SENSITIVE BUT UNCLASSIFIED INFORMATION

Sensitive-But-Unclassified Information. Protect From Unauthorized Disclosure. This document requires Administrative Control. This is not a classified document, however it warrants physical protection and control.

Warning

The enclosed document(s) is (are) property of the United States Government. Release of or disclosure of the contents is prohibited. Contents may be disclosed only to persons whose official duties require access hereto. Remove this cover prior to external transmission or destruction of the document. Copying, dissemination, or distribution of these materials to unauthorized users is prohibited.

[redacted]

INTERNET SECURITY SYSTEMS™

[redacted]

Management Report for

[redacted] **Test**

Prepared by:
X-Force Professional Security Services

Testing conducted February/March 2005

For
DOI Office of Inspector General

Sites assessed in this report:
- DOI Bureau of Land Management

The Power to Protect

www.iss.net

Confidentiality

This document contains company confidential information of a proprietary and sensitive nature. As such this document should be afforded the security and handling precautions that a confidential document warrants. This document should have a controlled distribution to relevant parties only, and should not be copied without written permission.

ISS treats the contents of a security audit as company confidential material, and will not disclose the contents of this document to anyone without written permission.

Version Control

[redacted]	Department of Interior Office of Inspector General
	Roger Mahach
	FINAL-02
	Scott Miles
	Don Pollicino
	Department of Interior ISS File
	ISS and DOI Confidential

Table of Contents

List of Figures

Document Organization

This document is organized into three sections. The first section, scope of testing, outlines the parameters and extent of the [redacted] test. A summary of the findings is then provided, indicating the overall level of risk observed along with the major security issues and activities that occurred during testing. Finally, a break-down of the vulnerability data is provided.

Executive Summary

This report documents the findings of a [redacted] Test conducted by Internet Security Systems (ISS) on a portion of the Department of Interior (DOI) network as part of an ongoing project to evaluate the security of each of the DOI bureaus. A more detailed technical report has also been provided for security management and network and system administrators.

Scope of Testing

Bureau/Office Tested

This test was conducted against networks belonging to the Bureau of Land Management ("BLM"). The DOI Office of Inspector General (OIG) authorized ISS to perform an [redacted] test on BLM networks to ascertain potential security weaknesses of network devices and hosts.

Dates of Testing

The assessment was conducted [redacted] from [redacted] from February 21st through March 11th 2005. Documentation and some additional validation of testing results were performed through March 31st, 2005.

Relevant Standards, Federal and Departmental Guidelines

- Federal Information Security Management Act
- Inspector Generals Act
- Office of Management and Budget Circular A-130, Management of Federal Information Resources. Appendix III Management of Federal Information Resources
- General Accountability Office Federal Information Systems Controls Audits Manual FISCAM
- National Institute of Standards and Technology. Special Publication 800-42, Guideline on Network Security Testing.
- Department of the Interior Network Security Policy (February 14, 2003)
- Department of the Interior, Departmental Manual Chapter 375.19, Information Technology Security Program
- SANS Top 20 Most Critical Internet Security Vulnerabilities

Testing Methodology

This [redacted] test was performed in [redacted] mode. ISS was only provided with the [redacted] No systems were excluded from testing.

Only the primary contact at the DOI was informed of the exact start date and targets. No one at BLM was informed of testing in order to more closely mimic real attack activity and to evaluate response mechanisms.

Testing was divided into three phases:

- ***Network Reconnaissance*** was performed in order to gain a better knowledge of the network that was being tested.
- ***Vulnerability Identification*** was initiated with all the hosts that were discovered in the previous phase through the use of automated tools as well as extensive testing with customized tools and manual testing.
- ***Validation and Exploitation*** of the discovered vulnerabilities was attempted. This consists primarily of manual review of all vulnerability data, validating vulnerabilities by exploiting them, and combining data and vulnerabilities to penetrate the target networks.

Summary of Findings

Some significant vulnerabilities were found that allow penetration into BLM networks or allow unauthorized access to information. The environment exhibits some good security practices and controls that can help mitigate the effect of vulnerabilities, but is still at a significant risk of system compromise or access to unauthorized data as a result of the issues identified.

Risk Rating: High Risk

Security Impact

ISS was able to penetrate the tested environment in multiple ways.

[redacted]

These issues resulted in remote interactive access to many systems on the BLM network, including administrative access to [redacted] servers and [redacted] servers.

The [redacted] systems were configured with some attention paid to security, although there appear to be significant weaknesses in the overall security architecture. There

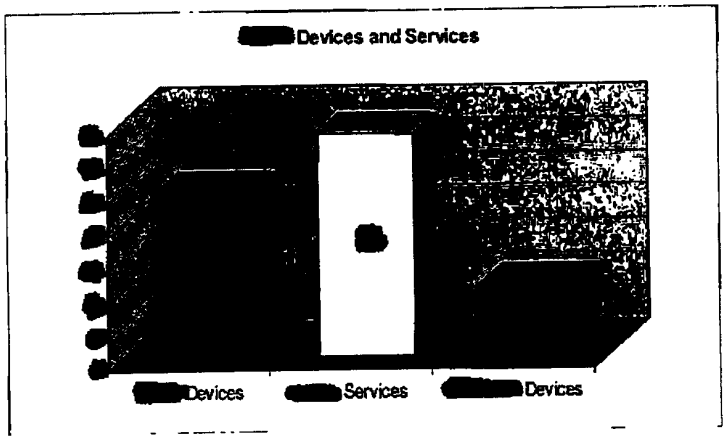
is evidence of firewalls, with only those systems intended for [redacted] The systems that were compromised exhibited some good security practices such as up to date security patches and strong password policies that eliminate many common vulnerabilities and reduce the impact of identified vulnerabilities.

However, a relatively large number of different [redacted] servers are accessible [redacted] representing an increased risk that one will contain configuration issues or unpatched security vulnerabilities. There does not appear to be an effective [redacted] network for [redacted] exposed [redacted] putting [redacted] systems at a much higher risk of compromise.

[redacted] activity was [redacted] shortly after [redacted] began on Tuesday, February 22nd and Wednesday, February 23rd, resulting in the originating test [redacted] being [redacted] by [redacted]. None of the less intrusive and manual testing performed from [redacted] There was also no evidence that any of the activities that resulted in [redacted] of the [redacted] or actions carried out on [redacted] were ever identified; vulnerabilities were exploitable throughout the testing period and even as late as March 31st when they were used to access and collect additional information from the [redacted]

Active Services

The bureau tested consists of [redacted] network ranges. The largest of these is an [redacted] network range that is not directly connected [redacted] The remaining networks cover roughly [redacted] possible devices. A total of [redacted] active devices were found, allowing connections on [redacted] different active services. Of the services found, most are common services such as [redacted] and [redacted] servers that are intended to be [redacted] accessible. Of the [redacted] active devices [redacted] were found to have some degree of vulnerability. This is a relatively small number of hosts and services for such a large organization. Each additional system or service does represent one more potential avenue of attack, however, so keeping this footprint small and further reducing [redacted] exposure is recommended.



Summary of Vulnerabilities

Inappropriate access controls [redacted] BLM makes use of a [redacted] server that handles [redacted] requests [redacted] and passes the request on to the appropriate server. This [redacted] can be used to access some [redacted] servers such as the [redacted] server that should not be accessible [redacted]

The access controls [redacted] should be reviewed to ensure access is only allowed from [redacted] to appropriate [redacted]

[redacted] **in [redacted] applications.** The [redacted] server contains a [redacted] utility for sending comments [redacted] This program is vulnerable to a [redacted] Specially formatted input can manipulate the program into [redacted] on the [redacted] server. This vulnerability was used to penetrate the remote server and allowed many of the other vulnerabilities to be found and exploited resulting in further access to [redacted] systems.
The utility must be modified to prevent the [redacted] run by the program. Other modifications to the [redacted] server configuration should also be made to limit the [redacted]

[redacted] **vulnerabilities in [redacted] applications.** Two separate [redacted] applications were found with [redacted] vulnerabilities. An attacker can use these to [redacted] the application into [redacted] outside of the anticipated area. In this case, any file on the [redacted] server that is readable by the [redacted] server userid can be accessed [redacted] This exposes sensitive system configuration files as well as application data. One vulnerability in the [redacted] led to the discovery of the [redacted] vulnerability; the other in [redacted] led to the discovery of a file containing system and database passwords for every component supporting the [redacted] application.
These applications must be modified to use appropriate functions and [redacted] to prevent [redacted] issues.

[redacted] **in [redacted]** An [redacted] on the [redacted] network is accessible [redacted] Several accounts [redacted] are configured with [redacted] passwords, allowing access to the [redacted] No data was observed in the [redacted] but the [redacted] itself may be susceptible to other vulnerabilities that could be exploited once connected. This could compromise other data on the system and potentially provide a route into the [redacted]
All [redacted] passwords must be changed to comply with BLM/DOI password standards. This system should be further restricted so that it is not reachable by any [redacted]

[redacted] **vulnerabilities in [redacted] applications.** At least [redacted] are vulnerable to [redacted] This allows modification of the [redacted] sent to the [redacted] from the [redacted] This vulnerability can often be used to access or modify data in the [redacted] manipulate application logic, or gain access to the server [redacted] Manipulation of [redacted] was accomplished during testing, allowing access to arbitrary data [redacted] and bypassing a [redacted] login on another, but no significant access or sensitive data was observed.
The [redacted] applications must be modified to prevent [redacted] attacks. [redacted] can also help identify and prevent some of these vulnerabilities.

