: 911.54.151.118



3.2.8 Directory Listing

Reference No:	Vulnerability Rating:
EXT_PT_08	**Low**
Tools Used	**CVSS-3.0 Score**
Manually Tested	
Vulnerability Description:	
Directory listing is a web server function that displays a list of all the files when there is not an index file, such as index.php and default.asp in a specific website directory.	
Exploitation Summary	
For example, when a user requests http://911.54.151.28 without specifying a file, the web server will process this request and will return the index file for that directory and the actual website will show up. However, if the index file does not exist, the web server will return a list of the contents of that directory.	
Vulnerability Identified By / How It Was Discovered	
Manual Analysis	
Vulnerable URLs / IP Address	

IP Address	Port
911.54.151.28	
911.54.151.45	
911.54.151.44	

Vulnerable Parameter(s)
Image Path
Implications / Consequences of not Fixing the Issue
Displays sensitive files
Suggested Countermeasures
As a security best practice, it is recommended to disable directory listing. You can disable directory listing by creating an empty index file in the relevant directory.
High-Level Category
Image Path Disclosed
References
NA

Proof of Concept:

Fig 1: 911.54.151.28

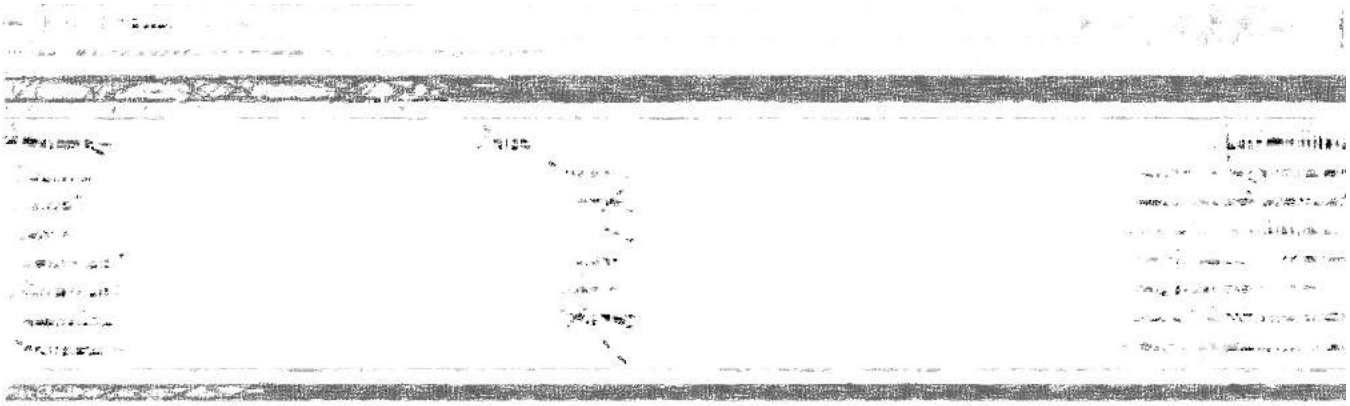


Fig 2: 911.54.151.44

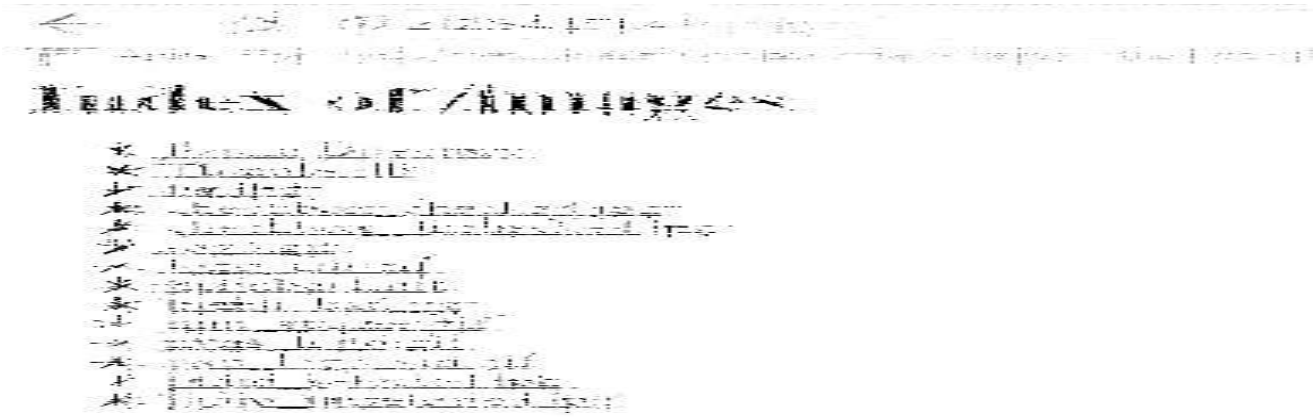
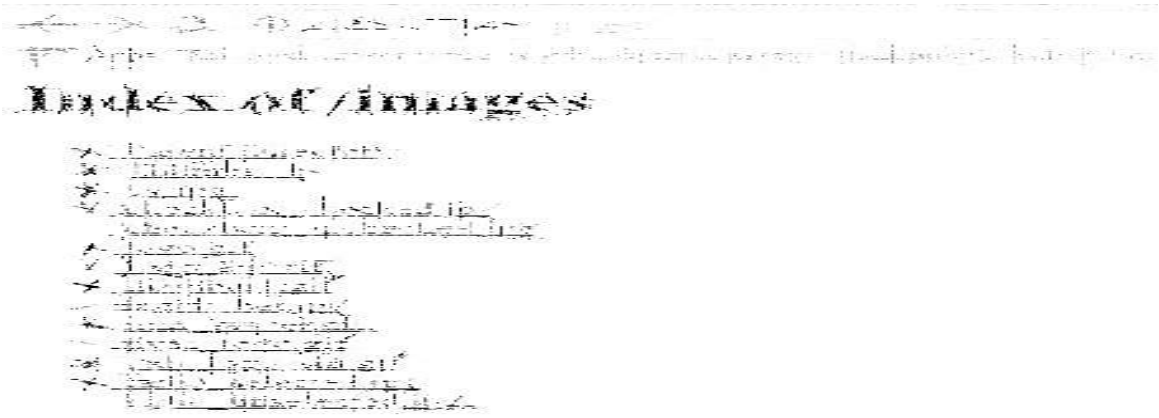


Fig 3: 911.54.151.45



3.2.9 BASH History Commands Disclosure

Reference No:	Vulnerability Rating:
EXT_PT_09	**Low**
Tools Used	**CVSS-3.0 Score**
Manual Analysis	

Vulnerability Description:

Bash keeps track of the commands users type on the command-line with the "history" utility. Once a user logs out, the history is flushed to the user's .bash_history file. For each user, this file resides at the same location: ~/.bash_history. Typically, this file keeps track of the user's last 500 commands. Users often type usernames and passwords on the command-line as parameters to programs, which then get saved to this file when they log out. Attackers can abuse this by looking through the file for potential credentials

Exploitation Summary

NA

Vulnerability Identified By / How It Was Discovered

Manual Analysis

Vulnerable URLs / IP Address

IP Address	Port
911.54.151.111	

Vulnerable Parameter(s)

BASH History File

Implications / Consequences of not Fixing the Issue

Attackers can abuse this by looking through the file for potential credentials

Suggested Countermeasures

There are multiple methods of preventing a user's command history from being flushed to their .bash_history file, including use of the following commands:

set +o history and set -o history to start logging again; unset HISTFILE being added to a user's .bash_rc file; and ln -s /dev/null ~/.bash_history to write commands to /dev/nullinstead.

High-Level Category

Security Misconfiguration

References

NA

Proof of Concept:

Fig 1: 911.54.151.111

3.2.10 SSL/ TLS Diffie-Hellman Modulus <=1024 Bits (Logjam)

Reference No:	Vulnerability Rating:
EXT_PT_010	**Low**
Tools Used	**CVSS-3.0 Score**
Manual Analysis	

Vulnerability Description:

Diffie-Hellman key exchange is a popular cryptographic algorithm that allows Internet protocols to agree on a shared key and negotiate a secure connection. It is fundamental to many protocols including HTTPS, SSH, IPsec, SMTPS, and protocols that rely on TLS.

Exploitation Summary

There are several weaknesses in how Diffie-Hellman key exchange like the below

Logjam attack against The TLS protocol:
The Logjam attack allows a man-in-the-middle attacker to downgrade vulnerable TLS connections to 512-bit export-grade cryptography. This allows the attacker to read and modify any data passed over the connection.

Threats from state-level adversarie:
Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key exchange. Practitioners believed this was safe as long as new key exchange messages were generated for every connection. However, the first step in the number field sieve—the most efficient algorithm for breaking a Diffie-Hellman connection—is dependent only on this prime. After this first step, an attacker can quickly break individual connections.

Vulnerability Identified By / How It Was Discovered

Manual Analysis

Vulnerable URLs / IP Address

IP Address	Port
911.19.107.202	
911.54.151.32	
911.54.151.33	
911.54.151.40	
911.54.151.28	
911.54.151.31	
911.54.151.34	
911.54.151.45	
911.54.151.44	
911.54.151.41	
911.54.151.80	
911.54.151.85	
911.54.151.86	
911.54.151.110	

911.54.151.101	
911.54.151.118	

Vulnerable Parameter(s)
Diffie-Hellman Modulus <=1024 Bi
Implications / Consequences of not Fixing the Issue
NA
Suggested Countermeasures
Use a Strong, Diffie Hellman Group. A few 1024-bit groups are used by millions of servers, which makes them an optimal target for precomputation, and potential eavesdropping. Administrators should use 2048-bit or stronger Diffie-Hellman groups with "safe" primes.
High-Level Category
NA
References
NA

Proof of Concept:

Fig 1: 911.19.107.202

Fig 2: 911.54.151.28

Fig 3: 911.54.151.31

Fig 4: 911.54.151.32

Fig 5: 911.54.151.33

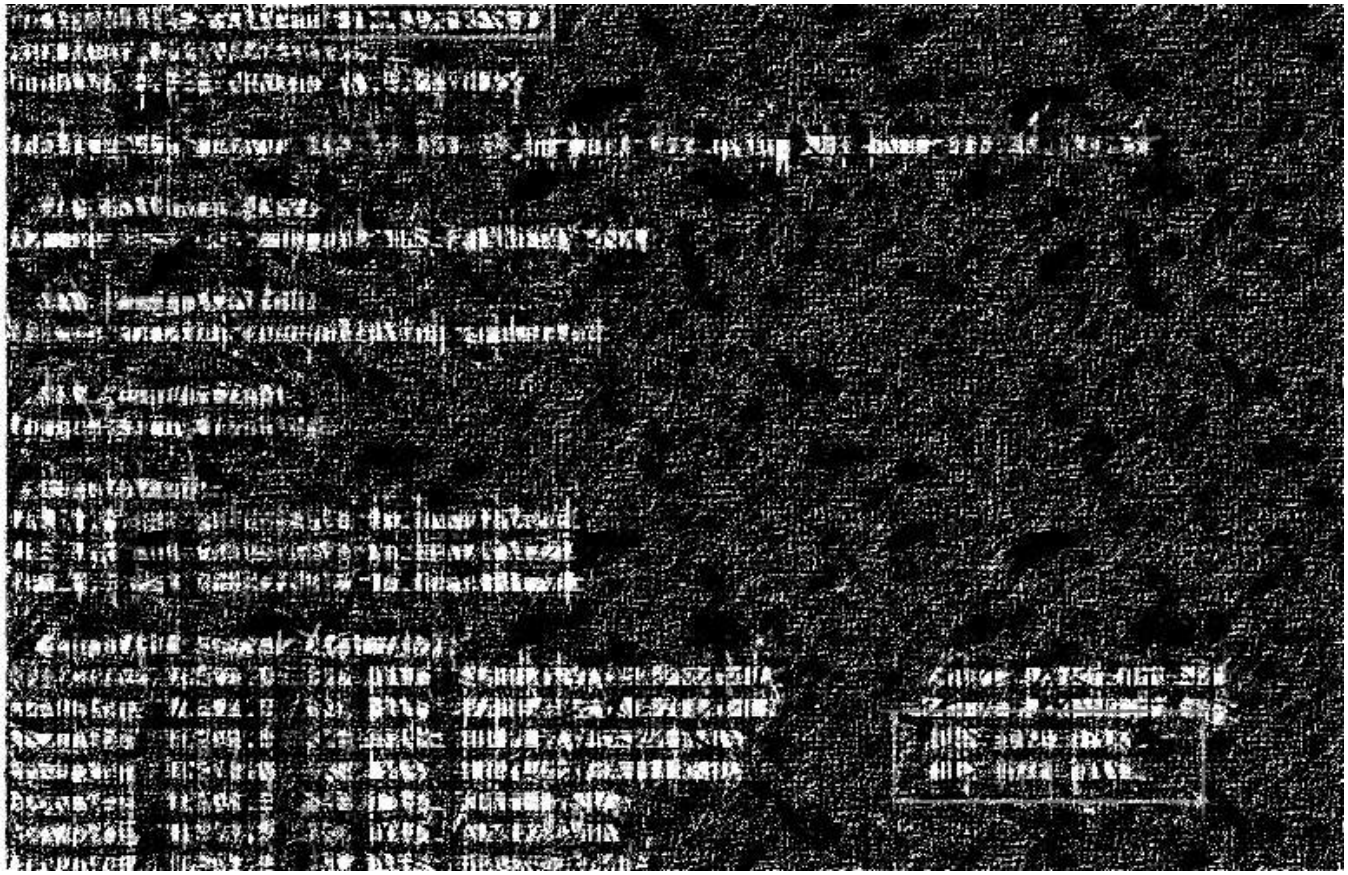


Fig 6: 911.54.151.34

Fig 7: 911.54.151.40

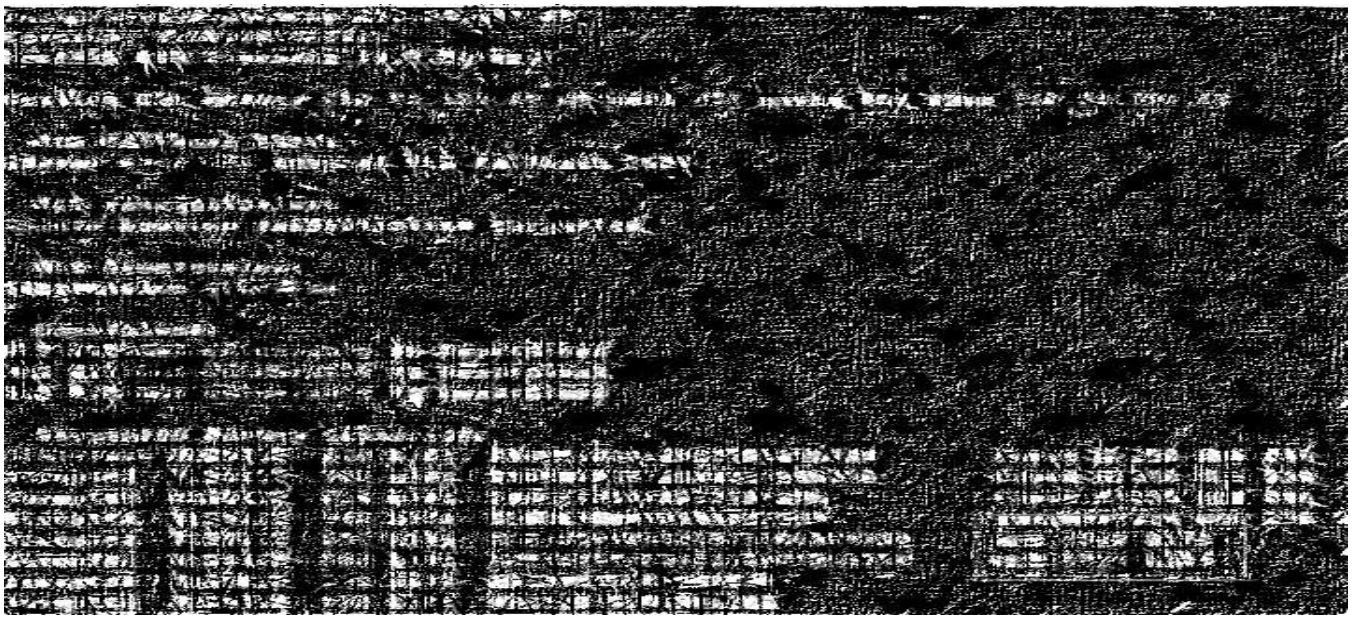


Fig 8: 911.54.151.41

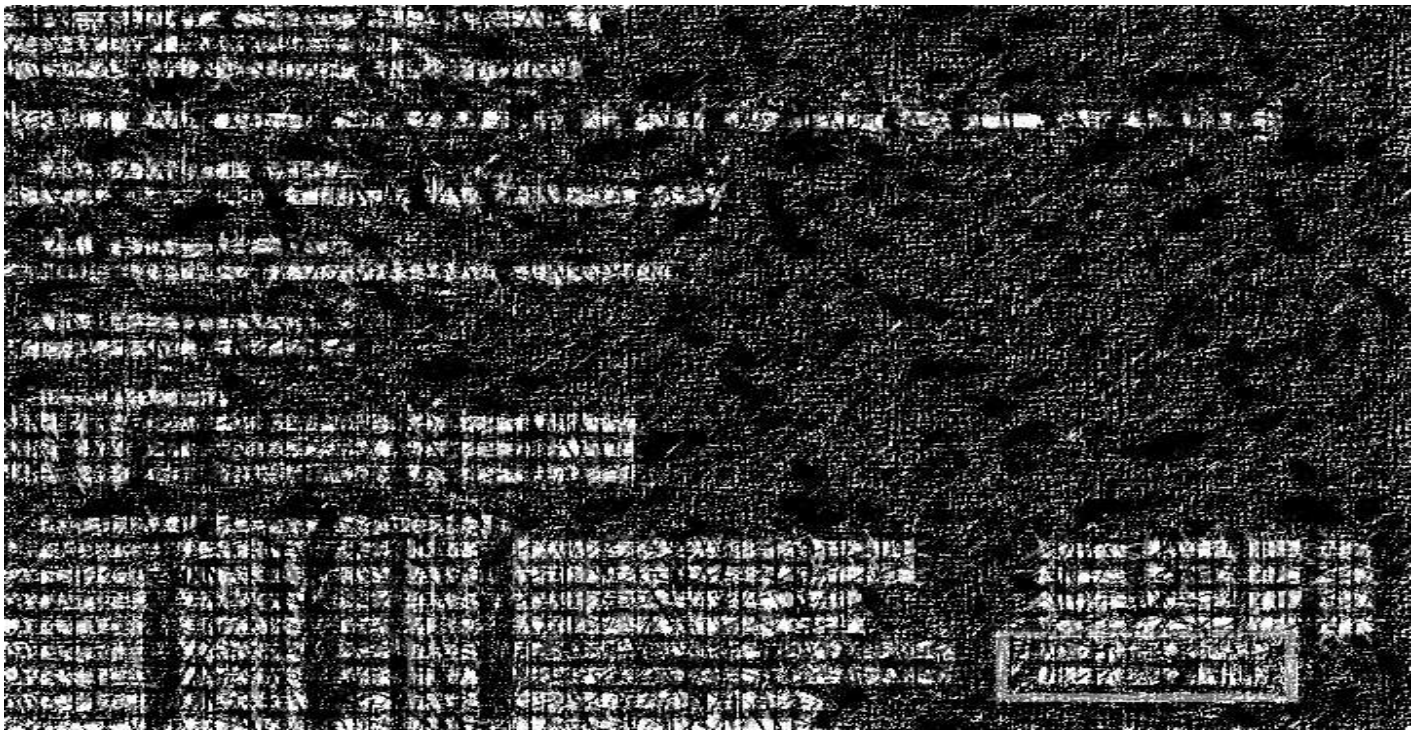


Fig 9: 911.54.151.44

Fig 10: 911.54.151.45

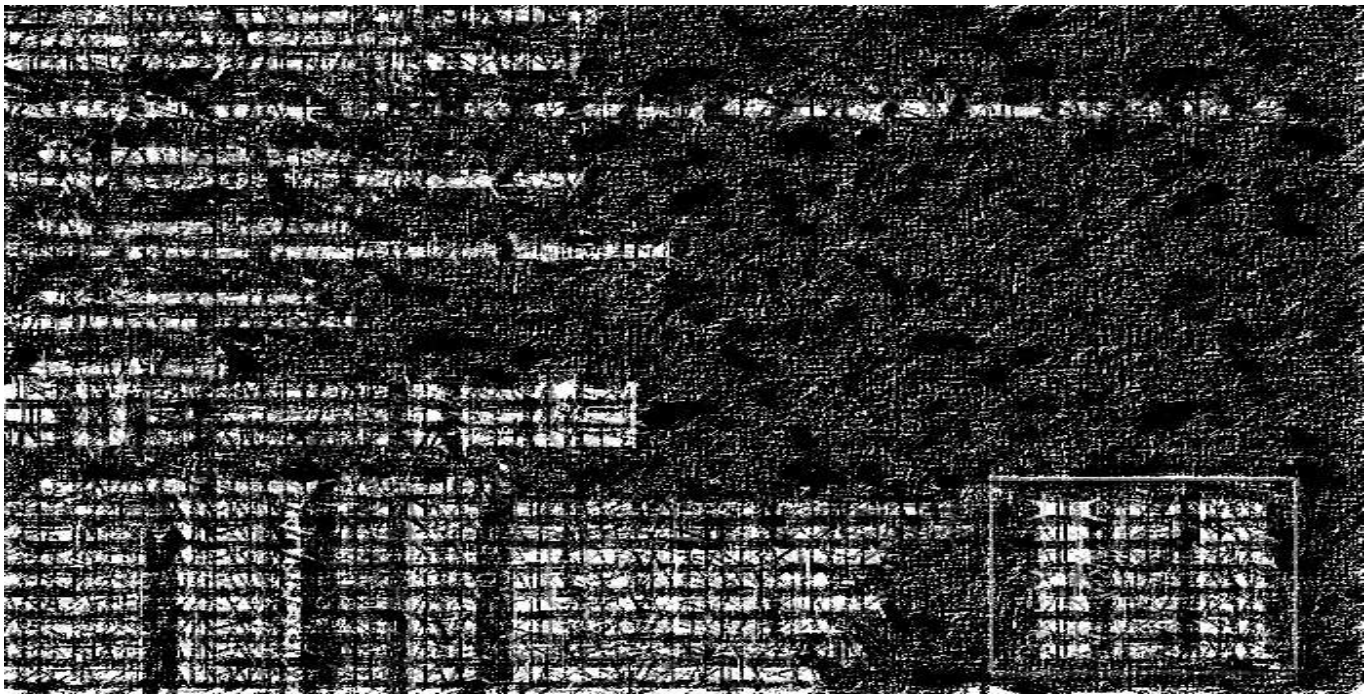


Fig 11: 911.54.151.80

Fig 12: 911.54.151.85

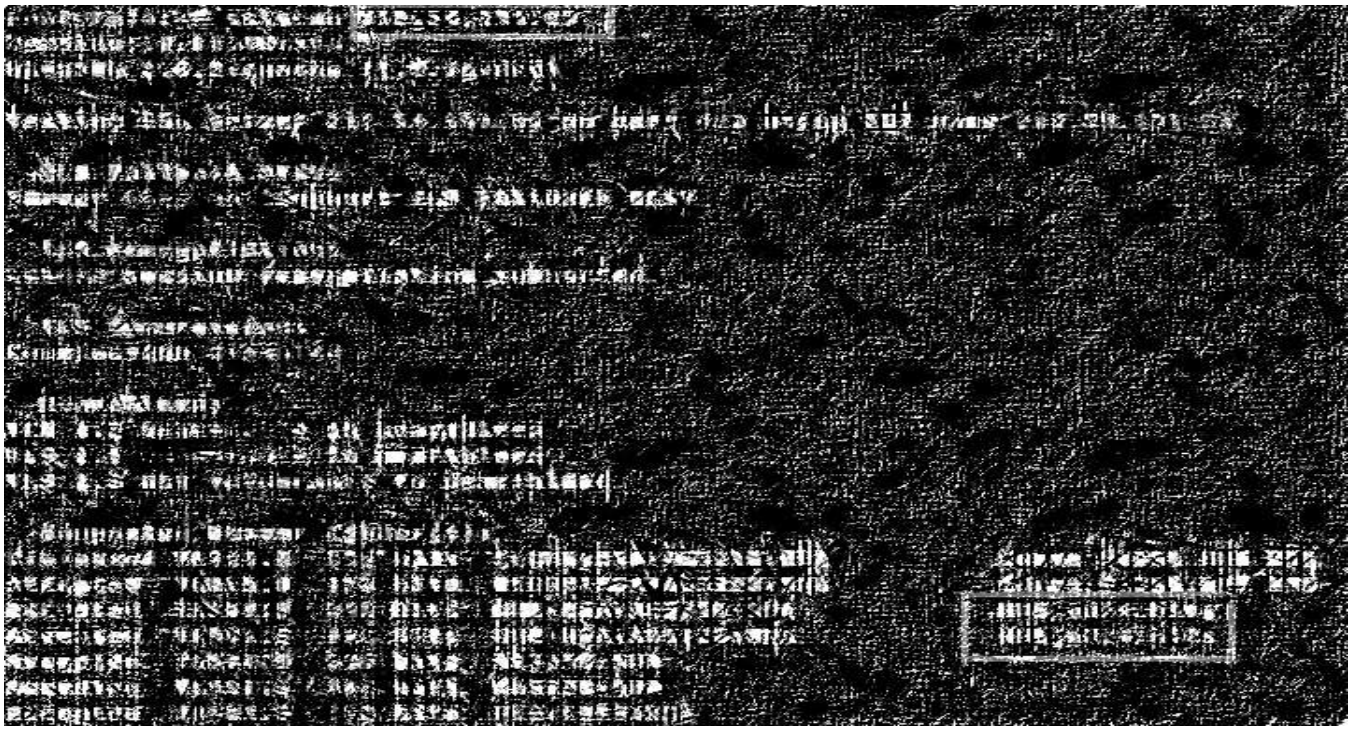
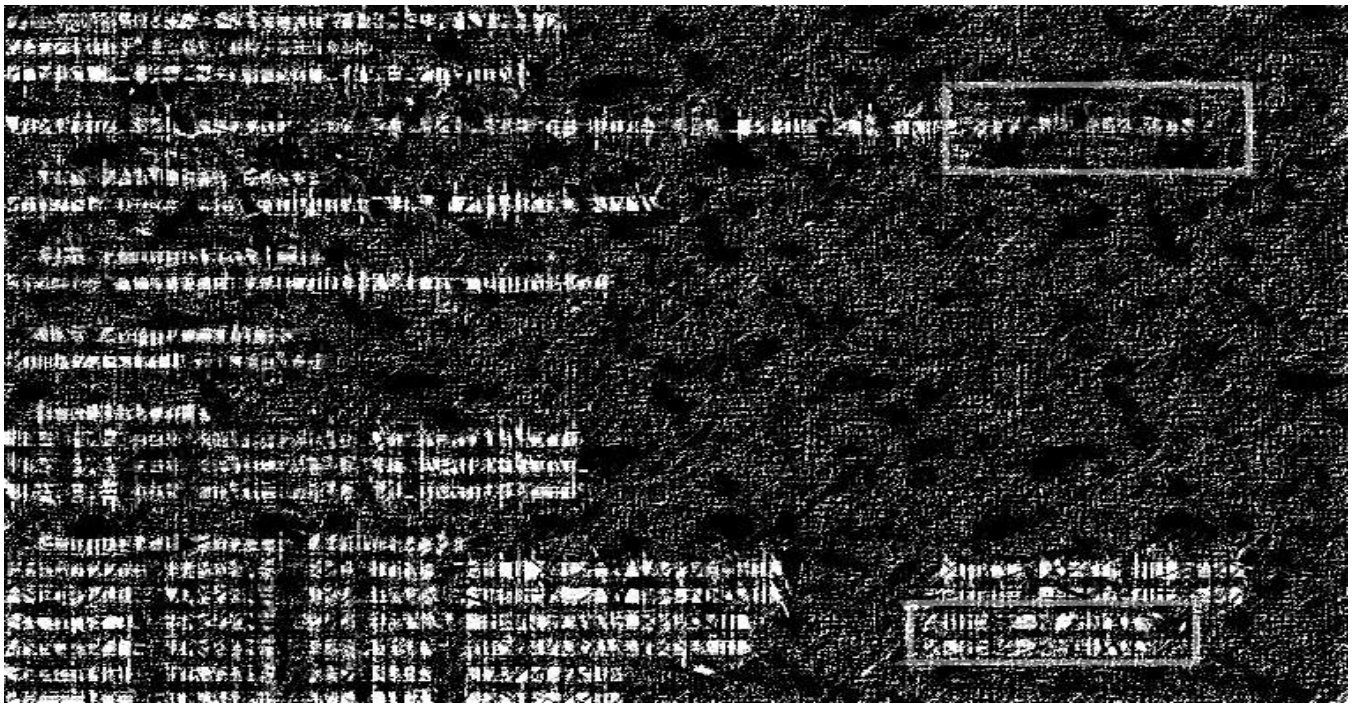


Fig 13: 911.54.151.86

Fig 14: 911.54.151.101

Fig 15: 911.54.151.110

Fig 16: 911.54.151.118



3.2.11 IIS Server Version Known Vulnerabilities

Reference No:	Vulnerability Rating:
EXT_PT_011	**Low**
Tools Used	**CVSS-3.0 Score**
Manual Analysis	

Vulnerability Description:

The vulnerability could allow elevation of privilege if a user clicks a specially crafted URL which is hosted by an affected Microsoft IIS server. An attacker who successfully exploited this vulnerability could potentially execute scripts in the user's browser to obtain information from web sessions.

Exploitation Summary

NA

Vulnerability Identified By / How It Was Discovered

Manual Analysis

Vulnerable URLs / IP Address

IP Address	Port
911.54.151.33	
911.54.151.85	
911.54.151.86	
911.54.151.87	
911.54.151.118	
911.54.151.80	
911.54.151.110	
911.54.151.16	
911.54.151.37	
911.54.151.76	

Vulnerable Parameter(s)

IIS 7.5
IIS 8.0
IIS 8.5

Implications / Consequences of not Fixing the Issue

NA

Suggested Countermeasures

https://technet.microsoft.com/en-us/library/security/ms17-016.aspx

High-Level Category

NA

References

NA

Proof of Concept:

Fig 1: Microsoft IIS Server Known Vulnerabilities

MICROSOFT IIS 7.0/7.5/8.0/8.5/10 /UNCPATH/ CROSS SITE SCRIPTING

Microsoft

CVSSv3 Temp Score	Current Exploit Price (≈)
3.9	$0-$5k

A vulnerability was found in Microsoft IIS 7.0/7.5/8.0/8.5/10. It has been classified as problematic. This affects an unknown function of the file */uncpath/*. The manipulation with an unknown input leads to a cross site scripting vulnerability. CWE is classifying the issue as CWE-79. This is going to have an impact on integrity. An attacker might be able to inject arbitrary html and script code into the web site. This would alter the appearance and would make it possible to initiate further attacks against site visitors.

The weakness was disclosed 03/14/2017 as *MS17-016* as confirmed bulletin (Technet). The advisory is shared for download at technet.microsoft.com. This vulnerability is uniquely identified as CVE-2017-0055 since 09/09/2016. It is possible to initiate the attack remotely. No form of authentication is needed for exploitation. Technical details and a public exploit are known. The advisory points out:

Microsoft » Internet Information Services » 8.5 : Security Vulnerabilities

Cpe Name:*cpe:/a:microsoft:internet_information_services:8.5*

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2014-4078	264		Bypass	2014-11-11	2014-12-31	5.1	None	Remote	High	Not required	Partial	Partial	Partial

The IP Security feature in Microsoft Internet Information Services (IIS) 8.0 and 8.5 does not properly process wildcard allow and deny rules for domains within the "IP Address and Domain Restrictions" list, which makes it easier for remote attackers to bypass an intended rule set via an HTTP request, aka "IIS Security Feature Bypass Vulnerability."

Total number of vulnerabilities : 1 Page : 1 (This Page)

MICROSOFT IIS 8.0/8.5 IP AND DOMAIN RESTRICTION PRIVILEGE ESCALATION

Microsoft

CVSSv3 Temp Score	Current Exploit Price (≈)
5.7	$5k-$25k

A vulnerability classified as critical has been found in Microsoft IIS 8.0/8.5. This affects an unknown function of the component *IP and Domain Restriction*. The manipulation with an unknown input leads to a privilege escalation vulnerability. CWE is classifying the issue as CWE-264. This is going to have an impact on confidentiality, and integrity.

The weakness was presented 11/11/2014 with Microsoft as *MS14-076* as confirmed bulletin (Technet). The advisory is shared for download at technet.microsoft.com. This vulnerability is uniquely identified as CVE-2014-4078 since 06/12/2014. It is possible to initiate the attack remotely. No form of authentication is needed for exploitation. Neither technical details nor an exploit are publicly available. The price for an exploit might be around USD $5k-$25k at the moment (estimation calculated on 04/11/2017).

3.2.12 Apache Multiple Vulnerabilities

Reference No:	Vulnerability Rating:
EXT_PT_012	**Low**
Tools Used	**CVSS-3.0 Score**
Manual Analysis	CVE-2006-0987

Vulnerability Description:

Older versions of Apache HTTPD (prior to 2.2.X) are no longer officially supported. There may exist unreported vulnerabilities for these versions. An upgrade to the latest version should be applied to mitigate these unknown risks.

Exploitation Summary

Remote attacker can leverage this 'amplification' to launch a denial of service attack against a third party host using the remote DNS server.

Vulnerability Identified By / How It Was Discovered

Manual Analysis

Vulnerable URLs / IP Address

IP Address	Port
Apache 2.2.17	
911.54.151.15	
911.54.151.11	
Apache Tomcat/7.0.26	
911.54.151.20	
Apache 2.4.6	
911.54.151.54	
911.54.151.114	
911.54.151.105	
Apache 2.2.3	
911.54.151.72	
911.54.151.45	
911.54.151.44	
Apache 2.2.15	
911.54.151.111	
Apache 2.2.19	
911.54.151.32	
911.54.151.31	

911.54.151.120	
Vulnerable Parameter(s)	
Apache 2.2.17 Apache Tomcat/7.0.26 Apache 2.2.19 Apache 2.4.6 Apache 2.2.3 Apache 2.2.15	
Implications / Consequences of not Fixing the Issue	
NA	
Suggested Countermeasures	
https://httpd.apache.org/	
High-Level Category	
NA	
References	
NA	

Proof of Concept:

Fig: Apache Known Vulnerabilities

Apache » Http Server » 2.2.17 : Security Vulnerabilities

Cpe Name:*cpe:/a:apache:http_server:2.2.17*

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2017-7679	119		Overflow	2017-06-19	2017-10-30	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.														
2	CVE-2017-7668	20			2017-06-19	2017-10-30	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
The HTTP strict parsing changes added in Apache httpd 2.2.32 and 2.4.24 introduced a bug in token list parsing, which allows ap_find_token() to search past the end of its input string. By maliciously crafting a sequence of request headers, an attacker may be able to cause a segmentation fault, or to force ap_find_token() to return an incorrect value.														
3	CVE-2017-3169	476			2017-06-19	2017-10-30	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port.														
4	CVE-2017-3167	287		Bypass	2017-06-19	2017-10-30	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.														
5	CVE-2014-0231	399		DoS	2014-07-20	2017-01-06	5.0	None	Remote	Low	Not required	None	None	Partial
The mod_cgid module in the Apache HTTP Server before 2.4.10 does not have a timeout mechanism, which allows remote attackers to cause a denial of service (process hang) via a request to a CGI script that does not read from its stdin file descriptor.														
6	CVE-2014-0098	20		DoS	2014-03-18	2017-01-06	5.0	None	Remote	Low	Not required	None	None	Partial
The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.														
7	CVE-2013-6438	20		DoS	2014-03-18	2017-01-06	5.0	None	Remote	Low	Not required	None	None	Partial
The dav_xml_get_cdata function in main/util.c in the mod_dav module in the Apache HTTP Server before 2.4.8 does not properly remove whitespace characters from CDATA sections, which allows remote attackers to cause a denial of service (daemon crash) via a crafted DAV WRITE request.														

Apache » Http Server » 2.2.19 : Vulnerability Statistics

Vulnerabilities (23) Related Metasploit Modules (Cpe Name:*cpe:/a:apache:http_server:2.2.19*)

Vulnerability Feeds & Widgets

Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2011	5	2		1								1			2
2012	6	3					1				1	1			
2013	5	1	1				2								
2014	3	3													
2017	4			1						1					
Total	23	9	1	2			3			1	1	2			2
% Of All		39.1	4.3	8.7	0.0	0.0	13.0	0.0	0.0	4.3	4.3	8.7	0.0	0.0	

Warning : Vulnerabilities with publish dates before 1999 are not included in this table and chart. (Because there are too many of them and they make the page look bad; and they may not b

Apache » Tomcat » 7.0.26 : Security Vulnerabilities

Cpe Name:*cpe:/a:apache:tomcat:7.0.26*

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2017-12617	434		Exec Code	2017-10-03	2017-10-23	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial
When running Apache Tomcat versions 9.0.0.M1 to 9.0.0, 8.5.0 to 8.5.22, 8.0.0.RC1 to 8.0.46 and 7.0.0 to 7.0.81 with HTTP PUTs enabled (e.g. via setting the readonly initialisation parameter of the Default servlet to false) it was possible to upload a JSP file to the server via a specially crafted request. This JSP could then be requested and any code it contained would be executed by the server.														
2	CVE-2017-12616	200		Bypass +Info	2017-09-19	2017-09-27	5.0	None	Remote	Low	Not required	Partial	None	None
When using a VirtualDirContext with Apache Tomcat 7.0.0 to 7.0.80 it was possible to bypass security constraints and/or view the source code of JSPs for resources served by the VirtualDirContext using a specially crafted request.														
3	CVE-2017-12615	434		Exec Code	2017-09-19	2017-10-04	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial
When running Apache Tomcat 7.0.0 to 7.0.79 on Windows with HTTP PUTs enabled (e.g. via setting the readonly initialisation parameter of the Default to false) it was possible to upload a JSP file to the server via a specially crafted request. This JSP could then be requested and any code it contained would be executed by the server.														
4	CVE-2017-5664	254			2017-06-06	2017-10-19	5.0	None	Remote	Low	Not required	None	Partial	None
The error page mechanism of the Java Servlet Specification requires that, when an error occurs and an error page is configured for the error that occurred, the original request and response are forwarded to the error page. This means that the request is presented to the error page with the original HTTP method. If the error page is a static file, expected behaviour is to serve content of the file as if processing a GET request, regardless of the actual HTTP method. The Default Servlet in Apache Tomcat 9.0.0.M1 to 9.0.0.M20, 8.5.0 to 8.5.14, 8.0.0.RC1 to 8.0.43 and 7.0.0 to 7.0.77 did not do this. Depending on the original request this could lead to unexpected and undesirable results for static error pages including, if the DefaultServlet is configured to permit writes, the replacement or removal of the custom error page. Notes for other user provided error pages: (1) Unless explicitly coded otherwise, JSPs ignore the HTTP method. JSPs used as error pages must must ensure that they handle any error dispatch as a GET request, regardless of the actual method. (2) By default, the response generated by a Servlet does depend on the HTTP method. Custom Servlets used as error pages must ensure that they handle any error dispatch as a GET request, regardless of the actual method.														
5	CVE-2017-5648	284			2017-04-17	2017-07-10	6.4	None	Remote	Low	Not required	Partial	Partial	None
While investigating bug 60718, it was noticed that some calls to application listeners in Apache Tomcat 9.0.0.M1 to 9.0.0.M17, 8.5.0 to 8.5.11, 8.0.0.RC1 to 8.0.41, and 7.0.0 to 7.0.75 did not use the appropriate facade object. When running an untrusted application under a SecurityManager, it was therefore possible for that untrusted application to retain a reference to the request or response object and thereby access and/or modify information associated with another web application.														

Apache Tomcat Information Disclosure Vulnerability (CVE-2013-4286)

Publish date: July 21, 2015

Severity: MEDIUM

CVE Identifier: CVE-2013-4286

Advisory Date: JUL 21, 2015

DESCRIPTION

Apache Tomcat before 6.0.39, 7.x before 7.0.47, and 8.x before 8.0.0-RC3, when an HTTP connector or AJP connector is used, does not properly handle certain inconsistent HTTP request headers, which allows remote attackers to trigger incorrect identification of a request's length and conduct request-smuggling attacks via (1) multiple Content-Length headers or (2) a Content-Length header and a "Transfer-Encoding: chunked" header. NOTE: this vulnerability exists because of an incomplete fix for CVE-2005-2090.

Fixed in Apache httpd 2.4.26

important: ap_get_basic_auth_pw() Authentication Bypass (CVE-2017-3167)

Use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.

Third-party module writers SHOULD use ap_get_basic_auth_components(), available in 2.2.34 and 2.4.26, instead of ap_get_basic_auth_pw(). Modules which call the legacy ap_get_basic_auth_pw() during the authentication phase MUST either immediately authenticate the user after the call, or else stop the request immediately with an error response, to avoid incorrectly authenticating the current request.

Acknowledgements: We would like to thank Emmanuel Dreyfus for reporting this issue.

Reported to security team	6th February 2017
Issue public	19th June 2017
Update Released	19th June 2017
Affects	2.4.25, 2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1

EXPLOIT DATABASE

Home Exploits Shellcode Papers Google Hacking Database Submit Search

Apache Struts 2.2.3 - Multiple Open Redirections

EDB-ID: 38666	**Author:** Takeshi Terada	**Published:** 2013-07-16
CVE: CVE-2013-2248	**Type:** Remote	**Platform:** Multiple
Aliases: N/A	**Advisory/Source:** Link	**Tags:** Vulnerability
E-DB Verified: ✔	**Exploit:** Download / View Raw	**Vulnerable App:** N/A

« Previous Exploit Next Exploit »

```
source: http://www.securityfocus.com/bid/61196/info

Apache Struts is prone to multiple open-redirection vulnerabilities because the application fails to properly sanitize user-
supplied input.

An attacker can leverage these issues by constructing a crafted URI and enticing a user to follow it. When an unsuspecting
victim follows the link, they may be redirected to an attacker-controlled site; this may aid in phishing attacks. Other attacks
are possible.

Apache Struts 2.0.0 prior to 2.3.15.1 are vulnerable.

http://www.example.com/struts2-showcase/fileupload/upload.action?redirect:http://www.example.com/
http://www.example.com/struts2-showcase/modelDriven/modelDriven.action?redirectAction:http://www.example.com/%23
```

Fixed in Apache httpd 2.2.35-dev

low: Use-after-free when using <Limit > with an unrecognized method in .htaccess ("OptionsBleed") (CVE-2017-9798)

When an unrecognized HTTP Method is given in an <Limit {method}> directive in an .htaccess file, and that .htaccess file is processed by the corresponding request, the global methods table is corrupted in the current worker process, resulting in erratic behaviour.

This behavior may be avoided by listing all unusual HTTP Methods in a global httpd.conf RegisterHttpMethod directive in httpd release 2.2.32 and later.

To permit other .htaccess directives while denying the <Limit > directive, see the AllowOverrideList directive.

Source code patch is at;

- http://www.apache.org/dist/httpd/patches/apply_to_2.2.34/CVE-2017-9798-patch-2.2.patch

Note 2.2 is end-of-life, no further release with this fix is planned. Users are encouraged to migrate to 2.4.28 or later for this and other fixes.

Acknowledgements: We would like to thank Hanno Böck for reporting this issue.