[redacted] **software configurations introduce vulnerabilities.** [redacted] is an application server that provides a framework for applications on a [redacted] server. The configuration of [redacted] on this server provides programs with excessive access to the underlying

operating system. The access controls on [redacted] on the [redacted] can also lead to them being used to run commands on the server.
Changes should be made to the [redacted] and [redacted] servers and [redacted] configurations to limit the potential for exploitation.

[redacted] ISS did not observe [redacted] controls that limited the [redacted] that could be [redacted] was obtained to the [redacted] servers. It also appears that many of the [redacted] do not reside in a single [redacted] but instead reside in locations inside the [redacted] that are simply [redacted] by the [redacted]
BLM should review the systems processing [redacted] requests and ensure that each such system is sufficiently [redacted] from the [redacted] to mitigate the effects should the system be compromised.

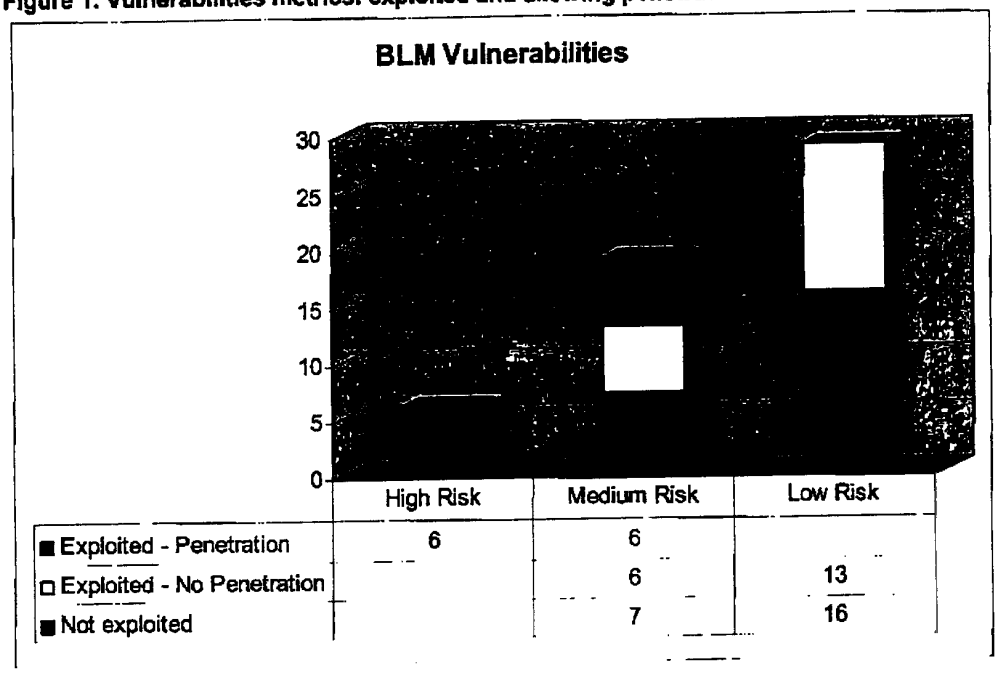
[redacted] **encryption.** The [redacted] servers allow [redacted] for [redacted] Many of these passwords [redacted] providing a list of userids and passwords that can be used to access [redacted] None of the BLM [redacted] servers are accessible from [redacted] limiting the exposure of this issue. However, the [redacted] can be used to access [redacted] servers accessible on the [redacted] It is also assumed that [redacted] could be used to access other [redacted] servers that are reachable.
The [redacted] and [redacted] should be migrated to the stronger [redacted] encryption algorithm.

Other medium and low-risk vulnerabilities also identified that can be used to [redacted] the [redacted] or [redacted] that may be useful when carrying out other attacks. These vulnerabilities should also be addressed by making the recommended changes.

Risk/Vulnerability Metrics

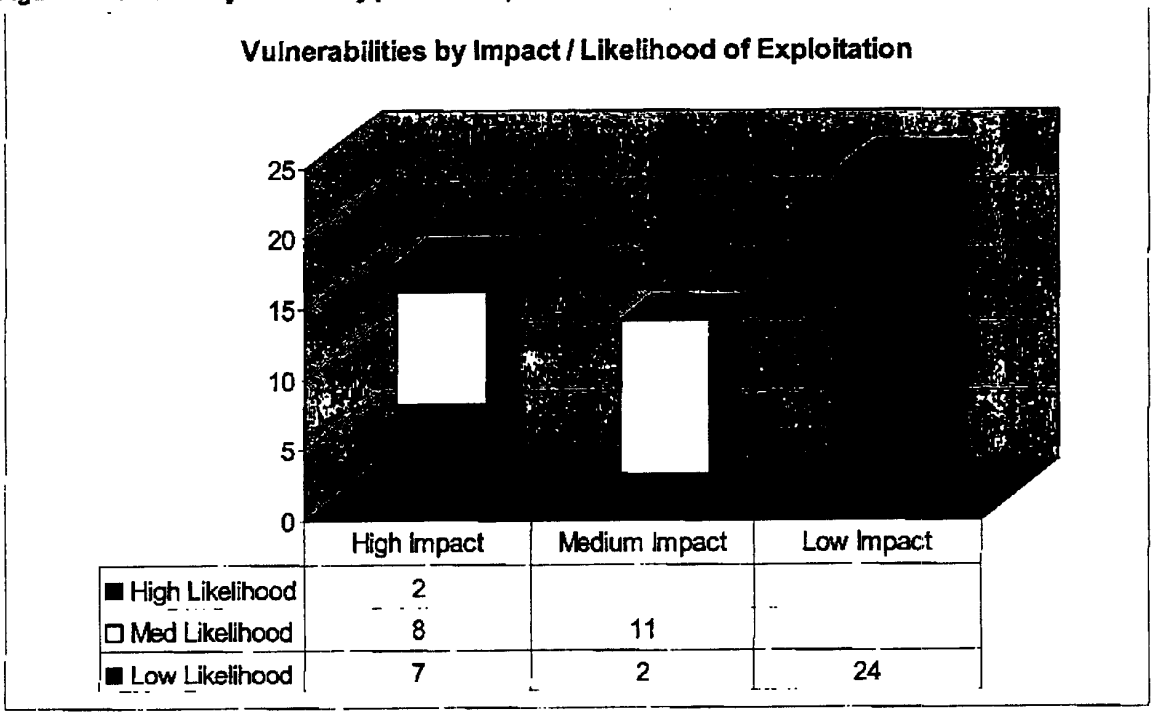
A total of 12 vulnerability instances resulted in penetration as defined in the Rules of Engagement. Nineteen other medium and low-risk vulnerabilities were exploited to gain access to some type of information or resource, but did not result in penetration. Twenty three other medium and low-risk vulnerabilities were not exploited. The vulnerabilities that were not exploited were [redacted] vulnerabilities such as [redacted] that were already demonstrated, [redacted] vulnerabilities, and vulnerabilities for which there are currently no publicly available programs or information on how to exploit the issue.

Figure 1: Vulnerabilities metrics: exploited and allowing penetration



As indicated above, only 6 vulnerabilities classified as "high risk" were identified, with another 19 classified as "medium risk" and 29 as "low risk". The determination of risk is based on the potential impact of the vulnerability combined with the likelihood that the vulnerability could be exploited. Viewed solely by potential impact, there are 17 high impact vulnerabilities, but many of these have a medium to low likelihood of exploitation that result in a lower overall risk for the vulnerability. This is because many of these vulnerabilities are only exploitable once some level of access has been obtained to the target environment. Most medium and low-risk vulnerabilities are not exploited unless there is a need for additional information about the system or network being attacked, since these vulnerabilities tend to be informational in nature.

Figure 2: Vulnerability metrics: by potential impact & likelihood

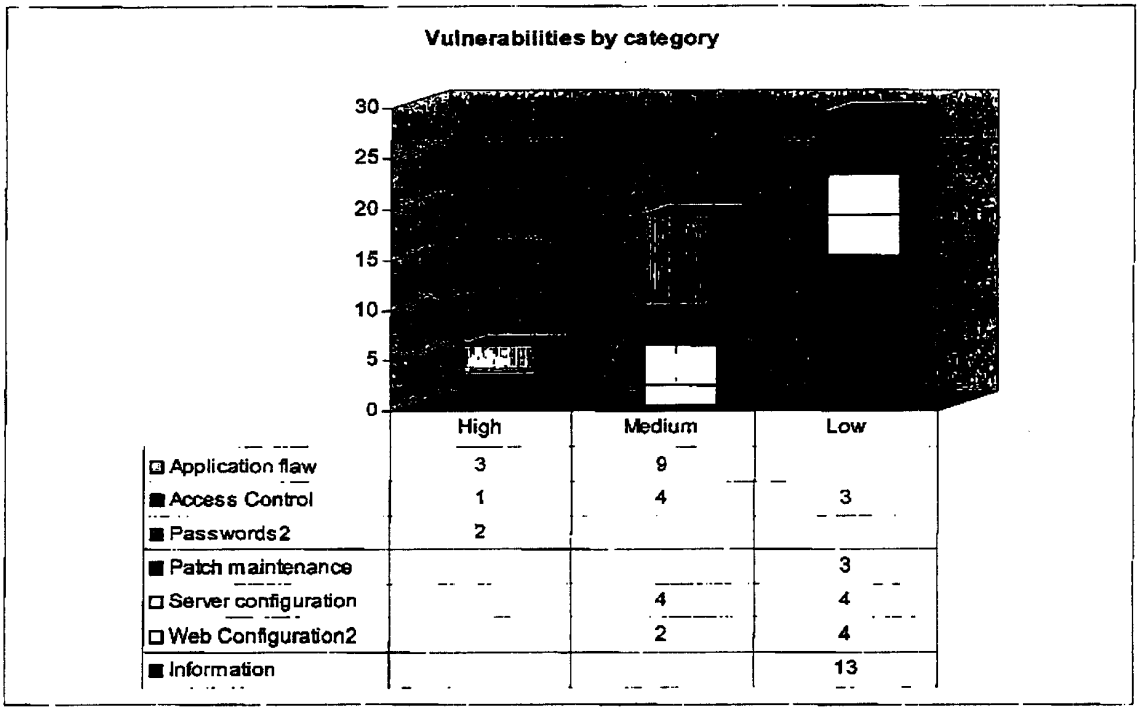


Each vulnerability was categorized into the following root causes:

- **Access control**: The vulnerability is a result of inappropriate access controls.
- **Application flaw**: The vulnerability is a result of a flaw in a custom application.
- **Passwords**: System, application, or other passwords are easily discovered or guessed.
- **Patch maintenance**: The vulnerability is fixed by a software patch or a newer version of software, but which is not applied.
- **Server configuration**: The operating system is not secured or is configured in such a way that allows the vulnerability.
- **Web configuration**: The web server is not secured or is configured in such a way that allows the vulnerability.
- **Unnecessary services**: The service may not be inherently vulnerable, but is exposed to the Internet when it should not be if not necessary.

The high risk issues in the environment are related to application flaws, access control, and password issues. Other medium risk issues are caused by application flaws, access control, and configuration issues as shown in Figure 3.

Figure 3: Vulnerability metrics: by category



	High	Medium	Low
Application flaw	3	9	
Access Control	1	4	3
Passwords2	2		
Patch maintenance			3
Server configuration		4	4
Web Configuration2		2	4
Information			13

Tactical Recommendations

Review access controls on [redacted]

The access controls on the [redacted] should be reviewed to ensure only [redacted] that should be accessible from [redacted] can be reached.

Modify vulnerable [redacted] applications

The vulnerable [redacted] on the [redacted] should be modified to remove [redacted] vulnerabilities. In addition, both of th[redacted] applications that allow [redacted] should be modified as soon as possible to remove the vulnerability.

Implement practices to avoid [redacted] and [redacted]

Follow the recommendations provided to avoid [redacted] and [redacted] issues in custom application code.

Review accessibility to certain data

The ability to access data such as security vulnerability reports, system core files, and backups of system configuration files should be reviewed and modified to ensure this type of data is not accessible to unauthorized users.

Change [redacted] passwords

All of the [redacted] identified in this report should be changed to strong passwords that comply with the DOI/BLM password standards. The processes used to create and change these passwords should be changed to ensure that only strong passwords may be used.

Discontinue support for [redacted] passwords

The use of [redacted] passwords should be discontinued.

Harden [redacted] and [redacted] server configurations

The configuration of [redacted] and [redacted] should be hardened according to security best practices. The [redacted] server should be configured to run in a [redacted] environment with no [redacted] allowed on any server files or [redacted] content from the [redacted] server id. The [redacted] server should be run as a [redacted] with [redacted] disabled. These [redacted] should not have the ability t[redacted] any [redacted] that allow [redacted] or [redacted] to limit the ability to gain access to the system through [redacted] server.

Strengthen [redacted]

All [redacted] systems should reside in ar[redacted] The systems in this network should have access [redacted] that are [redacted] No access to [redacted] should be allowed from these systems. The systems should also be provided acces[redacted] those [redacted] required to function.

Improve [redacted] configuration of security tools

The security tools in place should be evaluated to determine if they are working effectively in the BLM environment. These systems should be replaced or appropriate changes made to improve [redacted]

Strategic Recommendations and Best Practices

In addition to the tactical recommendations set out in the above section, it is recommended that the following strategic recommendations be considered also. Many of these may already be in place.

Incorporate Security into Application Development Cycle

Security must be incorporated into the application development cycle to help reduce application security vulnerabilities. Security input should be provided in the requirements phase. Security standards and coding practices should be incorporated into the development process. Quality assurance testing should also perform basic security testing using security tools to catch common security vulnerabilities. Finally, an application security assessment should be performed by security professionals to identify any hidden vulnerabilities before a critical application is exposed to the public.

Conduct Regular Network Audits and Regular Penetration Tests

Information systems are always in flux with new attacks being discovered every day. Without auditing, it is not possible to objectively determine what the current state of security is. A penetration test can assist with a view of the network as seen by an attacker. Formal onsite assessments can provide a view of system security from an insider's perspective. This can greatly assist in obtaining true defense in depth.

Implement [redacted]

[redacted] is a critical part of any successful security policy. Were the [redacted] Were appropriate actions taken? If this test did not result in a security "fire-drill" consider conducting one. ISS recommends that BLM deploy [redacted] and [redacted] where lacking to minimize exposure to current and unknown threats. BLM should also evaluate if it is in its interests to manage its own [redacted] or if it should be outsourced to a Managed Service Services (MSS) organization.

Always adopt a "defense in depth" Security Strategy

Employ a multi-layer "defense in depth" approach to security:

- **Perimeter** access control such as firewalls, routers, and VPN technology
- **Network** Intrusion Protection Systems (IPS) on both external and internal networks.
- **Host** Intrusion Protection for critical servers and applications. Hardened Operating systems.
- **Application** security such as access control lists and user credentials.
- **Data** level security such as compartmentalization, encryption, and classification.

Adopt Risk Management Approach

Using a risk management approach ensures that BLM is making the best business decisions about security. In a nutshell, risk management involves:

- Ranking information assets by value
- Ranking the probability of threats for each asset
- Evaluating the countermeasures for each threat
- Deciding how to handle the risk from each threat
  - Reduce the risk by applying countermeasures
  - Transfer the risk by purchasing insurance
  - Accept the risk (i.e. put the annual loss estimate for the risk in the budget)

Formal Security Policy Development

Employ and enforce a security policy that educates all levels of the organization on expectations and responsibilities with respect to security. This policy should address issues such as anti-virus protection, Intrusion Protection and acceptable use.

[redacted]

INTERNET SECURITY SYSTEMS™

X-Force Professional Security Services

Technical Report for

[redacted] Test

Prepared by:
X-Force Professional Security Services

Testing conducted February/March 2005

For
DOI Office of Inspector General

Sites assessed in this report:
- DOI Bureau of Land Management

The Power to Protect

www.iss.net

Confidentiality

This document contains company confidential information of a proprietary and sensitive nature. As such this document should be afforded the security and handling precautions that a confidential document warrants. This document should have a controlled distribution to relevant parties only, and should not be copied without written permission.

ISS treats the contents of a security audit as company confidential material, and will not disclose the contents of this document to anyone without written permission.

Version Control

	Department of Interior Office of Inspector General
	Roger Mahach
	FINAL-02
	Scott Miles
	Don Pollicino
	Department of Interior ISS File
	ISS and DOI Confidential

Table of Contents

List of Figures

Document Organization

This document is organized into sections that follow the three major phases of testing.

- The *Executive Summary* provides an overview of the testing conducted and a summary of the vulnerabilities and impact to the environment.
- The *Reconnaissance* section outlines the information gathered about the target environment such as active devices, types of software in place, and the configuration of mail and web servers.
- The *Vulnerability* section provides full details on each vulnerability identified, along with a description, the systems affected, an assessment of impact, likelihood, and risk, and specific recommendations for addressing the vulnerability.
- The *Penetration* section provides a narrative explaining how many of the vulnerabilities are found, exploited, and used together to gain access to the environment.

Each vulnerability is referenced in this report with a unique number, followed by "H", "M", or "L" indicating a "high", "medium", or "low" risk issue. The numbering simply reflects the order the vulnerabilities appear in the report and is provided to allow items to be easily referenced within the report. Each vulnerability and instance is also assigned a unique vulnerability key for external tracking.

Executive Summary

This report documents the findings of a Penetration Test conducted by Internet Security Systems (ISS) on a portion of the Department of Interior (DOI) network as part of an ongoing project to evaluate the security of each of the DOI bureaus.

Scope of Testing

Bureau/Office Tested

This test was conducted against networks belonging to the Bureau of Land Management ("BLM"). The DOI Office of Inspector General (OIG) authorized ISS to perform an external penetration test on BLM networks to ascertain potential security weaknesses of network devices and hosts.

Dates of Testing

The assessment was conducted remotely [redacted] from February 21st through March 11th 2005. Documentation and some additional validation of testing results were performed through March 31st, 2005.

Address Ranges

The IP addresses provided to ISS from OIG for the engagement are defined as follows:

Figure 1: Target address ranges provided by OIG

Registered Organization Name (from ARIN)	Network Range
US DOI Bureau of Land Management (Denver, CO)	[redacted]

The [redacted] publicly accessible Internet resource was also checked for other BLM networks. The networks in Figure 2 are also registered to BLM and were approved for inclusion in the testing scope.

Figure 2: BLM address ranges found in Internet registries

Registered Organization Name (from ARIN)	Network Range
BUREAU LAND MANAGEMENT (Springfield, VA)	[redacted]
Bureau of Land Management (Denver, CO)	
Bureau of Land Management (Portland, OR)	
US DOI Bureau of Land Management (Denver, CO)	
Bureau of Land Management (Denver, CO)	
Bureau of Land Management (Santa Fe, NM)	
Bureau of Land Management / National Interagency (Boise, ID)	

Testing Methodology

[redacted]

Only the primary contact at the DOI was informed of the exact start date and targets. No one at BLM was informed of testing in order to more closely mimic real attack activity and to evaluate response mechanisms.

Testing was divided into three phases:

- ***Network Reconnaissance*** was performed in order to gain a better knowledge of the network that was being tested. This includes [redacted] ns and probes o[redacted] nd other Internet services to determine potential targets.
- ***Vulnerability Identification*** was initiated with all the hosts that were discovered in the previous phase. This consists of scanning with [redacted]
- ***Validation and Exploitation*** of the discovered vulnerabilities was attempted. This consists primarily of manual review of all vulnerability data, validating vulnerabilities by exploiting them, and combining data and vulnerabilities to penetrate the target networks.

Summary of Findings

Some significant vulnerabilities were found that allow penetration into BLM networks or allow unauthorized access to information. The environment exhibits some good security practices and controls that can help mitigate the effect of vulnerabilities, but is still at a significant risk of system compromise or access to unauthorized data as a result of the issues identified.

Risk Rating: High Risk

Security Impact

ISS was able to penetrate the tested environment in multiple ways.

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

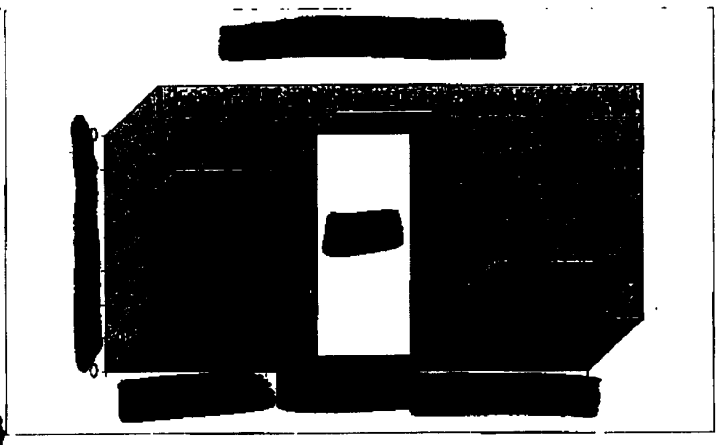
[redacted]

The Internet-accessible systems were configured with some attention paid to security, although there appear to be significant weaknesses in the overall security architecture. There is evidence of [redacted] with only those systems intended for public access directly accessible from the Internet. The systems that were compromised exhibited some good security practices such as [redacted] many common vulnerabilities and reduce the impact of identified vulnerabilities.

[redacted]

Active Services

The bureau tested consists o network ranges. The largest of these is an internal network range that is not directly connected to the Internet. The remainin networks cover roughly possible devices. A total o active devices were found, allowing connections on different active services. Of the services found, most are common services such as and rvers that are intended to be Internet accessible. Of the active device re found to have some degree of vulnerability. This is a relatively small number of hosts and services for such a large organization. Each additional system or service does represent one more potential avenue of attack, however, so keeping this footprint small and further reducing sure is recommended.



Summary of Vulnerabilities

Inappropriate access controls o BLM makes use of a server that handles requests and passes the request on to the appropriate server. This an be used to access some servers such as the server that should not be accessible [Reference: 1H

The access control d be reviewed to ensure access is only allowed from to appropriat

pplications. The rver contains a tility for sending comments This program is vulnerable to a Specially formatted input can manipulate the program into on th server. This vulnerability was used to penetrate the remote server and allowed many of the other vulnerabilities to be found and exploited resulting in further access to systems. [Reference: 3H. Web mmand Injection]

The utility must be modified to prevent the un by the program. Other modifications to th erver configuration should also be made to limit the

erabilities in web applications. Two separate pplications were found wit lnerabilities. An attacker can use these t the application int outside of the anticipated area. In this case, any file on the server that is readable by the server userid can be accessed This exposes sensitive system configuration files as well as application data. One vulnerability in the ed to the discovery of th ; the other in led to the discovery of a file containing system and database

passwords for every component supporting the Land and Mineral Records application. [Reference: 4H. Web directory traversal]
These applications must be modified to use appropriate functions and application input filters to prevent directory traversal issues.

[redacted] An [redacted] on the [redacted] network is accessible [redacted] Several accounts [redacted] are configured with [redacted] passwords, allowing access to the [redacted] No data was observed in the [redacted] but the [redacted] itself may be susceptible to other vulnerabilities that could be exploited once connected. This could compromise other data on the system and potentially provide a route into the [redacted] [Reference: 2H. [redacted]
All [redacted] passwords must be changed to comply with BLM/DOI password standards. This system should be further restricted so that it is not reachable by any [redacted]

[redacted] **vulnerabilities in [redacted] applications.** At leas[redacted] are vulnerable to [redacted] This allows modification of the [redacted] ent to the [redacted] from the [redacted] This vulnerability can often be used to access or modify data in the [redacted] manipulate application logic, or gain access to the server hosting the database. Manipulation of [redacted] was accomplished during testing, allowing access to arbitrary data [redacted] and bypassing a [redacted] login on another, but no significant access or sensitive data was observed. [Reference: 1M. [redacted] Injection affects database-backed applications]
The [redacted] applications must be modified to prevent SQL injection attacks. Security monitoring can also help identify and prevent some of these vulnerabilities.

Web software configurations introduce vulnerabilities. [redacted] is an application server that provides a framework for applications on a [redacted] rver. The configuration of [redacted] on this server provides programs with excessive access to the underlying operating system. The access controls or [redacted] on the [redacted] web servers can also lead to them being used to run commands on the server. [Reference: 5M. Writable web [redacted] directory; 8M. [redacted] cripts allowed excessive permissions]
Changes should be made to the [redacted] servers and [redacted] configurations to limit the potential for exploitation.

[redacted] ISS did not observe [redacted] controls that limited th[redacted] hat could be [redacted] as obtained to the [redacted] or [redacted] t also appears that many of the [redacted] do not reside in a single [redacted] but instead reside in locations inside the [redacted] that are simpl[redacted] by the [redacted] [References: 1H. Reverse [redacted] lows access to internal web servers; Web server provides access to internal systems; Numerous BLM systems accessed using web server and compromised passwords]
BLM should review the systems processing [redacted] equests and ensure that each such system is sufficiently [redacted] from the [redacted] ork to mitigate the effects should the system be compromised.

[redacted] **encryption.** The [redacted] servers allow [redacted] for [redacted] Many of these passwords [redacted] viding a list of userids

and passwords that can be used to acces[redacted]rvers. None of the BLM[redacted]rvers are accessible from [redacted]ng [redacted] limiting the exposure of this issue. However, the [redacted] can be used to access [redacted] servers accessible on the [redacted] It is also assumed that [redacted] could be used to access other [redacted] servers that are reachable [redacted] [Reference: 6M[redacted]

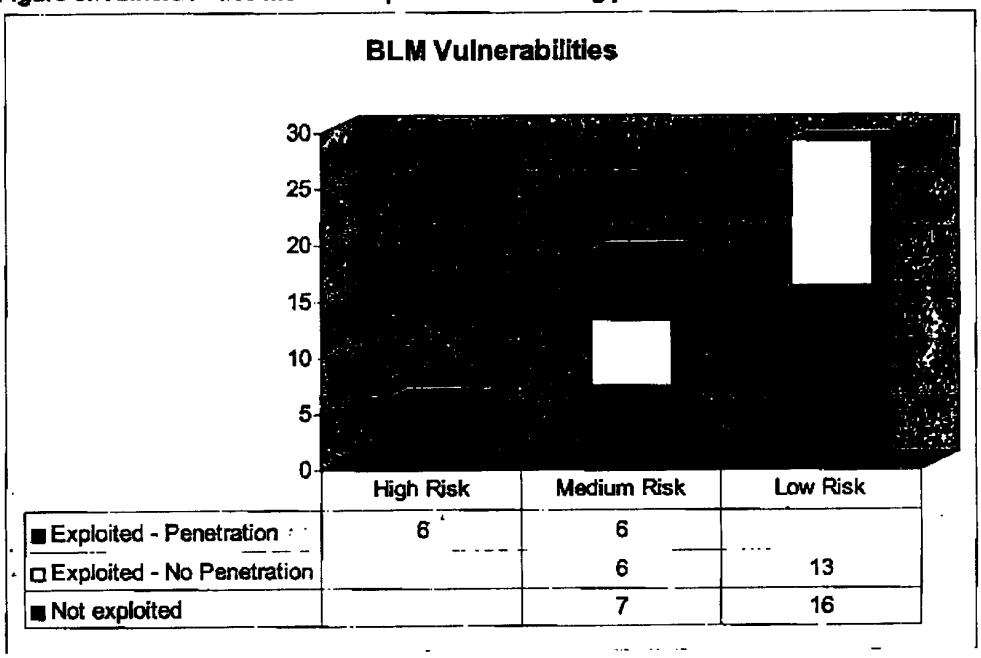
The [redacted]d [redacted] should be migrated to the stronger [redacted] encryption algorithm.

Other medium and low-risk vulnerabilities also identified that can be used to [redacted]ne [redacted]o [redacted] that may be useful when carrying out other attacks. These vulnerabilities should also be addressed by making the recommended changes.