Reported to security team	12th July 2017
Issue public	18th September 2017
Affects	2.2.34, 2.2.32, 2.2.31, 2.2.29, 2.2.27, 2.2.26, 2.2.25, 2.2.24, 2.2.23, 2.2.22, 2.2.21, 2.2.20, 2.2.19, 2.2.18, 2.2.17, 2.2.16, 2.2.15, 2.2.14, 2.2.13, 2.2.12, 2.2.11, 2.2.10, 2.2.9, 2.2.8, 2.2.6, 2.2.5, 2.2.4, 2.2.3, 2.2.2, 2.2.0

3.2.13 RTC 5.0 Vulnerabilities

Reference No:	**Vulnerability Rating:**
EXT_PT_013	**Low**
Tools Used	**CVSS-3.0 Score**
Manually Analysis	
Vulnerability Description:	
IBM Rational Team Concert (RTC) 4.0, 5.0 and 6.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	
Exploitation Summary	
NA	
Vulnerability Identified By / How It Was Discovered	
Manual Analysis	
Vulnerable URLs / IP Address	

IP Address	**Port**
911.54.151.40	

Vulnerable Parameter(s)
RTC 5.0
Implications / Consequences of not Fixing the Issue
NA
Suggested Countermeasures
Upgrade to Latest version
High-Level Category
NA
References
NA

Proof of Concept:

Fig 1: RTC 5.0 Server Known Vulnerabilities

IBM » Rational Team Concert » 5.0.0 : Security Vulnerabilities

Cpe Name:*cpe:/a:ibm:rational_team_concert:5.0.0*

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2017-1113	79		XSS	2017-07-05	2017-07-25	3.5	None	Remote	Medium	Single system	None	Partial	None
IBM Rational Team Concert (RTC) 4.0, 5.0 and 6.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 121151.														
2	CVE-2017-1103	611		DoS	2017-05-10	2017-05-15	7.5	None	Remote	Low	Single system	Partial	None	Complete
IBM Team Concert (RTC) is vulnerable to a denial of service, caused by an XML External Entity Injection (XXE) error when processing XML data. A remote attacker could exploit this vulnerability to expose highly sensitive information or consume all available memory resources. IBM X-Force ID: 120665.														
3	CVE-2016-9746	79		XSS	2017-07-05	2017-07-25	3.5	None	Remote	Medium	Single system	None	Partial	None
IBM Team Concert (RTC) 4.0, 5.0 and 6.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 119821.														
4	CVE-2016-9733	79		XSS	2017-07-05	2017-07-25	3.5	None	Remote	Medium	Single system	None	Partial	None
IBM Team Concert (RTC) 4.0, 5.0 and 6.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 119762.														
5	CVE-2016-9701	79		XSS	2017-07-05	2017-07-25	3.5	None	Remote	Medium	Single system	None	Partial	None
IBM Team Concert 4.0, 5.0 and 6.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 119529.														
6	CVE-2016-9700	200		+Info	2017-07-05	2017-07-11	4.0	None	Remote	Low	Single system	Partial	None	None
IBM Jazz Foundation could allow an authenticated attacker to obtain sensitive information from error message stack traces. IBM X-Force ID: 119528.														
7	CVE-2016-6037	79		Exec Code XSS	2017-05-10	2017-05-15	3.5	None	Remote	Medium	Single system	None	Partial	None
IBM Rational Team Concert (RTC) is vulnerable to HTML injection. A remote attacker with project administrator privileges could send a project that contains malicious HTML code, which when the project is														

3.2.14 Jetty 6.1.12 Vulnerabilities

Reference No:	**Vulnerability Rating:**
EXT_PT_014	**Low**
Tools Used	**CVSS-3.0 Score**
Manually Analysis	CVE-2011-4461
Vulnerability Description:	
Multiple cross-site scripting (XSS) vulnerabilities in the WebApp JSP Snoop page in Mort Bay Jetty 6.1.x through 6.1.21 allow remote attackers to inject arbitrary web script or HTML via the PATH_INFO to the default URI under (1) jspsnoop/ (2) jspsnoop/ERROR/ (3) jspsnoop/IOException/, and possibly the PATH_INFO to (4) snoop.jsp.	
Exploitation Summary	
NA	
Vulnerability Identified By / How It Was Discovered	
Manual Analysis	
Vulnerable URLs / IP Address	

IP Address	**Port**
911.54.151.25	

Vulnerable Parameter(s)
DNS
Implications / Consequences of not Fixing the Issue
An adversary may identify known vulnerabilities in the installed version of the PHP and exploit those vulnerability further.
Suggested Countermeasures
Upgrade to Latest Version
High-Level Category
NA
References
NA

Proof of Concept:

Fig 1: Jetty 6.1.12 Known Vulnerabilities

Mortbay » Jetty » 6.1.12 RC2 : Security Vulnerabilities

Cpe Name:*cpe:/a:mortbay:jetty:6.1.12:rc2*

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2011-4461	310		DoS	2011-12-29	2017-08-28	5.0	None	Remote	Low	Not required	None	None	Partial
Jetty 8.1.0.RC2 and earlier computes hash values for form parameters without restricting the ability to trigger hash collisions predictably, which allows remote attackers to cause a denial of service (CPU consumption) by sending many crafted parameters.														
2	CVE-2009-4612	79		XSS	2010-01-13	2011-08-08	4.3	None	Remote	Medium	Not required	None	Partial	None
Multiple cross-site scripting (XSS) vulnerabilities in the WebApp JSP Snoop page in Mort Bay Jetty 6.1.x through 6.1.21 allow remote attackers to inject arbitrary web script or HTML via the PATH_INFO to the default URI under (1) jspsnoop/, (2) jspsnoop/ERROR/, and (3) jspsnoop/IOException/, and possibly the PATH_INFO to (4) snoop.jsp.														
3	CVE-2009-4611	20		Exec Code	2010-01-13	2010-01-14	5.0	None	Remote	Low	Not required	Partial	None	None
Mort Bay Jetty 6.x and 7.0.0 writes backtrace data without sanitizing non-printable characters, which might allow remote attackers to modify a window's title, or possibly execute arbitrary commands or overwrite files, via an HTTP request containing an escape sequence for a terminal emulator, related to (1) a string value in the Age parameter to the default URI for the Cookie Dump Servlet in test-jetty-webapp/src/main/java/com/acme/CookieDump.java under cookie/, (2) an alphabetic value in the A parameter to jsp/expr.jsp, or (3) an alphabetic value in the Content-Length HTTP header to an arbitrary application.													
4	CVE-2009-4610	79		XSS	2010-01-13	2011-08-08	4.3	None	Remote	Medium	Not required	None	Partial	None
Multiple cross-site scripting (XSS) vulnerabilities in Mort Bay Jetty 6.x and 7.0.0 allow remote attackers to inject arbitrary web script or HTML via (1) the query string to jsp/dump.jsp in the JSP Dump feature, or the (2) Name or (3) Value parameter to the default URI for the Session Dump Servlet under session/.														
5	CVE-2009-4609	200		+Info	2010-01-13	2011-08-08	5.0	None	Remote	Low	Not required	Partial	None	None
The Dump Servlet in Mort Bay Jetty 6.x and 7.0.0 allows remote attackers to obtain sensitive information about internal variables and other data via a request to a URI ending in /dump/, as demonstrated by discovering the value of the getPathTranslated variable.														
6	CVE-2009-1524	79		XSS	2009-05-05	2010-07-20	4.3	None	Remote	Medium	Not required	None	Partial	None
Cross-site scripting (XSS) vulnerability in Mort Bay Jetty before 6.1.17 allows remote attackers to inject arbitrary web script or HTML via a directory listing request containing a ; (semicolon) character.														

3.2.15 Glass Fish 2.1 Vulnerabilities

Reference No:	**Vulnerability Rating:**
EXT_PT_015	**Low**
Tools Used	**CVSS-3.0 Score**
Manual Analysis	CVE-2011-0807 CVE-2010-4438
Vulnerability Description:	
Vulnerability in the Oracle GlassFish Server component of Oracle Fusion Middleware. Supported versions that are affected are 2.1.1, 3.0.1 and 3.1.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle GlassFish Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle GlassFish Server accessible data as well as unauthorized read access to a subset of Oracle GlassFish Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle GlassFish Server.	
Exploitation Summary	
Remote attacker can leverage this 'amplification' to launch a denial of service attack against a third party n unauthenticated, remote attacker could exploit the vulnerability by sending malicious HTTP requests to the targeted system. If successful, the attacker could gain unauthorized access to the targeted system and view sensitive information.using the remote DNS server.	
Vulnerability Identified By / How It Was Discovered	
Manual Analysis	
Vulnerable URLs / IP Address	

IP Address	**Port**
911.54.151.28	

Vulnerable Parameter(s)
Glass Fish 2.1
Implications / Consequences of not Fixing the Issue
An adversary may identify known vulnerabilities in the installed version of the PHP and exploit those vulnerability further.
Suggested Countermeasures
Upgrade to Latest Version
High-Level Category
NAs
References
NA

Proof of Concept:

Fig 1: Glass Fish 2.1 Known Vulnerabilities

Oracle » Glassfish Server » 2.1 : Security Vulnerabilities (Cross Site Scripting (XSS))

Cpe Name:*cpe:/a:oracle:glassfish_server:2.1*

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2009-1553	79		XSS	2009-05-06	2017-08-16	4.3	None	Remote	Medium	Not required	None	Partial	None

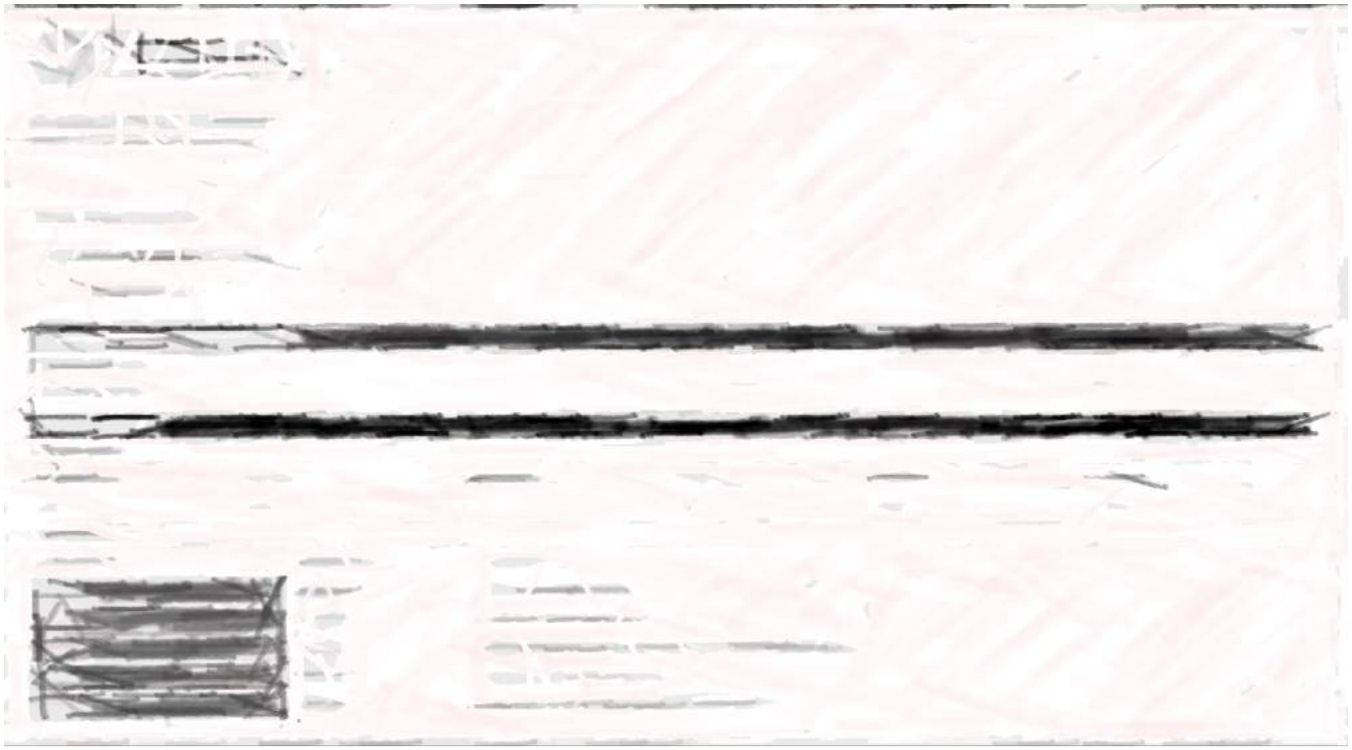
Multiple cross-site scripting (XSS) vulnerabilities in the Admin Console in Sun GlassFish Enterprise Server 2.1 allow remote attackers to inject arbitrary web script or HTML via the query string to (1) applications/applications.jsf, (2) configuration/configuration.jsf, (3) customMBeans/customMBeans.jsf, (4) resourceNode/resources.jsf, (5) sysnet/registration.jsf, or (6) webService/webServicesGeneral.jsf; or the name parameter to (7) configuration/auditModuleEdit.jsf, (8) configuration/httpListenerEdit.jsf, or (9) resourceNode/jdbcResourceEdit.jsf.

4 Tested for Scenarios

4.1 911.54.151.101

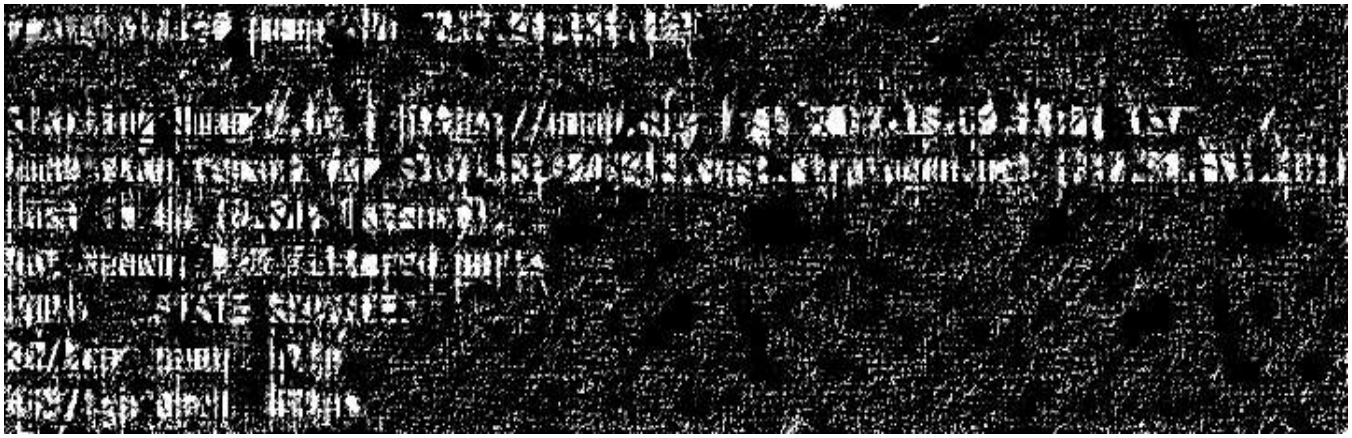
Nessus

Screenshot:



Nmap

Screenshot:

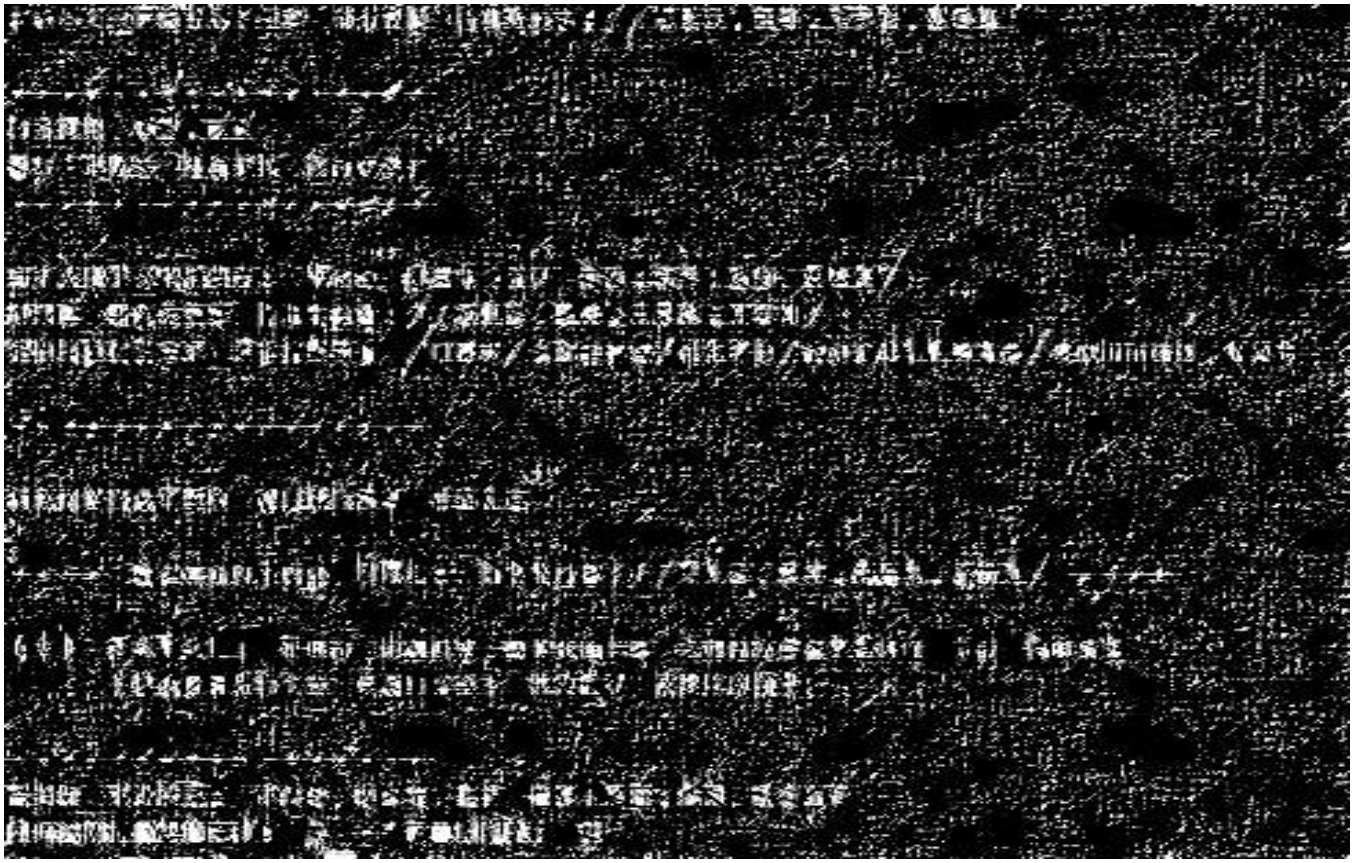


NIKTO

Screenshot:

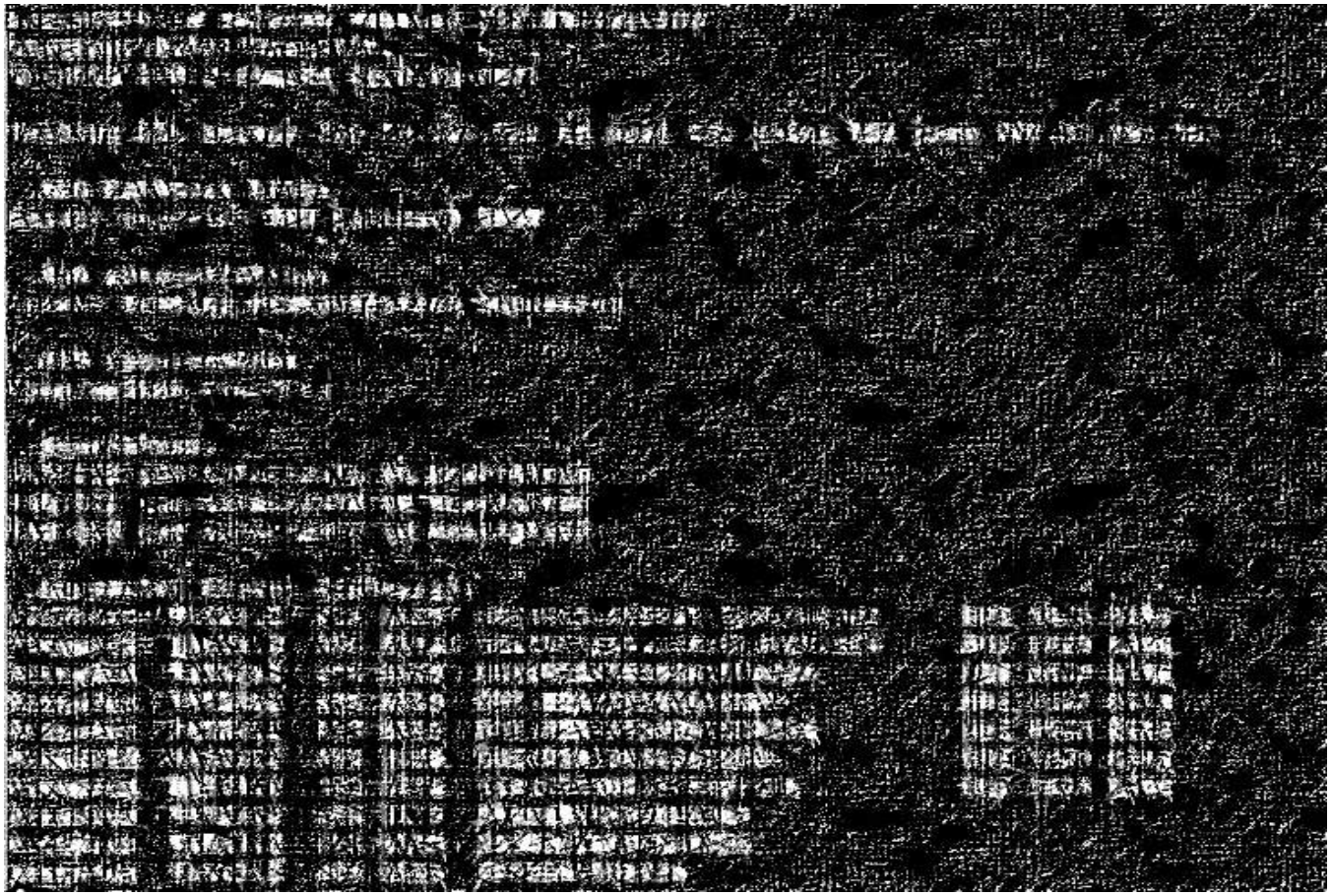
DIRB

Screenshot:



PoodleBleed

Screenshot:



Telnet

Screenshot:

Trace Method

Screenshot:

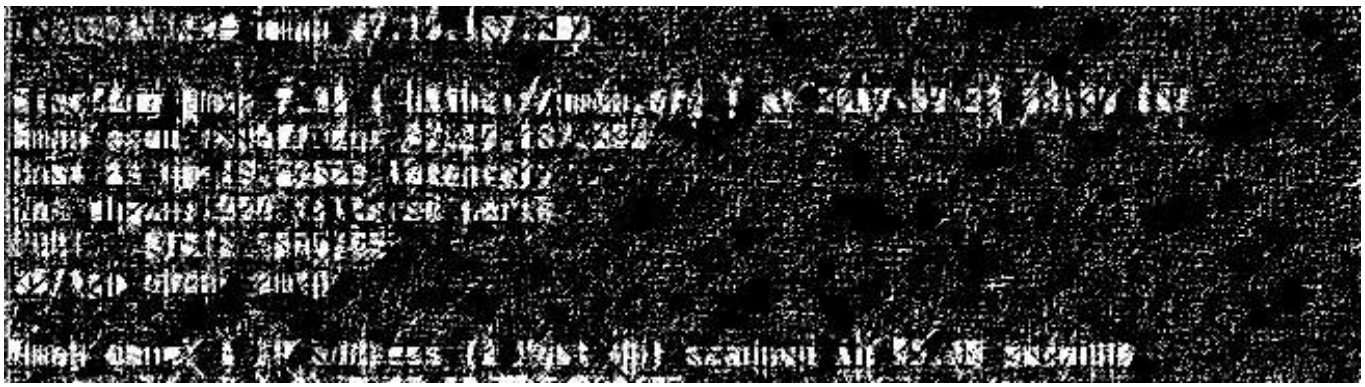
4.2 911.19.107.202

Nessus

Screenshot:

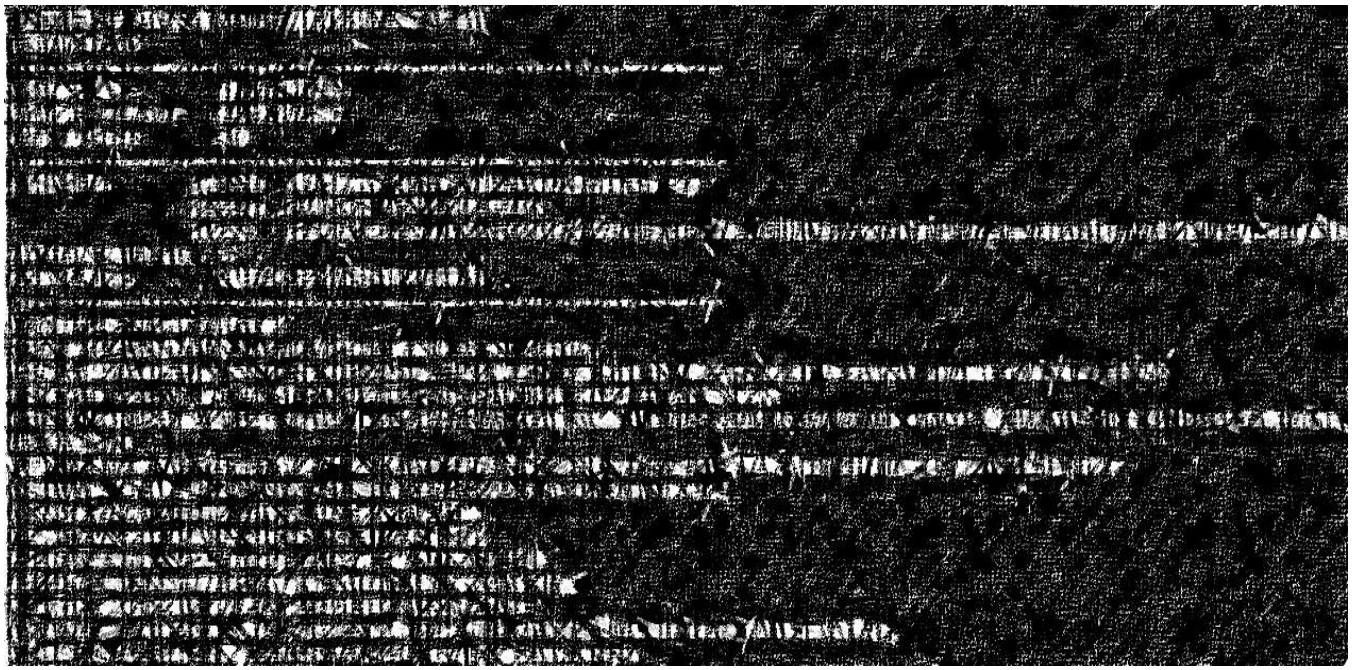
Nmap

Screenshot:



NIKTO

Screenshot:

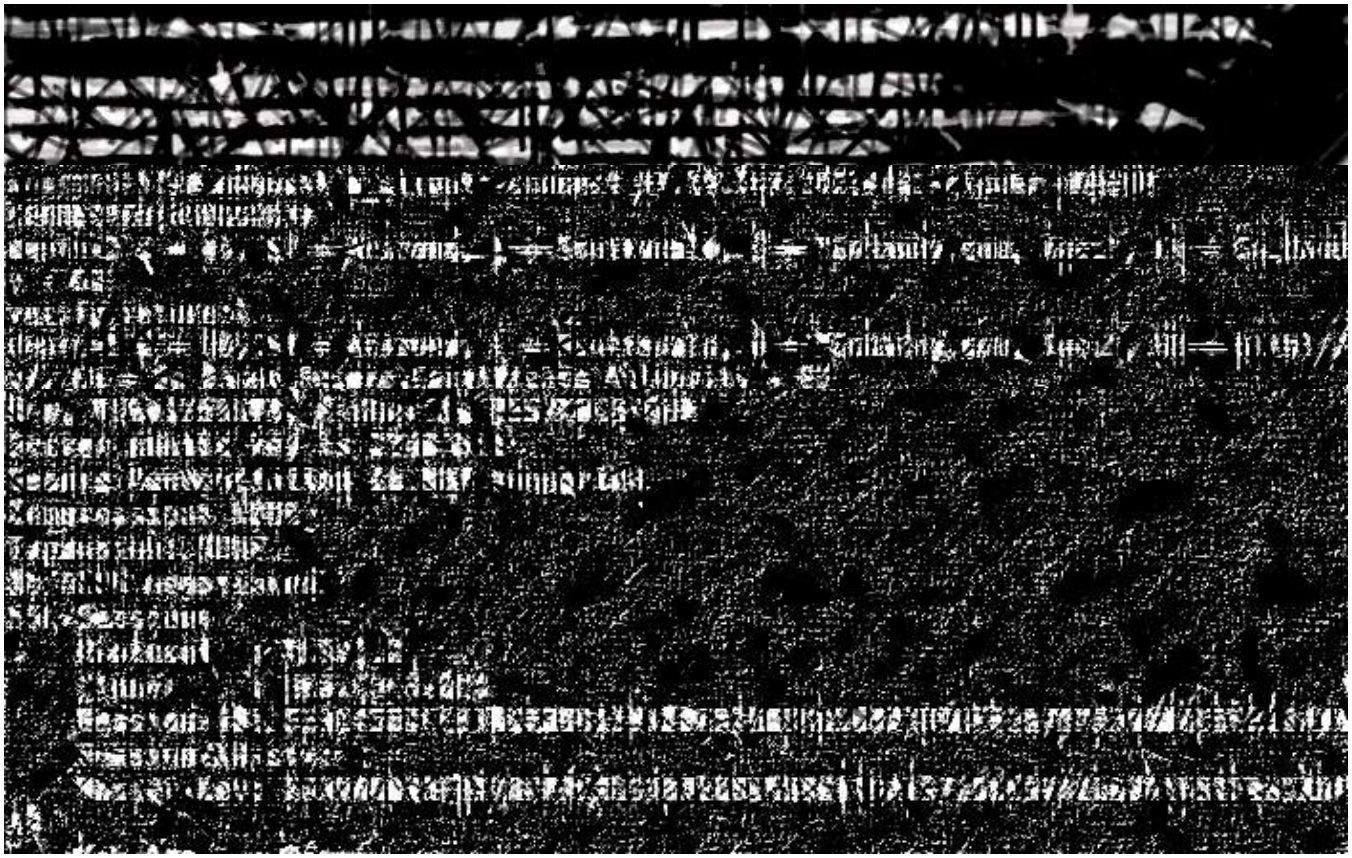


SSL Scan

Screenshot:

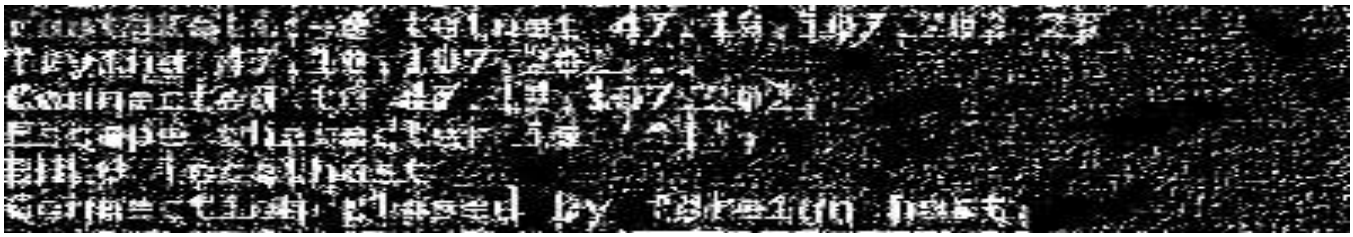
Tested for Weak Ciphers

Screenshot:



Telnet

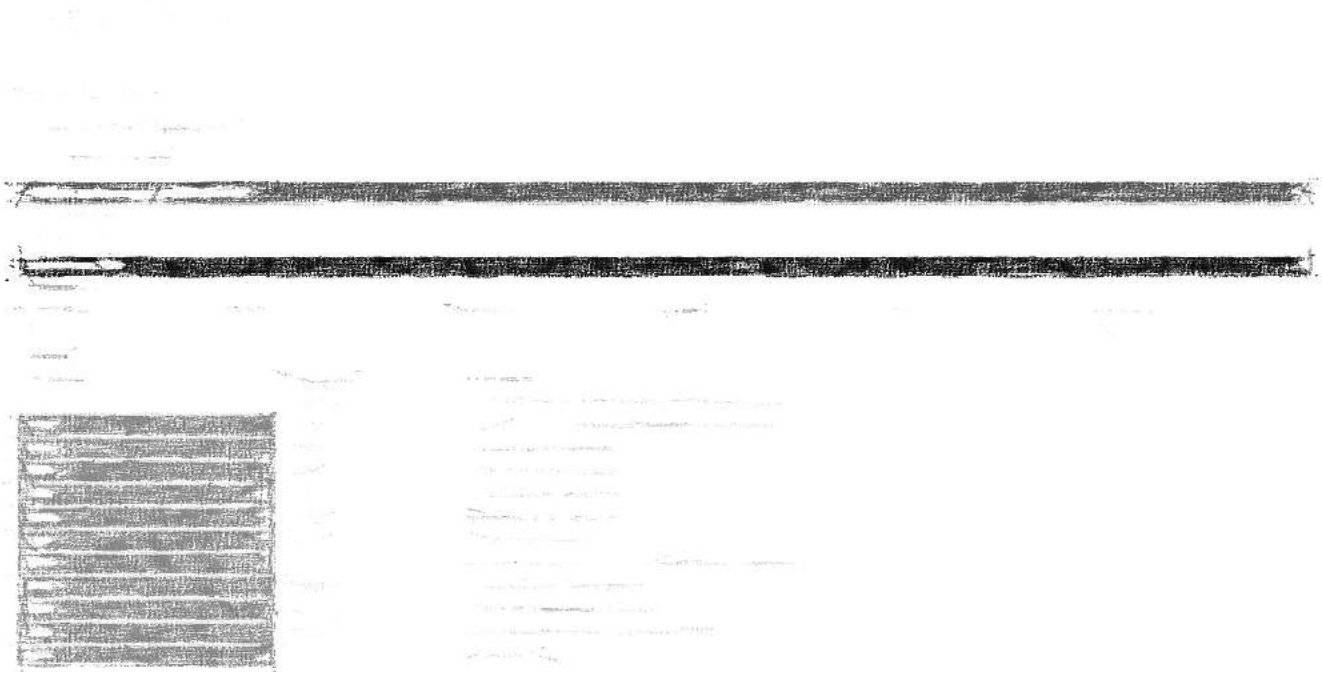
Screenshot:



4.3 911.54.138.125

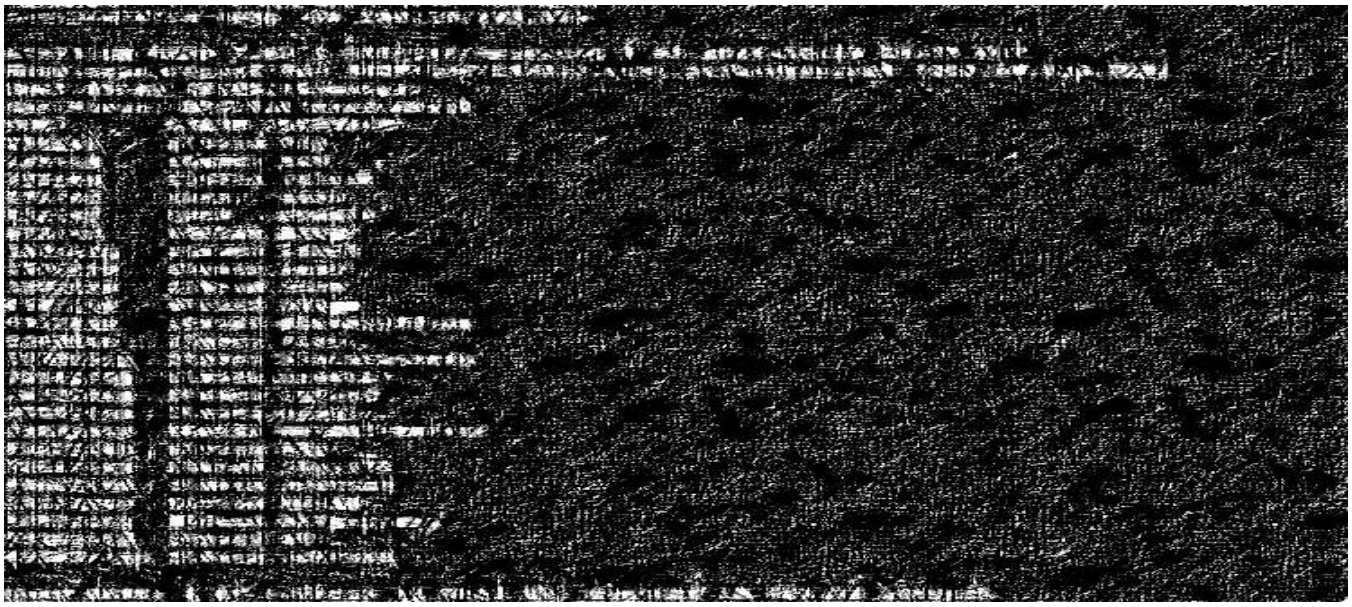
Nessus

Screenshot:



Nmap

Screenshot:

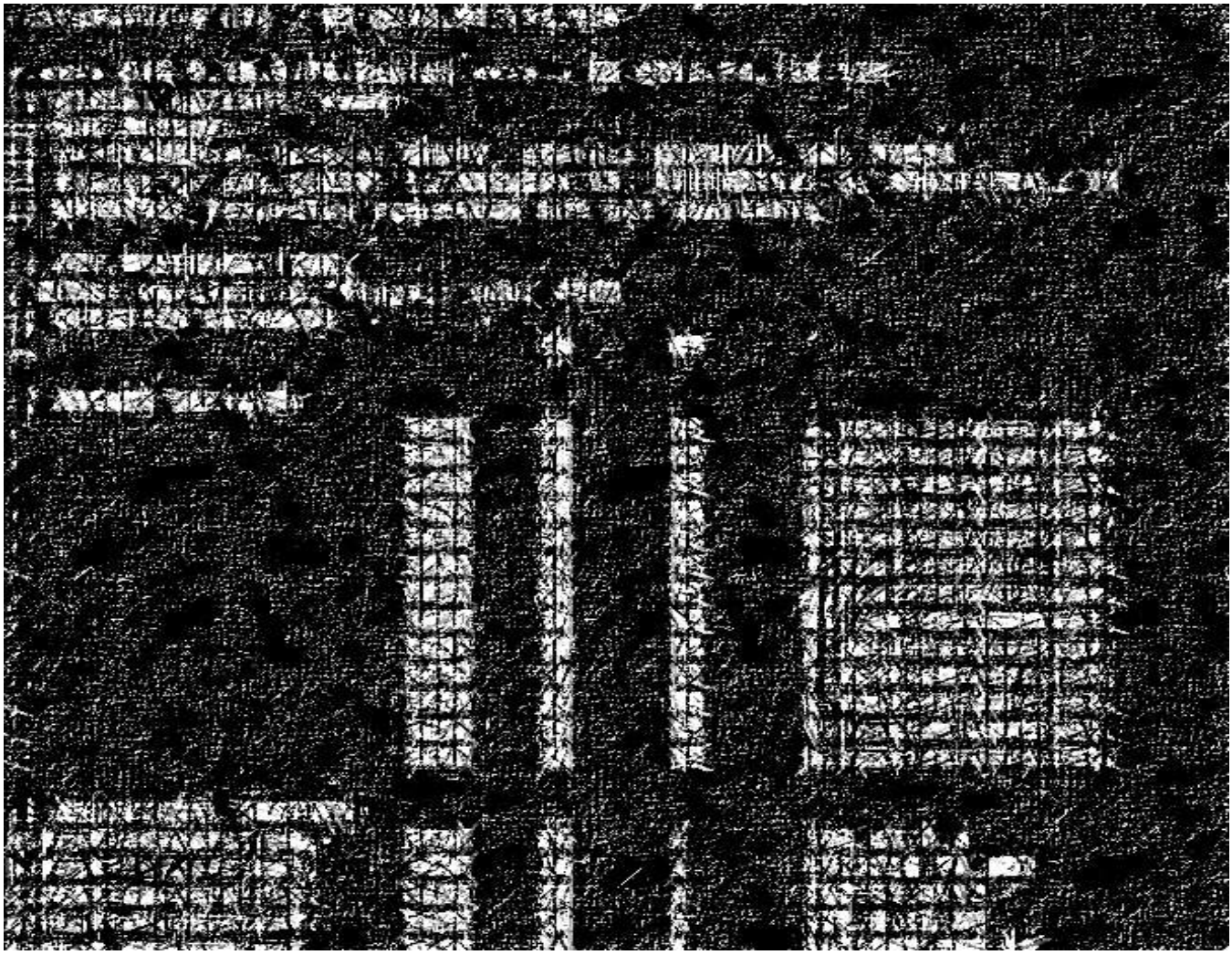


NIKTO

Screenshot:

DNS Amplification

Screenshot:



4.4 911.54.149.132

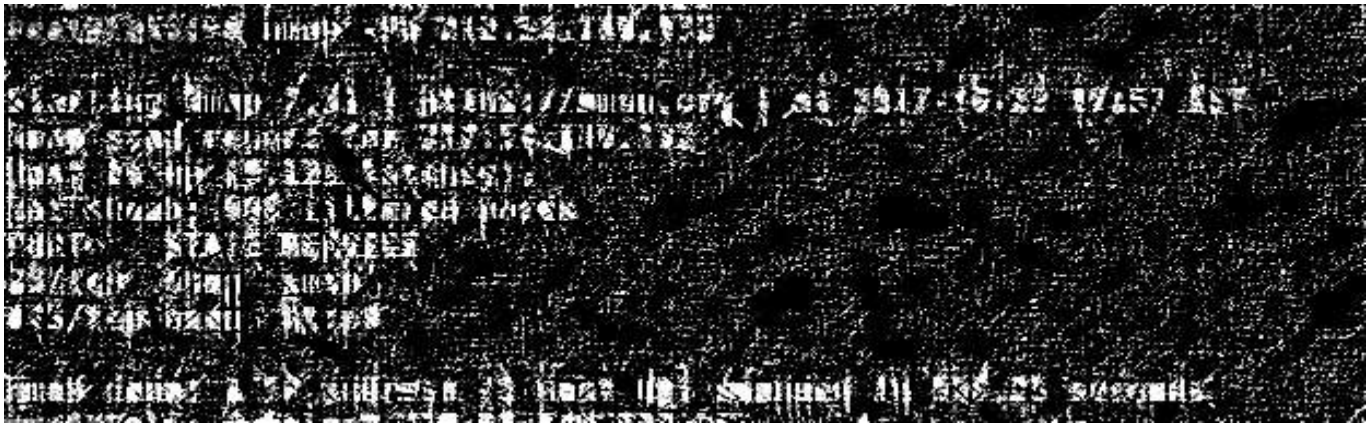
Nessus

Screenshot:

MEDIUM	TLS Padding Oracle Information Disclosure Vulnerability	General	1
LOW	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	General	1
INFO	Nessus SYN scanner	Port scanners	2
INFO	Service Detection	Service detection	2
INFO	Device Type	General	1
INFO	Host Fully Qualified Domain Name (FQDN) Resolution	General	1
INFO	IPSEC Internet Key Exchange (IKE) Version 1 Detection	Service detection	1
INFO	IPSEC Internet Key Exchange (IKE) Version 2 Detection	Service detection	1
INFO	Nessus Scan Information	Settings	1
INFO	OS Identification	General	1
INFO	Patch Report	General	1
INFO	SSL / TLS Versions Supported	General	1
INFO	SSL Certificate commonName Mismatch	General	1

Nmap

Screenshot:

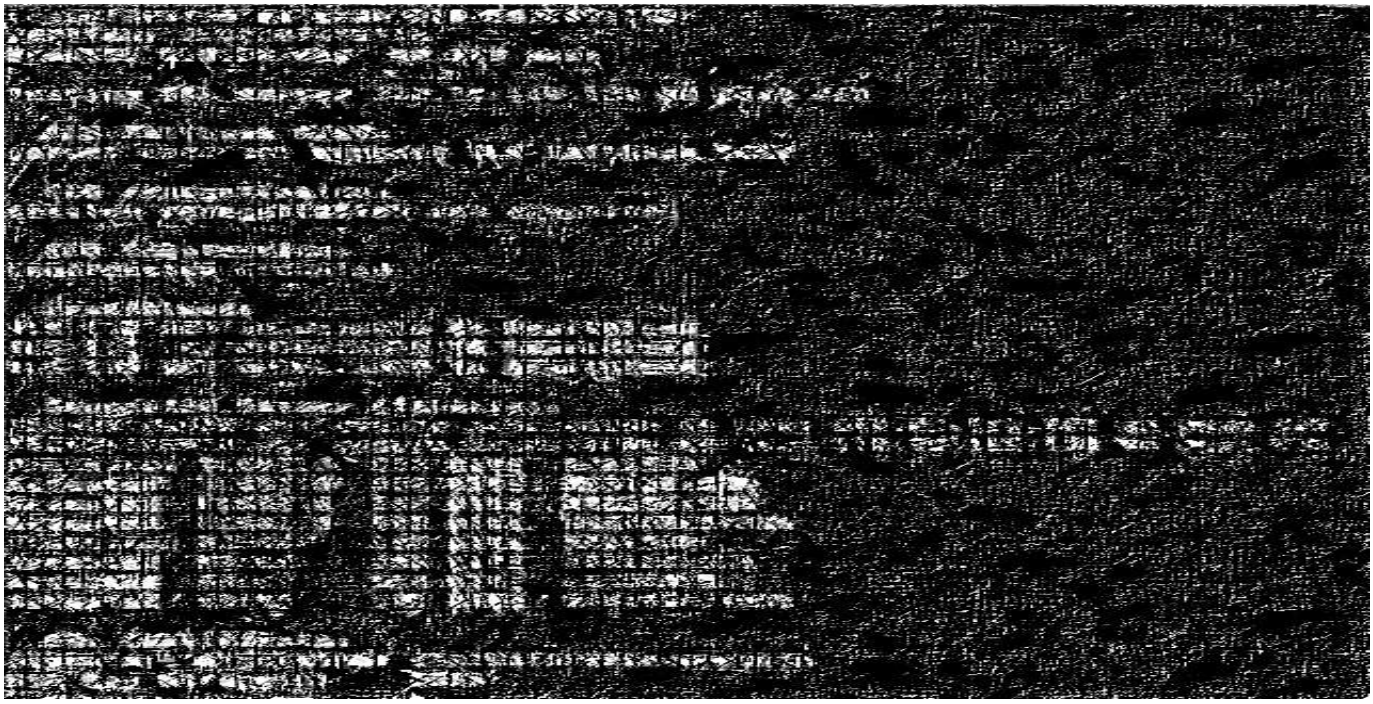


Telnet

Screenshot:

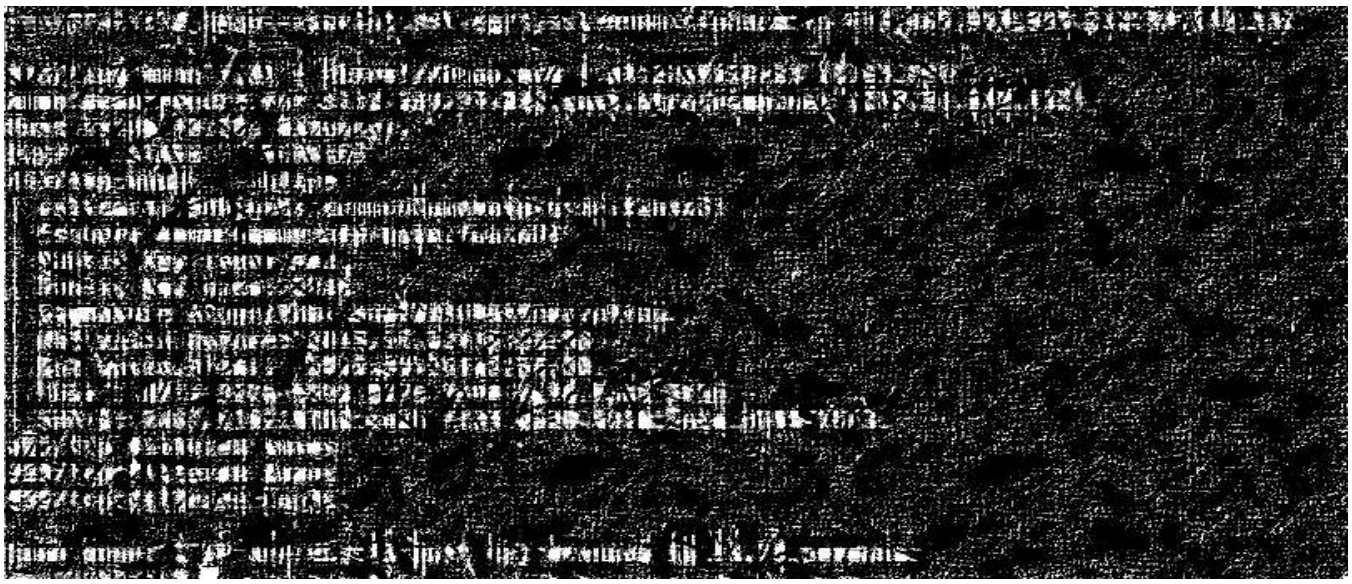
SSL Scan

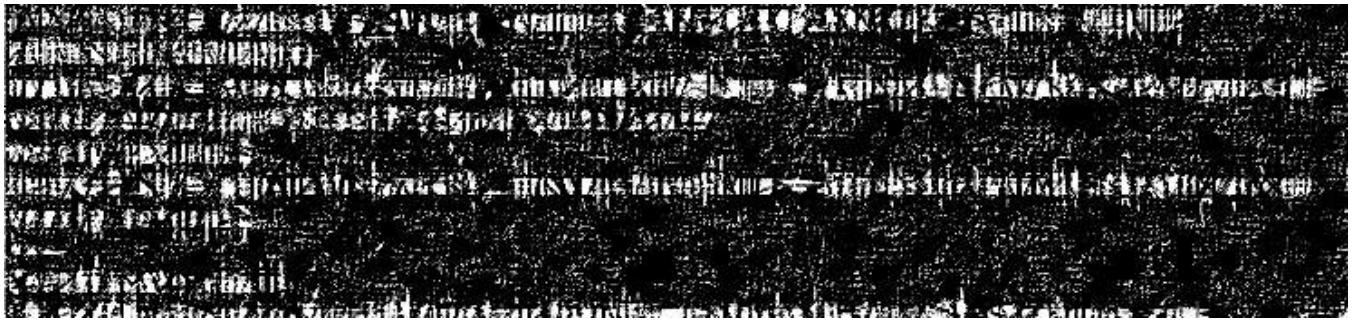
Screenshot:



Tested for Weak Ciphers

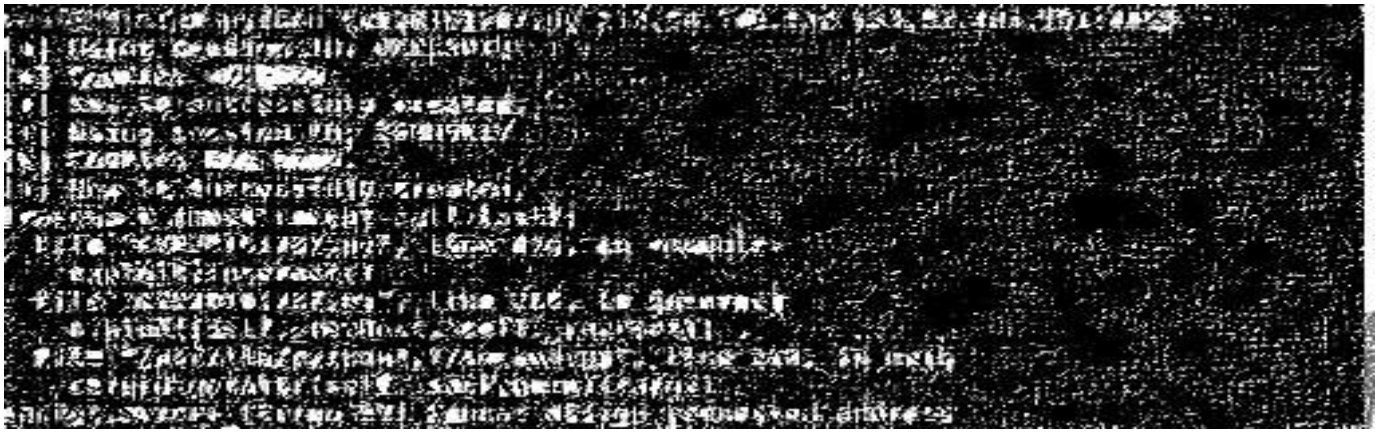
Screenshot:





IKE Fragmented

Screenshot:



4.5 911.54.151.11

Nessus

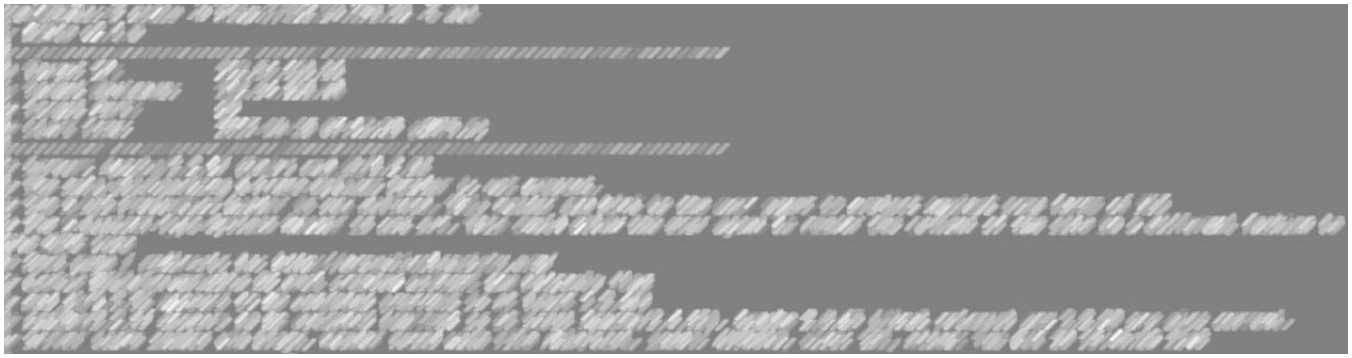
Screenshot:

Nmap

Screenshot:

NIKTO

Screenshot:



SSL Scan

Screenshot:

Clickjacking

Screenshot:

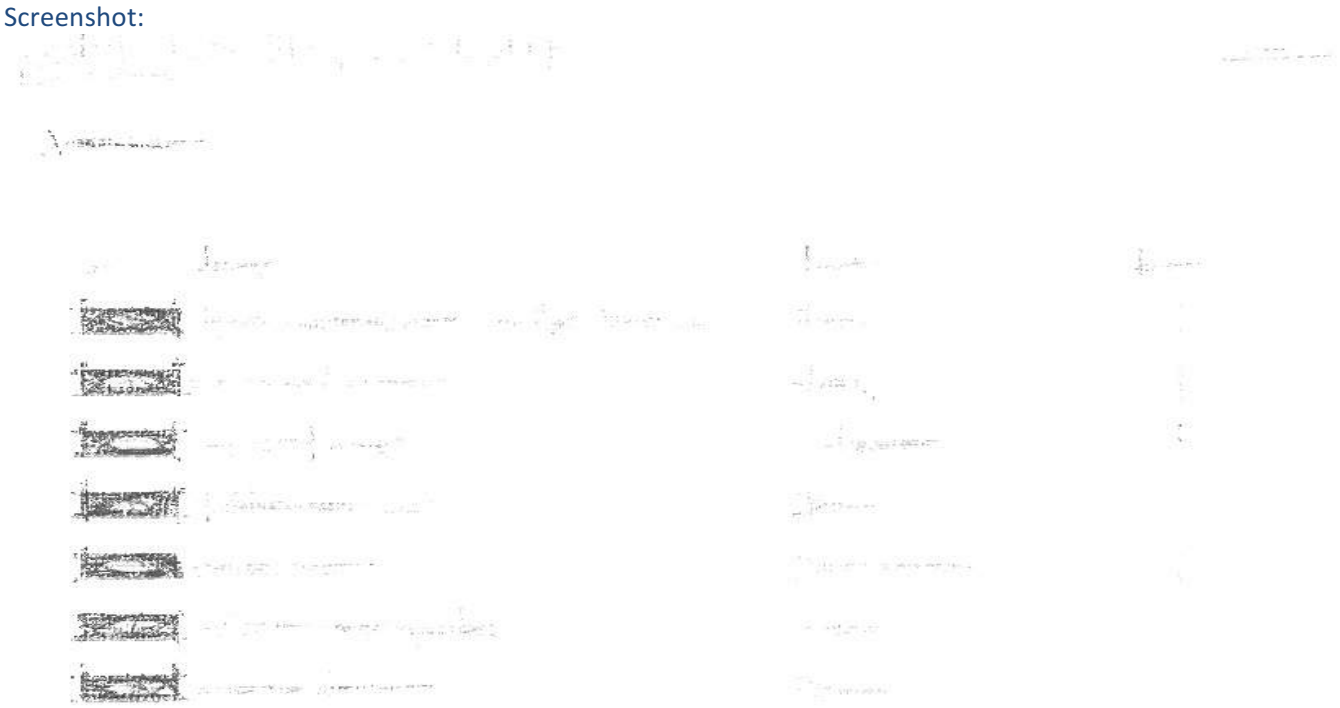
Telnet

Screenshot:

4.6 911.54.151.13

Nessus

Screenshot:

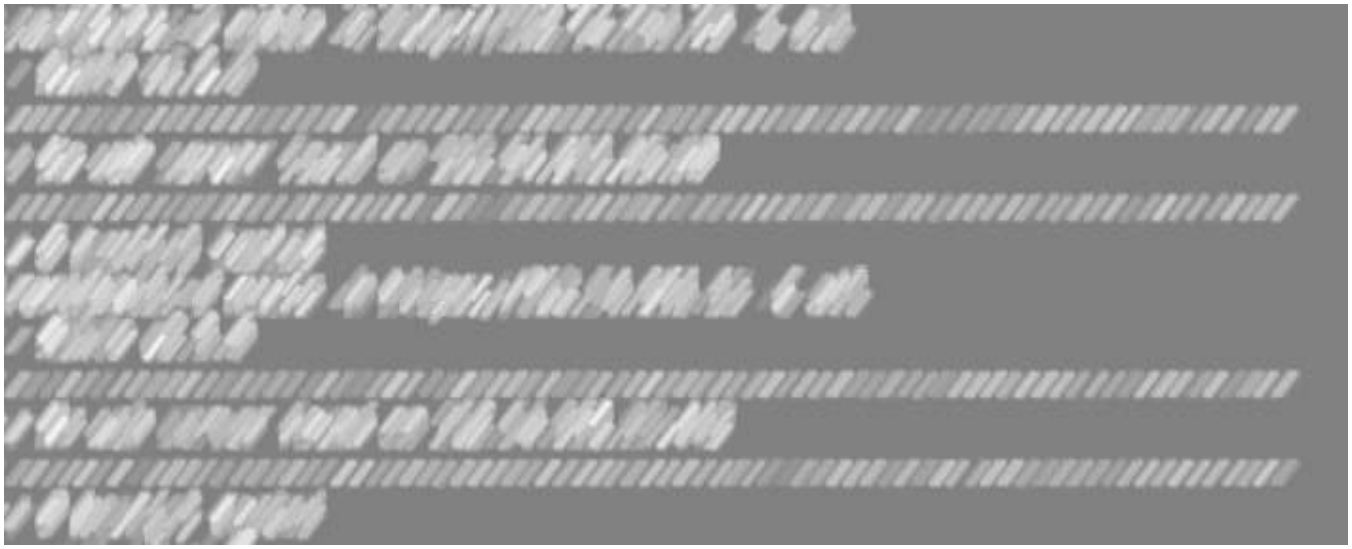


Nmap

Screenshot:

NIKTO

Screenshot:



Site not Accessing

Screenshot:

SSL Scan

Screenshot:

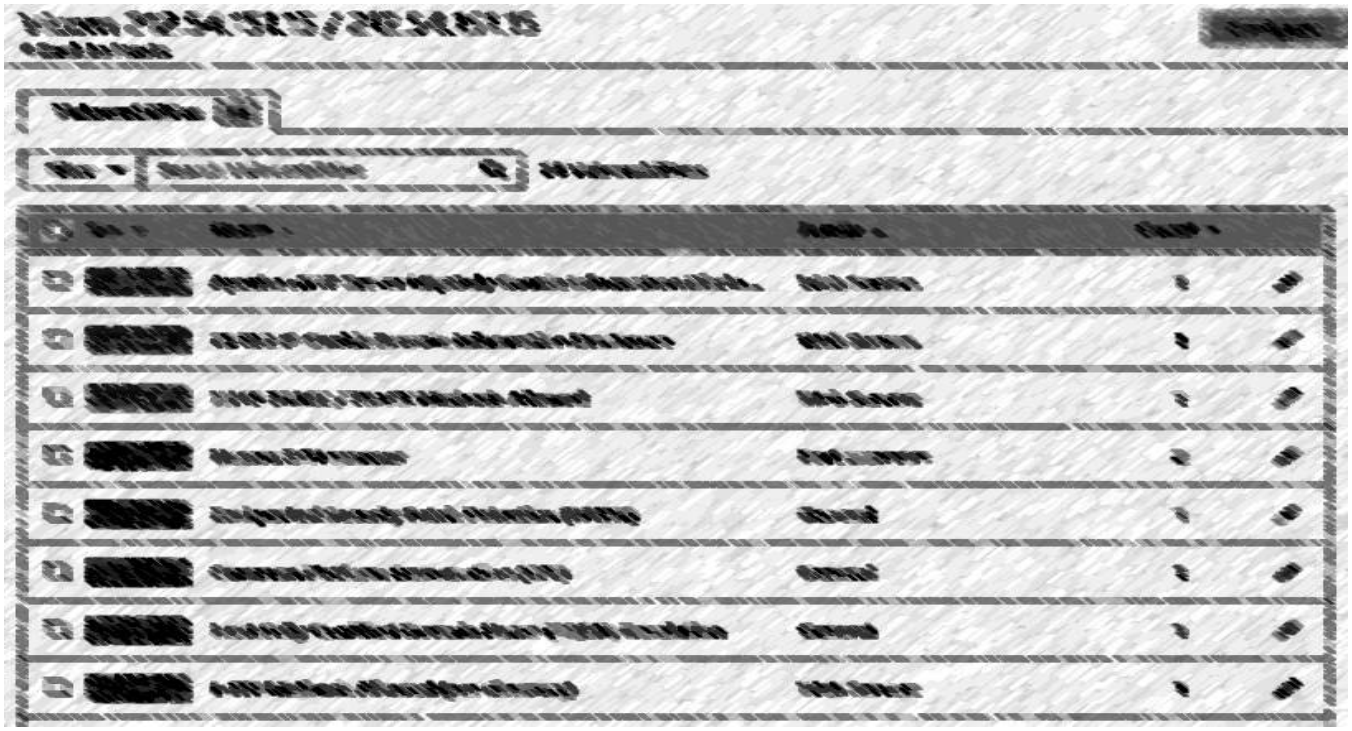
Telnet

Screenshot:

4.7 911.54.151.15

Nessus

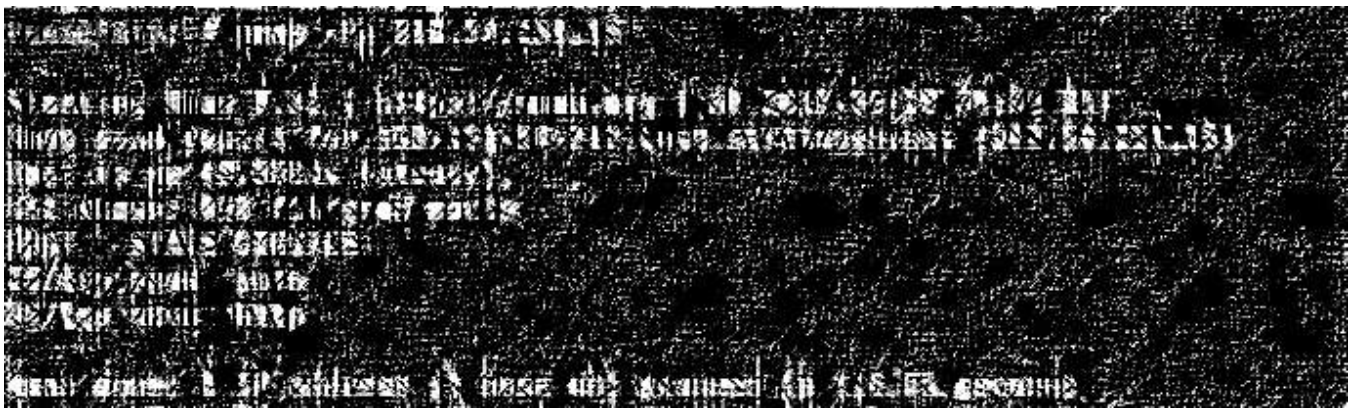
Screenshot:



☐	INFO	Common Platform Enumeration (CPE)	General	1	
☐	INFO	Host Fully Qualified Domain Name (FQDN) Resolution	General	1	
☐	INFO	HTTP Methods Allowed (per directory)	Web Servers	1	
☐	INFO	HTTP Server Type and Version	Web Servers	1	
☐	INFO	HyperText Transfer Protocol (HTTP) Information	Web Servers	1	
☐	INFO	Nessus Scan Information	Settings	1	
☐	INFO	Open Port Re-check	General	1	
☐	INFO	Patch Report	General	1	
☐	INFO	Service Detection	Service detection	1	

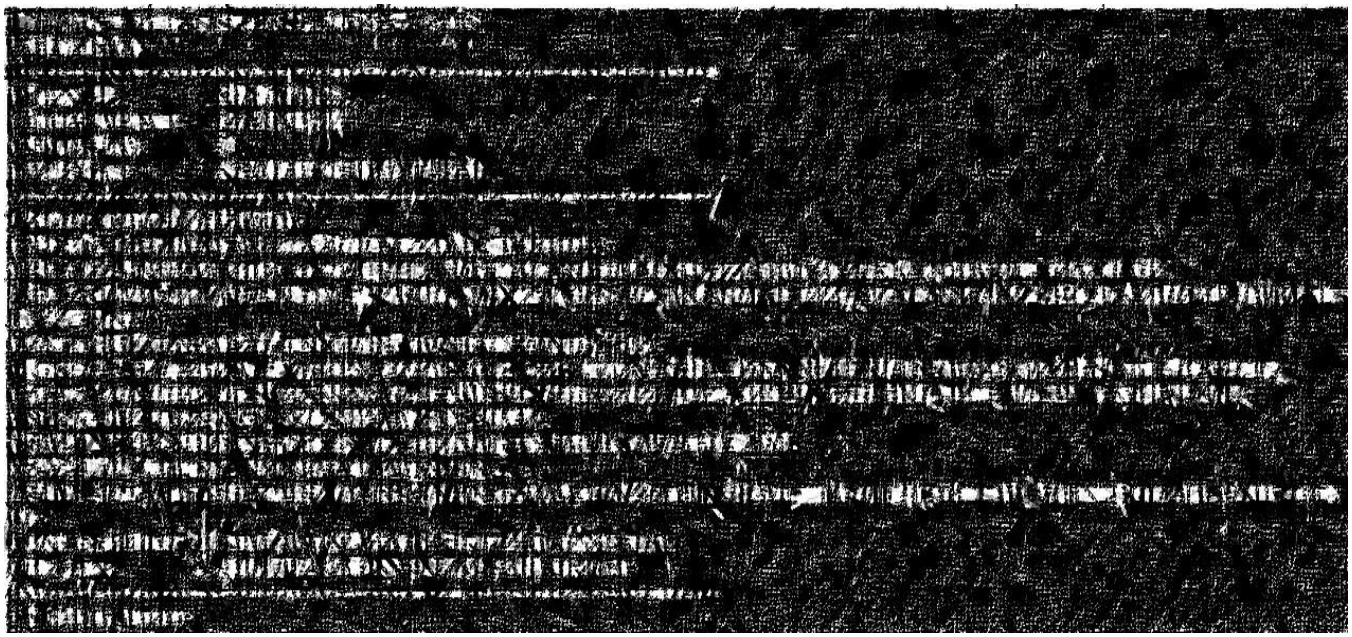
Nmap

Screenshot:



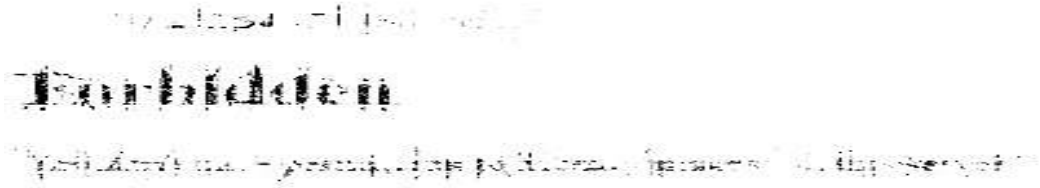
NIKTO

Screenshot:



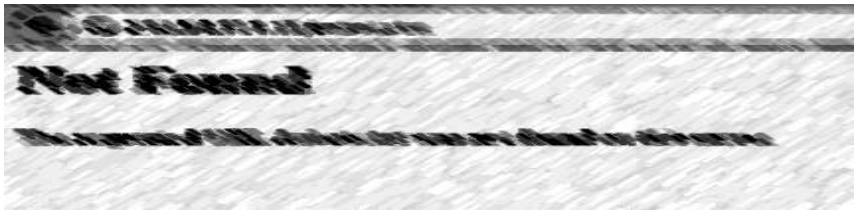
Directory Listing

Screenshot:



Robots

Screenshot:



Telnet

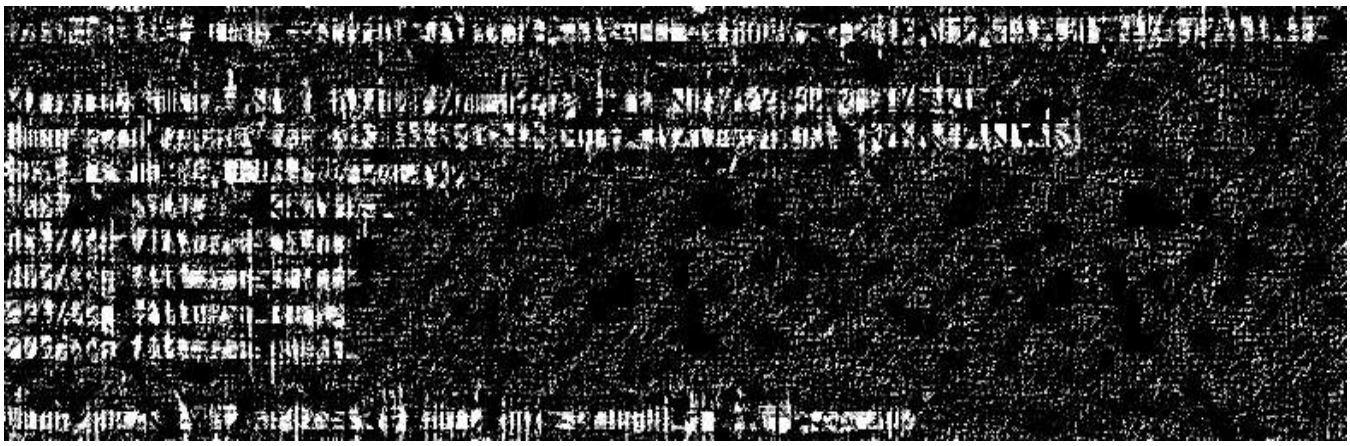
Screenshot:

SSL Scan

Screenshot:

Tested for Weak Ciphers

Screenshot:



Trace Method

Screenshot:

4.8 911.54.151.16

Nessus

Screenshot:

Nmap

Screenshot:

NIKTO

Screenshot:

Telnet

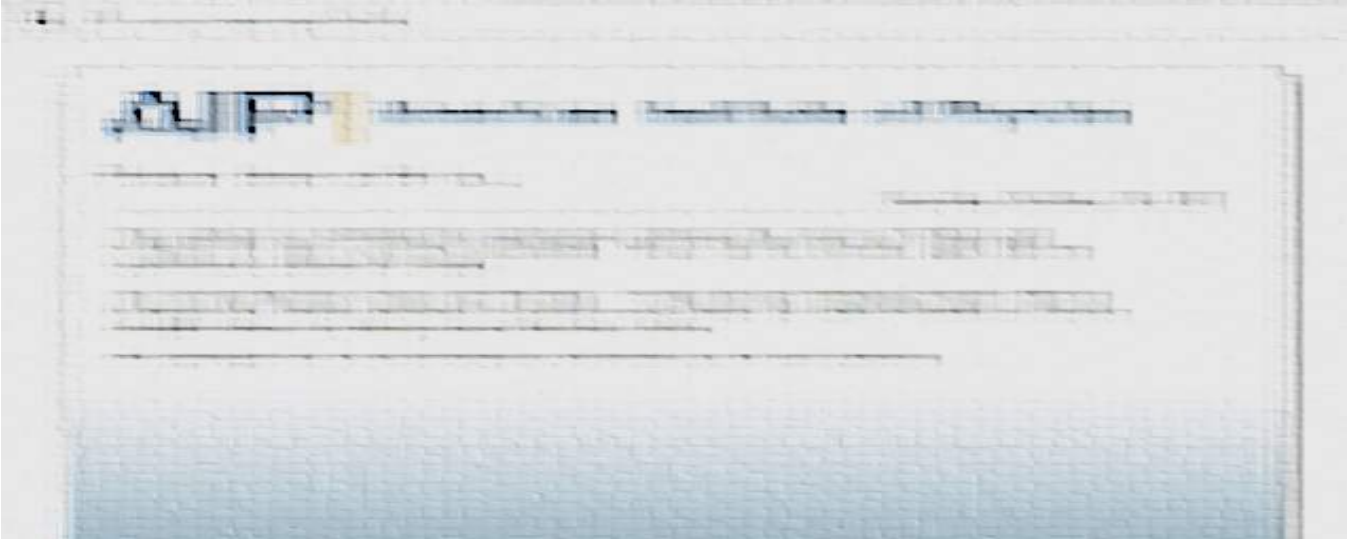
Screenshot:

SSL Scan

Screenshot:

IP redirecting to Web Page

Screenshot:



4.9 911.54.151.20

Nmap

Screenshot:

SQL Injection on Login

Screenshot:

Request	Payload1	Payload2	Status	Error	Timeout	Length	Comment
0			200			9863	baseline request
1	'	'	200			9863	
2	a' or 1=1--	'	200			9863	
3	"a"" or 1=1--"	'	200			9863	
4	or a = a	'	200			9863	
5	a' or 'a' = 'a	'	200			9863	
6	1 or 1=1	'	200			9863	
7	a' waitfor delay '0:0:10'--	'	200			9863	
8	1 waitfor delay '0:0:10'--	'	200			9863	
9	declare @q nvarchar (200) sele...	'	200			9863	
10	declare @s varchar(200) select...	'	200			9863	
11	declare @q nvarchar (200) 0x7...	'	200			9863	
12	declare @s varchar (200) selec...	'	200			9863	

Request | Response

Raw | Params | Headers | Hex

```
POST /j_security_check HTTP/1.1
Host: 212.54.151.20
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://212.54.151.20/HomePage.do?SkipNV2Filter=true
Content-Type: application/x-www-form-urlencoded
Content-Length: 295
Cookie: JSESSIONID=29347BA06A46EFB7B0405CD95AD56C08
Connection: close
Upgrade-Insecure-Requests: 1

j_username=1 or
1=1&j_password='&domain=2&DOMAIN_NAME=int.aip.org&LDAPEnable=false&hidden=Select+a+Domain&hidden
in=int.aip.org&dynamicUserAddition_status=true&localAuthEnable=true&logonDomainName=int.aip.org&
```

Request	Payload1	Payload2	Status	Error	Timeout	Length	Comment
0			200			9863	baseline request
1	'	'	200			9863	
2	a' or 1=1--	'	200			9863	
3	"a"" or 1=1--"	'	200			9863	
4	or a = a	'	200			9863	
5	a' or 'a' = 'a	'	200			9863	
6	1 or 1=1	'	200			9863	
7	a' waitfor delay '0:0:10'--	'	200			9863	
8	1 waitfor delay '0:0:10'--	'	200			9863	
9	declare @q nvarchar (200) sele...	'	200			9863	
10	declare @s varchar(200) select...	'	200			9863	
11	declare @q nvarchar (200) 0x7...	'	200			9863	
12	declare @s varchar (200) selec...	'	200			9863	

Request | Response

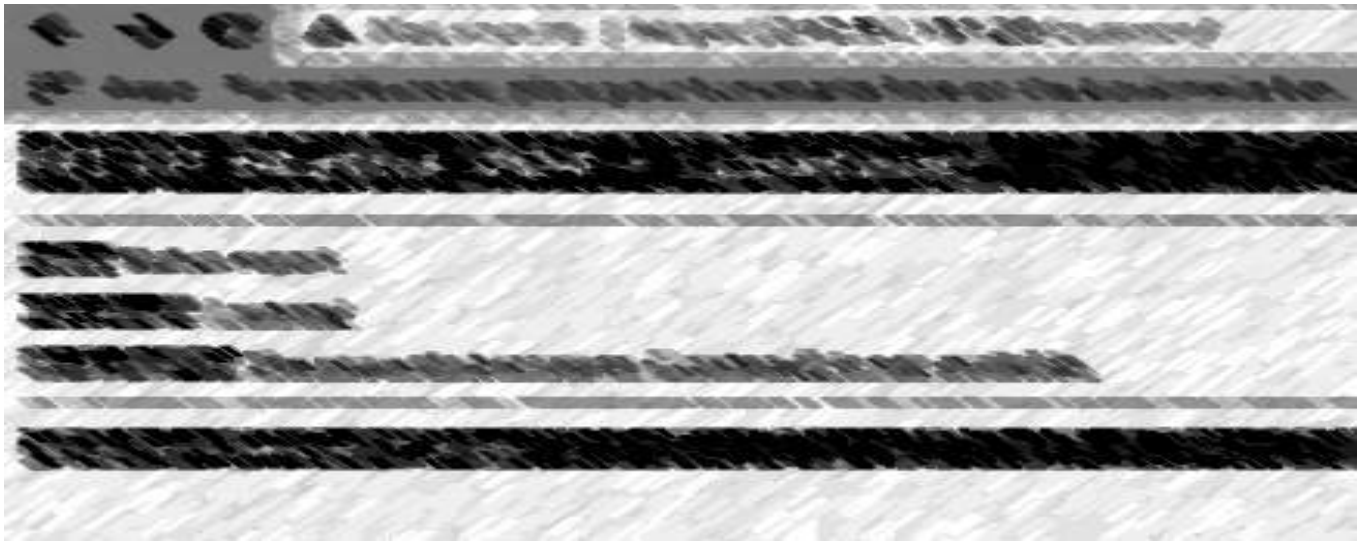
Raw | Headers | Hex | HTML | Render

```
HTTP/1.1 200 OK
Content-Type: text/html;charset=UTF-8
Vary: Accept-Encoding
Date: Tue, 10 Oct 2017 11:42:49 GMT
Connection: close
Server: -
Content-Length: 9693

<!DOCTYPE html>
<html>
<head>
<meta http-equiv="X-UA-Compatible" content="IE=Edge">
```

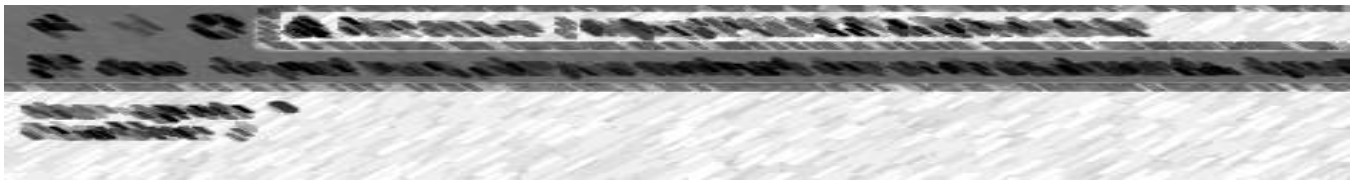
Directory Listing

Screenshot:



Robots

Screenshot:

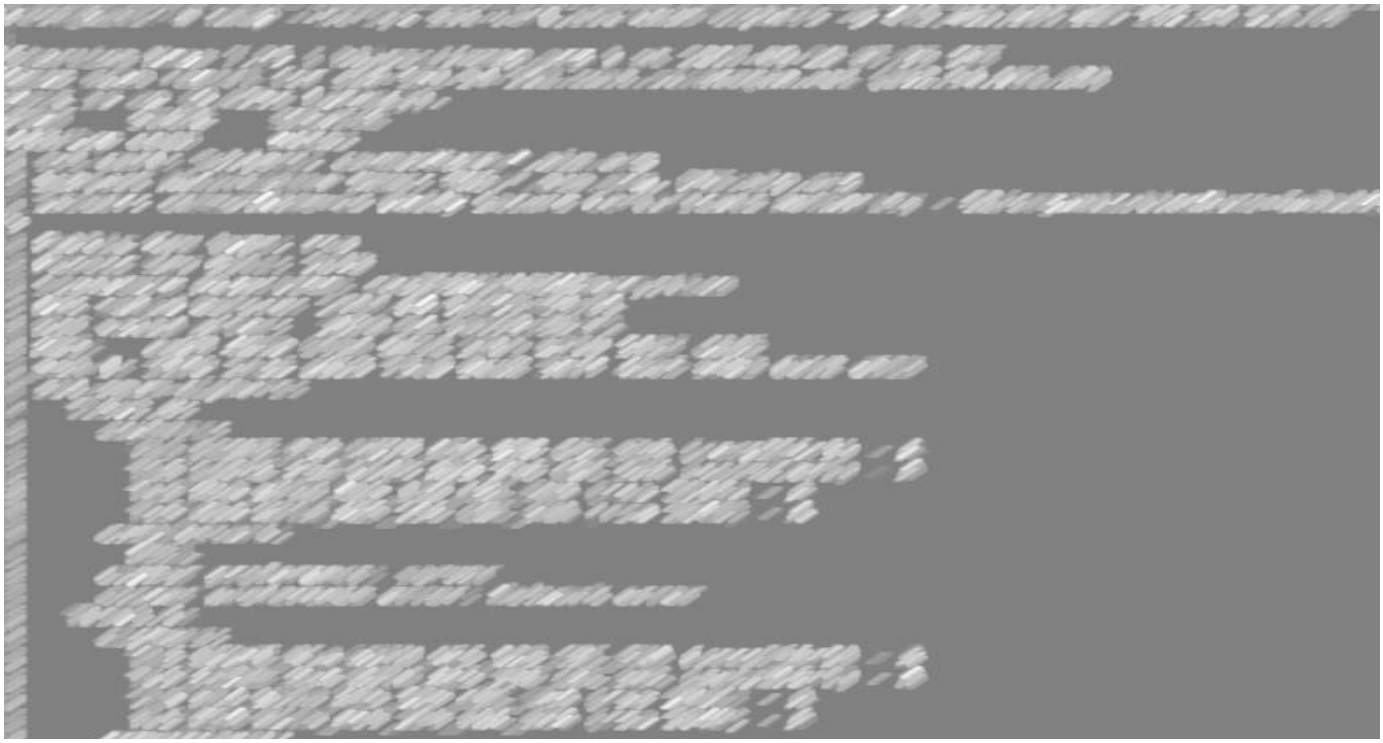


SSL Scan

Screenshot:

Tested for Weak Ciphers

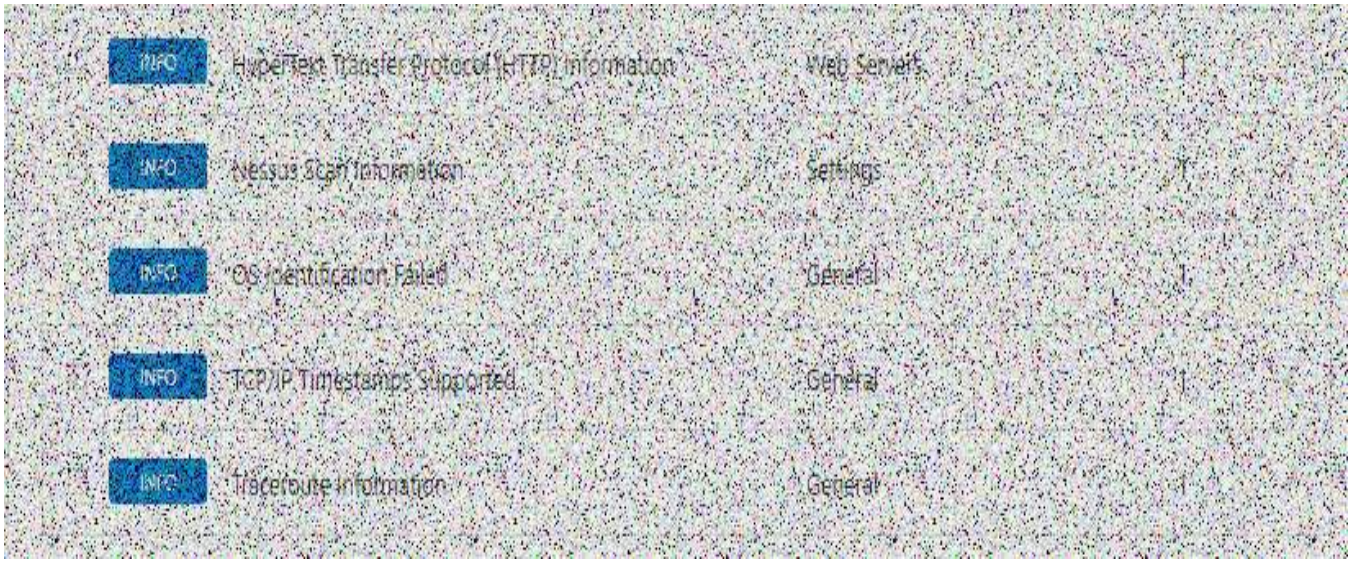
Screenshot:



4.10 911.54.151.25

Nessus

Screenshot:



Nmap

Screenshot:

Telnet

Screenshot:

SSL Scan

Screenshot:

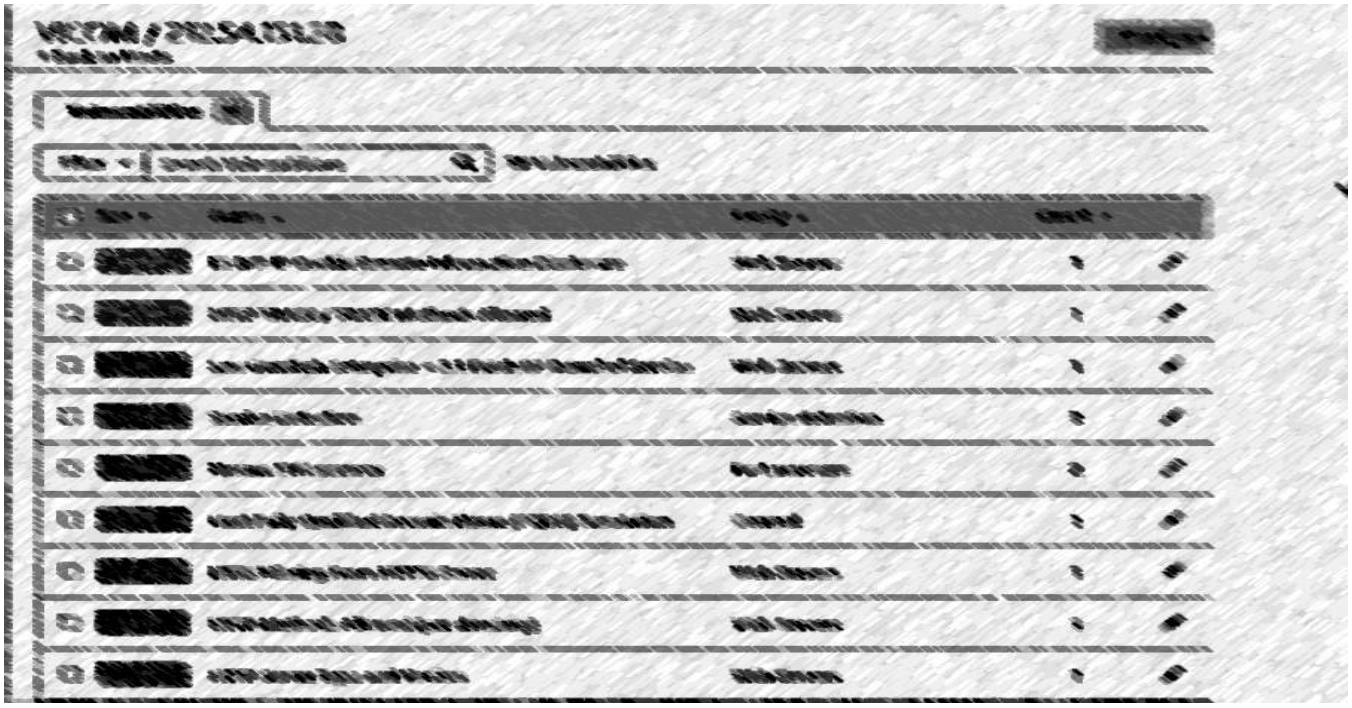
Tested for Weak Ciphers

Screenshot:

4.11 911.54.151.28

Nessus

Screenshot:



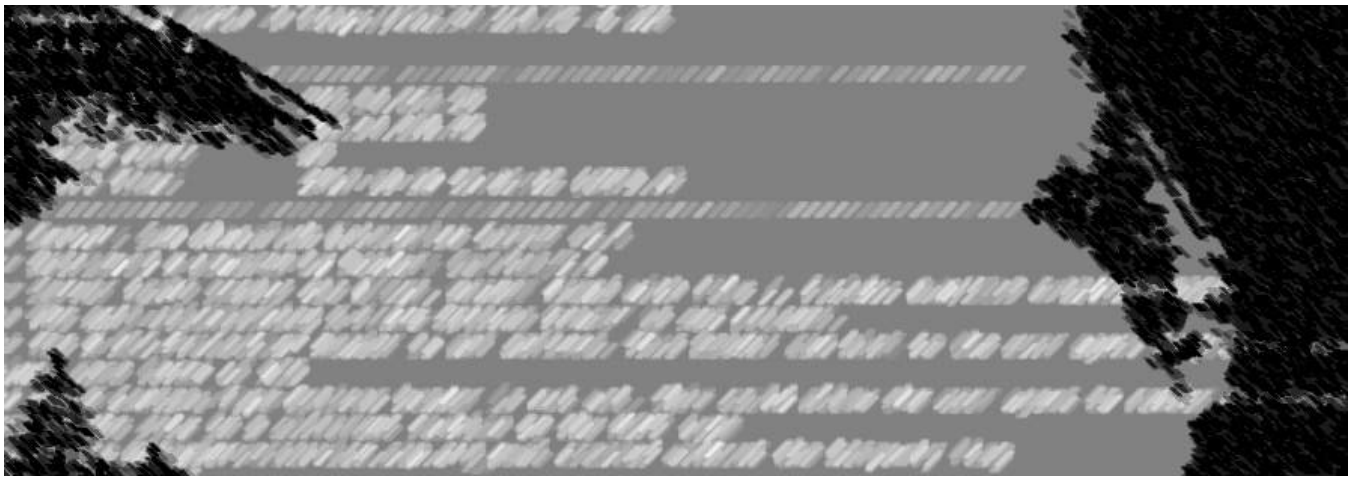
☐	INFO	HTTP Server Type and Version	Web Servers	1	
☐	INFO	HyperText Transfer Protocol (HTTP) Information	Web Servers	1	
☐	INFO	Nessus Scan Information	Settings	1	
☐	INFO	Oracle GlassFish HTTP Server Version	Web Servers	1	
☐	INFO	SSL / TLS Versions Supported	General	1	
☐	INFO	SSL Certificate 'commonName' Mismatch	General	1	
☐	INFO	SSL Certificate Information	General	1	
☐	INFO	SSL Certificate Signed Using Weak Hashing Algorithm (...	General	1	
☐	INFO	SSL Root Certification Authority Certificate Information	General	1	
☐	INFO	TCP/IP Timestamps Supported	General	1	
☐	INFO	Traceroute Information	General	1	

Nmap

Screenshot:

NIKTO

Screenshot:

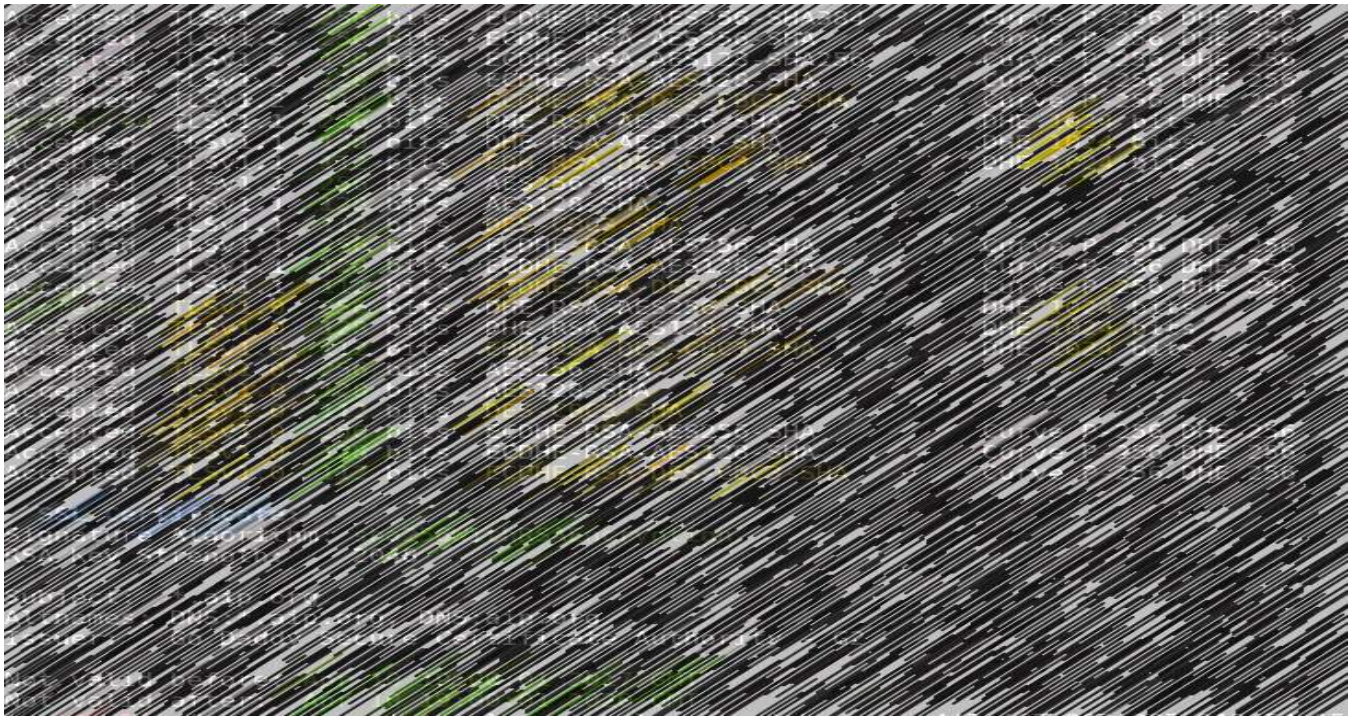


Telnet

Screenshot:

SSL Scan

Screenshot:



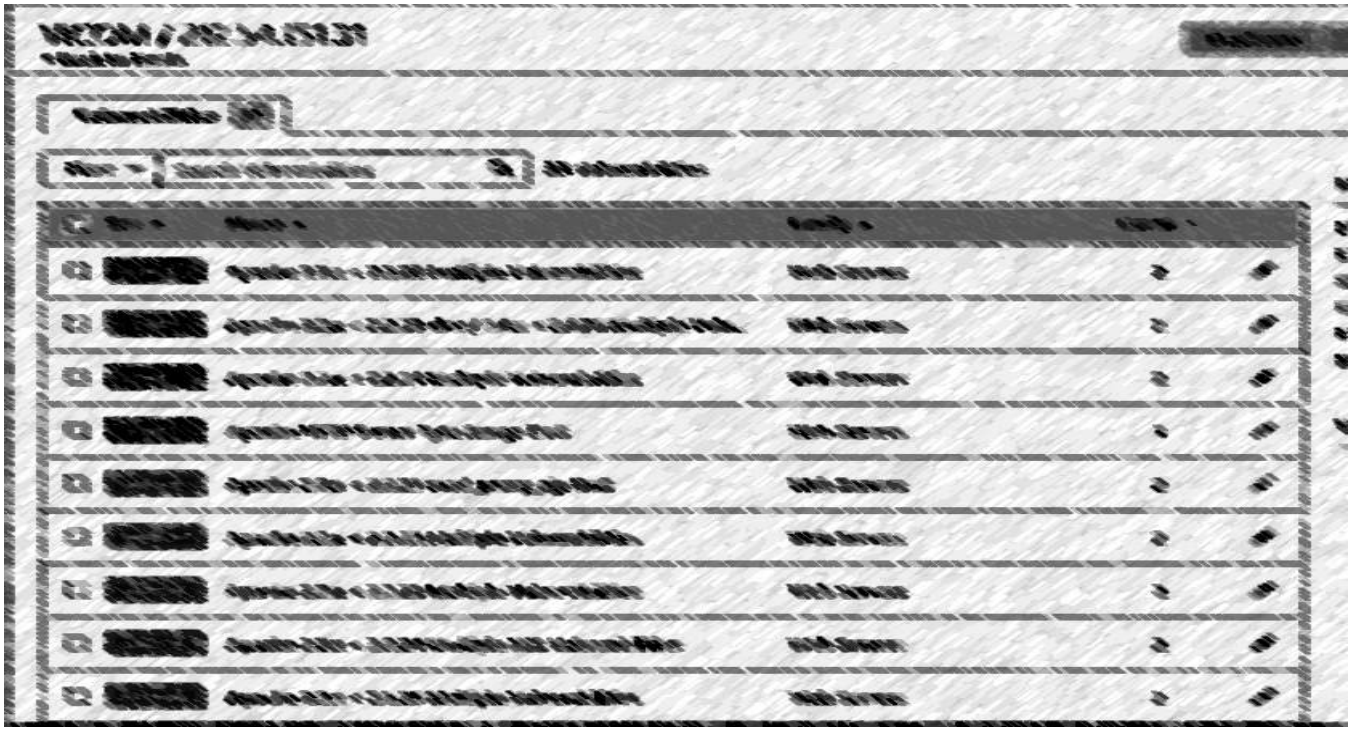
Tested for Weak Ciphers

Screenshot:

4.12 911.54.151.31

Nessus

Screenshot:

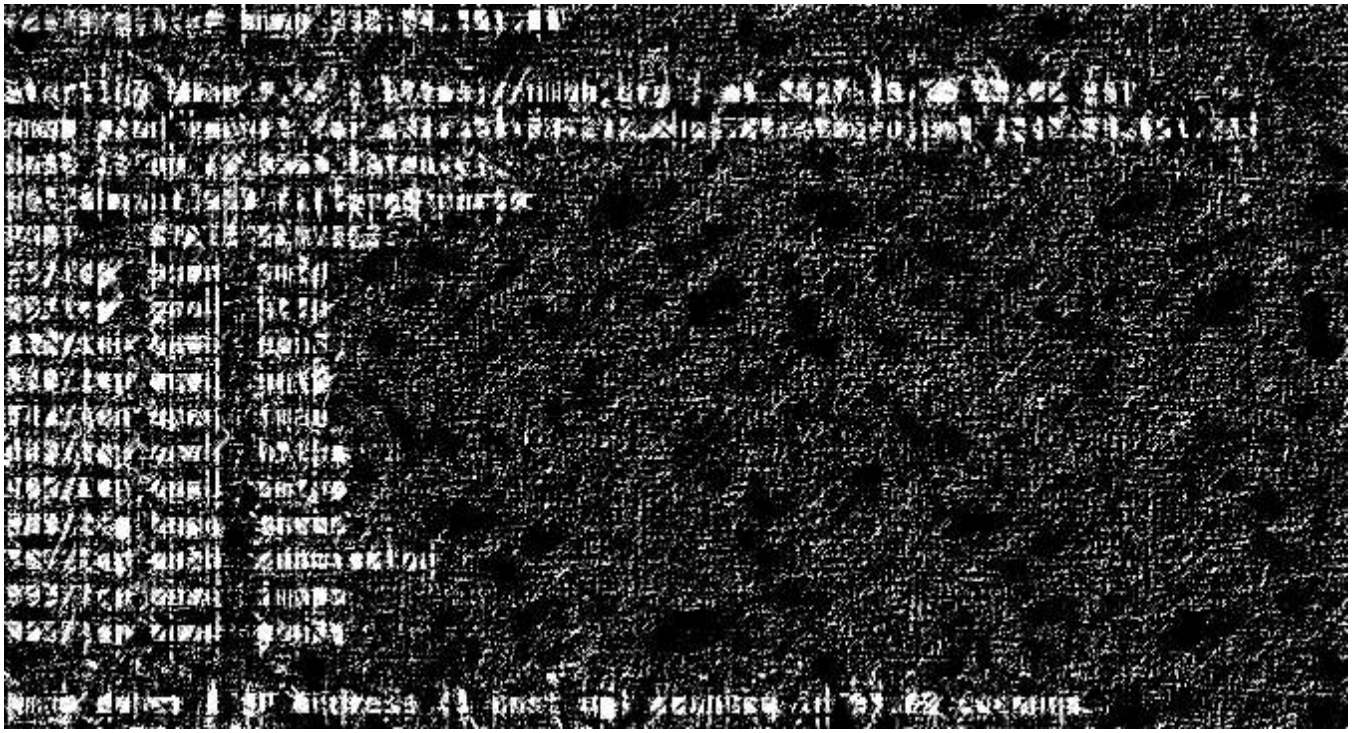


MEDIUM	Apache 2.2.x < 2.2.27 Multiple Vulnerabilities	Web Servers	2	
MEDIUM	Apache HTTP Server httpOnly Cookie Information Discl...	Web Servers	2	
MEDIUM	Apache Server ETag Header Information Disclosure	Web Servers	2	
MEDIUM	F5 BIG-IP Cookie Remote Information Disclosure	Web Servers	2	
MEDIUM	HTTP TRACE / TRACK Methods Allowed	Web Servers	2	
MEDIUM	Apache Tomcat Servlet / JSP Container Default Files	Web Servers	1	
INFO	Service Detection	Service detection	3	
INFO	HTTP Server Type and Version	Web Servers	2	
INFO	HyperText Transfer Protocol (HTTP) Information	Web Servers	2	
INFO	Nessus SYN scanner	Port scanners	2	
INFO	Common Platform Enumeration (CPE)	General	1	
INFO	Host Fully Qualified Domain Name (FQDN) Resolution	General	1	
INFO	HSTS Missing From HTTPS Server	Web Servers	1	
INFO	HTTP Methods Allowed (per directory)	Web Servers	1	

INFO	Host Fully Qualified Domain Name (FQDN) Resolution	General	1	
INFO	HSTS Missing From HTTPS Server	Web Servers	1	
INFO	HTTP Methods Allowed (per directory)	Web Servers	1	
INFO	Nessus Scan Information	Settings	1	
INFO	OS Identification Failed	General	1	
INFO	Patch Report	General	1	
INFO	SSL / TLS Versions Supported	General	1	
INFO	SSL Certificate 'commonName' Mismatch	General	1	
INFO	SSL Certificate Information	General	1	
INFO	SSL Certificate Signed Using Weak Hashing Algorithm (...	General	1	
INFO	SSL Root Certification Authority Certificate Information	General	1	
INFO	TCP/IP Timestamps Supported	General	1	
INFO	Traceroute Information	General	1	

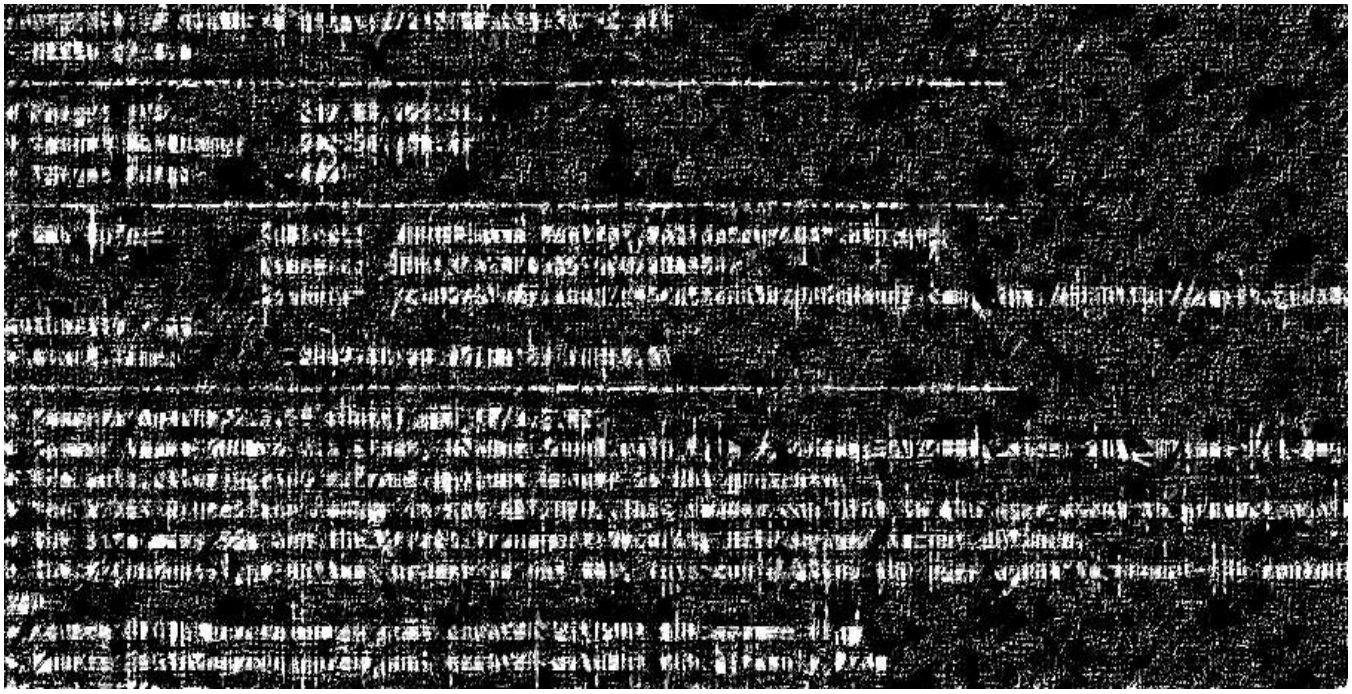
Nmap

Screenshot:



NIKTO

Screenshot:

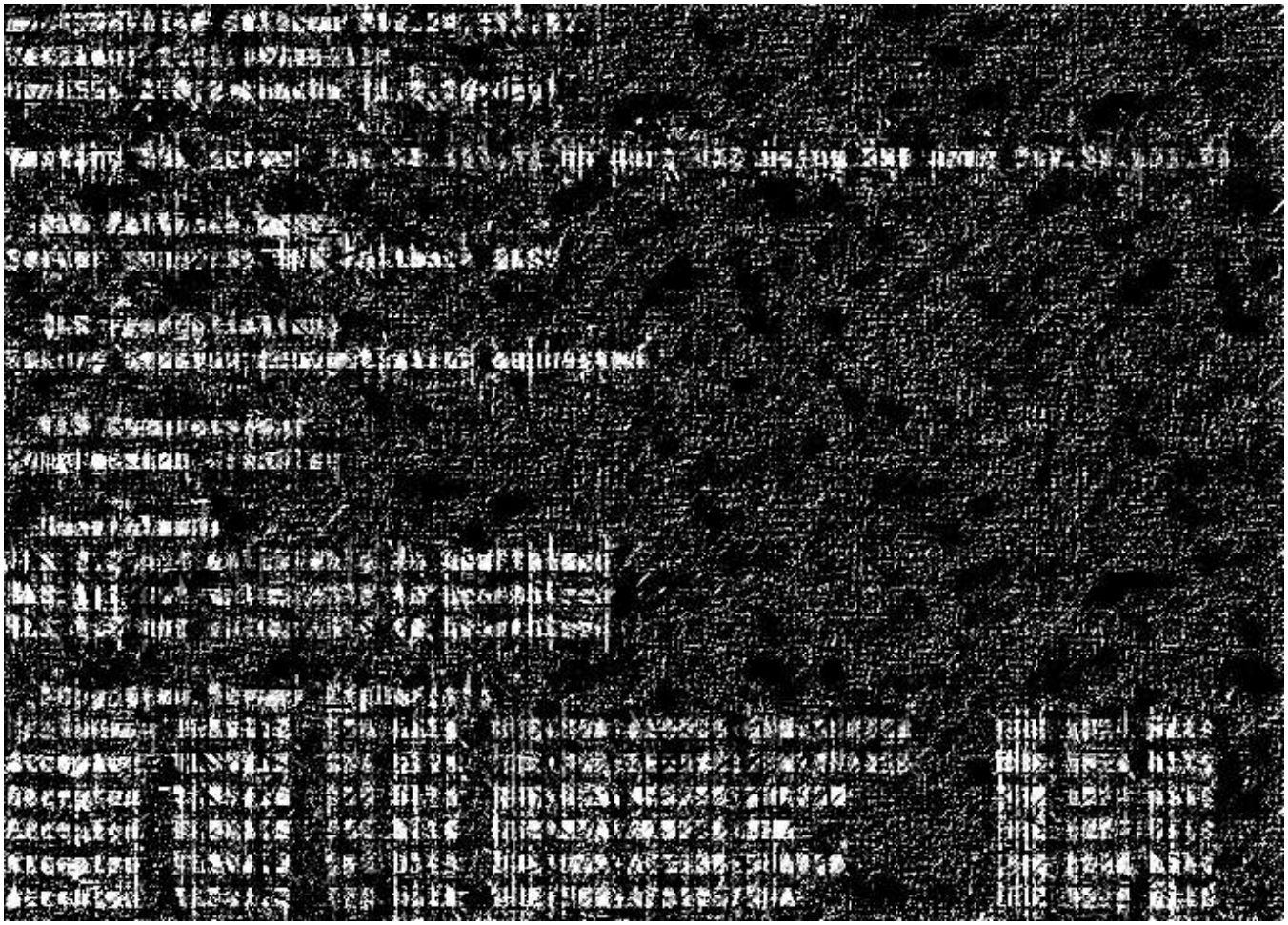


Telnet

Screenshot:

SSL Scan

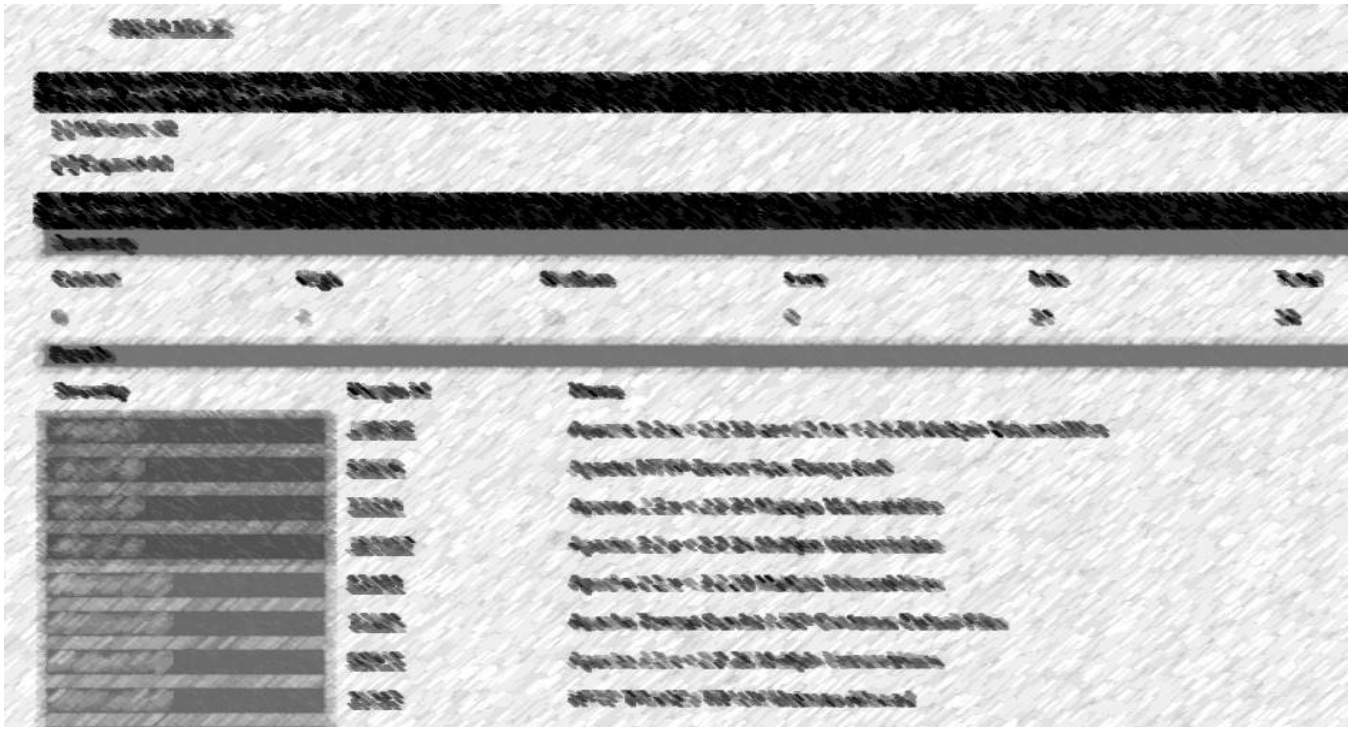
Screenshot:

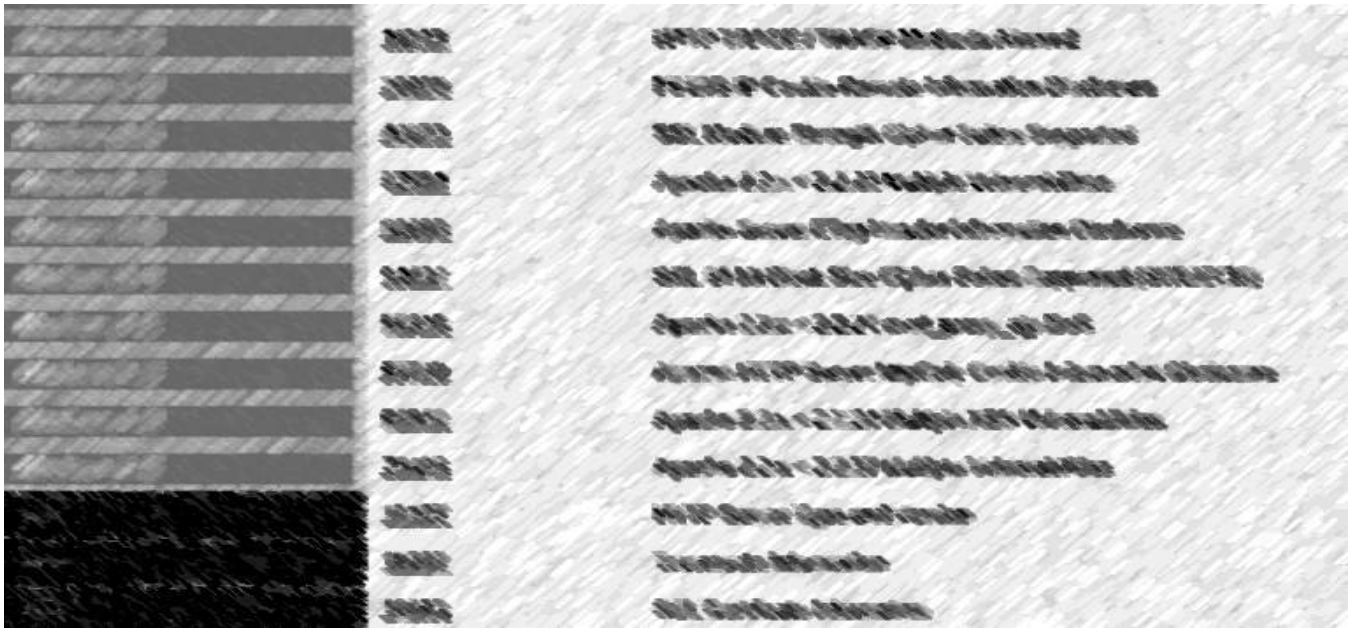


4.13 911.54.151.32

Nessus

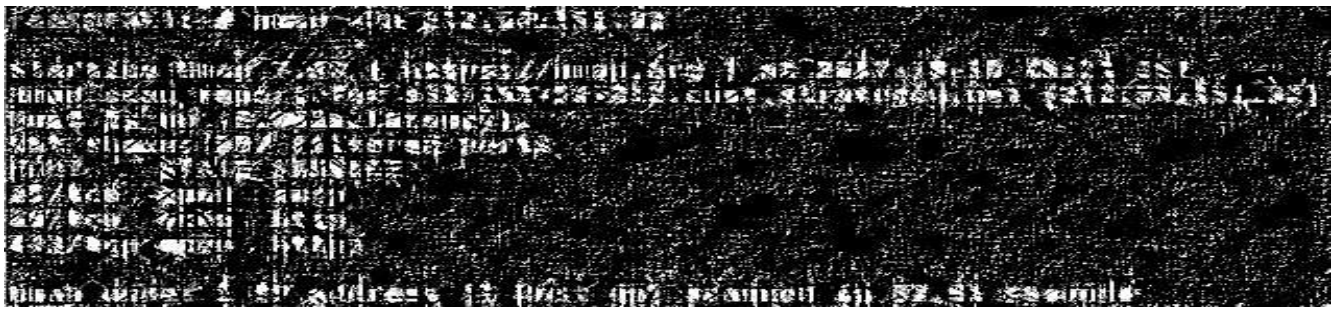
Screenshot:





Nmap

Screenshot:



Telnet

Screenshot:

SSL Scan

Screenshot:

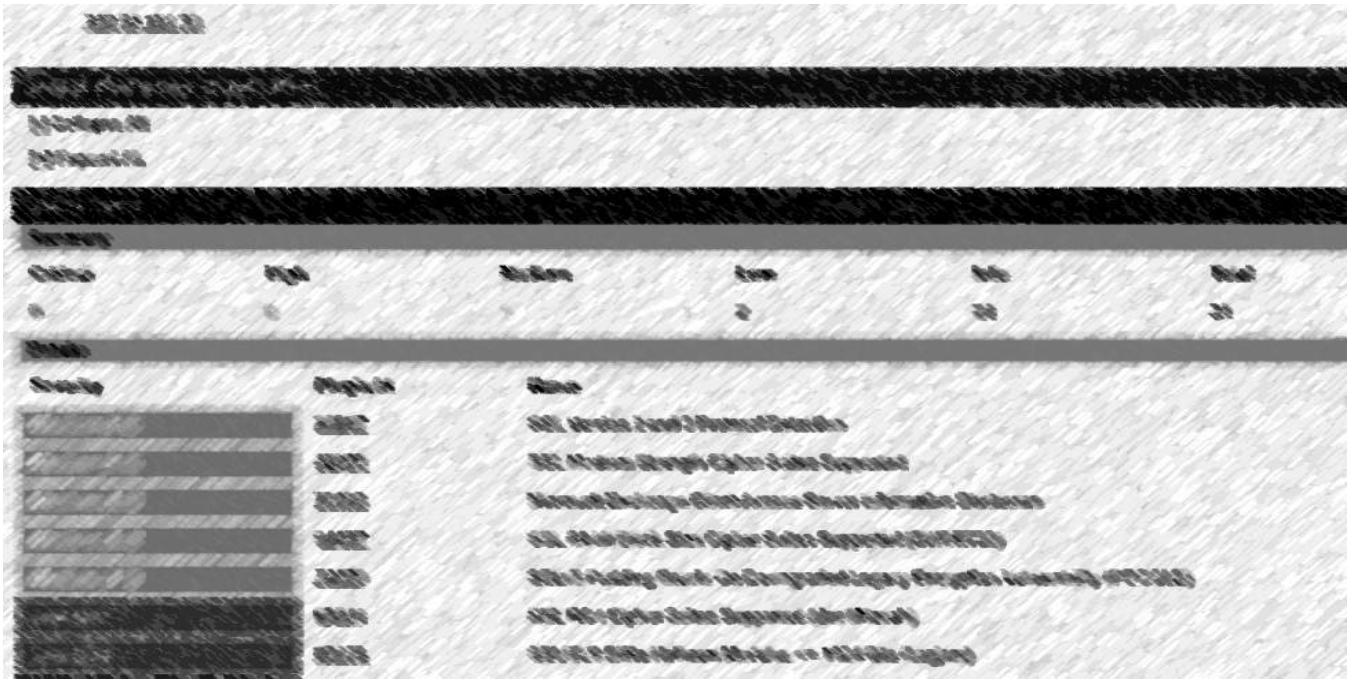
Tested for Weak Ciphers

Screenshot:

4.14 911.54.151.33

Nessus

Screenshot:



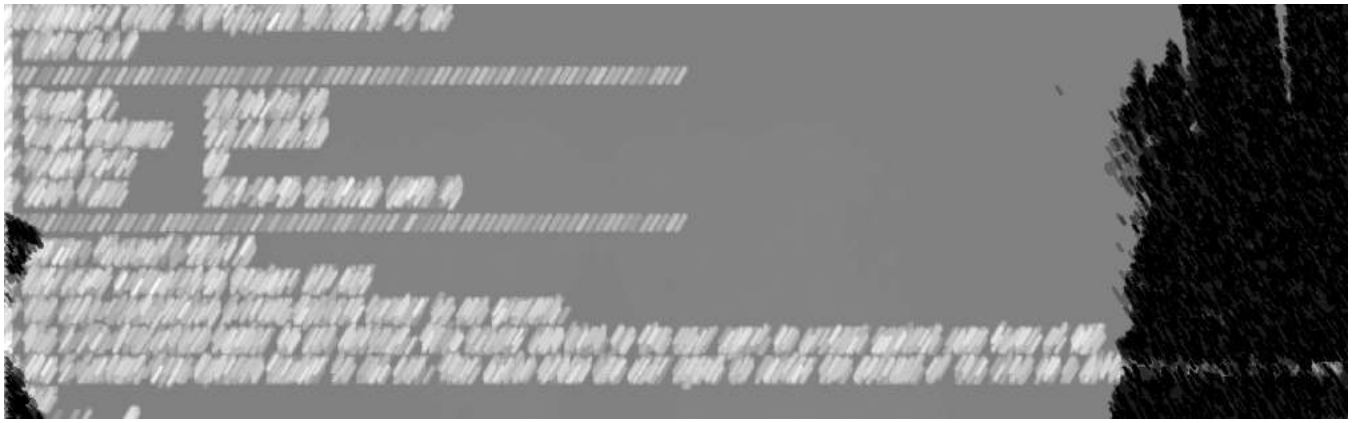
Info	10107	HTTP Server Type and Version
Info	10263	SMTP Server Detection
Info	10287	Traceroute Information
Info	10863	SSL Certificate Information
Info	11219	Nessus SYN scanner
Info	11414	IMAP Service Banner Retrieval
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	14255	Microsoft Outlook Web Access (OWA) Version Detection
Info	19506	Nessus Scan Information
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	42085	IMAP Service STARTTLS Command Support
Info	43111	HTTP Methods Allowed (per directory)
Info	45590	Common Platform Enumeration (CPE)
Info	46180	Additional DNS Hostnames

Nmap

Screenshot:

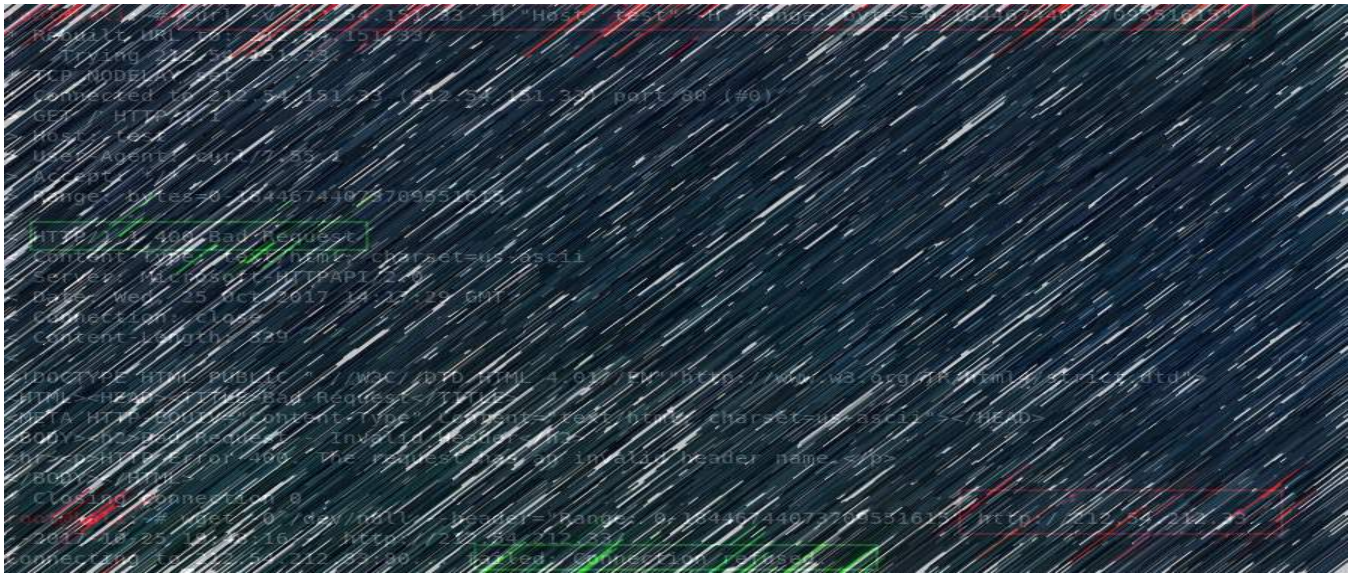
NIKTO

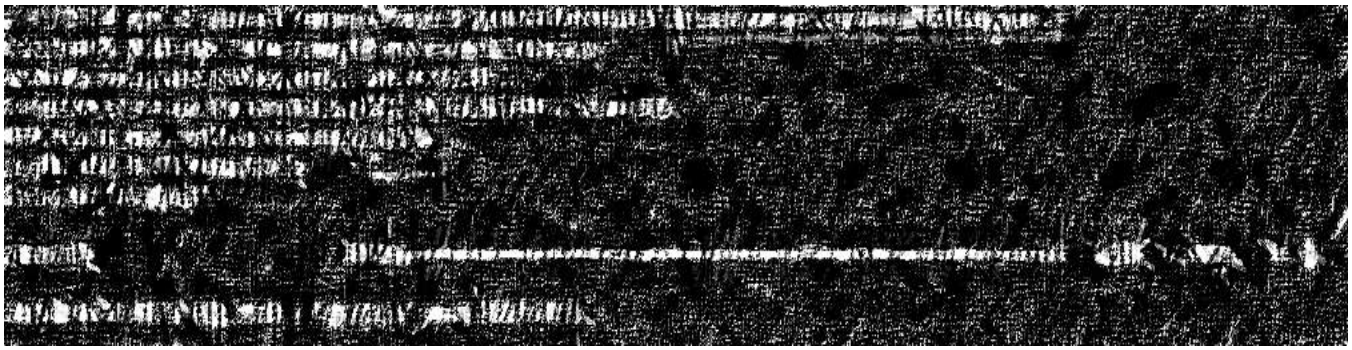
Screenshot:



IIS DoS Attacks - Tested

Screenshot:





Telnet

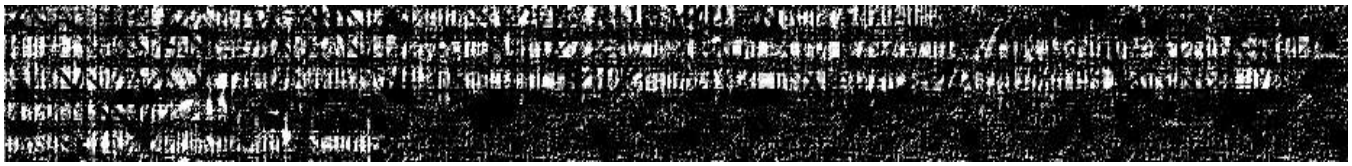
Screenshot:

SSL Scan

Screenshot:

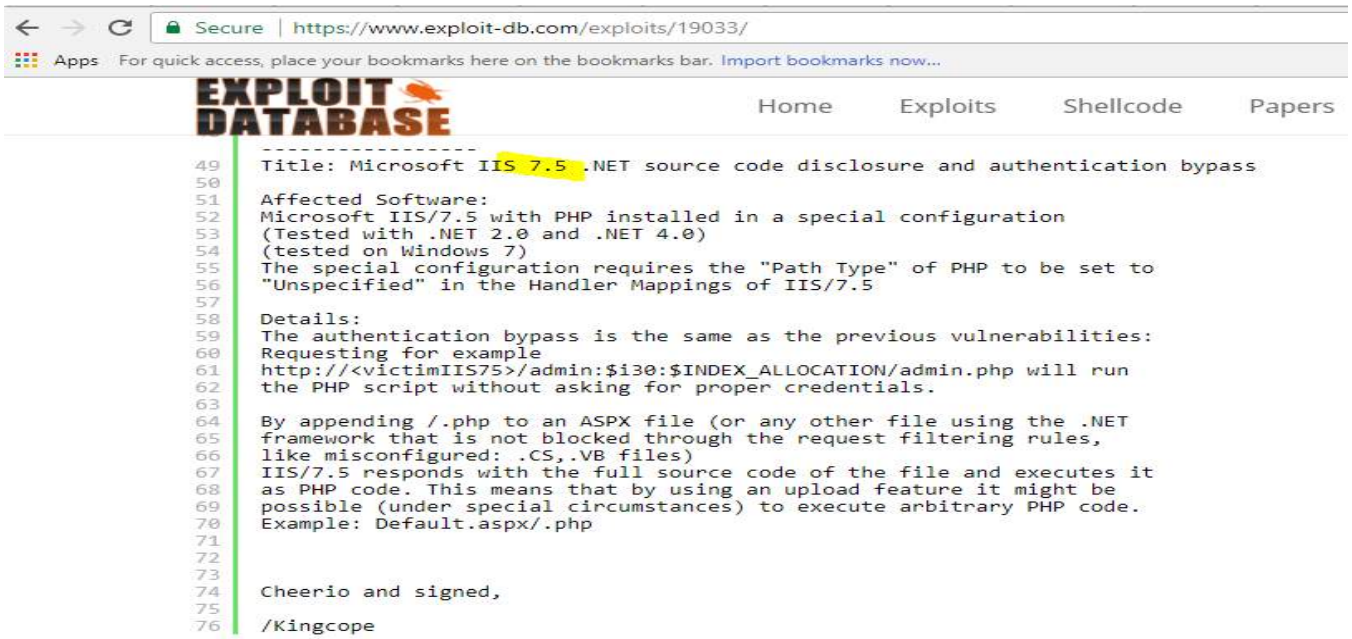
Tested for Weak Ciphers

Screenshot:



IIS Exploits

Screenshot:



Secure | https://www.exploit-db.com/exploits/19033/

Apps For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...