Risk/Vulnerability Metrics

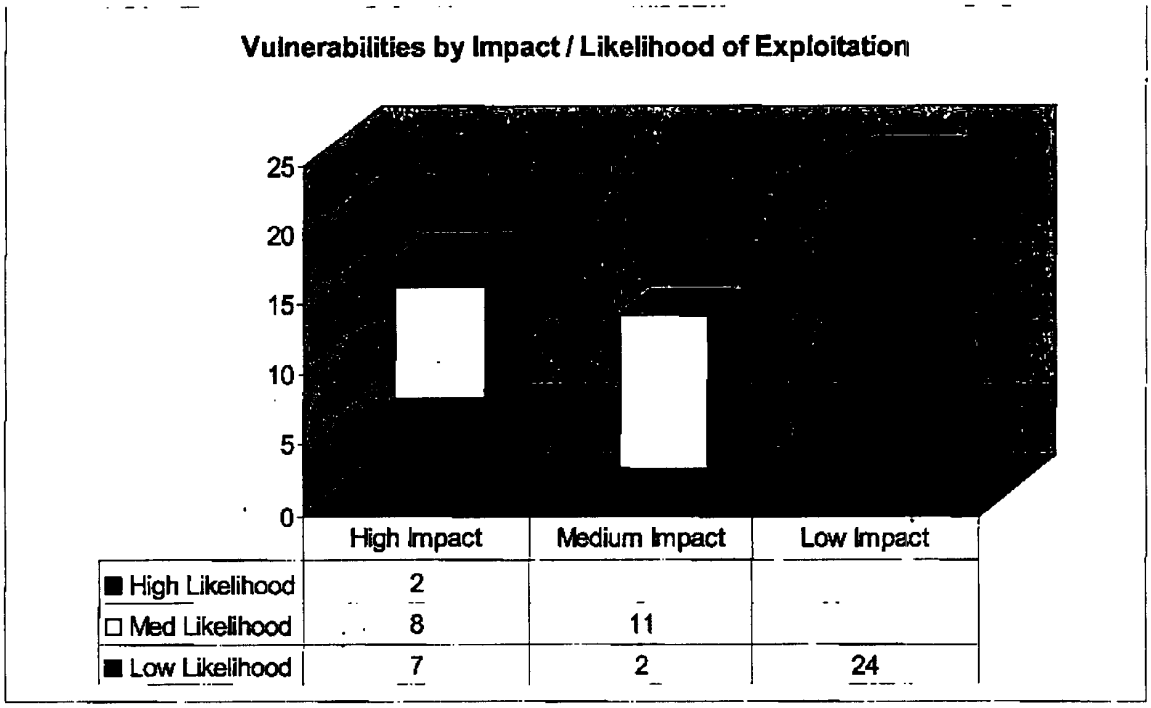
A total of 12 vulnerability instances resulted in penetration as defined in the Rules of Engagement. Nineteen other medium and low-risk vulnerabilities were exploited to gain access to some type of information or resource, but did not result in penetration. Twenty three other medium and low-risk vulnerabilities were not exploited. The vulnerabilities that were not exploited were [redacted]nerabilities such as [redacted] that were already demonstrated, [redacted] vulnerabilities, and vulnerabilities for which there are currently no publicly available programs or information on how to exploit the issue.

Figure 3: Vulnerabilities metrics: exploited and allowing penetration



As indicated above, only 6 vulnerabilities classified as "high risk" were identified, with another 19 classified as "medium risk" and 29 as "low risk". The determination of risk is based on the potential impact of the vulnerability combined with the likelihood that the vulnerability could be exploited. Viewed solely by potential impact, there are 17 high impact vulnerabilities, but many of these have a medium to low likelihood of exploitation that result in a lower overall risk for the vulnerability. This is because many of these vulnerabilities are only exploitable once some level of access has been obtained to the target environment. Most medium and low-risk vulnerabilities are not exploited unless there is a need for additional information about the system or network being attacked, since these vulnerabilities tend to be informational in nature.

Figure 4: Vulnerability metrics: by potential impact & likelihood

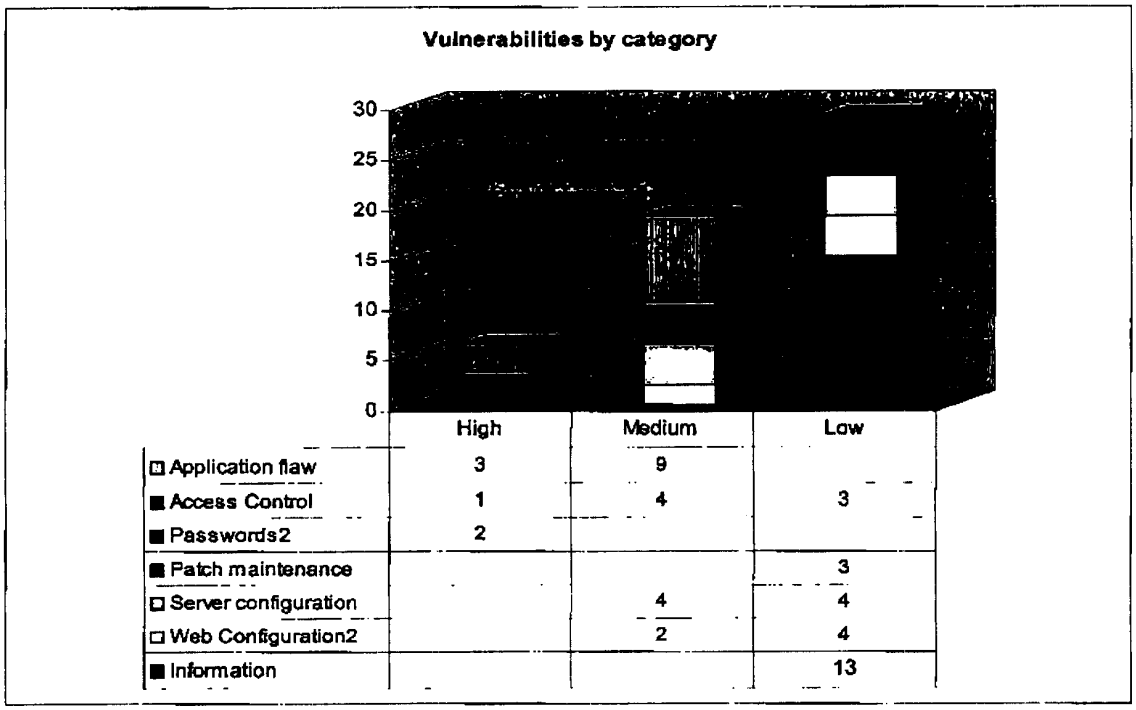


Each vulnerability was categorized into the following root causes:

- **Access control**: The vulnerability is a result of inappropriate access controls.
- **Application flaw**: The vulnerability is a result of a flaw in a custom application.
- **Passwords**: System, application, or other passwords are easily discovered or guessed.
- **Patch maintenance**: The vulnerability is fixed by a software patch or a newer version of software, but which is not applied.
- **Server configuration**: The operating system is not secured or is configured in such a way that allows the vulnerability.
- **Web configuration**: The web server is not secured or is configured in such a way that allows the vulnerability.
- **Unnecessary services**: The service may not be inherently vulnerable, but is exposed to the Internet when it should not be if not necessary.

The high risk issues in the environment are related to application flaws, access control, and password issues. Other medium risk issues are caused by application flaws, access control, and configuration issues as shown in Figure 5.

Figure 5: Vulnerability metrics: by category



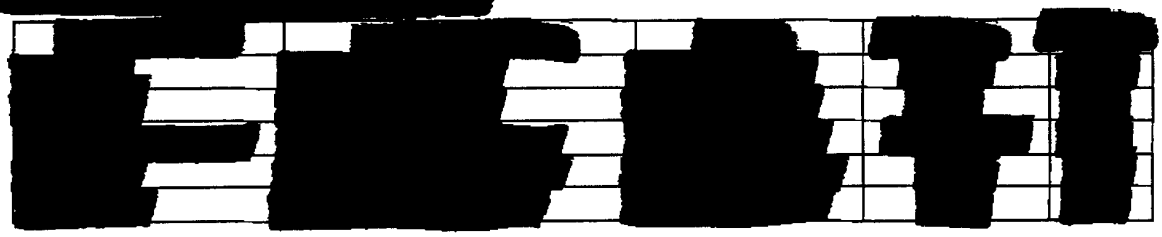
	High	Medium	Low
Application flaw	3	9	
Access Control	1	4	3
Passwords2	2		
Patch maintenance			3
Server configuration		4	4
Web Configuration2		2	4
Information			13

Relevant Standards, Federal and Departmental Guidelines

- Federal Information Security Management Act
- Inspector Generals Act
- Office of Management and Budget Circular A-130, Management of Federal Information Resources. Appendix III Management of Federal Information Resources
- General Accountability office Federal Information Systems Controls Audits Manual FISCAM
- National Institute of Standards and Technology. Special Publication 800-42, Guideline on Network Security Testing.
- Department of the Interior Network Security Policy (February 14, 2003)
- Department of the Interior, Departmental Manual Chapter 375.19, Information Technology Security Program
- SANS Top 20 Most Critical Internet Security Vulnerabilities

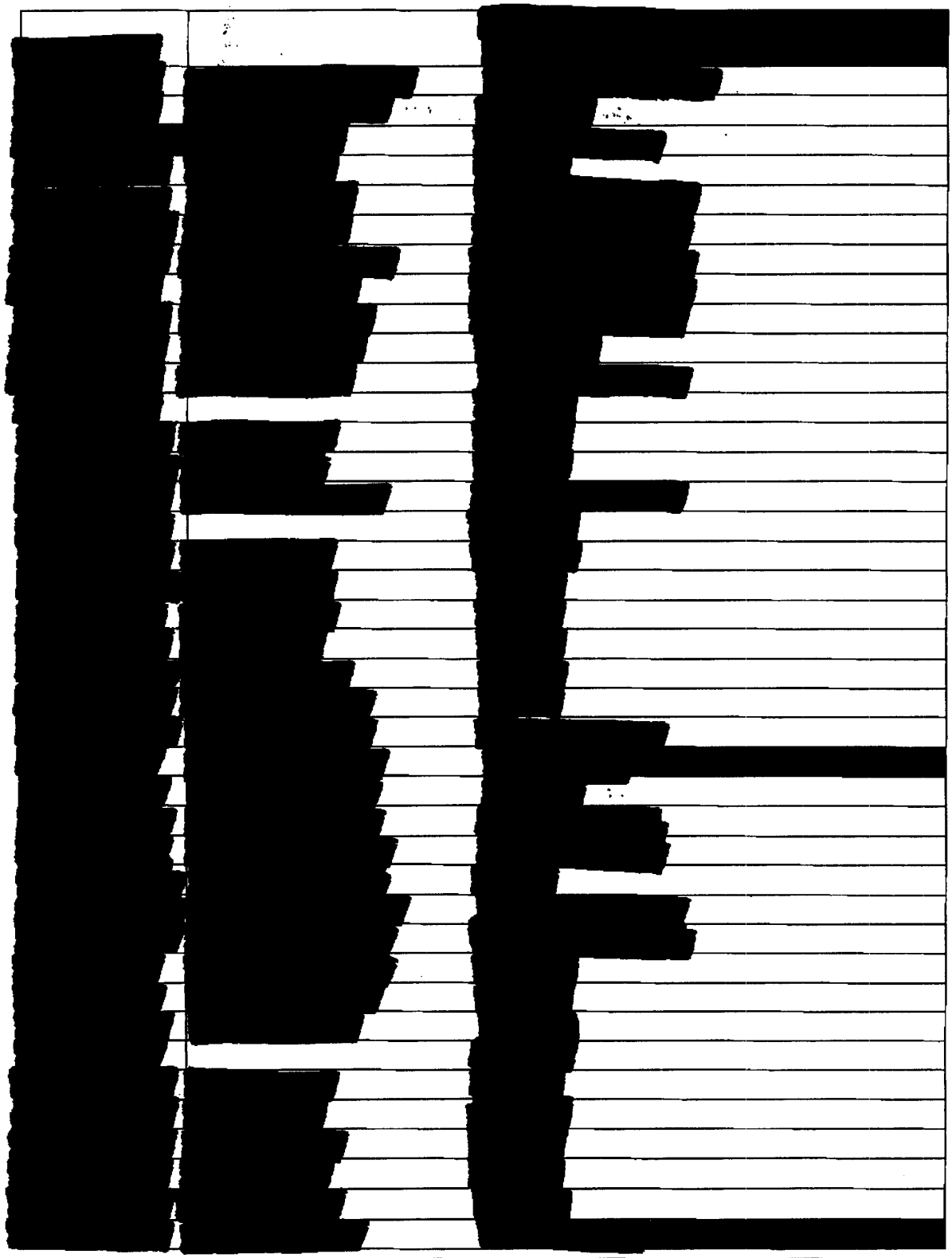
Reconnaissance Findings

[redacted]



[redacted]

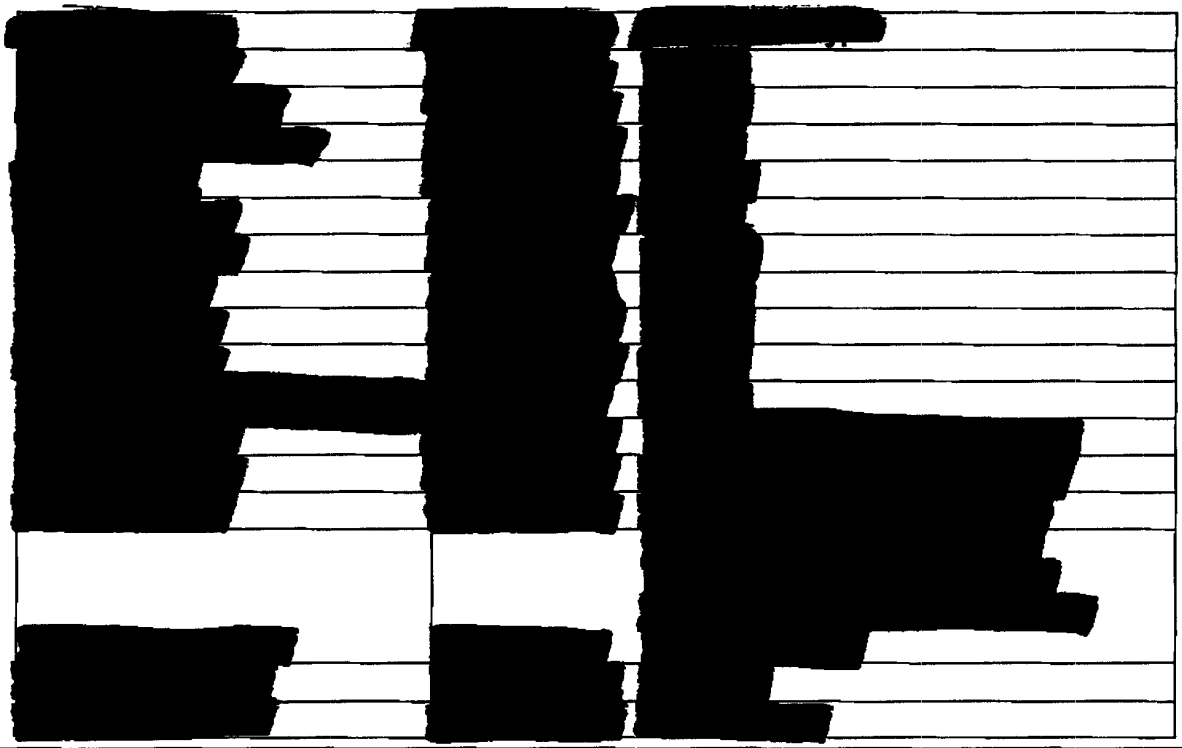
[redacted]



[redacted]

[redacted]

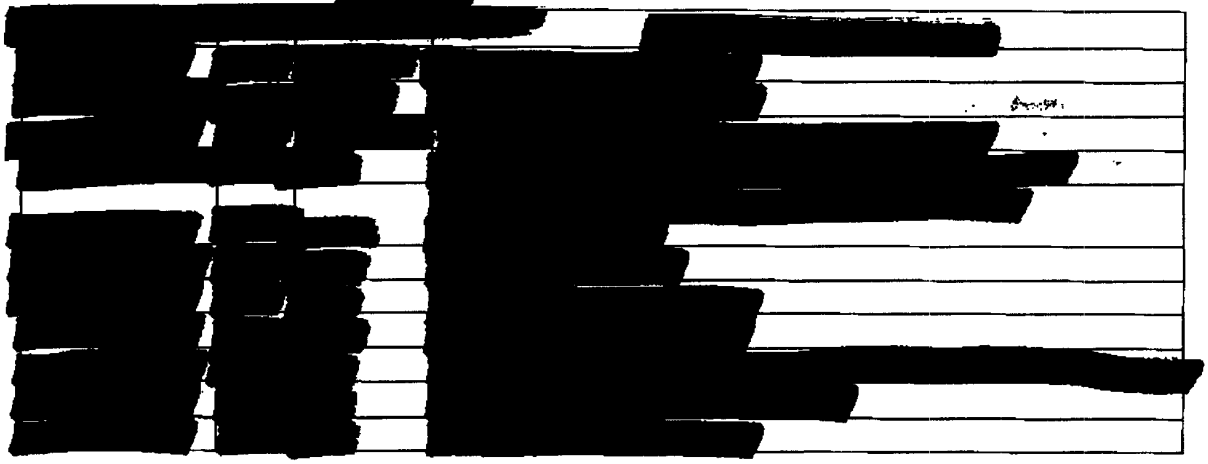
Figure 8: [redacted]