EXPLOIT DATABASE

Home Exploits Shellcode Papers

```
----------------
Title: Microsoft IIS 7.5 .NET source code disclosure and authentication bypass

Affected Software:
Microsoft IIS/7.5 with PHP installed in a special configuration
(Tested with .NET 2.0 and .NET 4.0)
(tested on Windows 7)
The special configuration requires the "Path Type" of PHP to be set to
"Unspecified" in the Handler Mappings of IIS/7.5

Details:
The authentication bypass is the same as the previous vulnerabilities:
Requesting for example
http://<victimIIS75>/admin:$i30:$INDEX_ALLOCATION/admin.php will run
the PHP script without asking for proper credentials.

By appending /.php to an ASPX file (or any other file using the .NET
framework that is not blocked through the request filtering rules,
like misconfigured: .CS,.VB files)
IIS/7.5 responds with the full source code of the file and executes it
as PHP code. This means that by using an upload feature it might be
possible (under special circumstances) to execute arbitrary PHP code.
Example: Default.aspx/.php



Cheerio and signed,

/Kingcope
```

4.15 911.54.151.34

Nessus

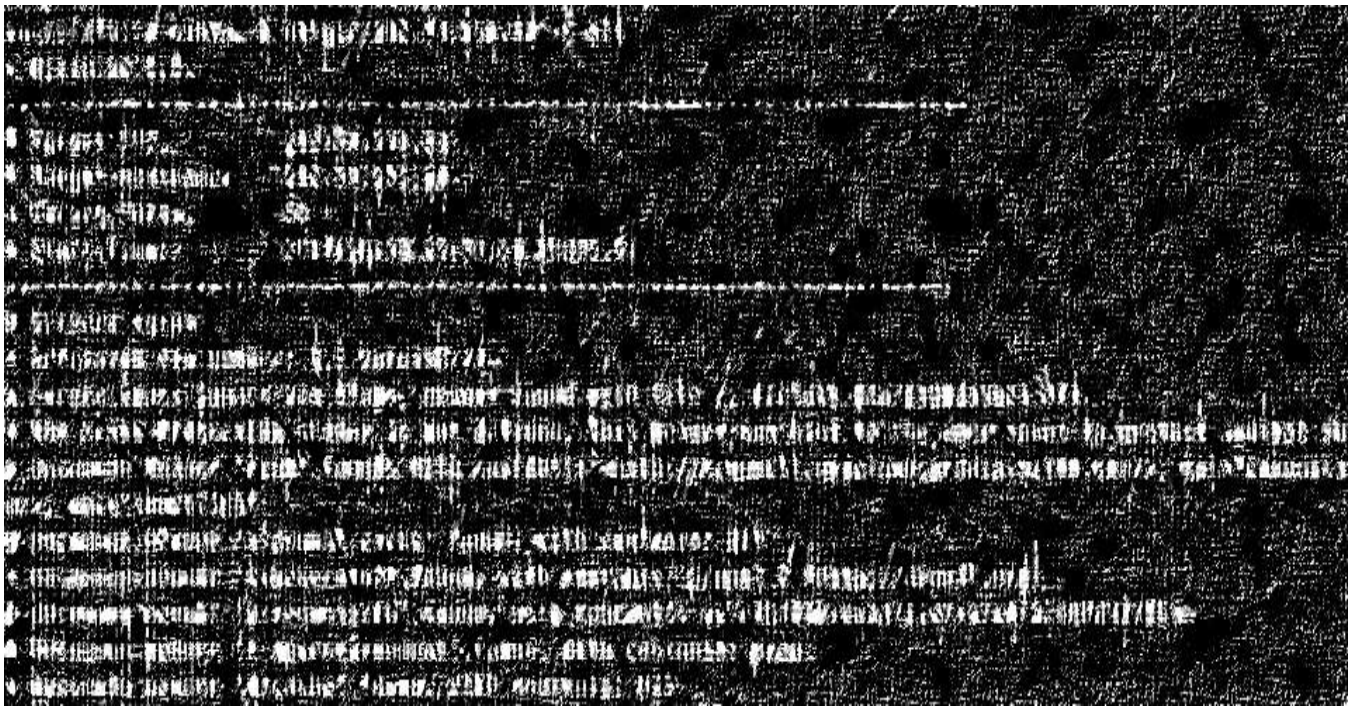
Screenshot:

Nmap

Screenshot:

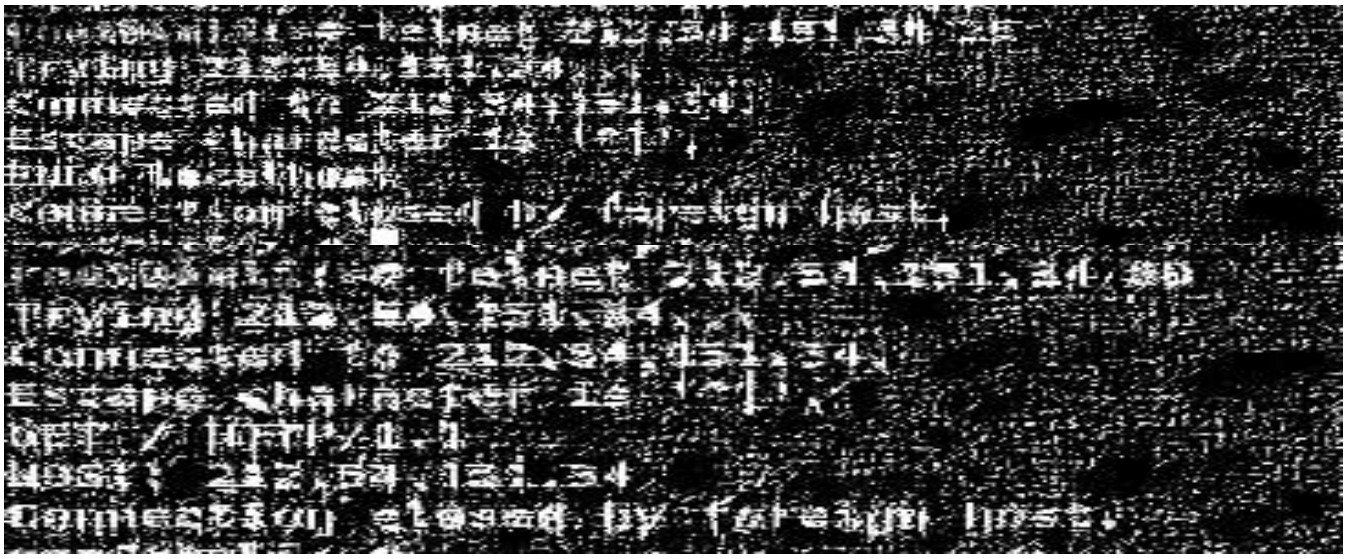
NIKTO

Screenshot:



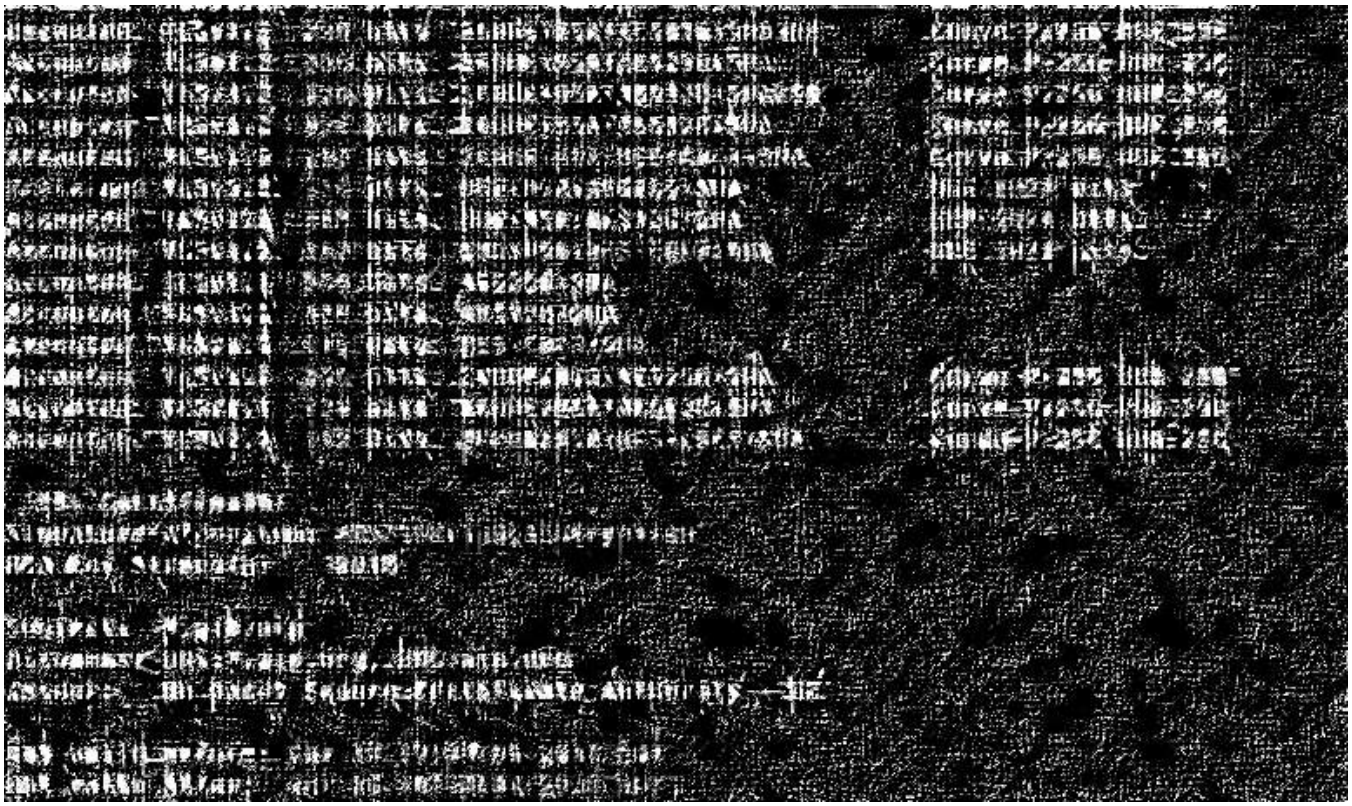
Telnet

Screenshot:



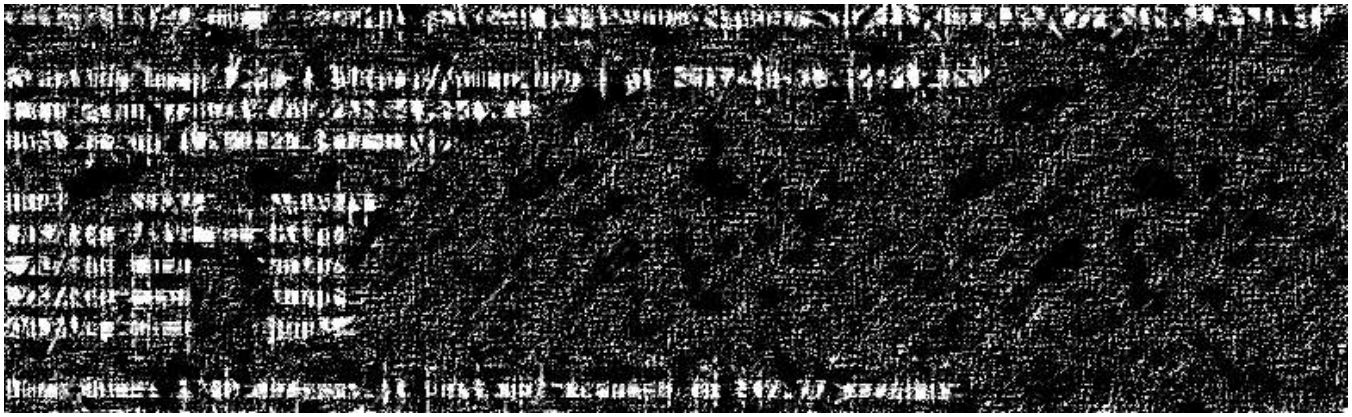
SSL Scan

Screenshot:



Tested for Weak Ciphers

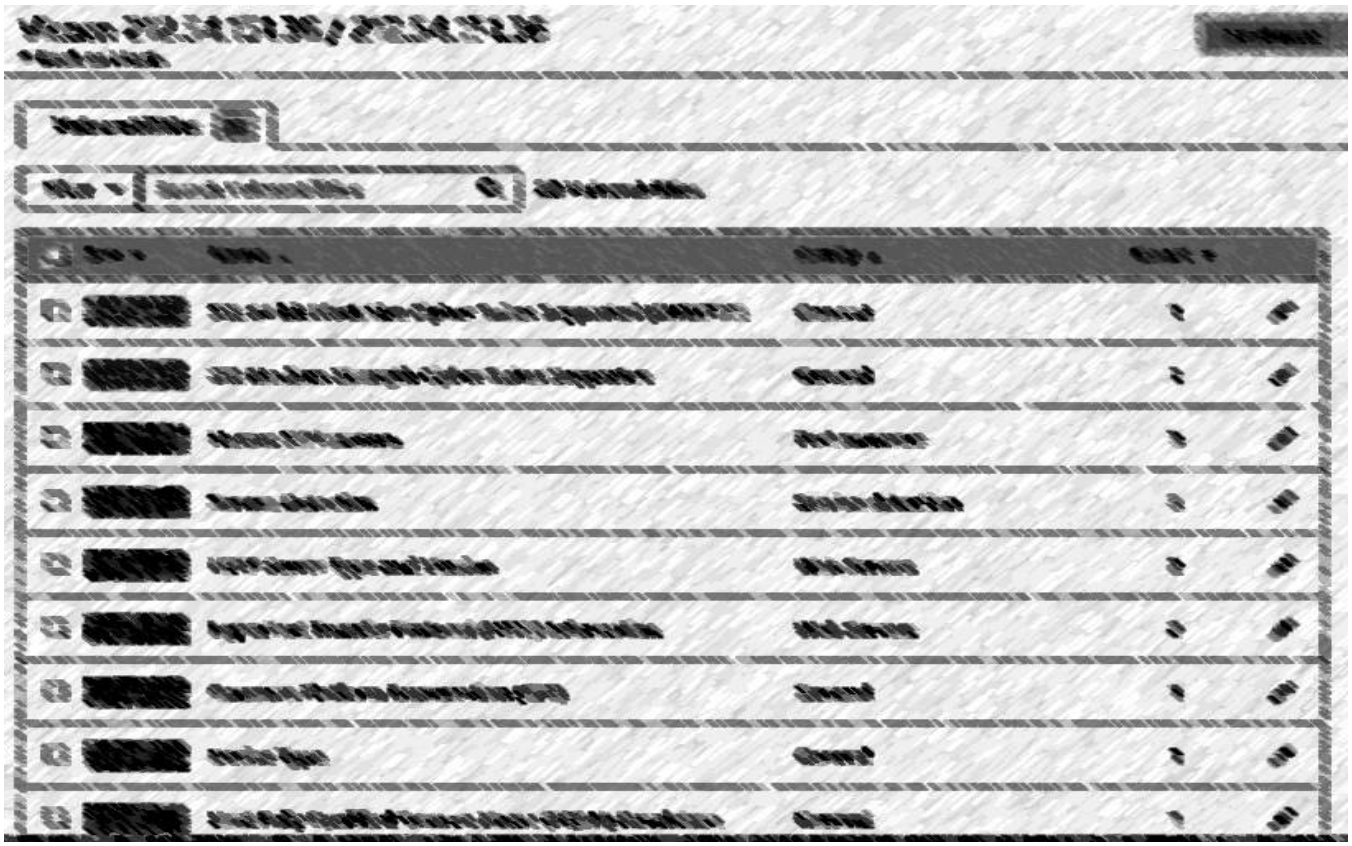
Screenshot:



4.16 911.54.151.36

Nessus

Screenshot:



INFO	Device Type	General	1	
INFO	Host Fully Qualified Domain Name (FQDN) Resolution	General	1	
INFO	HSTS Missing From HTTPS Server	Web Servers	1	
INFO	Nessus Scan Information	Settings	1	
INFO	OS Identification	General	1	
INFO	SSL / TLS Versions Supported	General	1	
INFO	SSL Certificate 'commonName' Mismatch	General	1	
INFO	SSL Certificate Information	General	1	
INFO	SSL Certificate Signed Using Weak Hashing Algorithm (K...	General	1	
INFO	SSL Cipher Block Chaining Cipher Suites Supported	General	1	
INFO	SSL Cipher Suites Supported	General	1	
INFO	SSL Perfect Forward Secrecy Cipher Suites Supported	General	1	
INFO	SSL Root Certification Authority Certificate Information	General	1	

Nmap

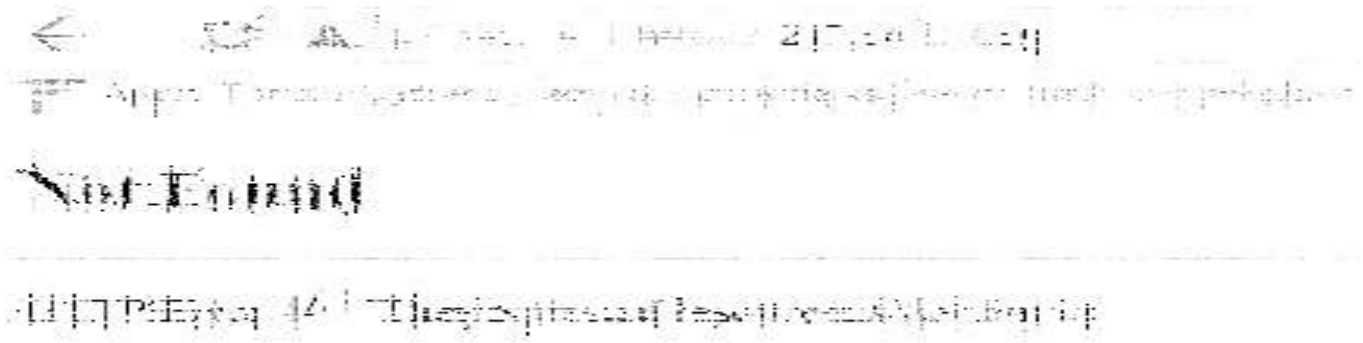
Screenshot:

SSL Scan

Screenshot:

Web Page not Found

Screenshot:



Trace Method

Screenshot:

4.17 911.54.151.37

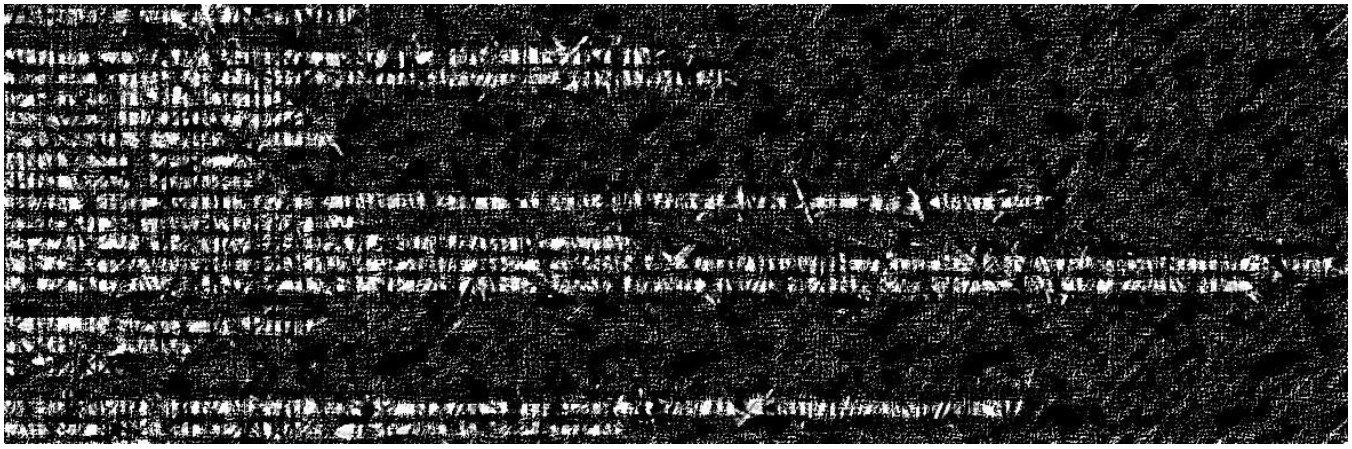
Nessus

Screenshot:

	INFO	HSTS Missing From HTTPS Server	Web Servers	1	
	INFO	Nessus Scan Information	Settings	1	
	INFO	Open Port Re-check	General	1	
	INFO	OS Identification	General	1	
	INFO	SSL / TLS Versions Supported	General	1	
	INFO	SSL Certificate 'commonName' Mismatch	General	1	
	INFO	SSL Certificate Information	General	1	
	INFO	SSL Certificate Signed Using Weak Hashing Algorithm (K...	General	1	
	INFO	SSL Root Certification Authority Certificate Information	General	1	
	INFO	TCP/IP Timestamps Supported	General	1	
	INFO	Traceroute Information	General	1	

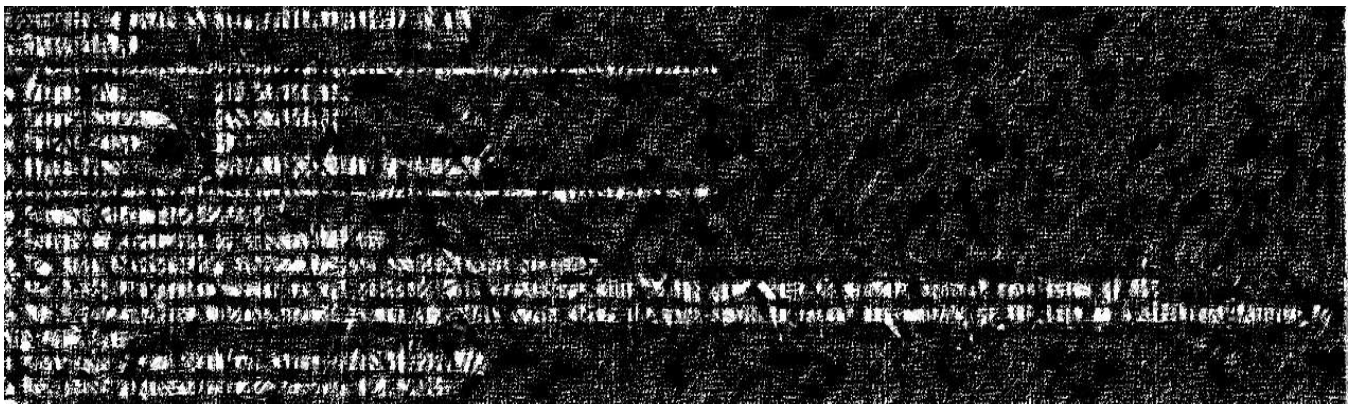
Nmap

Screenshot:



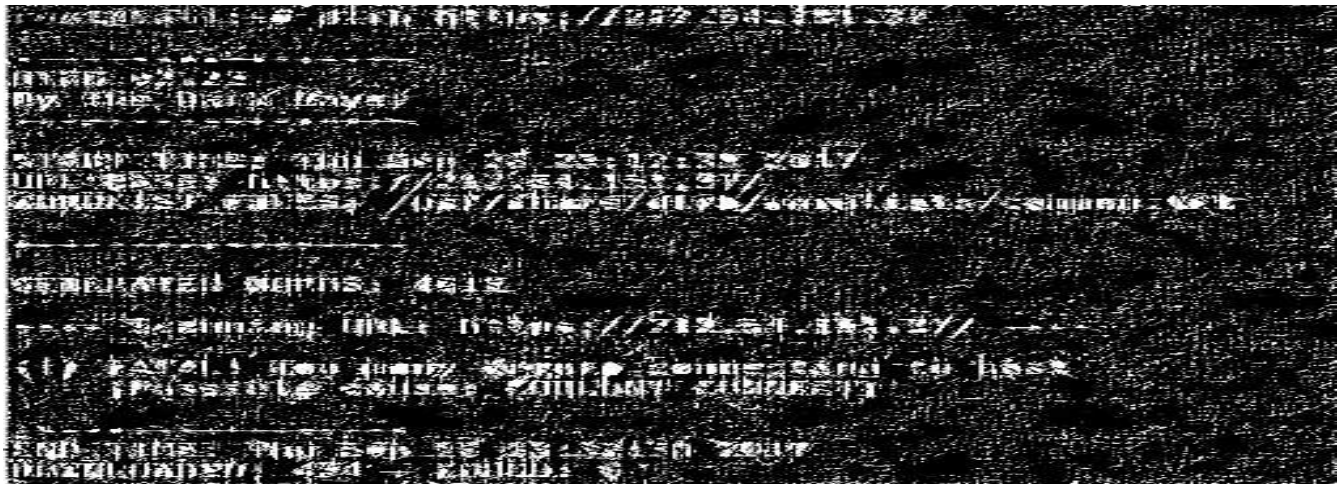
NIKTO

Screenshot:



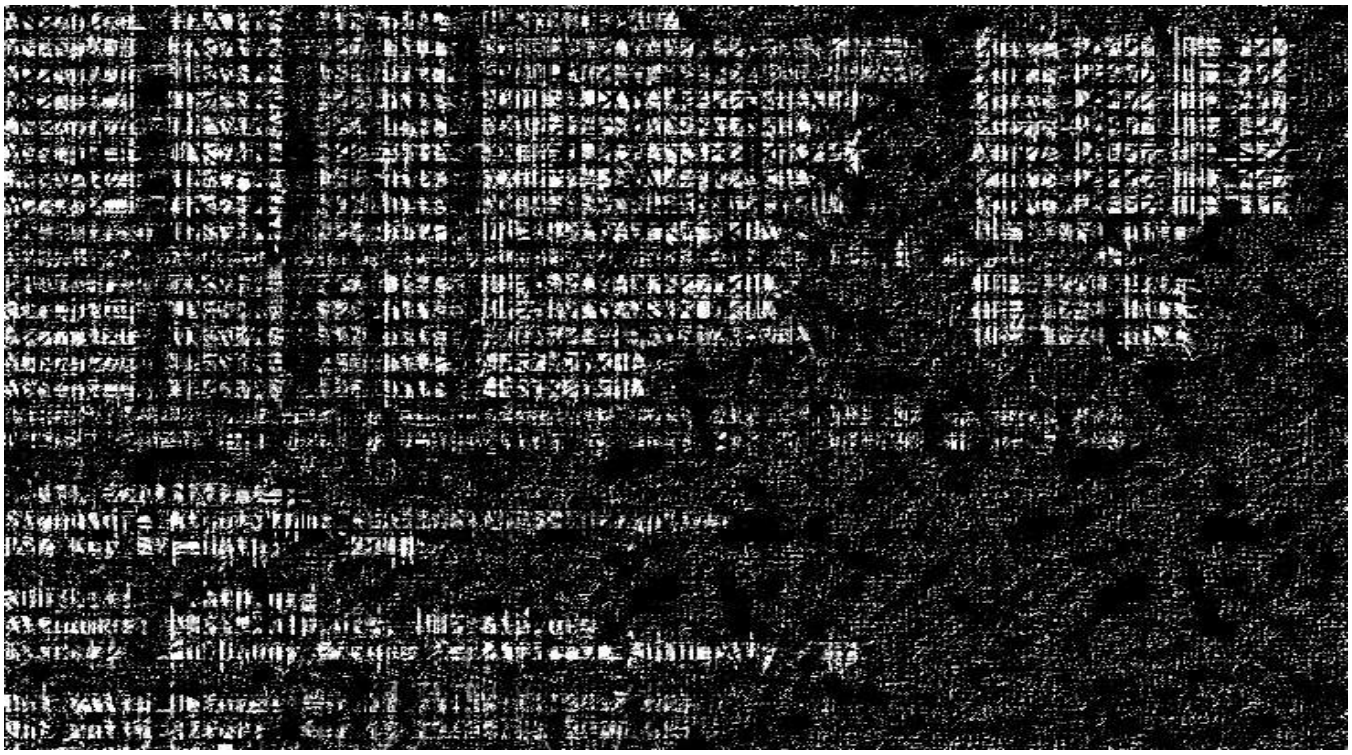
DIRB

Screenshot:



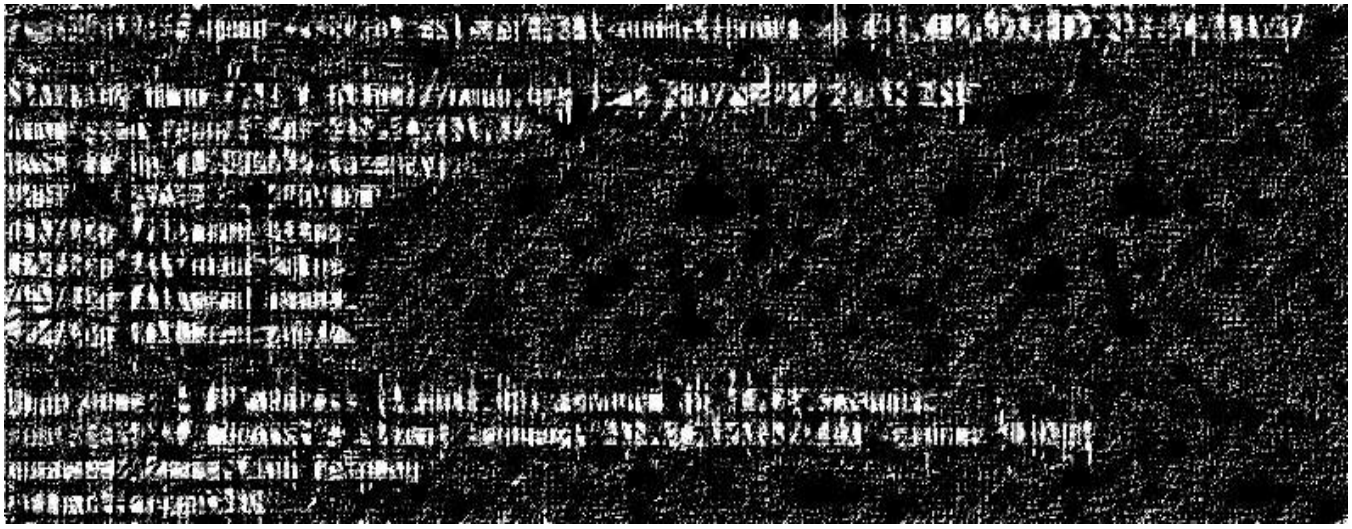
SSL Scan

Screenshot:



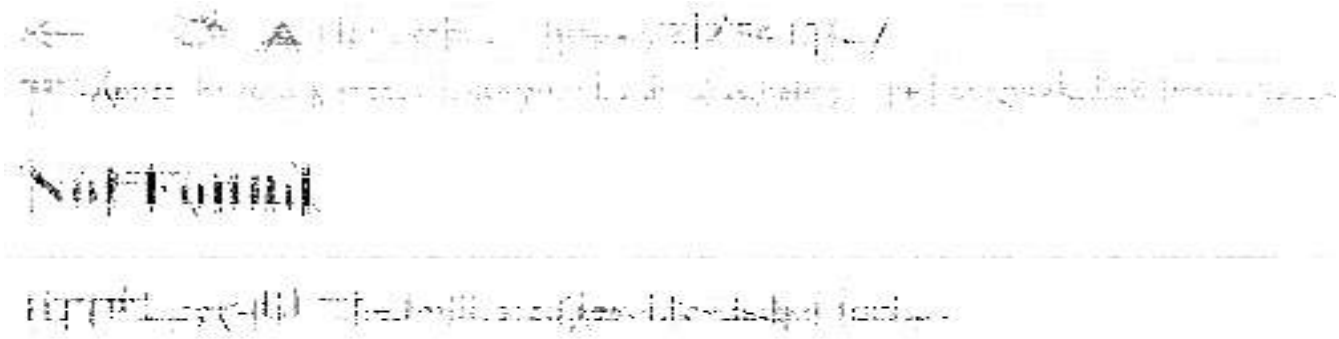
Tested for Weak Ciphers

Screenshot:



Web Page not Found

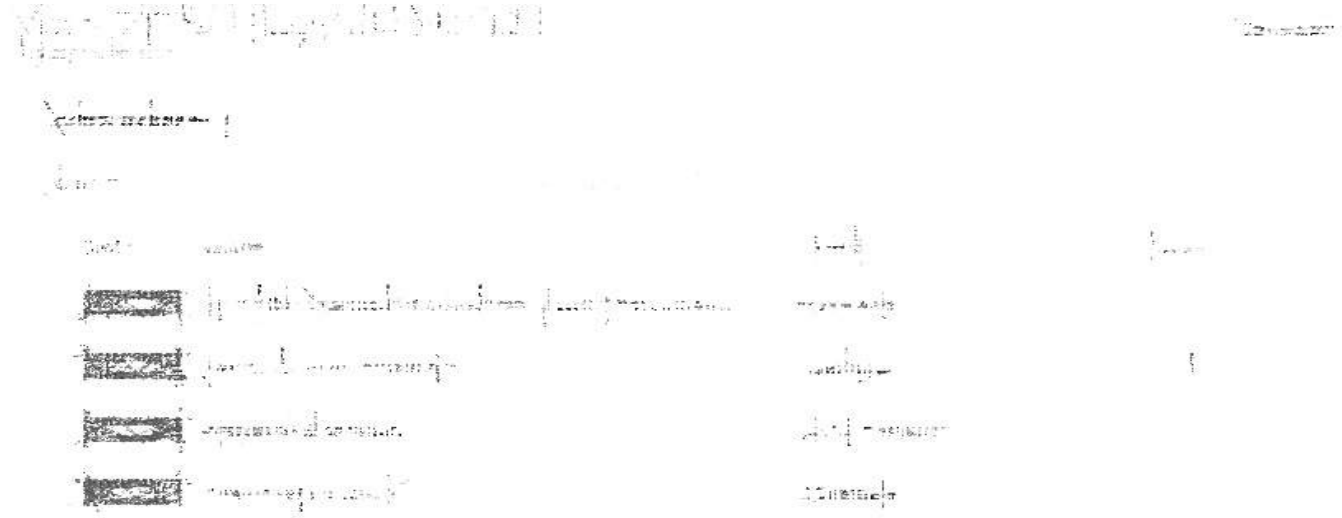
Screenshot:



4.18 911.54.151.39

Nessus

Screenshot:

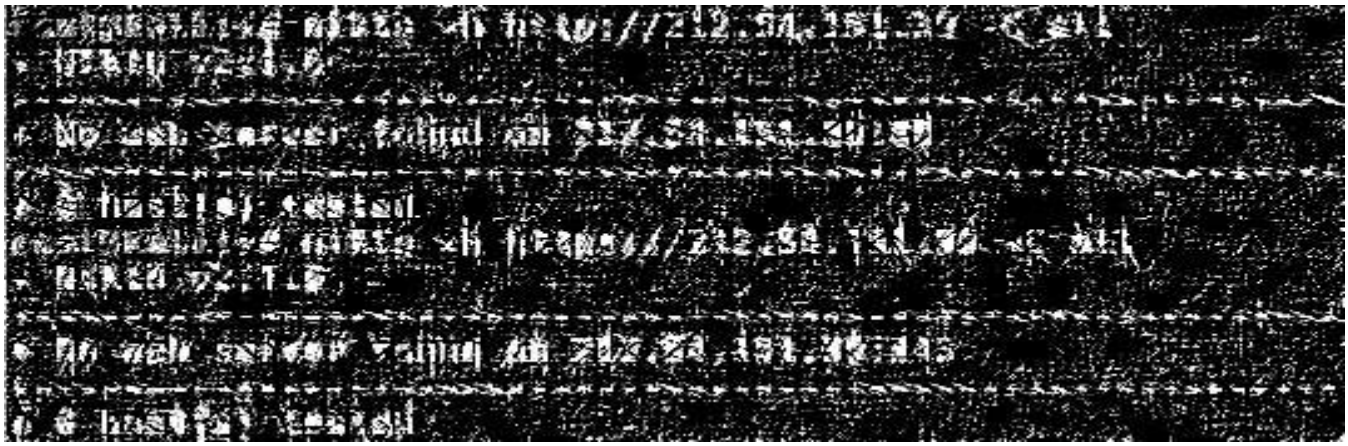


Nmap

Screenshot:

NIKTO

Screenshot:



SSL Scan

Screenshot:

Web Page not Found

Screenshot:

4.19 911.54.151.40

Nessus

Screenshot:

[redacted]

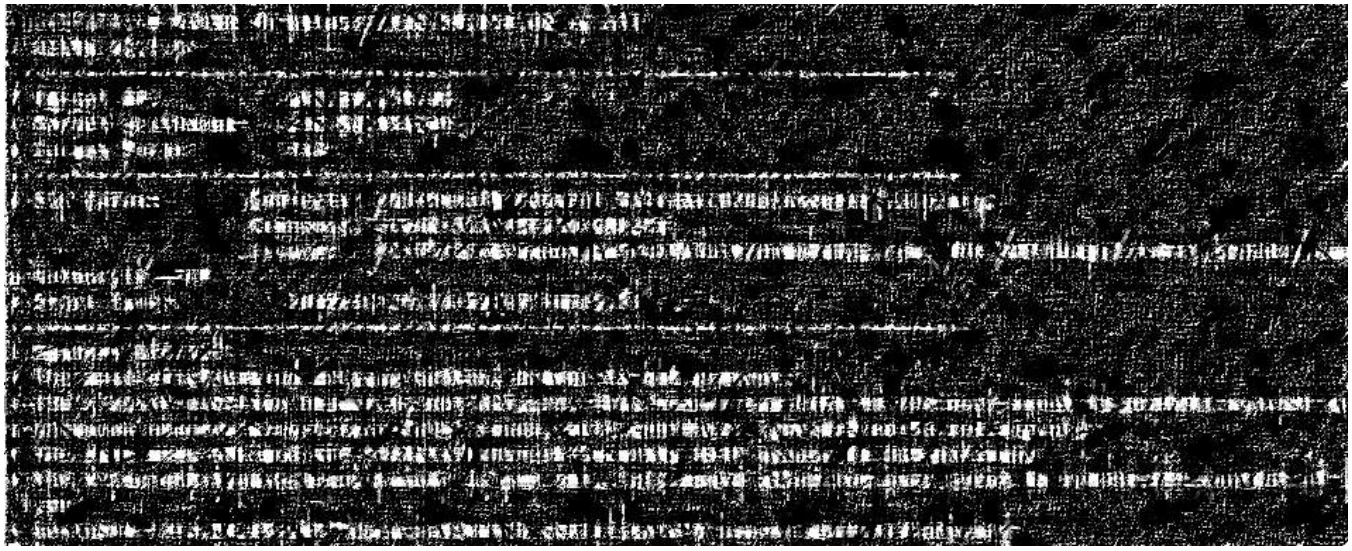
INFO	Service Detection	Service detection	1	
INFO	SSL / TLS Versions Supported	General	1	
INFO	SSL Certificate Information	General	1	
INFO	TCP/IP Timestamps Supported	General	1	
INFO	Traceroute Information	General	1	

Nmap

Screenshot:

NIKTO

Screenshot:

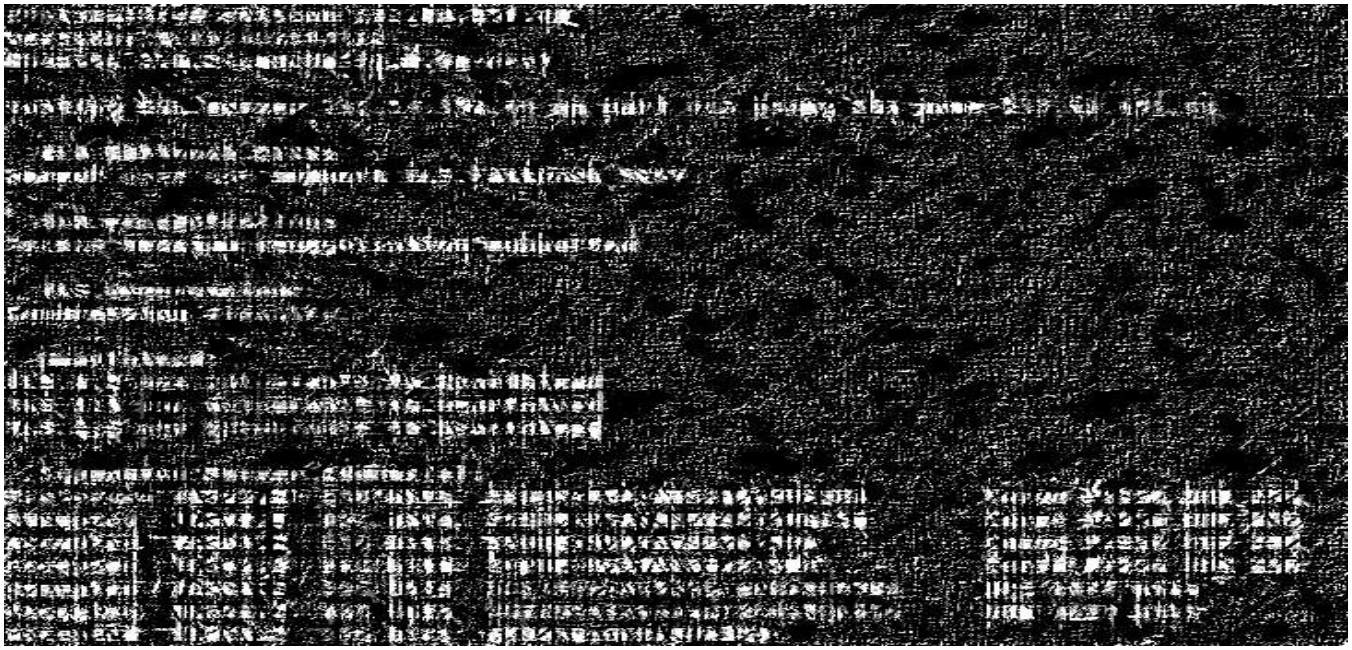


Telnet

Screenshot:

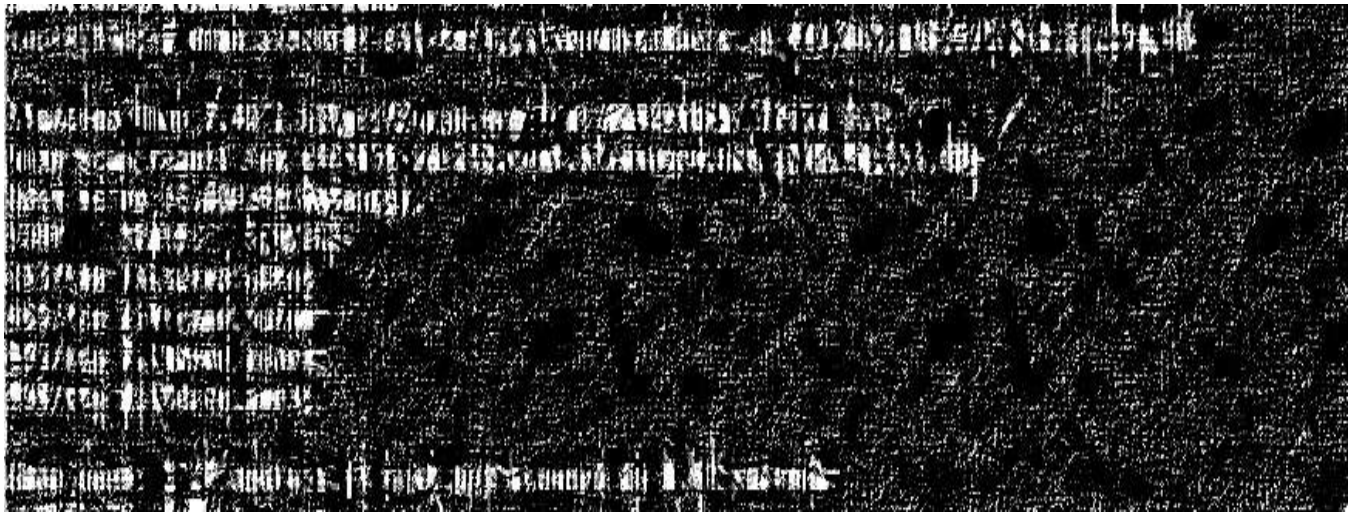
SSL Scan

Screenshot:



Tested for Weak Ciphers

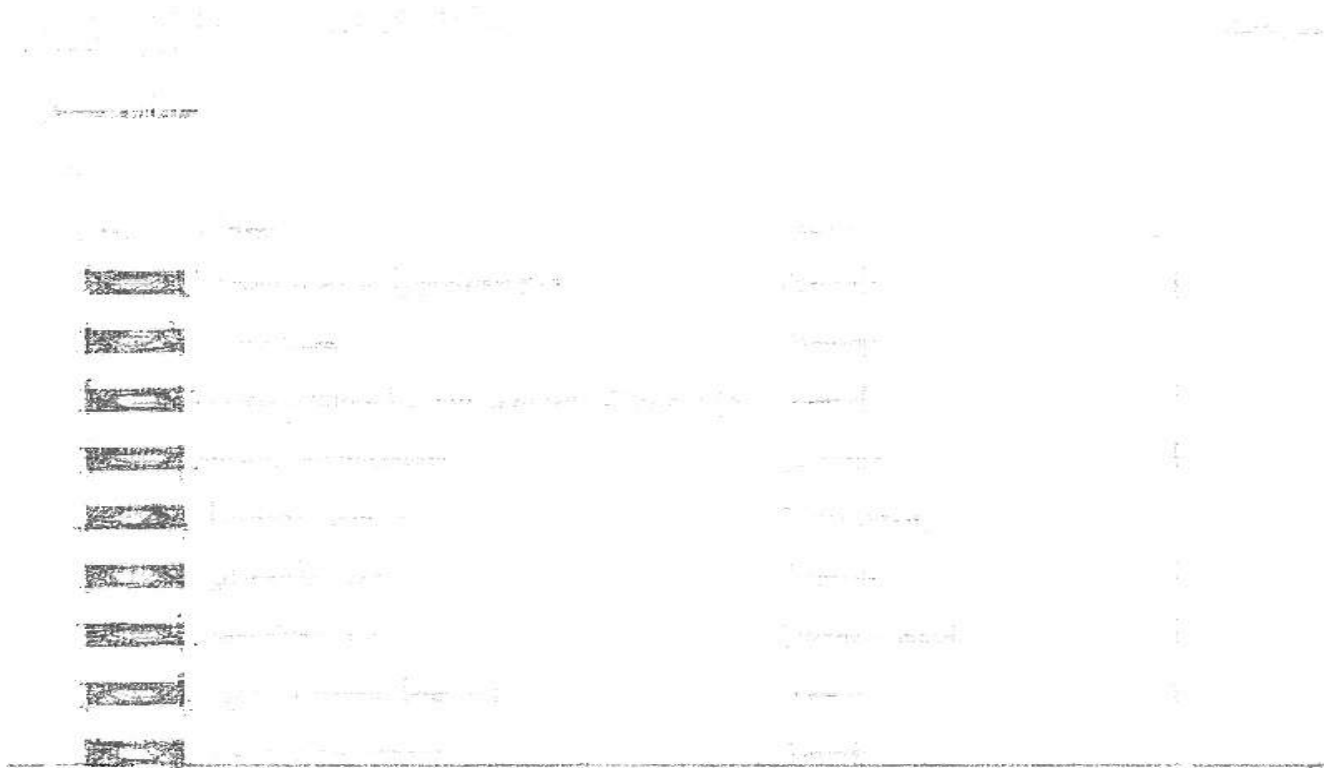
Screenshot:



4.20 911.54.151.41

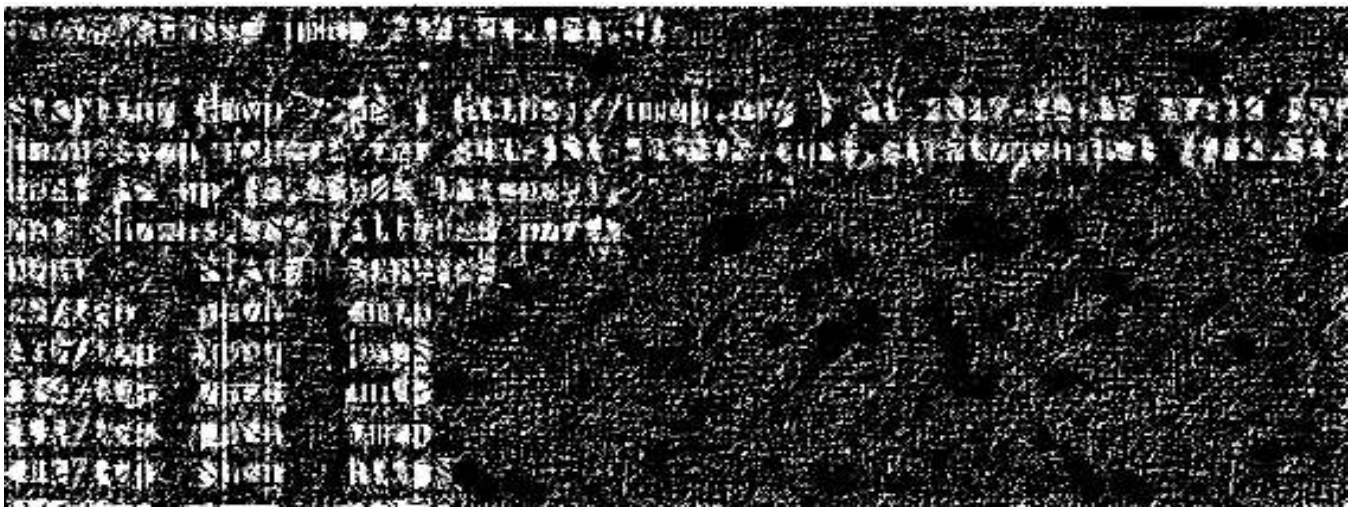
Nessus

Screenshot:



Nmap

Screenshot:



NIKTO

Screenshot:

Telnet

Screenshot:

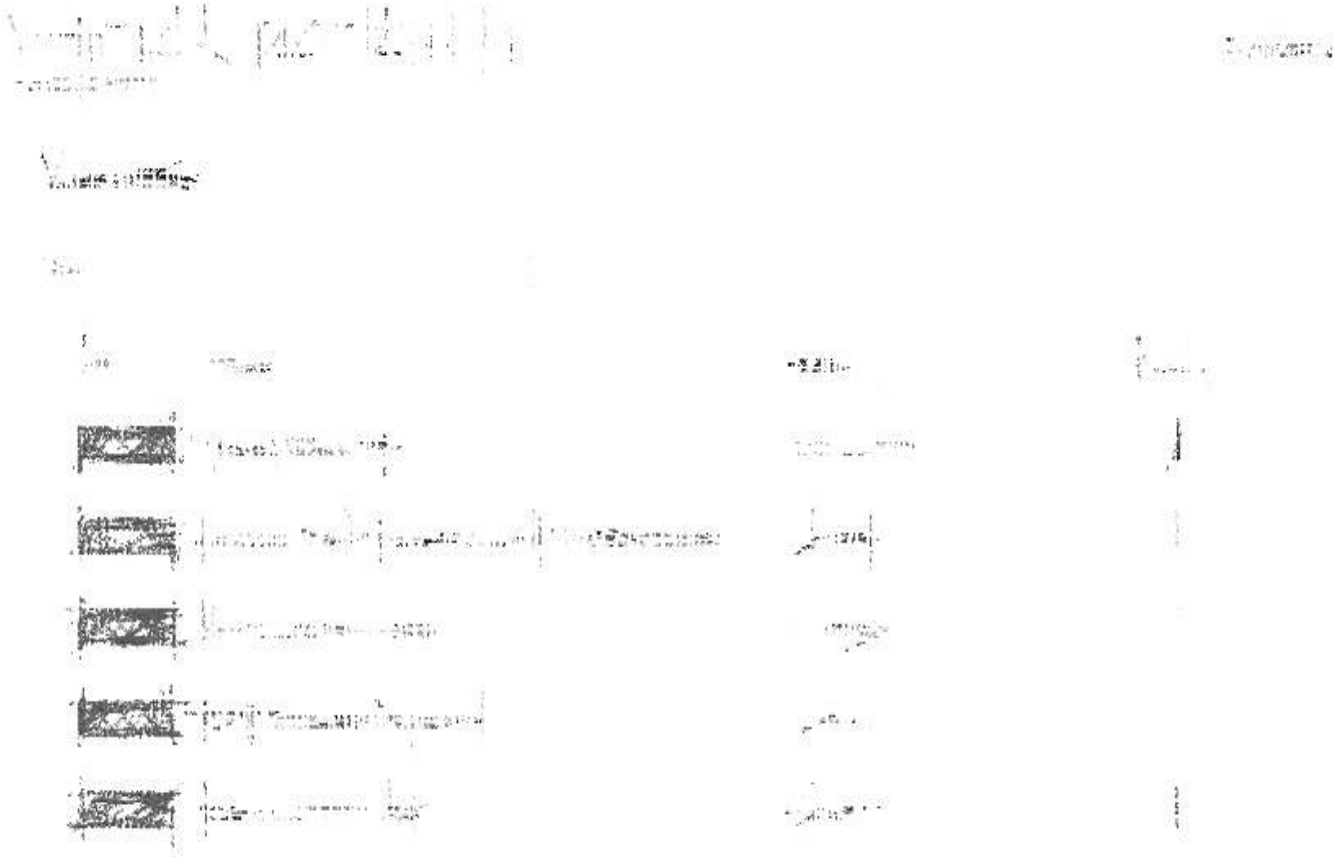
SSL Scan

Screenshot:

4.21 911.54.151.42

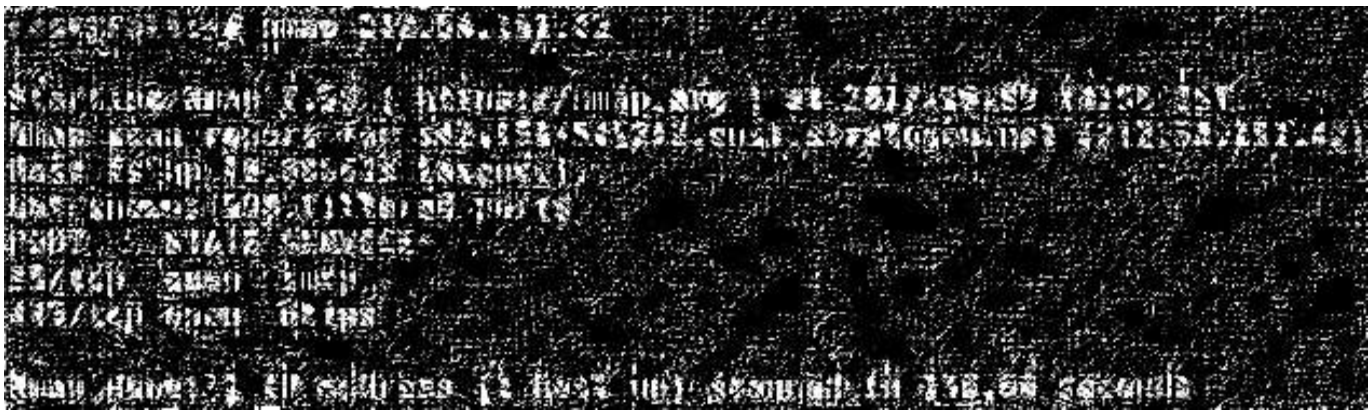
Nessus

Screenshot:



Nmap

Screenshot:

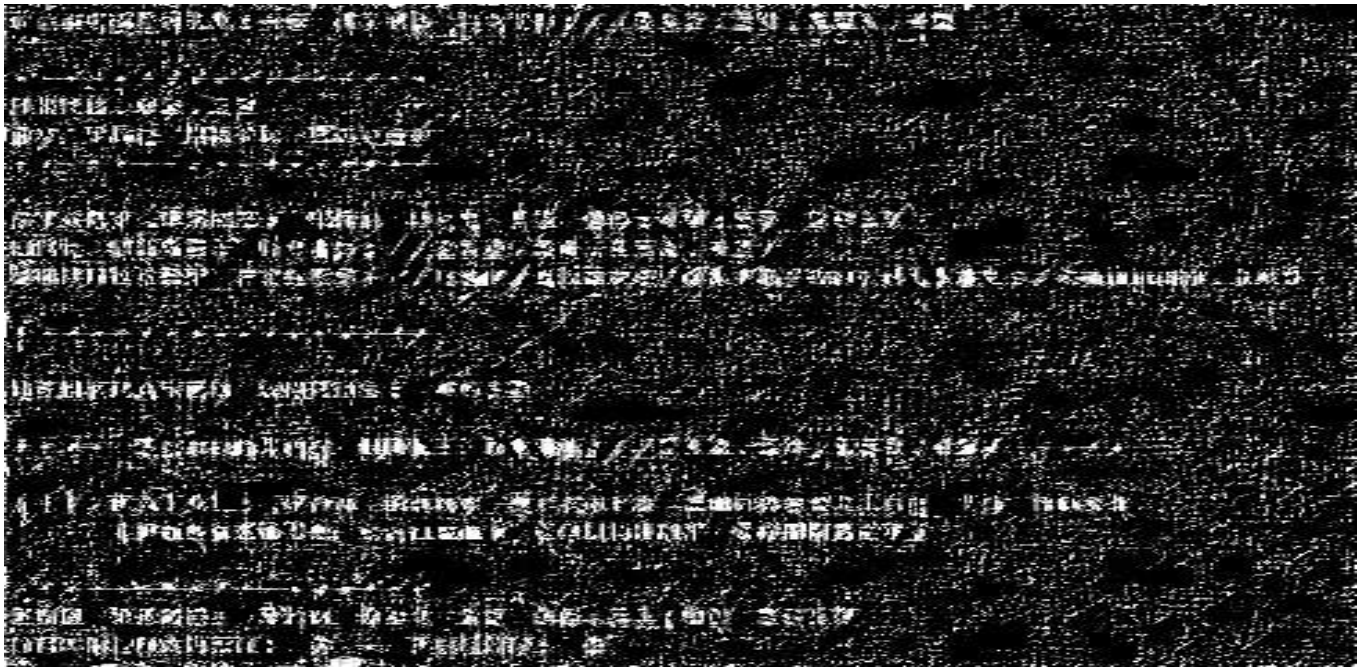


NIKTO

Screenshot:

DIRB

Screenshot:

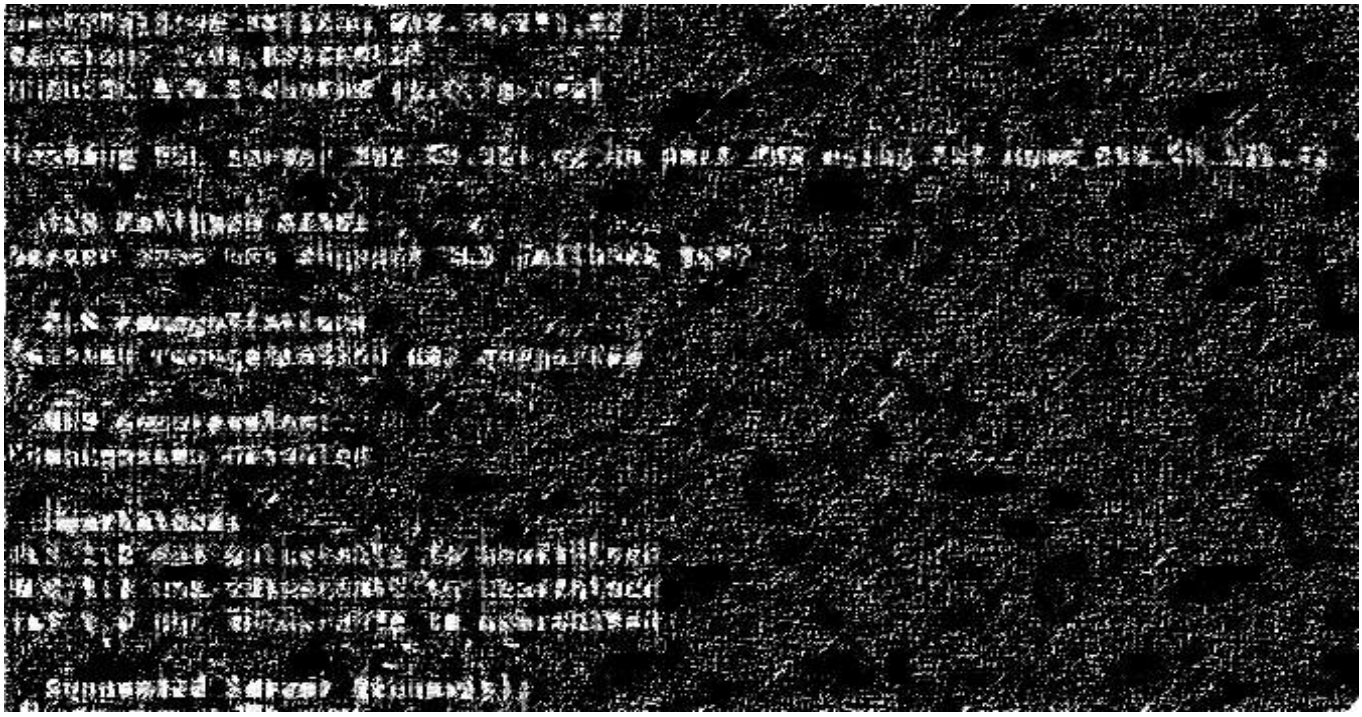


Telnet

Screenshot:

SSL Scan

Screenshot:



Zen Map

Screenshot:

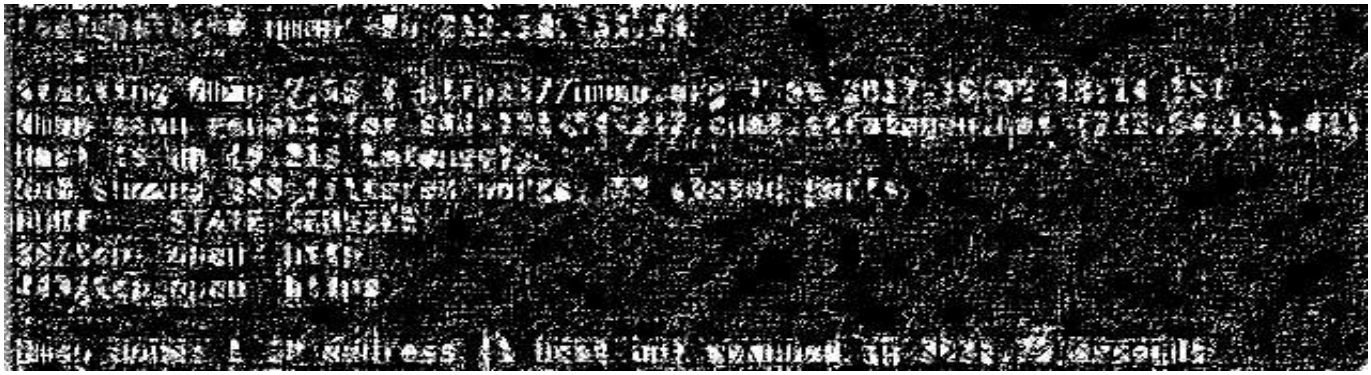
4.22 911.54.151.44

Nessus

Screenshot:

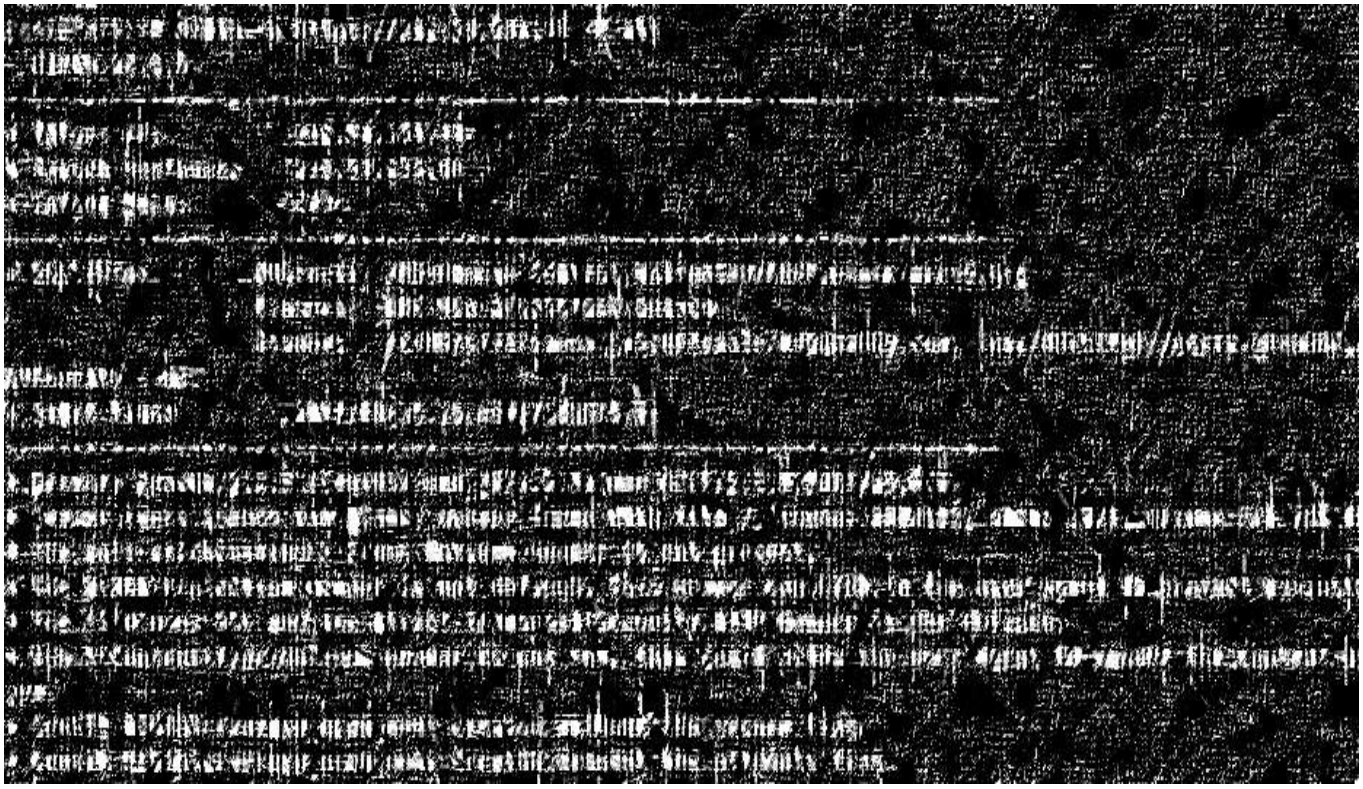
Nmap

Screenshot:



NIKTO

Screenshot:



Telnet

Screenshot:

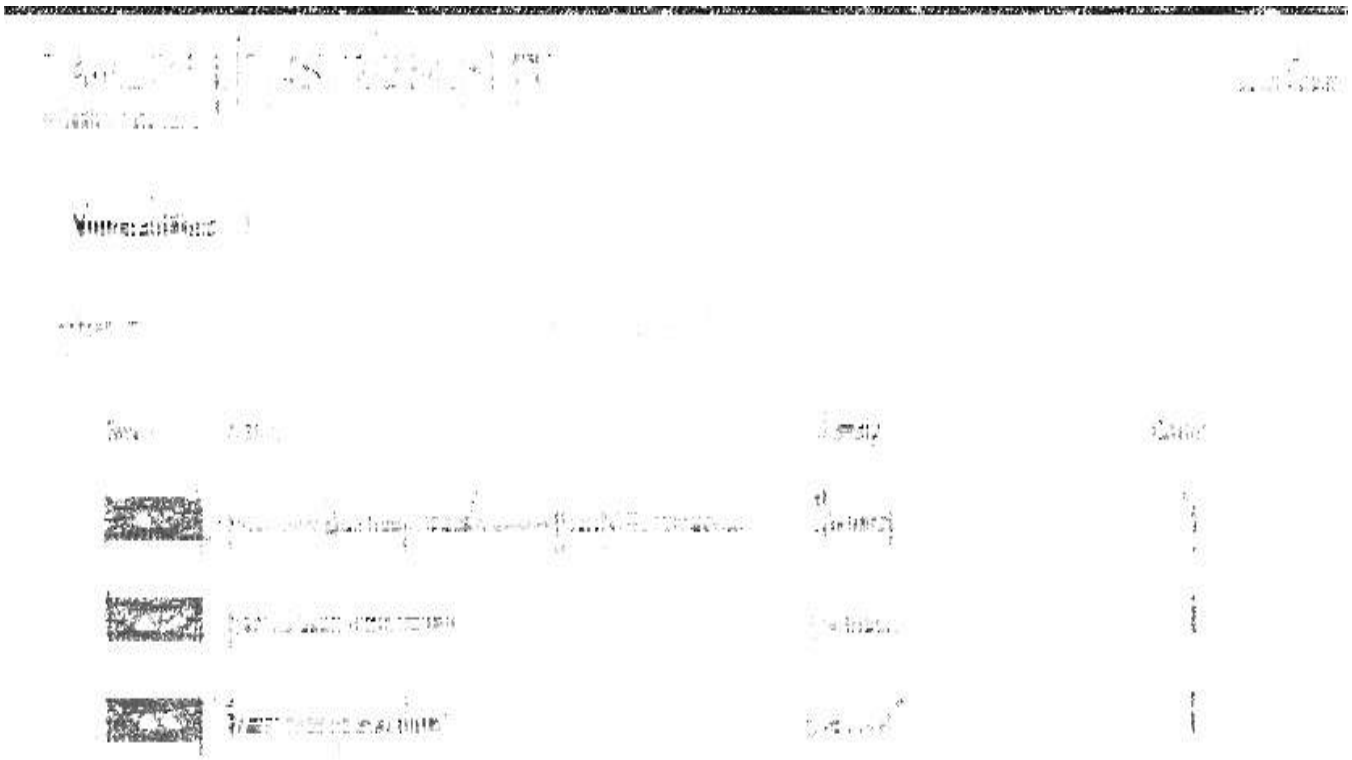
SSL Scan

Screenshot:

4.23 911.54.151.45

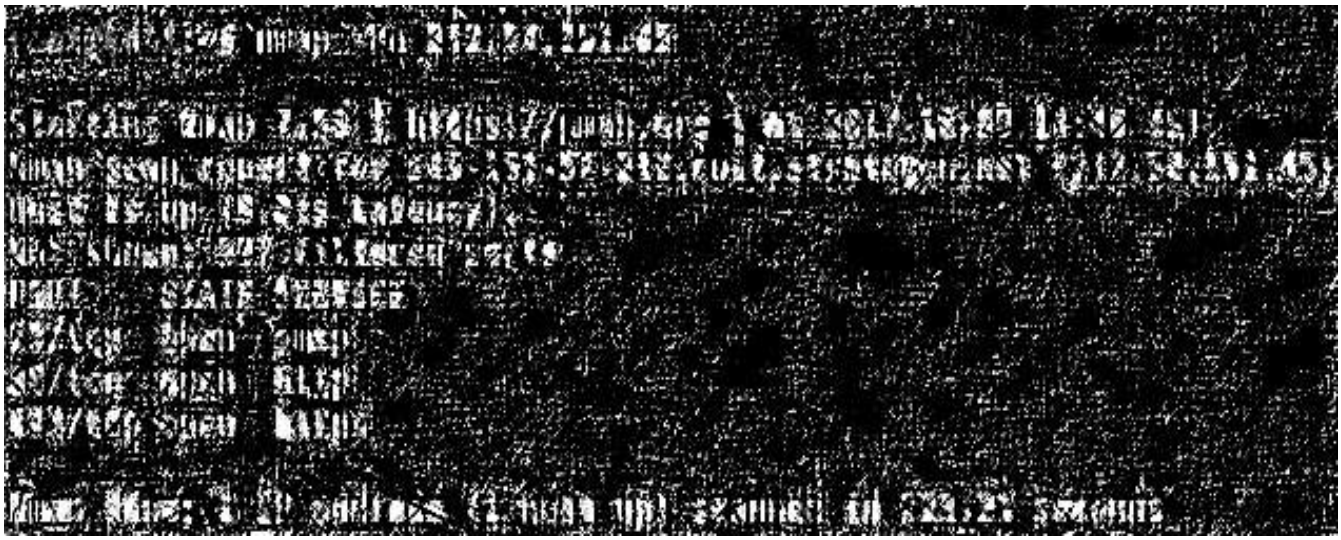
Nessus

Screenshot:



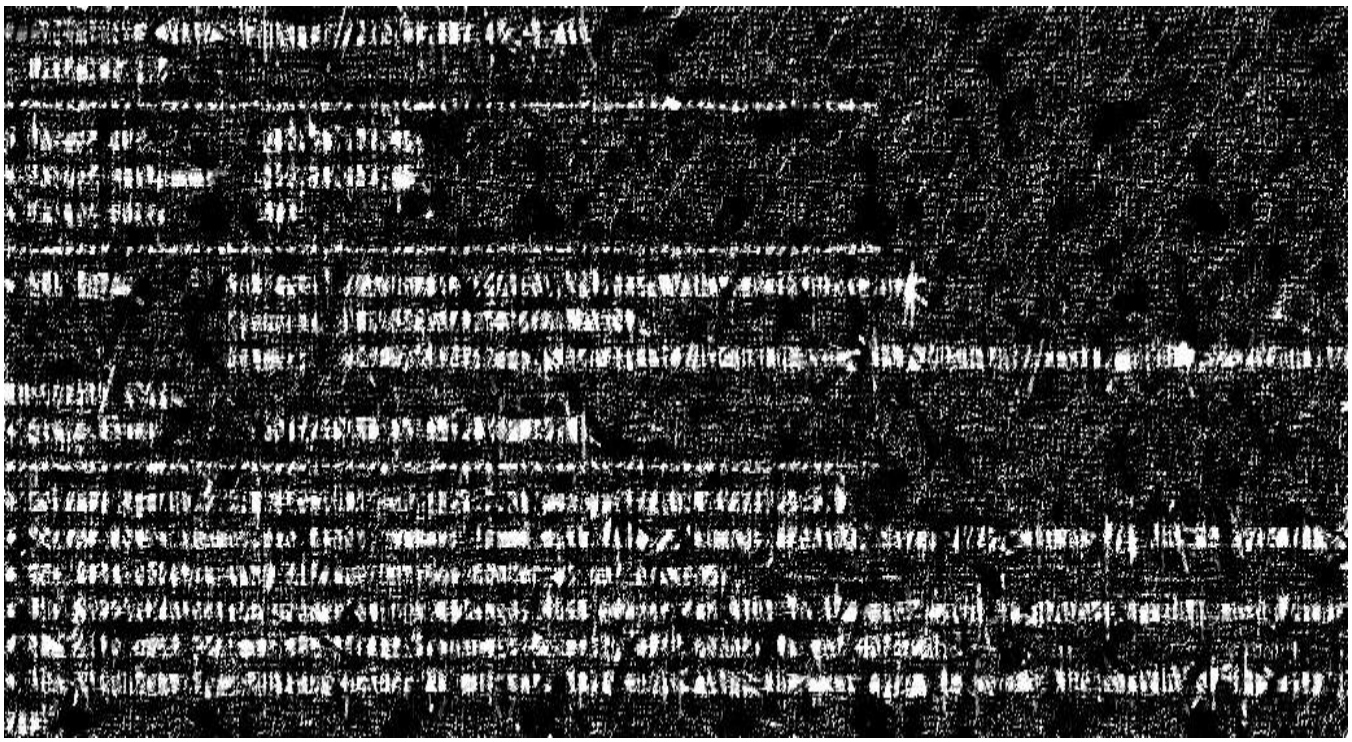
Nmap

Screenshot:



NIKTO

Screenshot:

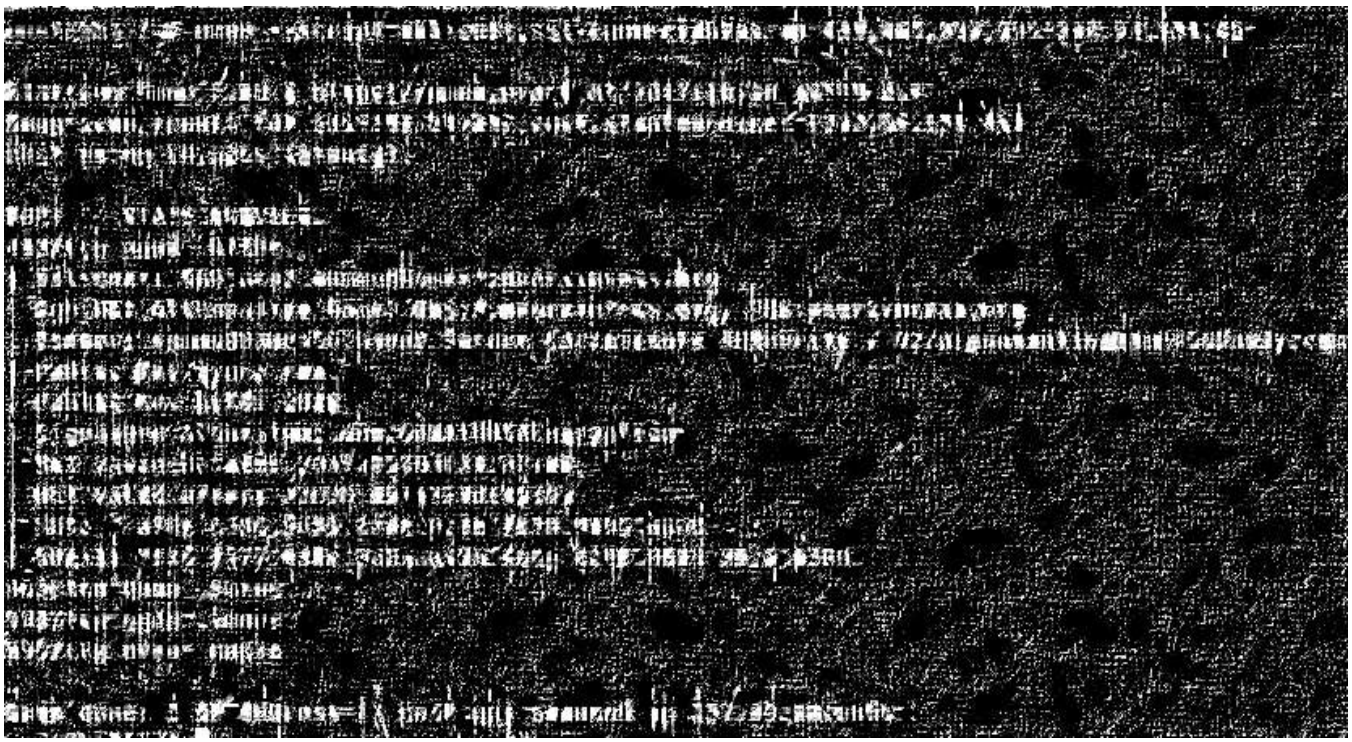


Telnet

Screenshot:

Tested for Weak Ciphers

Screenshot:



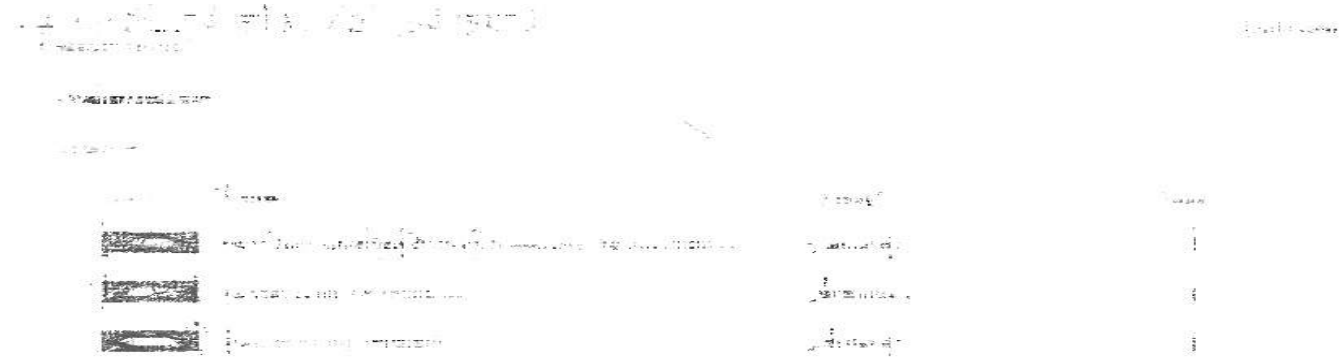
SSL Scan

Screenshot:

4.24 911.54.151.53

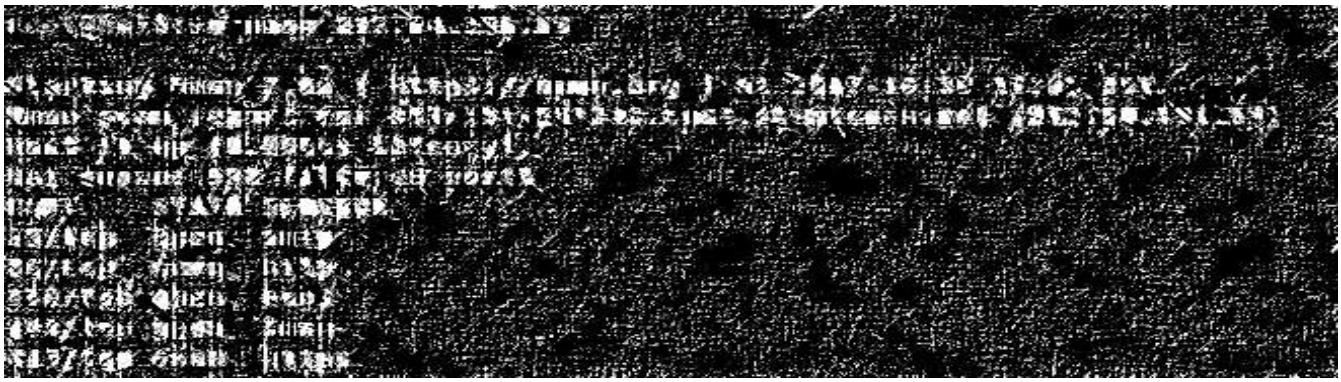
Nessus

Screenshot:



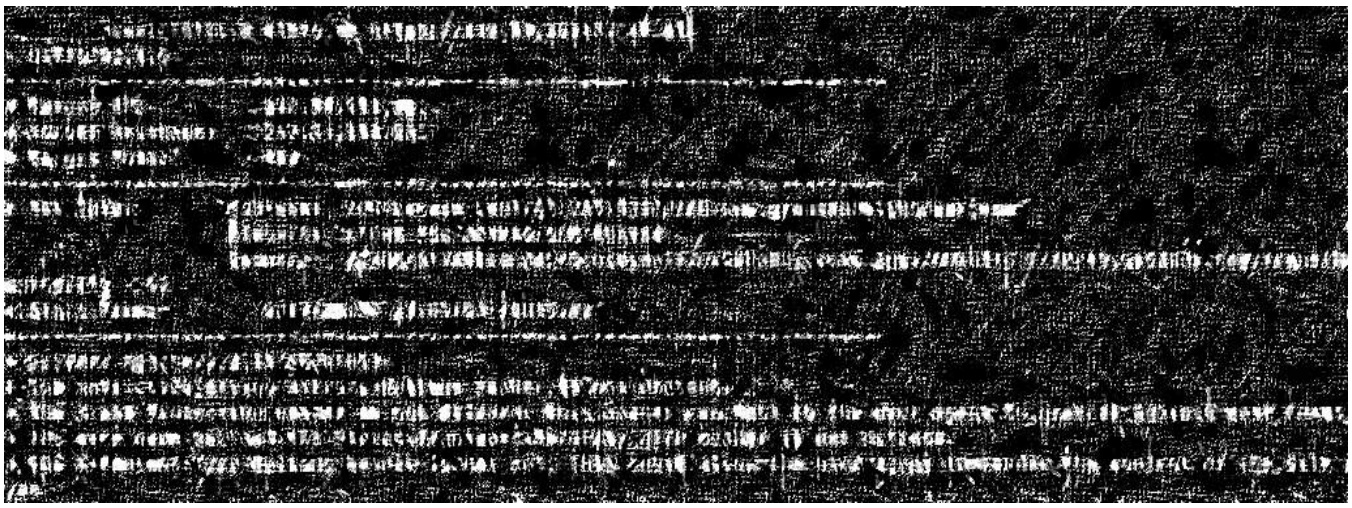
Nmap

Screenshot:



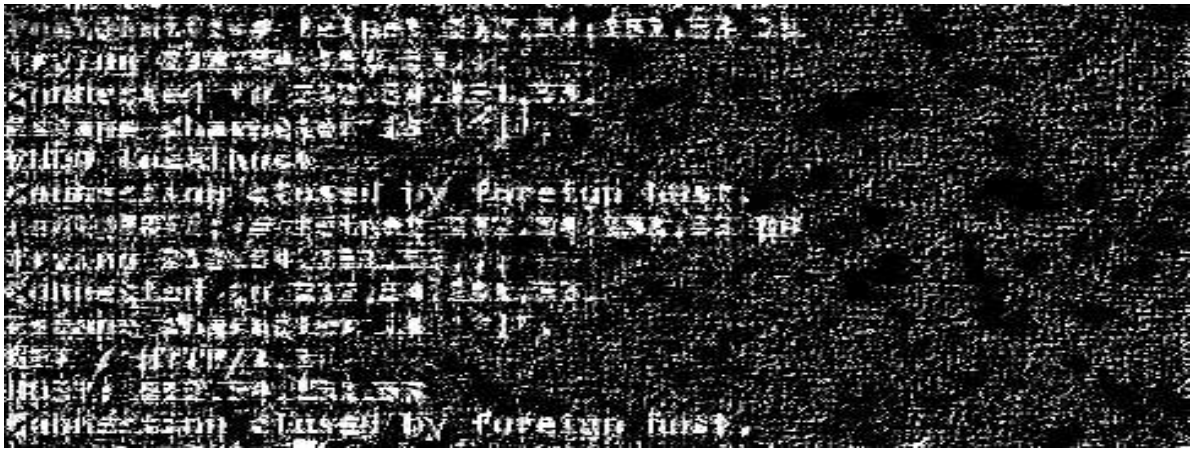
NIKTO

Screenshot:



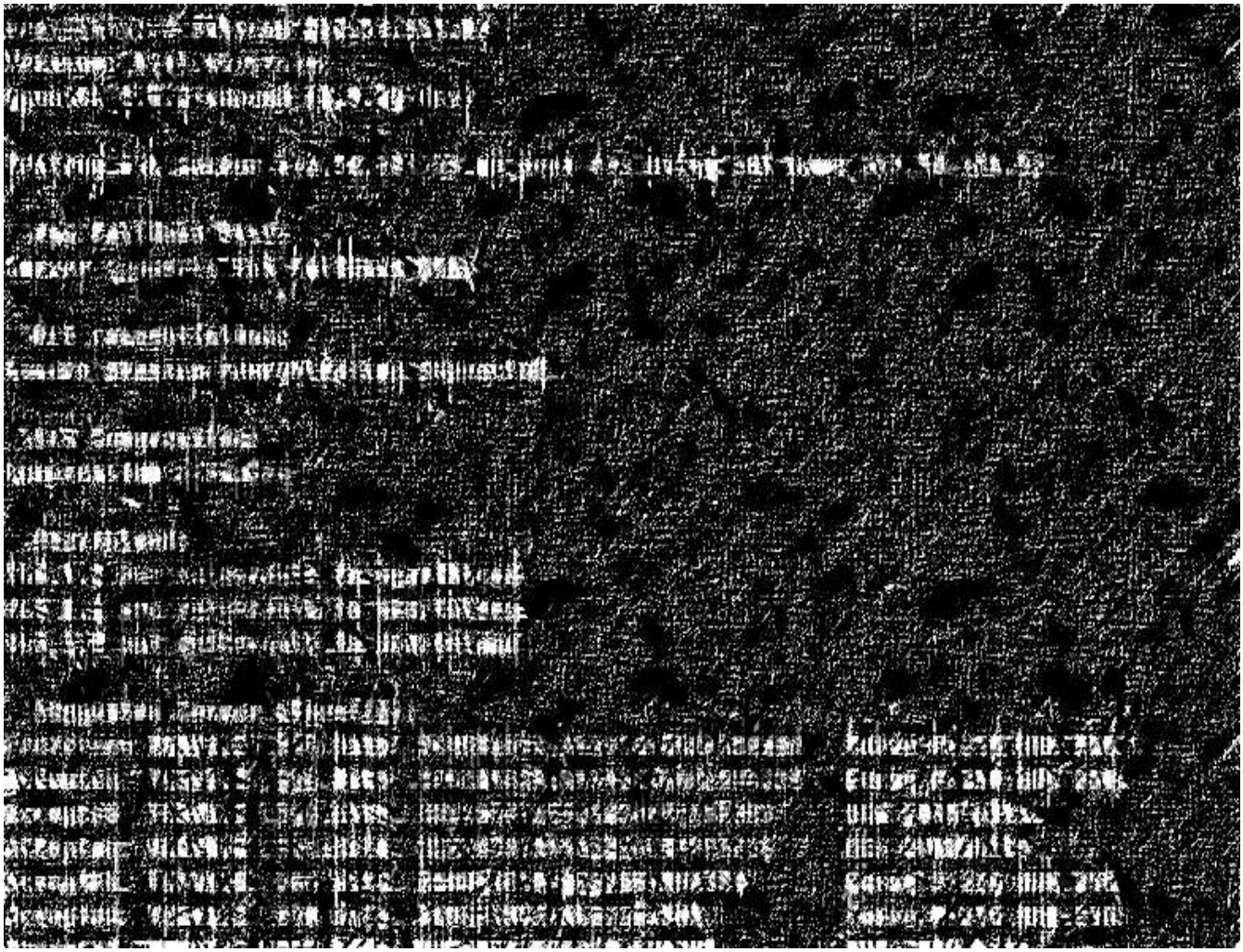
Telnet

Screenshot:



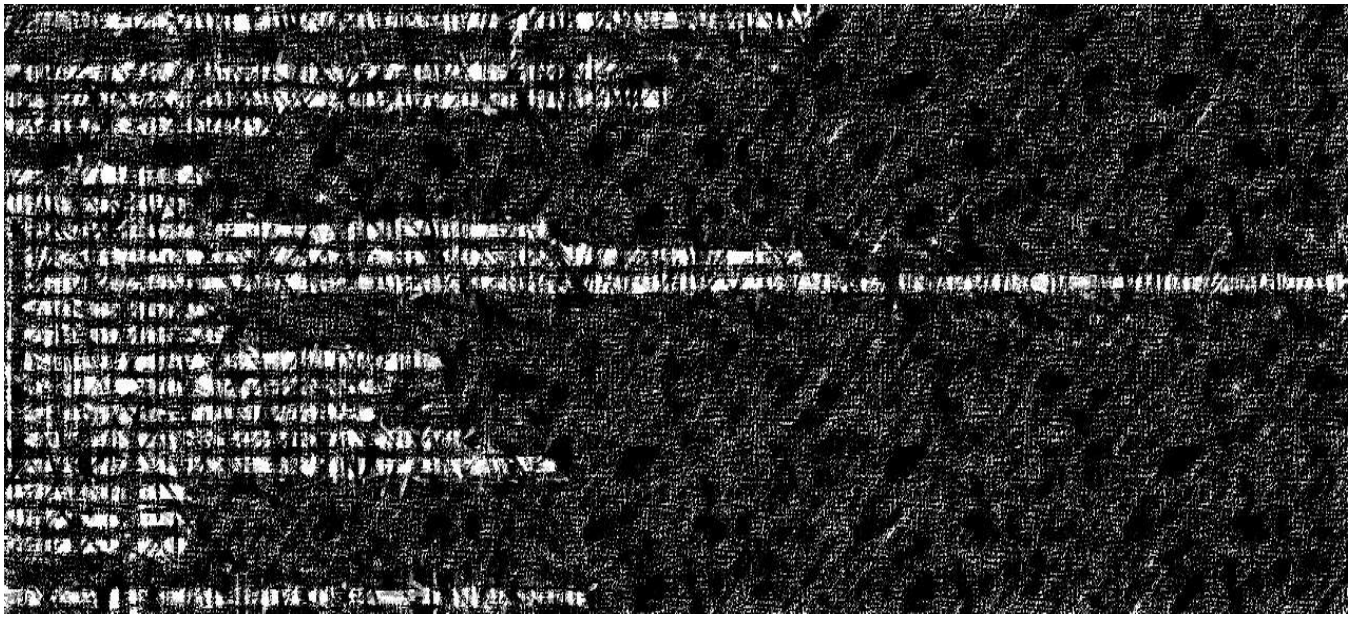
SSL Scan

Screenshot:



Tested for Weak Ciphers

Screenshot:



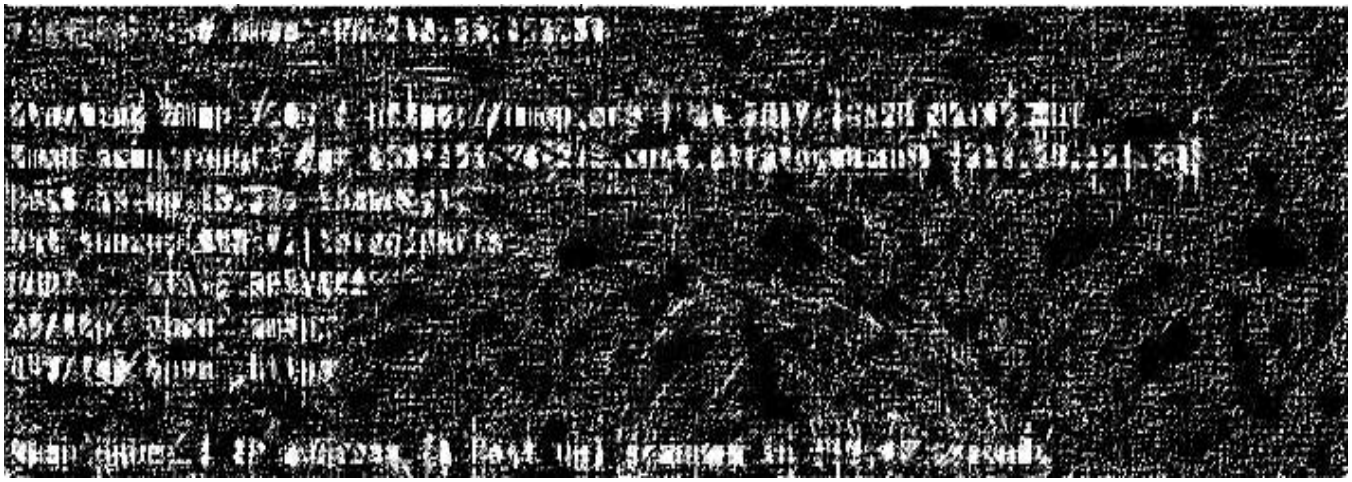
4.25 911.54.151.54

Nessus

Screenshot:

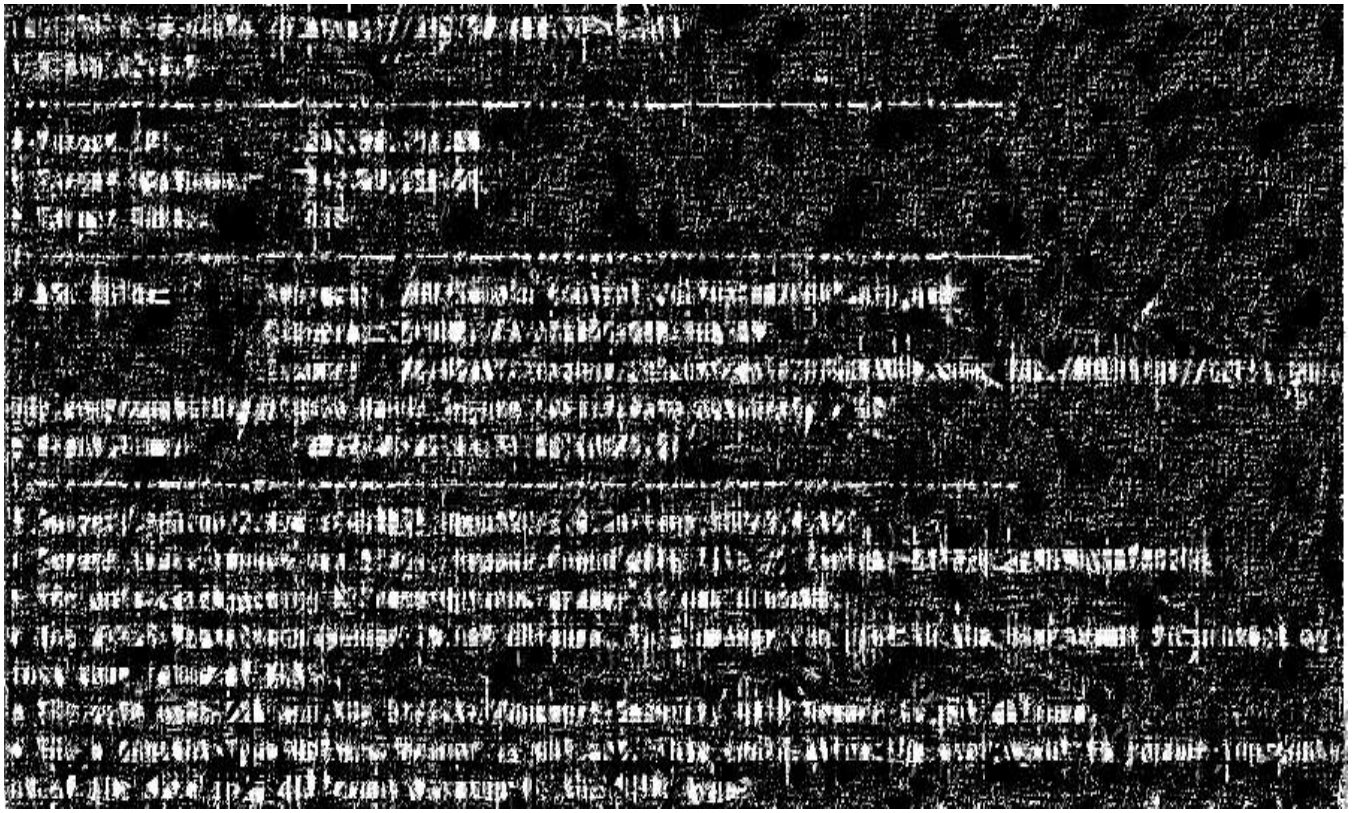
Nmap

Screenshot:



NIKTO

Screenshot:



Telnet

Screenshot:

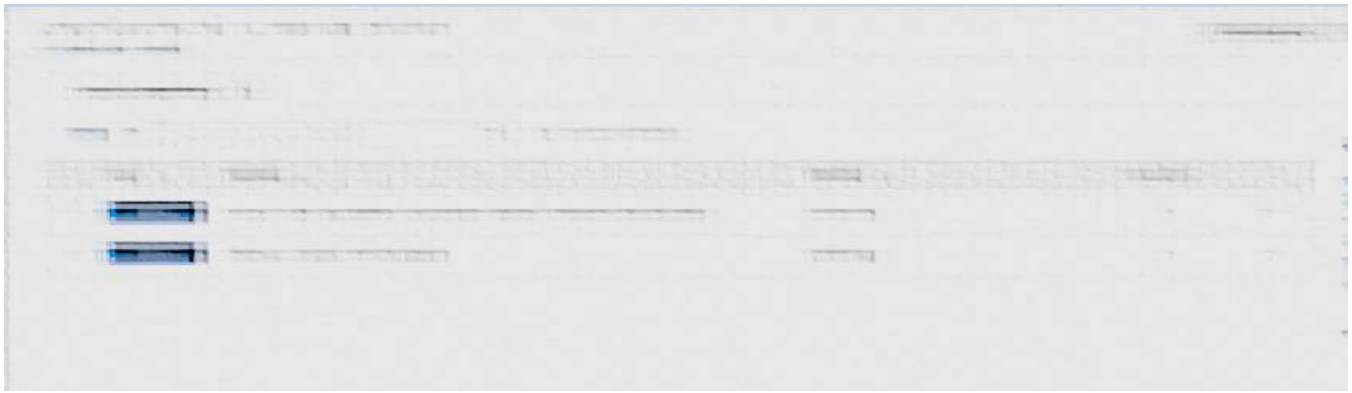
SSL Scan

Screenshot:

4.26 911.54.151.72

Nessus

Screenshot:



Nmap

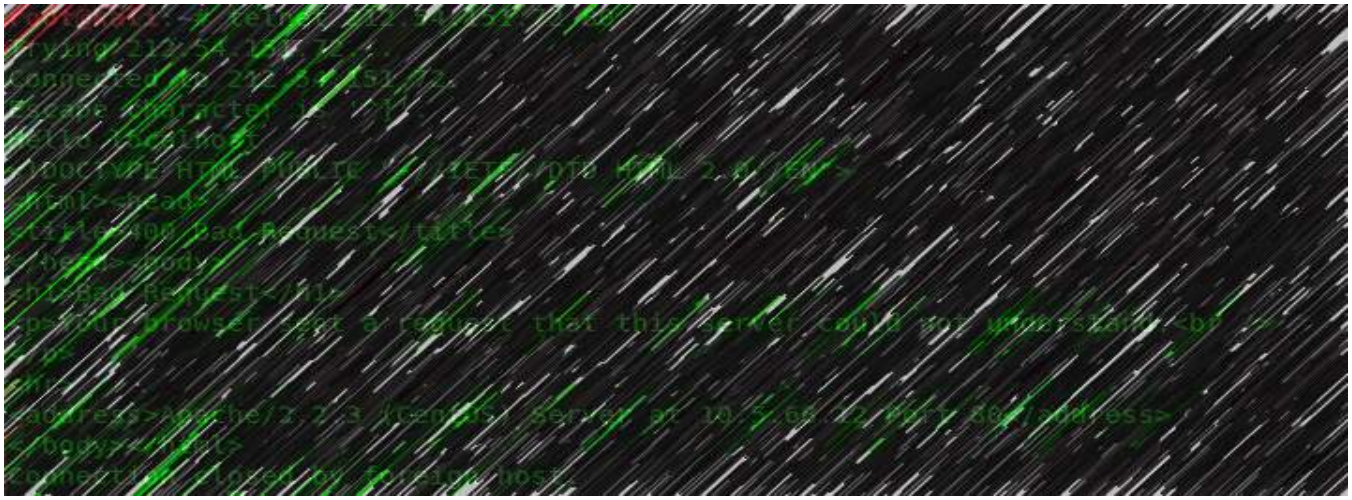
Screenshot:

NIKTO

Screenshot:

Telnet

Screenshot:



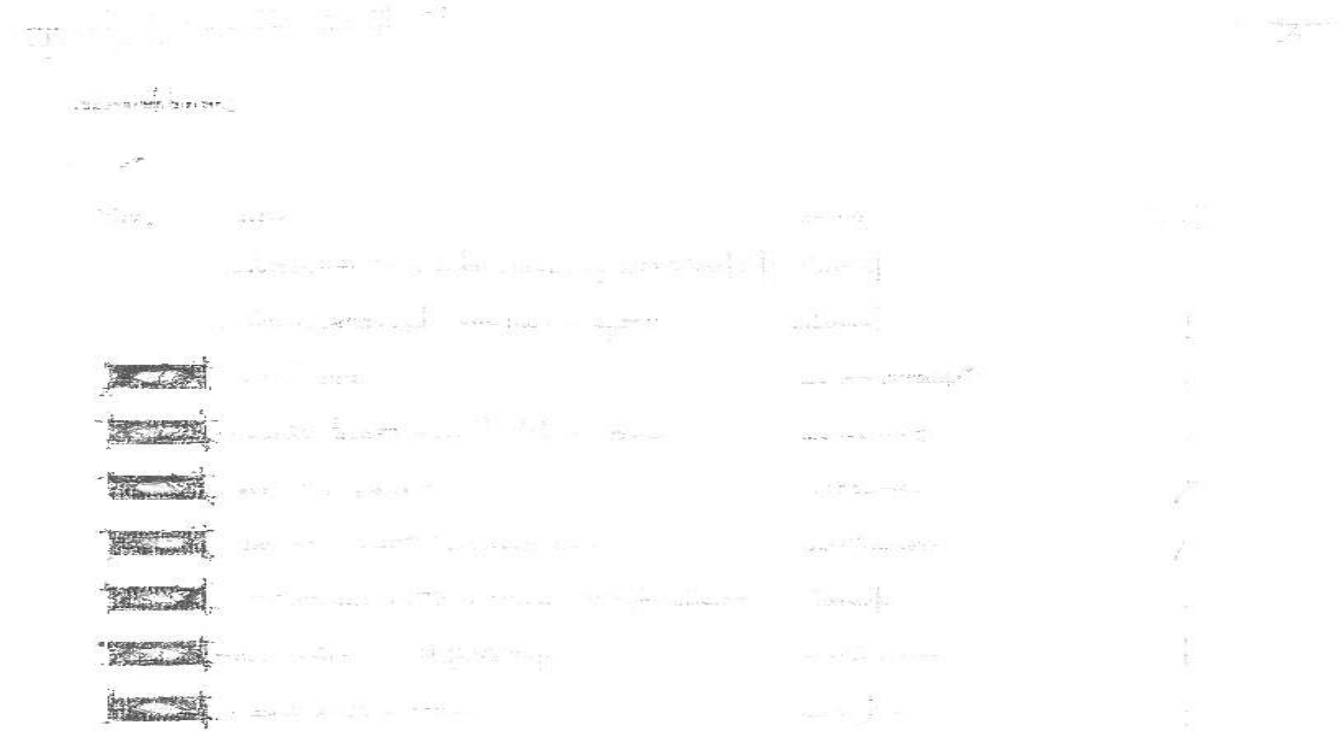
SSL Scan

Screenshot:

4.27 911.54.151.76

Nessus

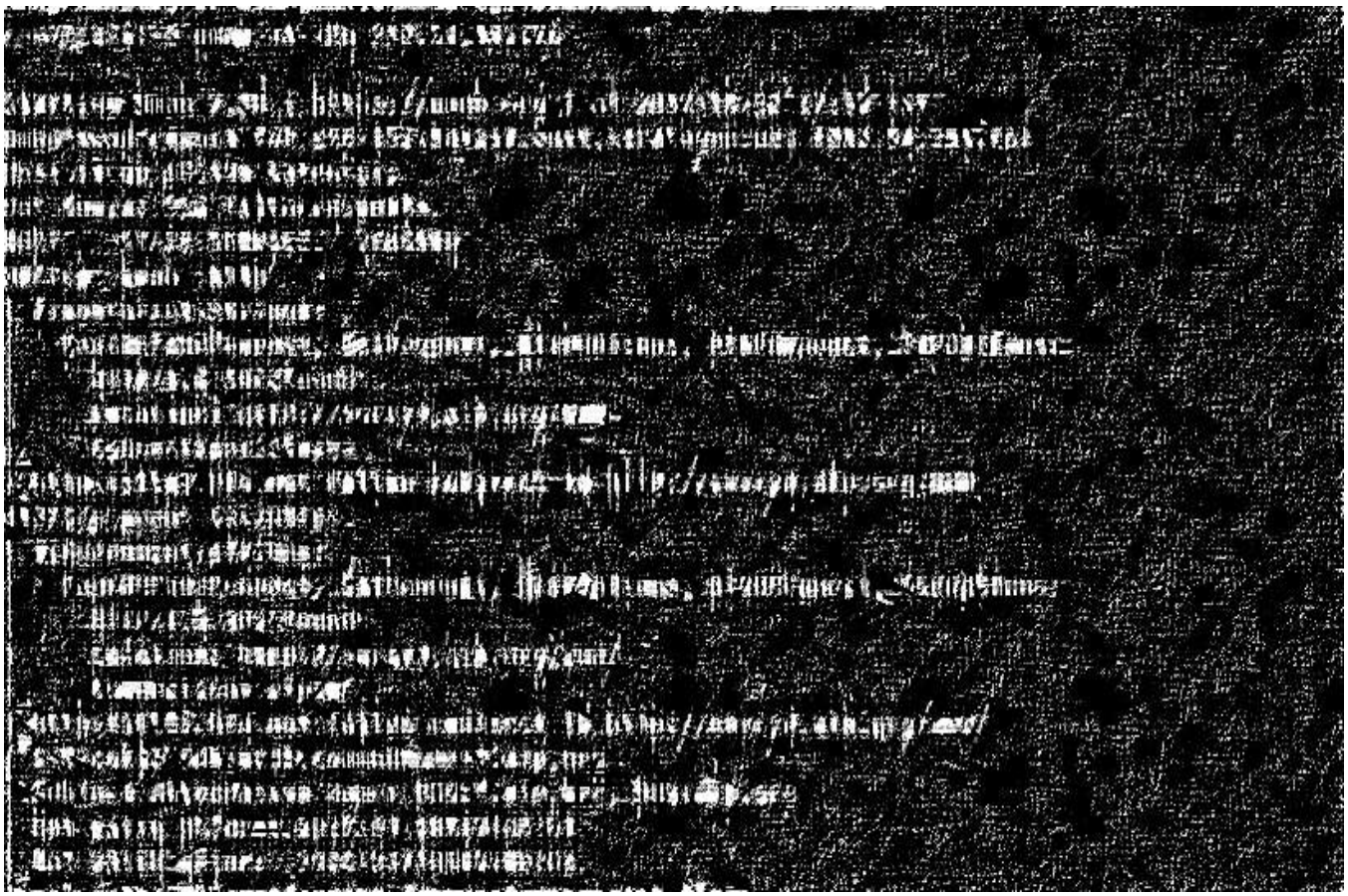
Screenshot:



INFO	SSL / TLS Versions Supported	General	1	
INFO	SSL Certificate 'commonName' Mismatch	General	1	
INFO	SSL Certificate Information	General	1	
INFO	SSL Certificate Signed Using Weak Hashing Algorithm (...	General	1	
INFO	SSL Cipher Block Chaining Cipher Suites Supported	General	1	
INFO	SSL Cipher Suites Supported	General	1	
INFO	SSL Perfect Forward Secrecy Cipher Suites Supported	General	1	
INFO	SSL Root Certification Authority Certificate Information	General	1	
INFO	TCP/IP Timestamps Supported	General	1	
INFO	Traceroute Information	General	1	

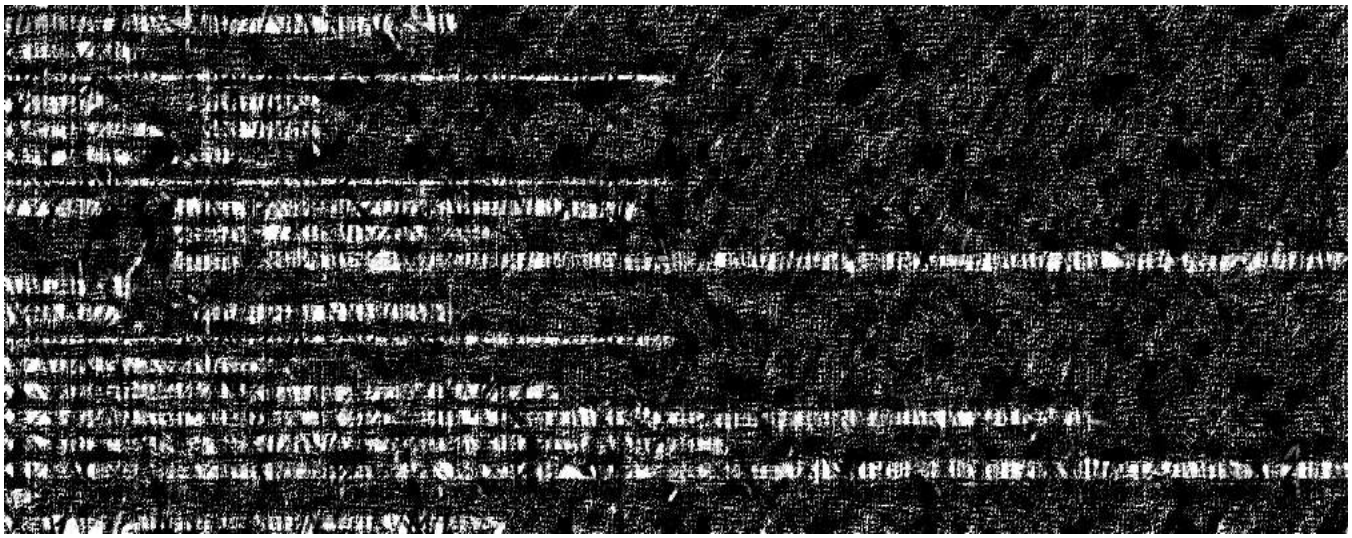
Nmap

Screenshot:



NIKTO

Screenshot:



IIS DoS Attack

Screenshot:

Telnet

Screenshot:

SSL Scan

Screenshot:

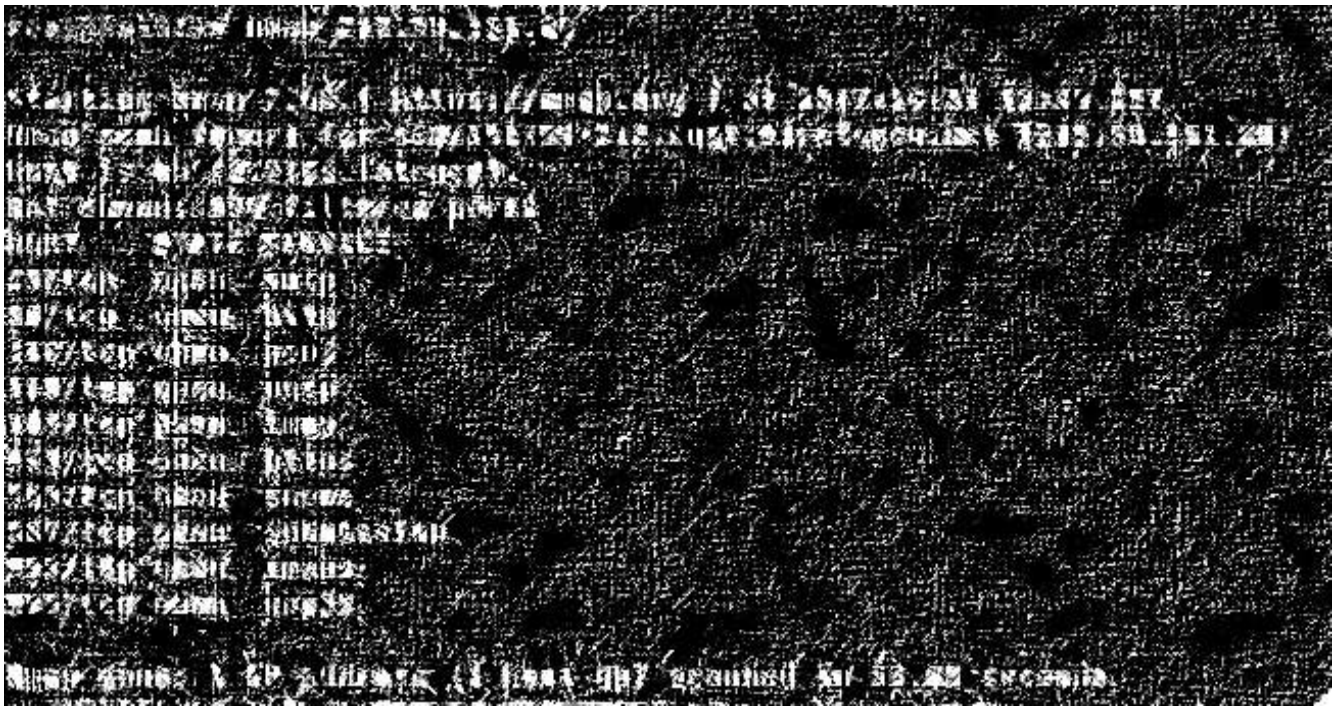
4.28 911.54.151.80

Nessus

Screenshot:

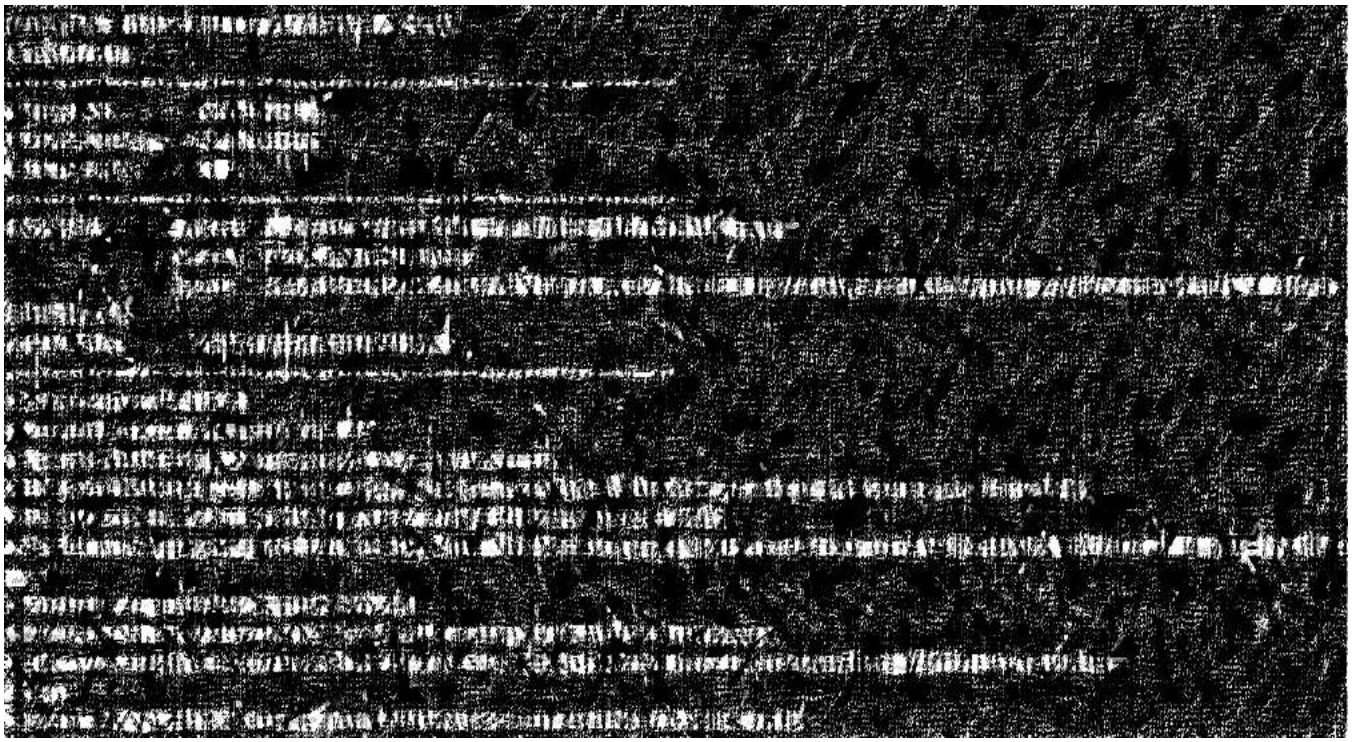
Nmap

Screenshot:



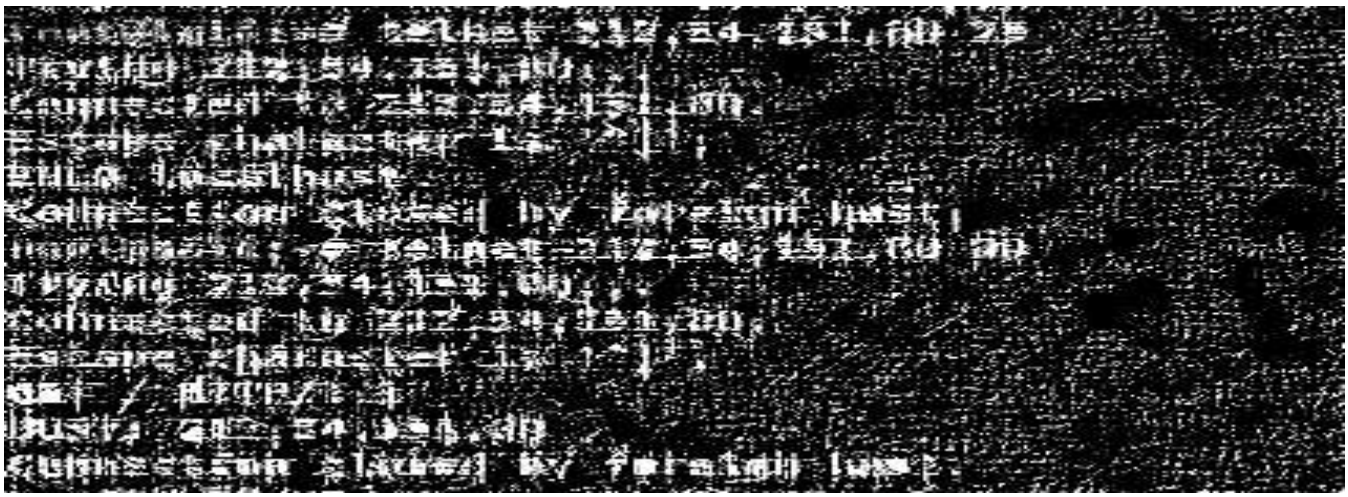
NIKTO

Screenshot:



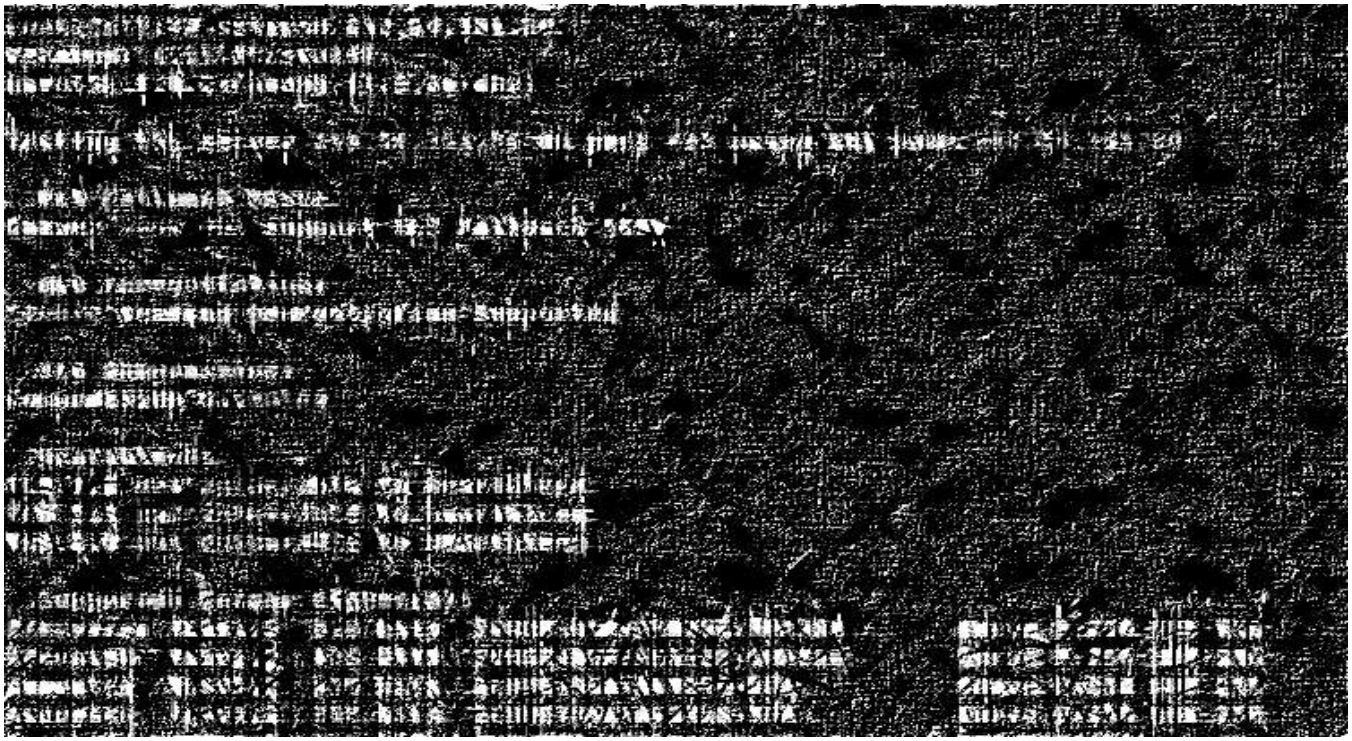
Telnet

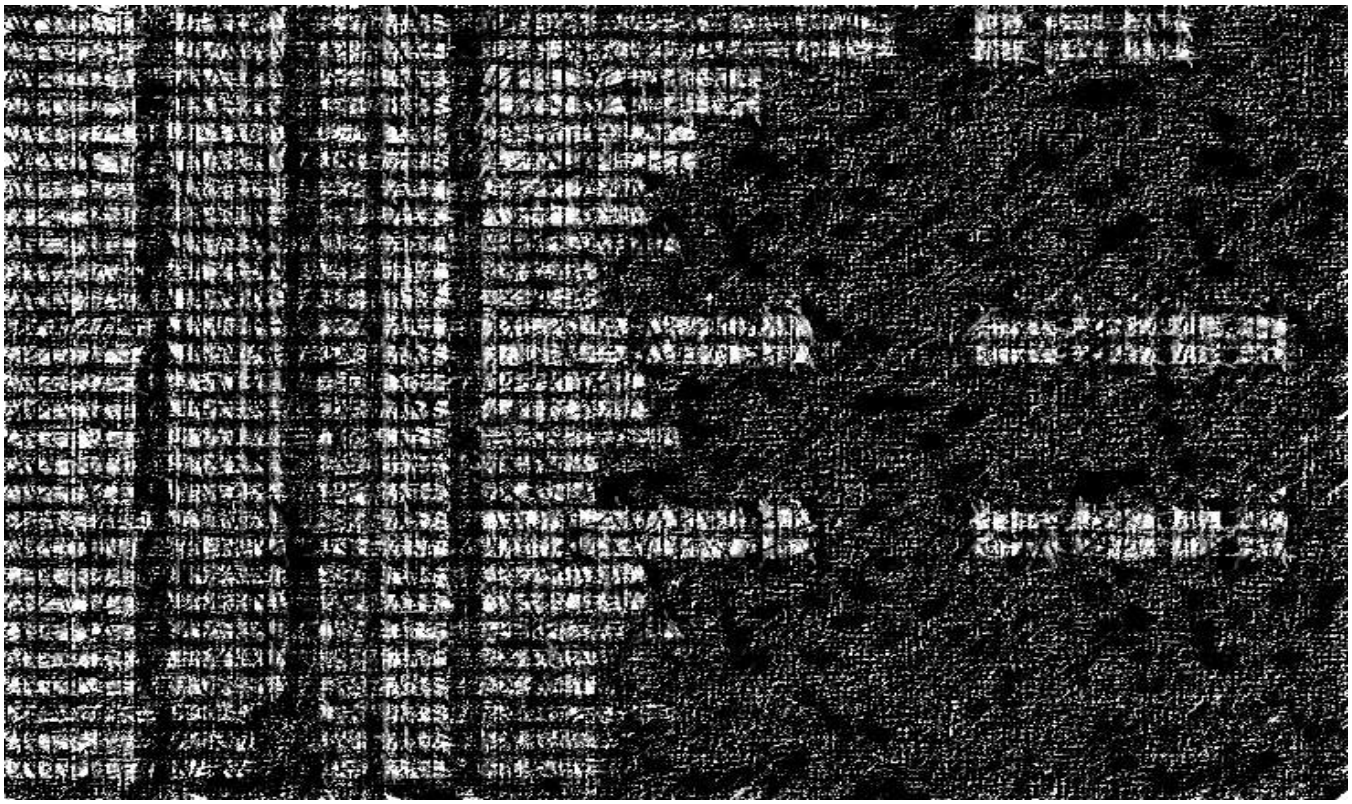
Screenshot:



SSL Scan

Screenshot:

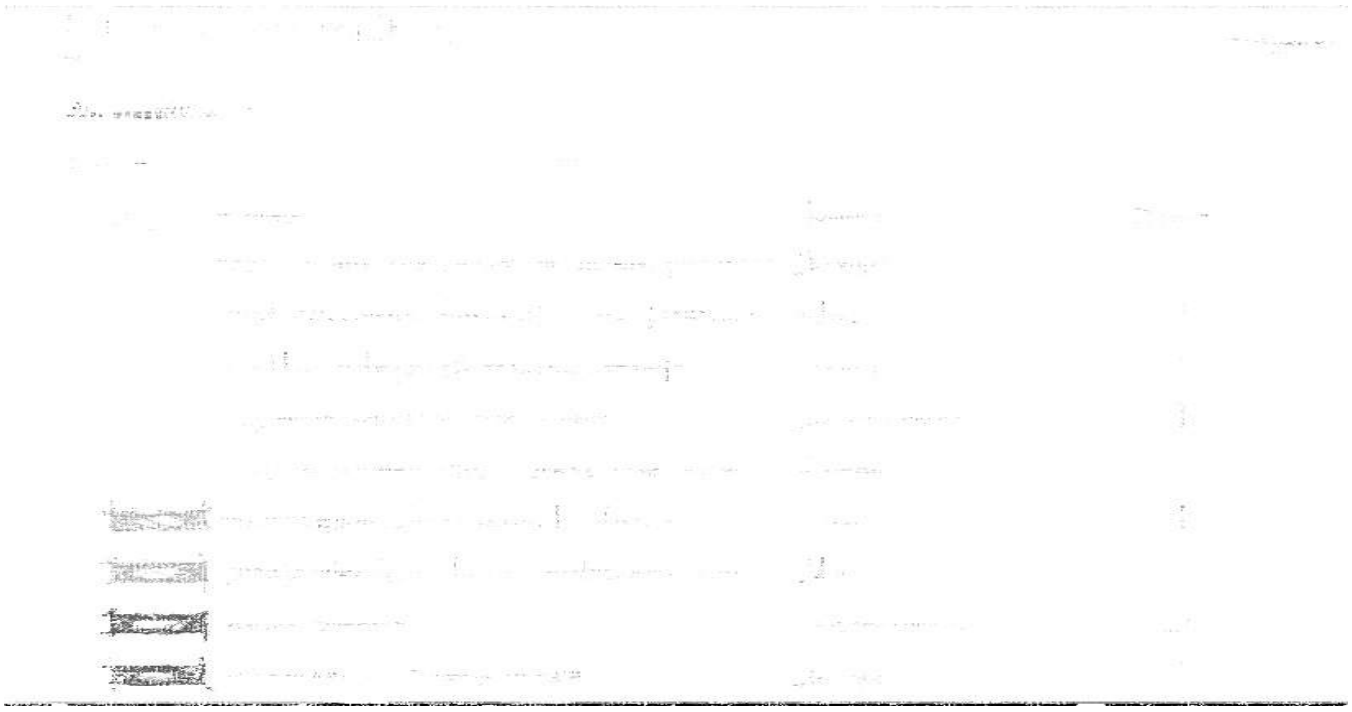




4.29 911.54.151.85

Nessus

Screenshot:

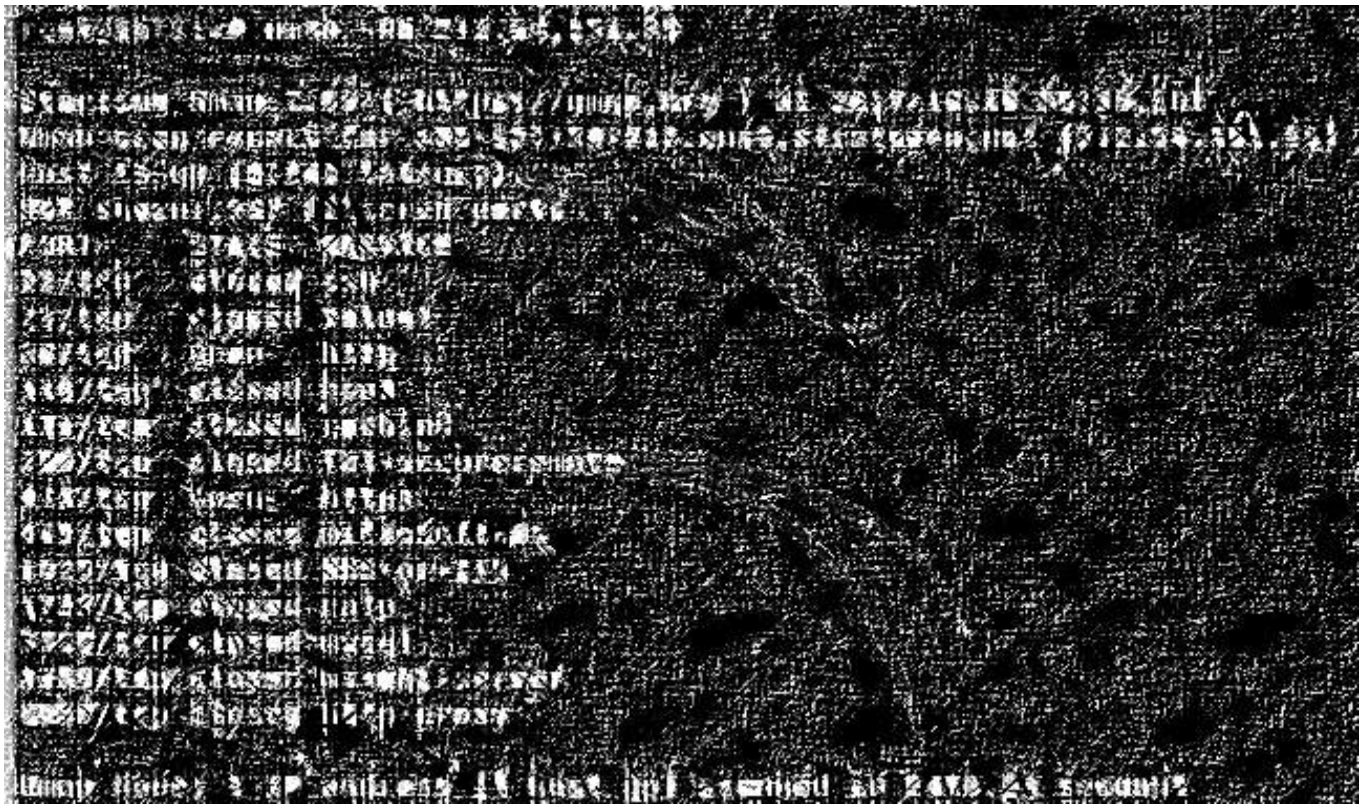


INFO	Device Type	General	1	
INFO	Host Fully Qualified Domain Name (FQDN) Resolution	General	1	
INFO	HSTS Missing From HTTPS Server	Web Servers	1	
INFO	HTTP Server Type and Version	Web Servers	1	
INFO	HyperText Transfer Protocol (HTTP) Information	Web Servers	1	
INFO	Nessus Scan Information	Settings	1	
INFO	Nessus SYN scanner	Port scanners	1	
INFO	OS Identification	General	1	
INFO	SSL / TLS Versions Supported	General	1	
INFO	SSL Certificate 'commonName' Mismatch	General	1	
INFO	SSL Certificate Information	General	1	
INFO	SSL Certificate Signed Using Weak Hashing Algorithm (...	General	1	
INFO	SSL Cipher Block Chaining Cipher Suites Supported	General	1	

INFO	SSL Certificate Information	General	1	
INFO	SSL Certificate Signed Using Weak Hashing Algorithm (...	General	1	
INFO	SSL Cipher Block Chaining Cipher Suites Supported	General	1	
INFO	SSL Cipher Suites Supported	General	1	
INFO	SSL Perfect Forward Secrecy Cipher Suites Supported	General	1	
INFO	SSL Root Certification Authority Certificate Information	General	1	
INFO	SSL Session Resume Supported	General	1	
INFO	TCP/IP Timestamps Supported	General	1	

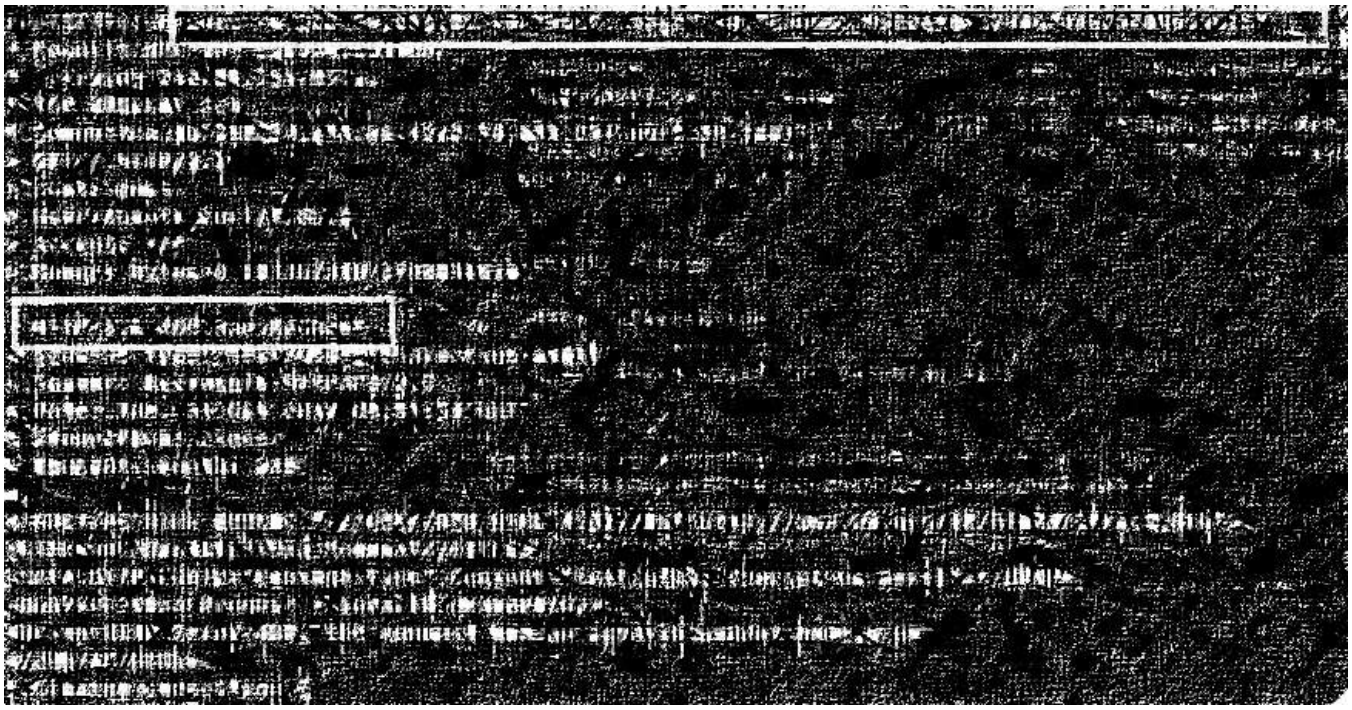
Nmap

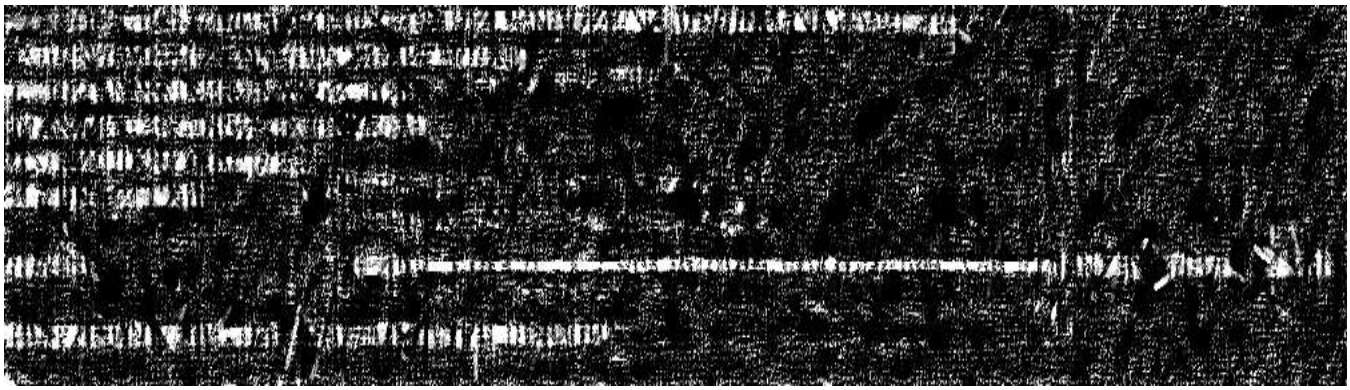
Screenshot:



IIS DoS Attack Tested

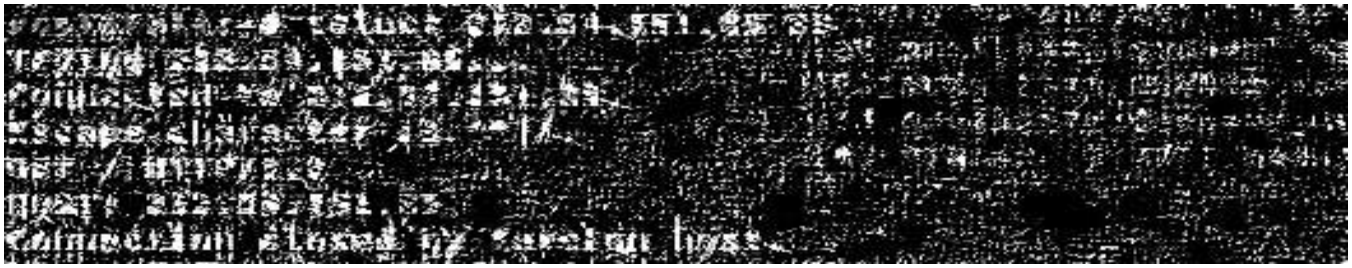
Screenshot:





Telnet

Screenshot:



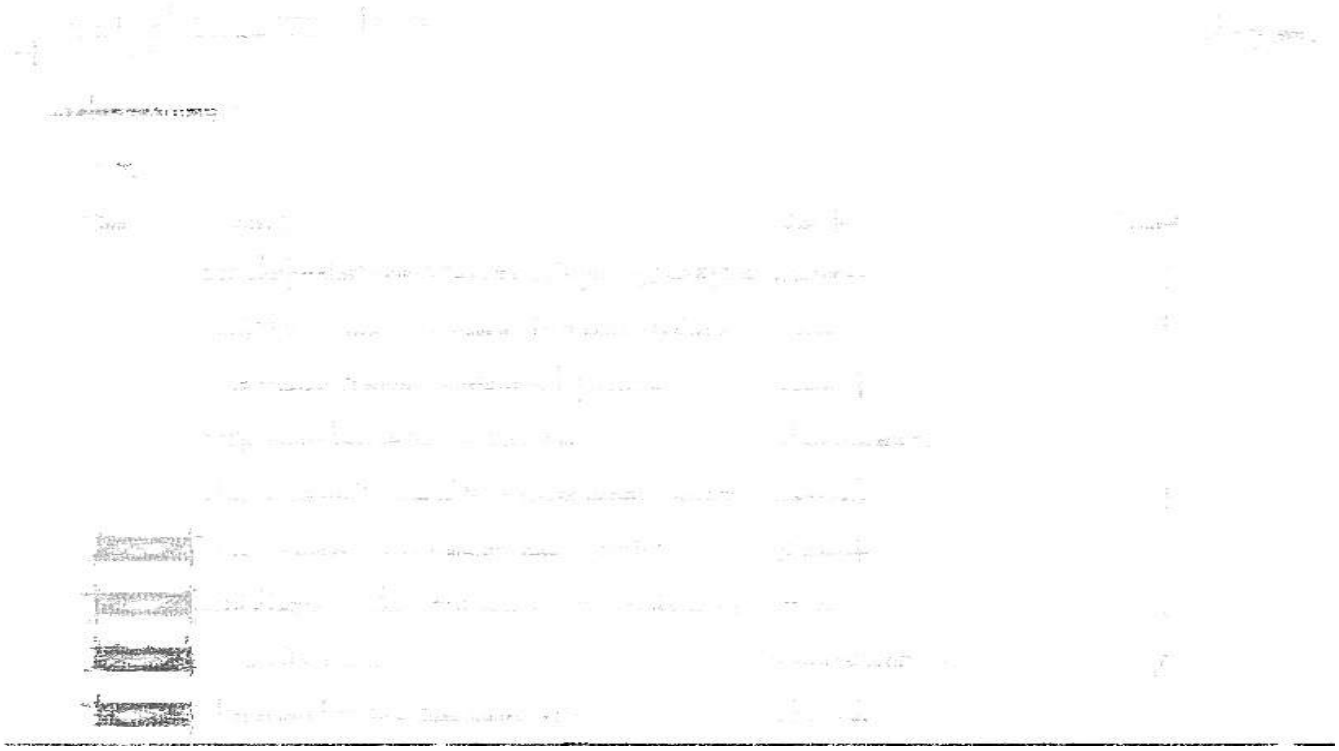
SSL Scan

Screenshot:

4.30 911.54.151.86

Nessus

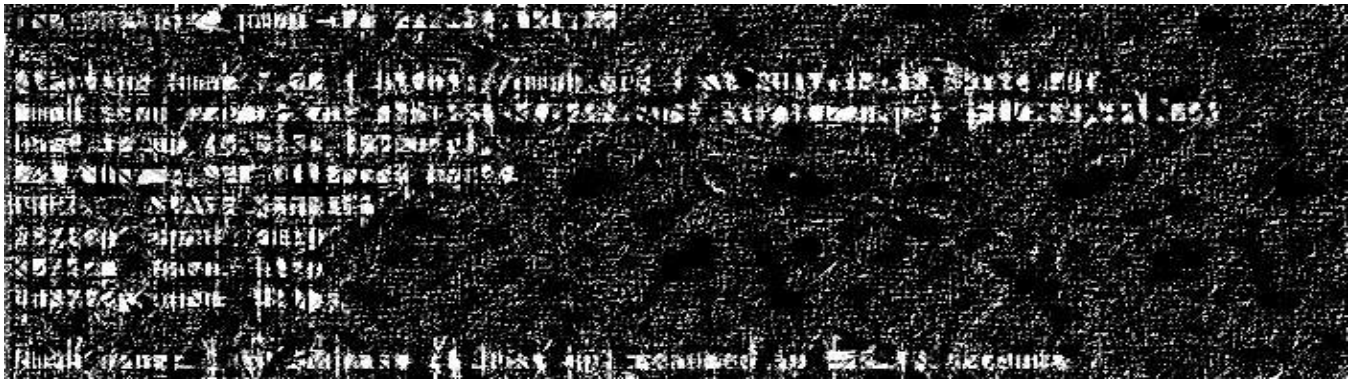
Screenshot:



INFO	Device Type	General	1	
INFO	Host Fully Qualified Domain Name (FQDN) Resolution	General	1	
INFO	HSTS Missing From HTTPS Server	Web Servers	1	
INFO	HTTP Server Type and Version	Web Servers	1	
INFO	HyperText Transfer Protocol (HTTP) Information	Web Servers	1	
INFO	Nessus Scan Information	Settings	1	
INFO	Nessus SYN scanner	Port scanners	1	
INFO	OS Identification	General	1	
INFO	SSL / TLS Versions Supported	General	1	
INFO	SSL Certificate 'commonName' Mismatch	General	1	
INFO	SSL Certificate Information	General	1	
INFO	SSL Certificate Signed Using Weak Hashing Algorithm (...	General	1	
INFO	SSL Cipher Block Chaining Cipher Suites Supported	General	1	
INFO	SSL Cipher Suites Supported	General	1	
INFO	SSL Cipher Block Chaining Cipher Suites Supported	General	1	
INFO	SSL Cipher Suites Supported	General	1	
INFO	SSL Perfect Forward Secrecy Cipher Suites Supported	General	1	
INFO	SSL Root Certification Authority Certificate Information	General	1	
INFO	SSL Session Resume Supported	General	1	
INFO	TCP/IP Timestamps Supported	General	1	

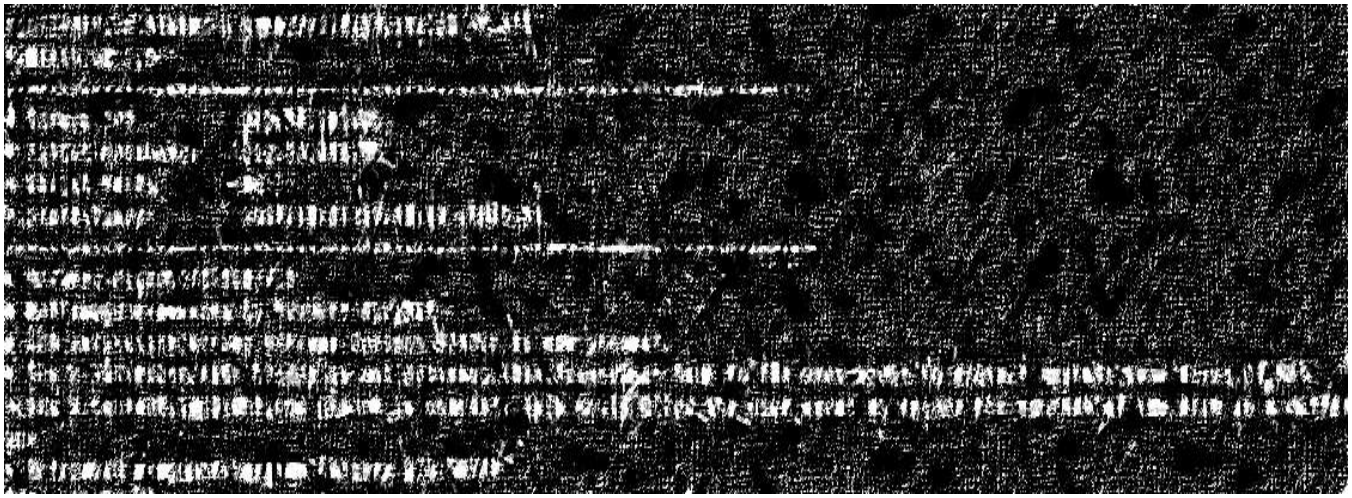
Nmap

Screenshot:



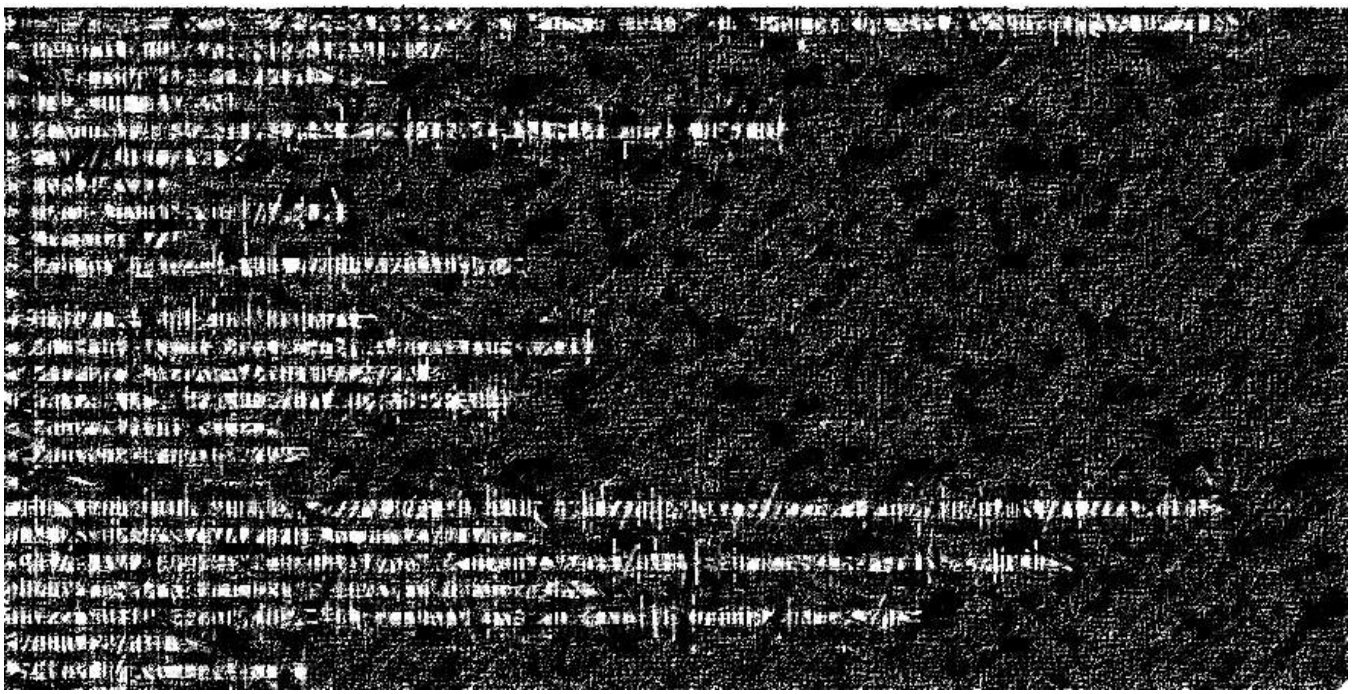
NIKTO

Screenshot:



IIS DoS Attack

Screenshot:



Telnet

Screenshot:

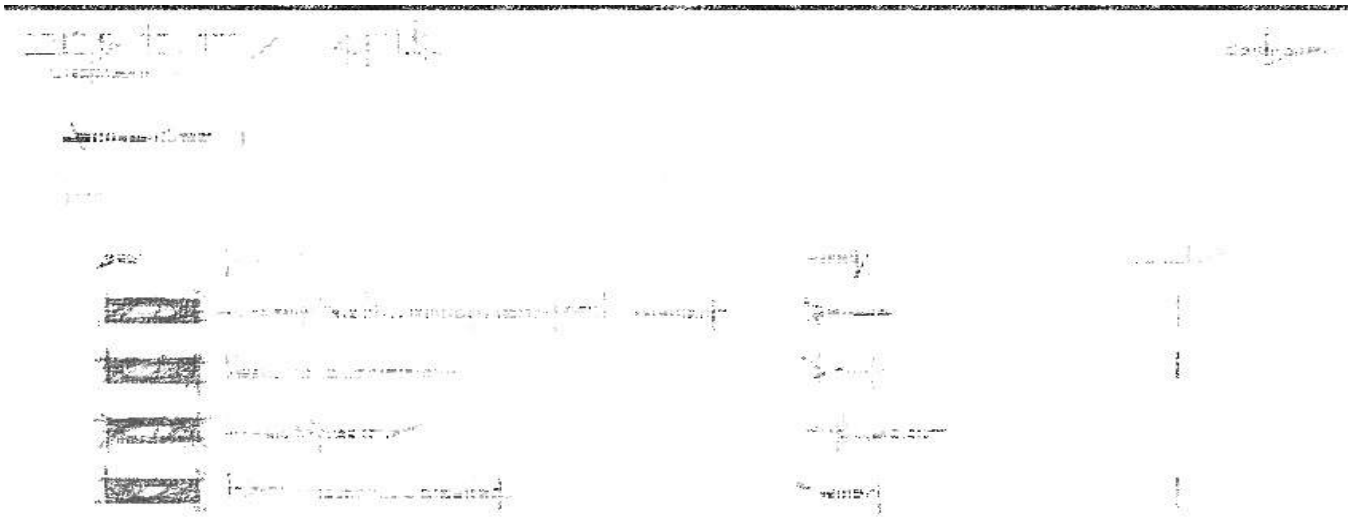
SSL Scan

Screenshot:

4.31 911.54.151.87

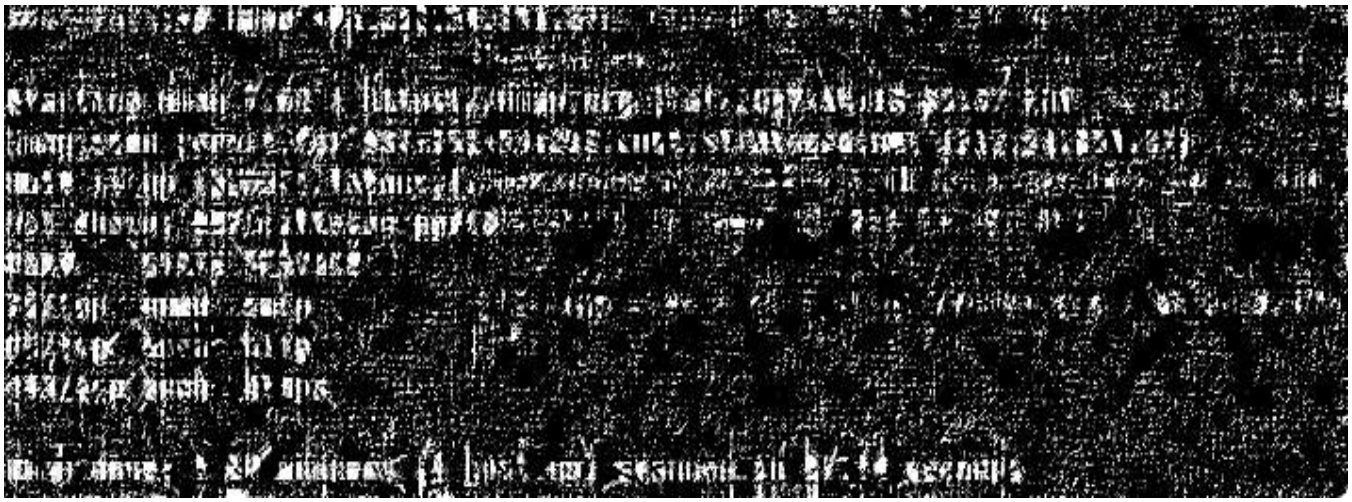
Nessus

Screenshot:



Nmap

Screenshot:



NIKTO

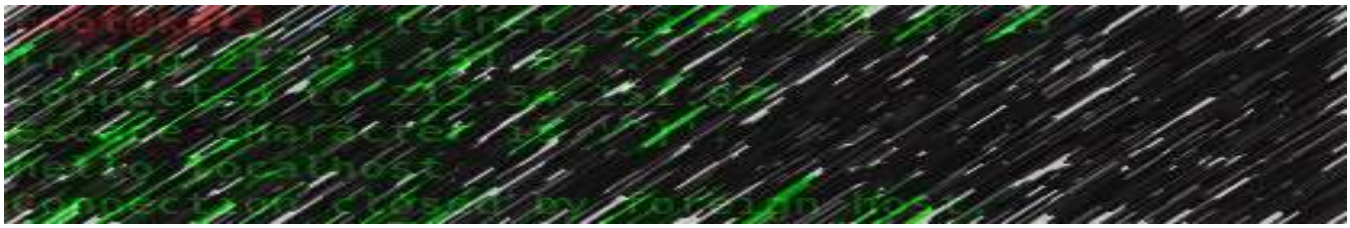
Screenshot:

IIS DoS Attack

Screenshot:

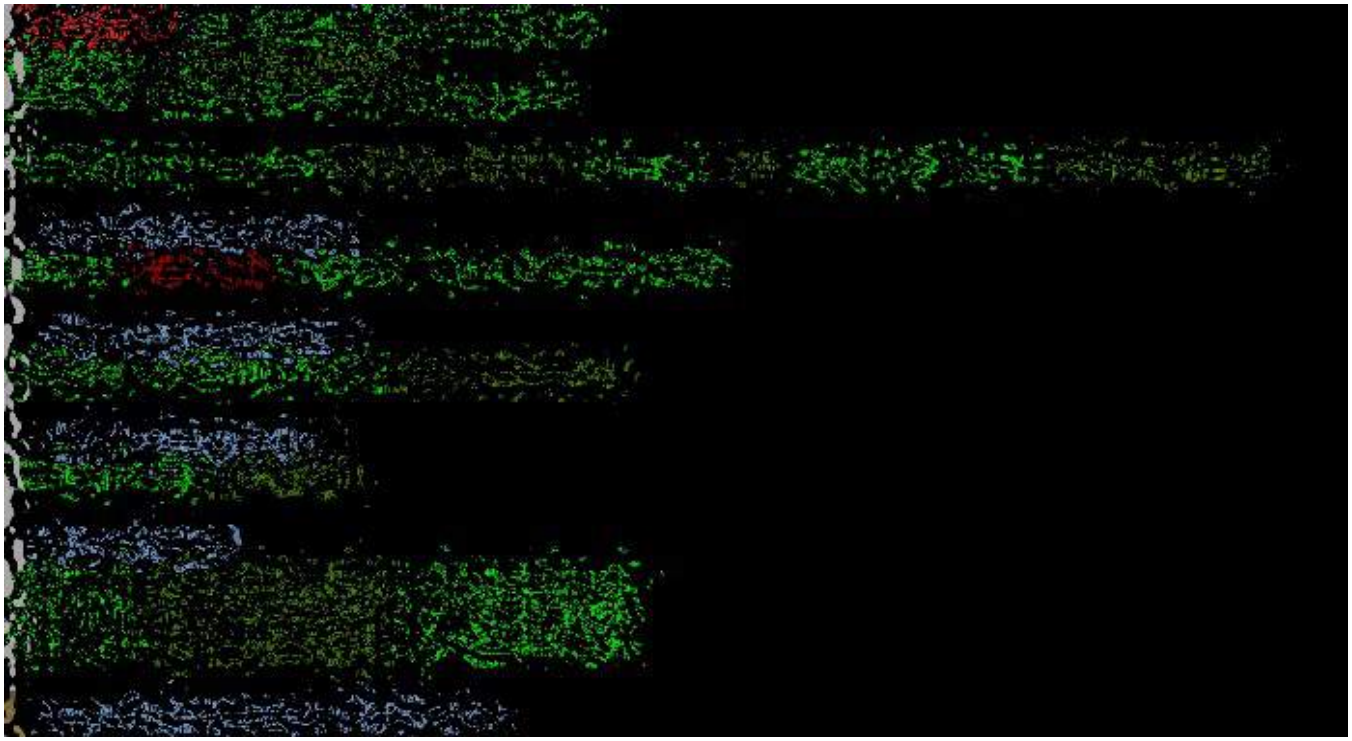
Telnet

Screenshot:



SSL Scan

Screenshot:



Tested for Weak Ciphers

Screenshot:

Trace Method

Screenshot:

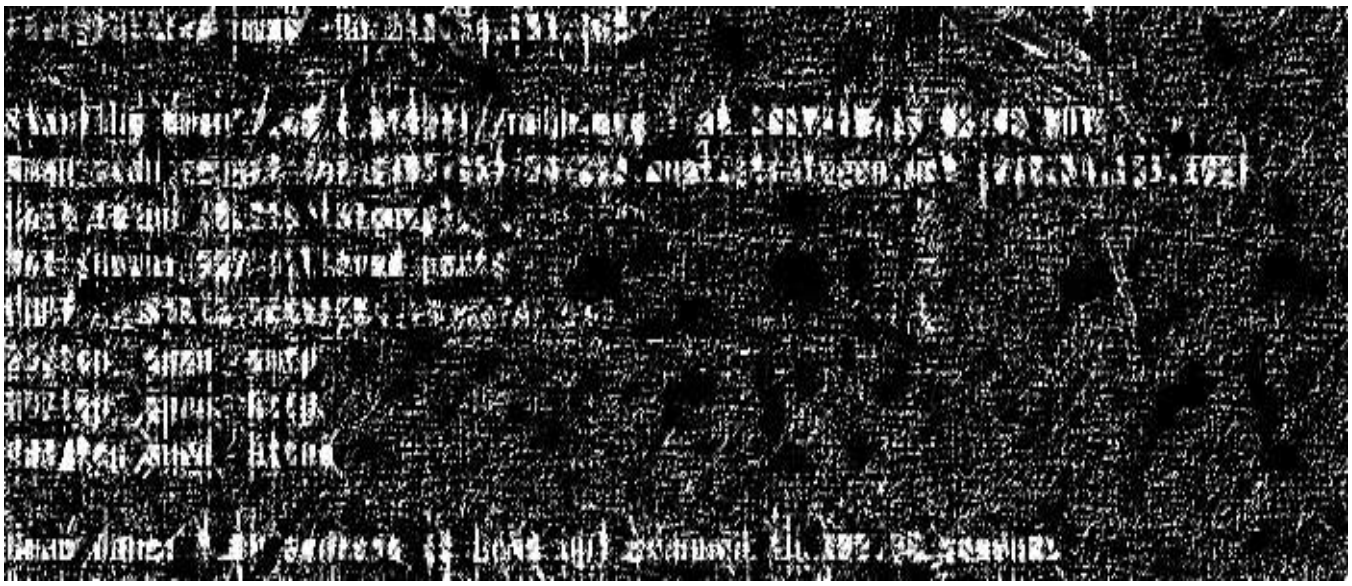
4.32 911.54.151.105

Nessus

Screenshot:

Nmap

Screenshot:

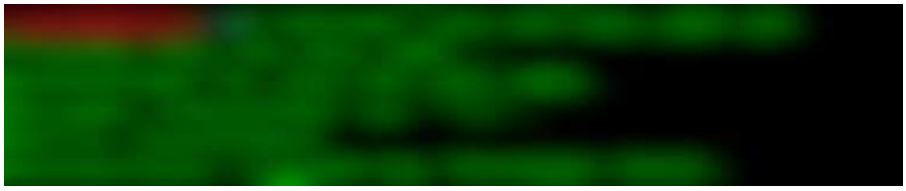


NIKTO

Screenshot:

Telnet

Screenshot:



Tested for Weak Ciphers

Screenshot:

Trace Method

Screenshot:

SSL Scan

Screenshot:

4.33 911.54.151.110

Nessus

Screenshot:

Nmap

Screenshot:

NIKTO

Screenshot:

Telnet

Screenshot:

SSL Scan

Screenshot:

4.34 911.54.151.111

Nessus

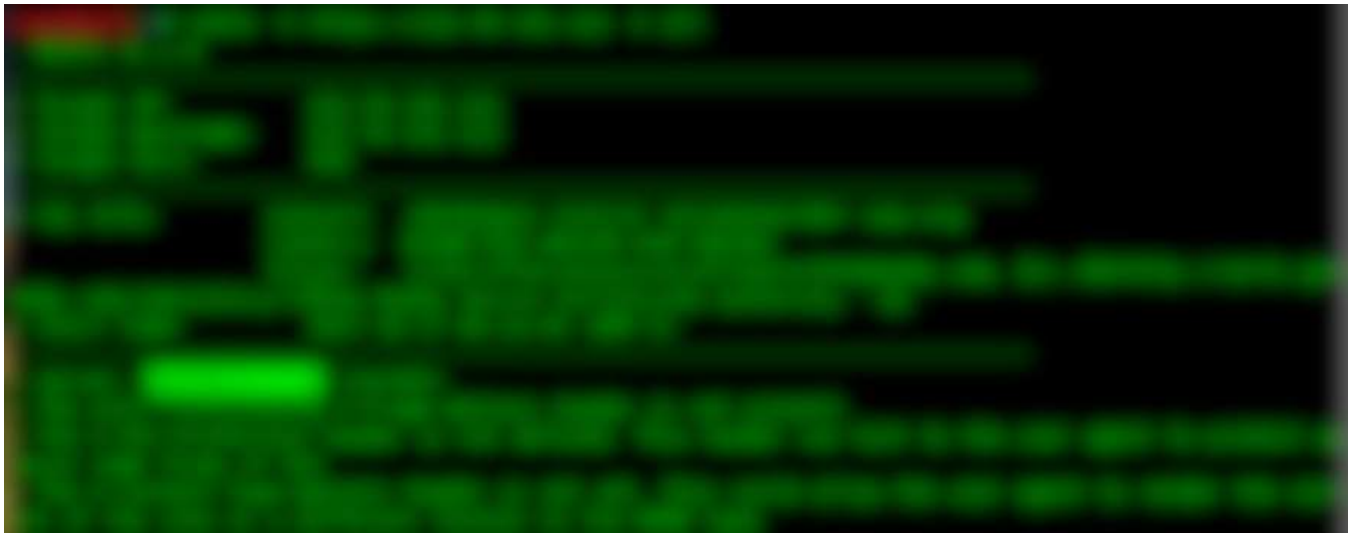
Screenshot:

Nmap

Screenshot:

NIKTO

Screenshot:



DIRB

Screenshot:

SSL Scan

Screenshot:

Tested for Weak Ciphers

Screenshot:

4.35 911.54.151.114

Nessus

Screenshot:

Nmap

Screenshot:

NIKTO

Screenshot:

Telnet

Screenshot:

SSL Scan

Screenshot:

Tested for Weak Ciphers

Screenshot:

Trace Method

Screenshot:

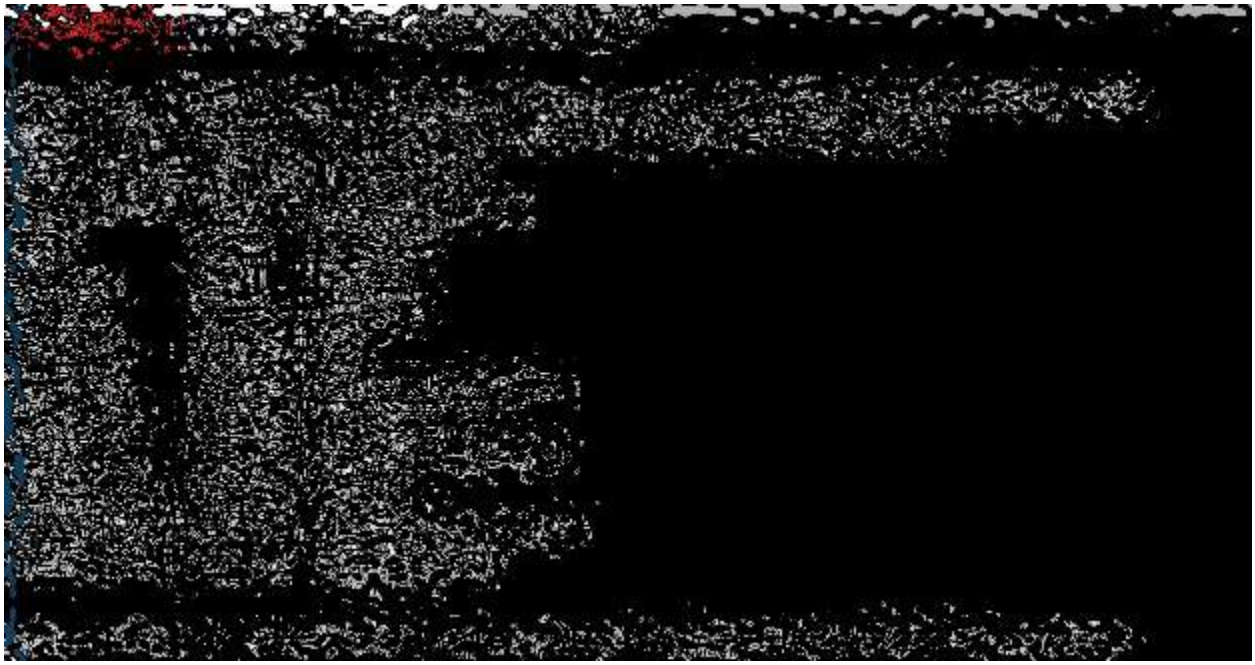
4.36 911.54.151.117

Nessus

Screenshot:

Nmap

Screenshot:



NIKTO

Screenshot:

DNS Amplification

Screenshot:

4.37 911.54.151.118

Nessus

Screenshot:

Info	19506	Nessus Scan Information
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	43111	HTTP Methods Allowed (per directory)
Info	45410	SSL Certificate 'commonName' Mismatch
Info	45590	Common Platform Enumeration (CPE)
Info	51891	SSL Session Resume Supported
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported
Info	84502	HSTS Missing From HTTPS Server
Info	94761	SSL Root Certification Authority Certificate Information
Info	95631	SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)

Nmap

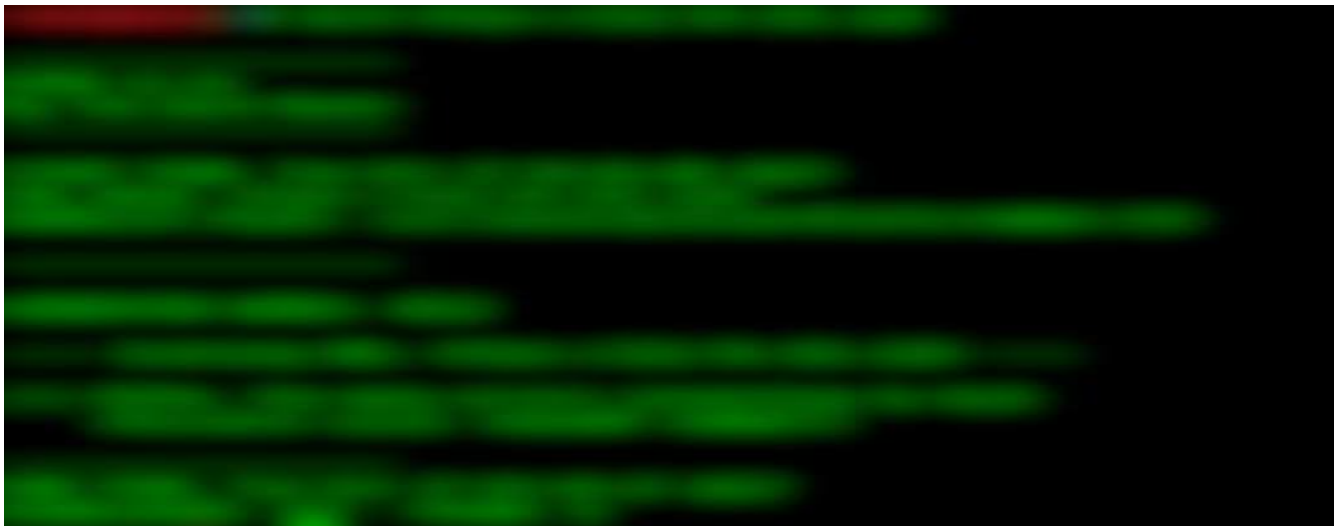
Screenshot:

NIKTO

Screenshot:

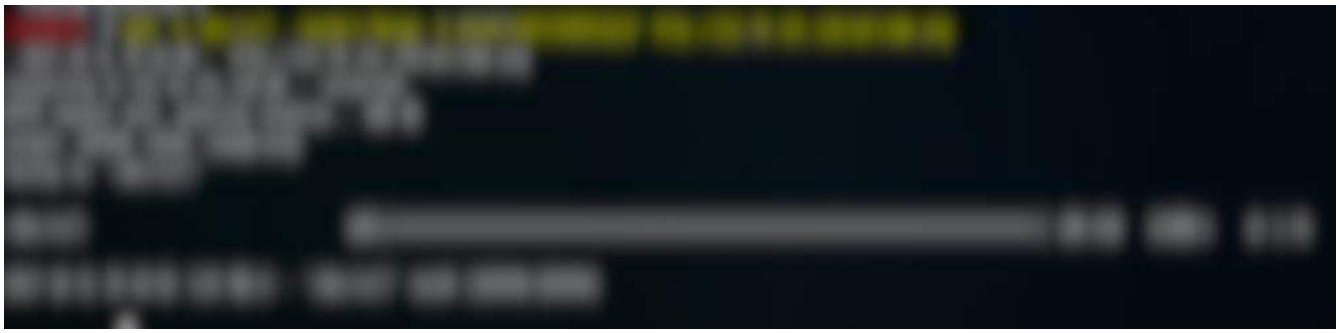
DIRB

Screenshot:



IIS Dos Attack

Screenshot:

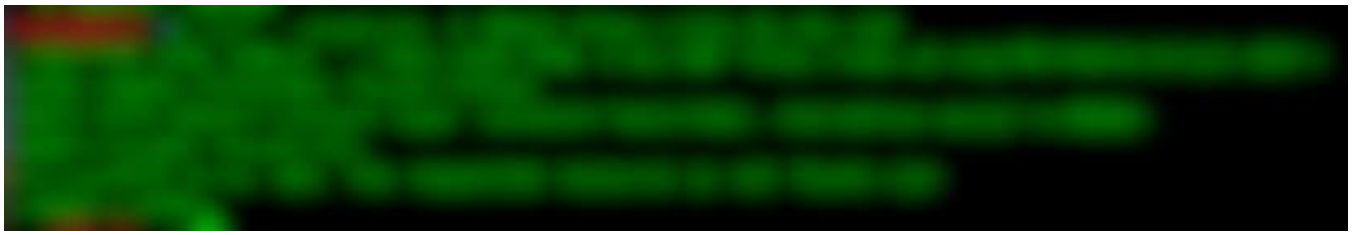


Telnet

Screenshot:

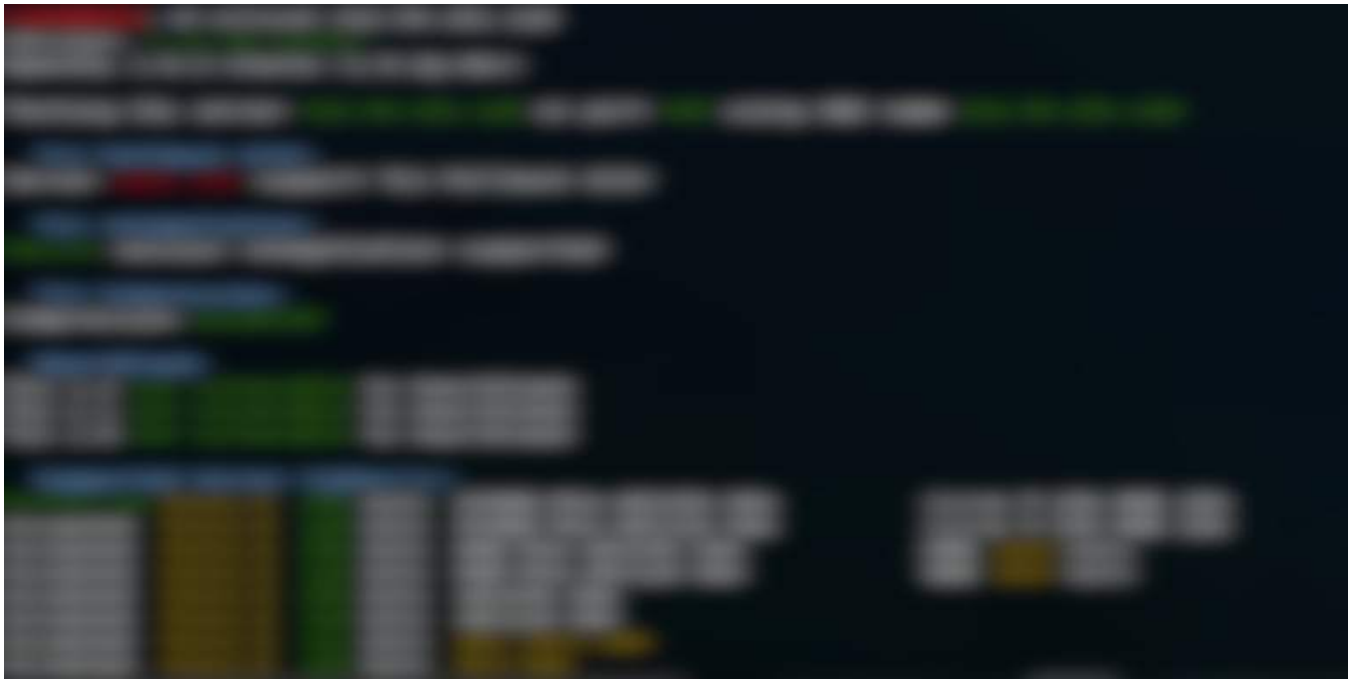
Trace Method

Screenshot:



SSL Scan

Screenshot:



4.38 911.54.151.119

Nessus

Screenshot:

Nmap

Screenshot:

DNS Amplification

Screenshot:

4.39 911.54.151.120

Nessus

Screenshot:

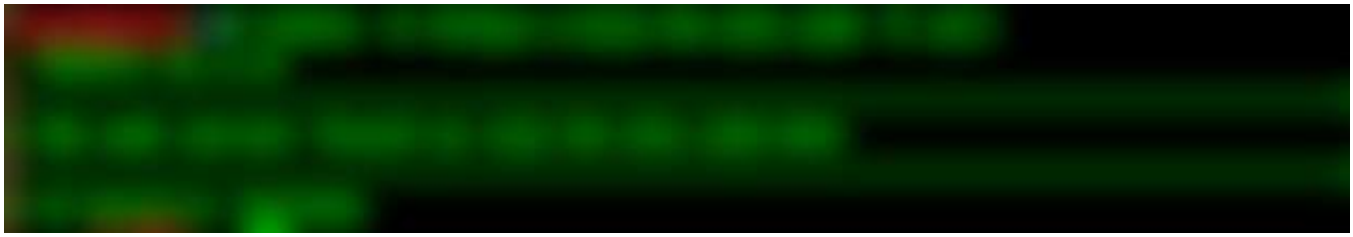
Info	10107	HTTP Server Type and Version
Info	10287	Traceroute Information
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	45590	Common Platform Enumeration (CPE)
Info	54615	Device Type
Info	66334	Patch Report

Nmap

Screenshot:

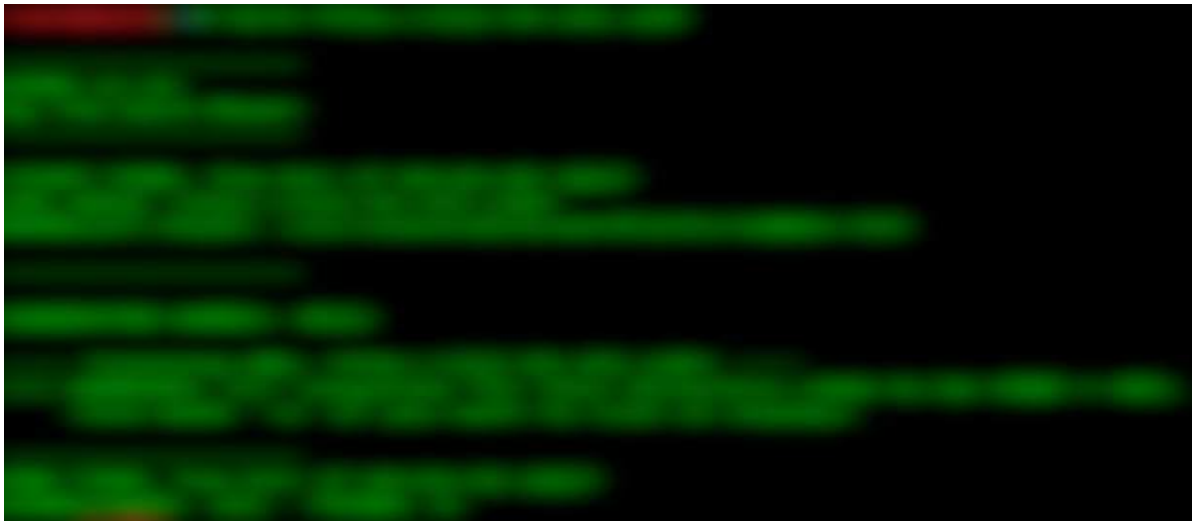
NIKTO

Screenshot:



DIRB

Screenshot:



Telnet

Screenshot:

SSL Scan

Screenshot:

Trace Method

Screenshot:

4.40 911.54.151.121

Nessus

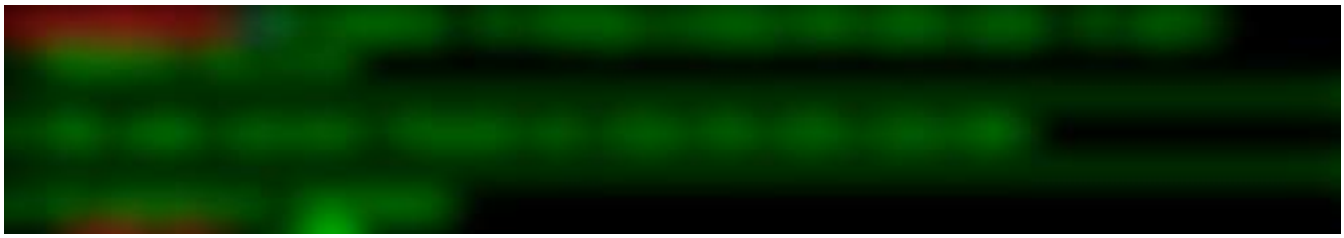
Screenshot:

Nmap

Screenshot:

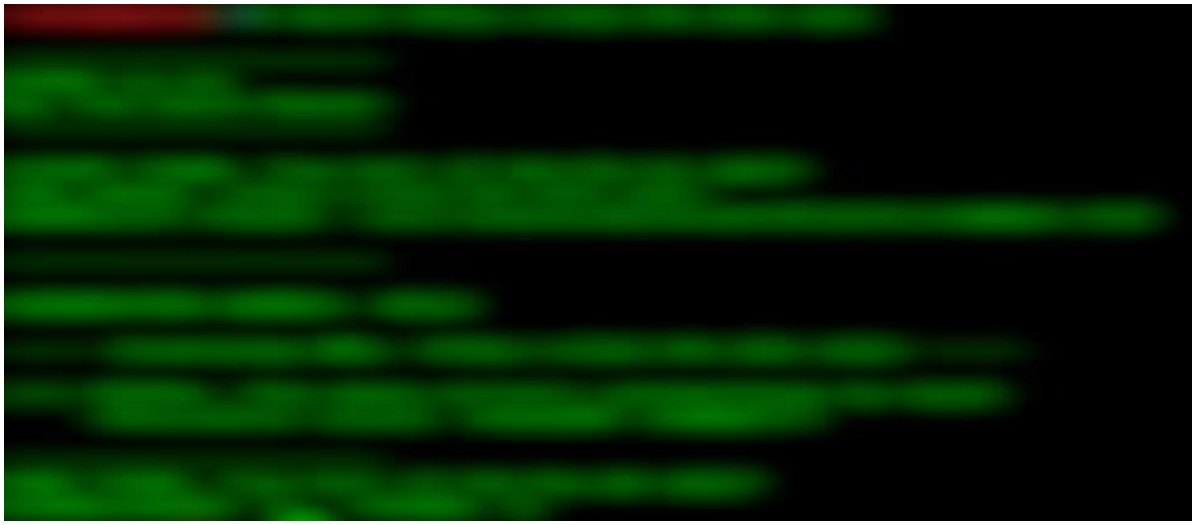
NIKTO

Screenshot:



DIRB

Screenshot:



SSL Scan

Screenshot:

Tested for Weak Ciphers

Screenshot:

RECOMMENDATIONS:
Please update all the servers to the latest versions.

5 Limitations on Disclosure and Use of this Report

This report contains information concerning potential vulnerabilities of ABC LTD and methods for exploiting them. Entersoft recommends that special precautions be taken to protect the confidentiality of both this document and the information contained herein.

Security Assessment is an uncertain process, based on past experiences, currently available information, and known threats. It should be understood that all information security systems, which by their nature are dependent on human beings, are vulnerable to some degree. Therefore, while Entersoft considers the major security vulnerabilities of the analyzed systems to have been identified, there can be no assurance that any exercise of this nature will identify all possible vulnerabilities or propose exhaustive and operationally viable recommendations to mitigate those exposures.

In addition, the analysis set forth herein is based on the technologies and known threats as of the date of this report. As technologies and risks change over time, the vulnerabilities associated with the operation of the ABC LTD Application described in this report, as well as the actions necessary to reduce the exposure to such vulnerabilities will also change. Entersoft makes no undertaking to supplement or update this report on the basis of changed circumstances or facts of which Entersoft becomes aware after the date hereof, absent a specific written agreement to perform the supplemental or updated analysis.

This report may recommend that Entersoft use certain software or hardware products manufactured or maintained by other vendors. Entersoft bases these recommendations upon its prior experience with the capabilities of those products. Nonetheless, Entersoft does not and cannot warrant that a particular product will work as advertised by the vendor, nor that it will operate in the manner intended.

This report was prepared by Entersoft for the exclusive benefit of ABC LTD and is proprietary information. The Non-Disclosure Agreement (NDA) in effect between Entersoft and ABC LTD govern the disclosure of this report to all other parties including product vendors and suppliers.

6 Disclaimer

This document or any of its content cannot account for, or be included in any form of legal advice. The outcome of a security assessment should be utilized to ensure that diligent measures are taken to lower the risk of potential exploits carried out to compromise data.

Legal advice must be supplied according to its legal context. All laws and the environments, in which they are applied, are constantly changed and revised. Therefore, no information provided in this document may ever be used as an alternative to a qualified legal body or representative.

End of Document