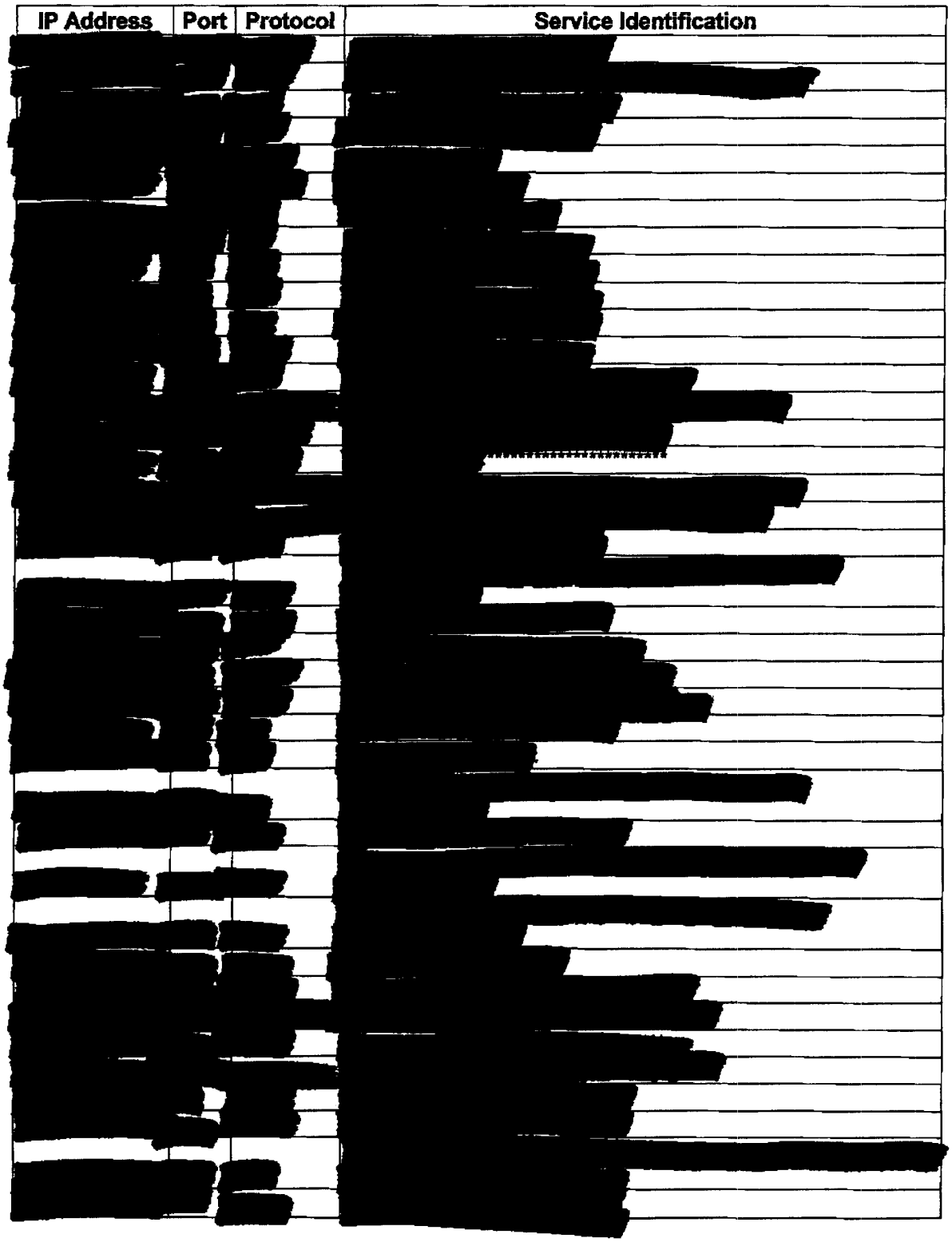


[redacted]

[redacted]

Figure 9[redacted]

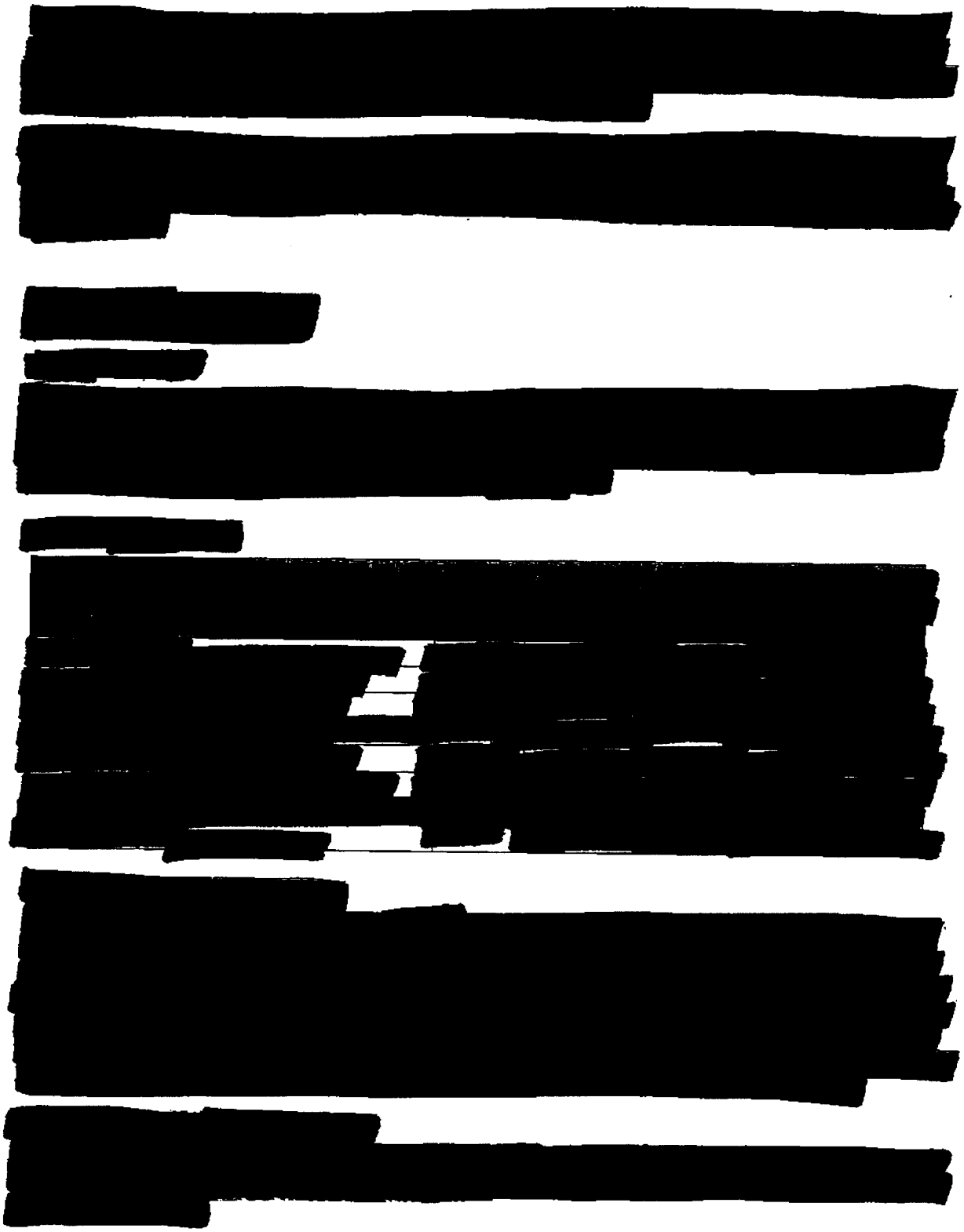


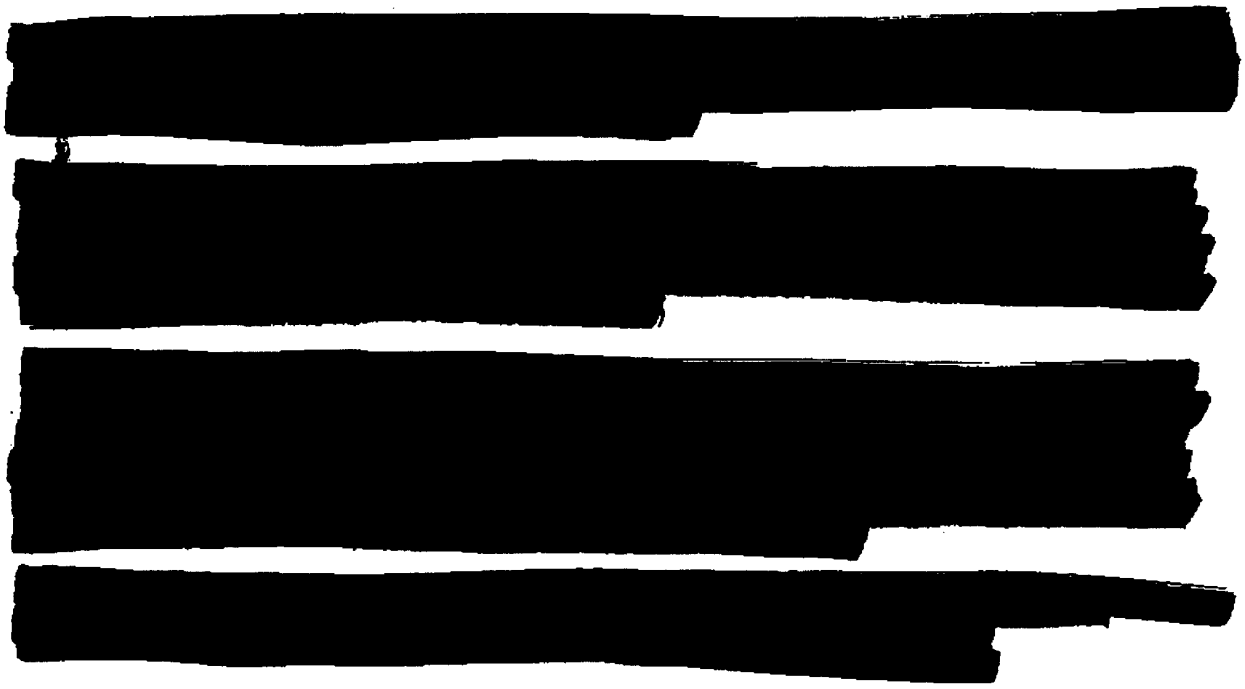


[redacted]

Address	Port	Banner				
[redacted]						

[redacted]





Vulnerability Risk Rankings

The identification and analysis of risk is carried out in accordance with the NIST 800-30 risk assessment process.

> ***Risk*** is a function of the ***likelihood*** of a given ***threat-source's*** exercising a particular potential ***vulnerability***, and the resulting ***impact*** of that adverse event on the organization or on individuals.

The penetration testing tasks are carried out to identify the threats to the environment, the potential vulnerabilities, and any mitigating controls in place. This information is then analyzed to determine the overall risk based on the likelihood and impact of each vulnerability.

Likelihood Analysis

The following governing factors are considered to derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the associated threat environment:

- Threat-source motivation and capability
- Nature of the vulnerability
- Availability of public exploit code or instructions
- Existence and effectiveness of current controls.

The likelihood that a potential vulnerability could be exercised by a given threat-source can be described as high, medium, or low. Table 1 below describes these three likelihood levels.

Table 1: Likelihood Definitions

Likelihood Level	Likelihood Definition
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Medium	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

Impact analysis

The adverse impact of a security event can be described in terms of loss or degradation of any combination of the following three security goals: integrity, availability, and confidentiality.

Table 2: Magnitude of Impact Definitions

Magnitude	Impact Definition
Low	The loss of confidentiality, integrity, or availability could be expected to have a

Magnitude	Impact Definition
	limited adverse effect on the system's operations or assets. This may cause minor degradation in capability, but the system is able to perform its primary functions. Minor but reversible damage to system assets, financial loss, or harm to individuals could occur. Exploit of such a vulnerability could lead to an attacker obtaining system statistics, user accounts, or other sensitive information that would aid in an attack.
Medium	The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on the system's operations or assets. This may cause significant degradation in capability, but the system is able to perform its primary functions. Significant but manageable damage to system assets, financial loss, or harm to individuals could occur. Exploit of such a vulnerability could allow indirect access to data and configuration files.
High	The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on the system's operations or assets. This may cause severe degradation in capability where the system is not able to perform one or more primary functions. Major damage to system assets, financial loss, or harm to individuals could occur. Exploit of such a vulnerability could provide system access, likely at the root or administrator level. System security would be fully compromised. High also includes those vulnerabilities believed to be serious enough to warrant immediate attention.

Risk Analysis

The likelihood and Impact rankings are combined to determine an overall risk analysis. In general, a 3x3 risk level matrix is utilized, although in some cases a subjective determination may be made to adjust a risk level up or down in cases where the risk is between two levels.

Table 3: Risk-Level Matrix

[redacted]	[redacted]		
	Low (10)	**Medium** (50)	**High** (100)
High (1.0)	**Low** 10 X 1.0 = 10	**Medium** 50 X 1.0 = 50	**High** 100 X 1.0 = 100
Medium (0.5)	**Low** 10 X 0.5 = 5	**Medium** 50 X 0.5 = 25	**Medium** 100 X 0.5 = 50
Low (0.1)	**Low**	**Low**	**Low**

	10 X 0.1 = 1	50 X 0.1 = 5	100 X 0.1 = 10

Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)

Table 4: Risk Scale and Necessary Actions

Risk Level	Risk Description and Necessary Actions
High	If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Medium	If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	If an observation is described as low risk, the system's authorizing official must determine whether corrective actions are still required or decide to accept the risk.

Vulnerabilities

This section identifies all of the vulnerabilities found during testing. The vulnerabilities are categorized into High, Medium, and Low-risk vulnerabilities based on the criteria described in the Vulnerability Risk Rankings section and the understanding of the environment gained during testing.

High-Risk Vulnerabilities

1H. [redacted]

Highest Risk: High

[redacted]

References: [redacted]

[redacted]

ID	Vulnerable IP	System Name	Impact	Likely	Risk
x1-1	[redacted]		High	High	[redacted]

[redacted]

Recommendation: [redacted]

[redacted]

Highest Risk: High

[redacted]

References: [redacted]

[redacted]

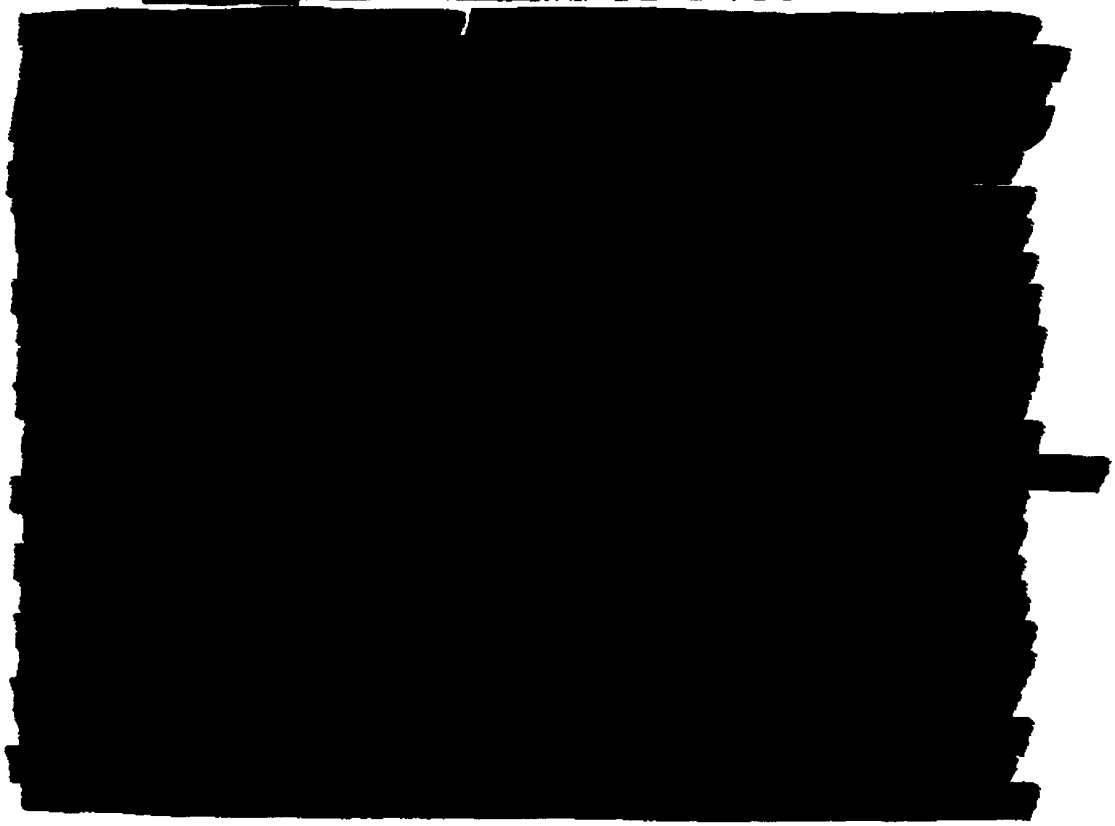
ID	Vulnerable IP	System Name	Impact	Likely	Risk
[redacted]			High	High	[redacted]

[redacted]

ID	Vulnerable IP	System Name	Impact	Likely	Risk
[redacted]			High	Medium	[redacted]

[redacted]

Figure 12: [redacted]



[redacted]

Recommendation:

[redacted]

3H. [redacted]

Highest Risk: High
Category: Application flaw
Identifier: [redacted]
References: [redacted]

[redacted]

ID	Vulnerable IP	System Name	Impact	Likely	Risk
x3-1	[redacted]	[redacted]	High	Low	[redacted]

[redacted]

[redacted]

Recommendation:

[redacted]

4H. [redacted]

Highest Risk: High
Category: Application flaw
Identifier:
References: [redacted]

[redacted]

ID	Vulnerable IP	System Name	Impact	Likely	Risk
x2-1	[redacted]	[redacted]	High	Medium	[redacted]

[redacted]

ID	Vulnerable IP	System Name	Impact	Likely	Risk
x2-2	[redacted]	[redacted]	High	Medium	[redacted]

[redacted]

[redacted]

Recommendation:

[redacted]

Medium-Risk Vulnerabilities

1M. [redacted]

Highest Risk: Medium
Category: Application flaw
Identifier: [redacted]
References: None

[redacted]

ID	Vulnerable IP	System Name	Impact	Likely	Risk
[redacted]					

[redacted]

ID	Vulnerable IP	System Name	Impact	Likely	Risk
[redacted]			Medium	Medium	Medium

[redacted]

ID	Vulnerable IP	System Name	Impact	Likely	Risk
[redacted]			High	Low	Medium

[redacted]

ID	Vulnerable IP	System Name	Impact	Likely	Risk
[redacted]			Medium	Medium	Medium
			Medium	Medium	Medium
			Medium	Medium	Medium
			Medium	Medium	Medium
			Medium	Medium	Medium
			Medium	Medium	Medium

[redacted]

[redacted]

Recommendation:

[redacted]

2M. [redacted]

Highest Risk: Medium
Category: Access control
Identifier: [redacted])
References: None

[redacted]

ID	Vulnerable IP	System Name	Impact	Likely	Risk
[redacted]			High	Medium	Medium

[redacted]

ID	Vulnerable IP	System Name	Impact	Likely	Risk
[redacted]			High	Low	Medium

[redacted]

[redacted]

ID	Vulnerable IP	System Name	Impact	Likely	Risk
[redacted]			High	Medium	Medium

[redacted]

ID	Vulnerable IP	System Name	Impact	Likely	Risk
[redacted]			[redacted]ow	Low	[redacted]
			[redacted]edium	Low	
			[redacted]Medium	Low	

[redacted]

Recommendation:

[redacted]

3M. [redacted]

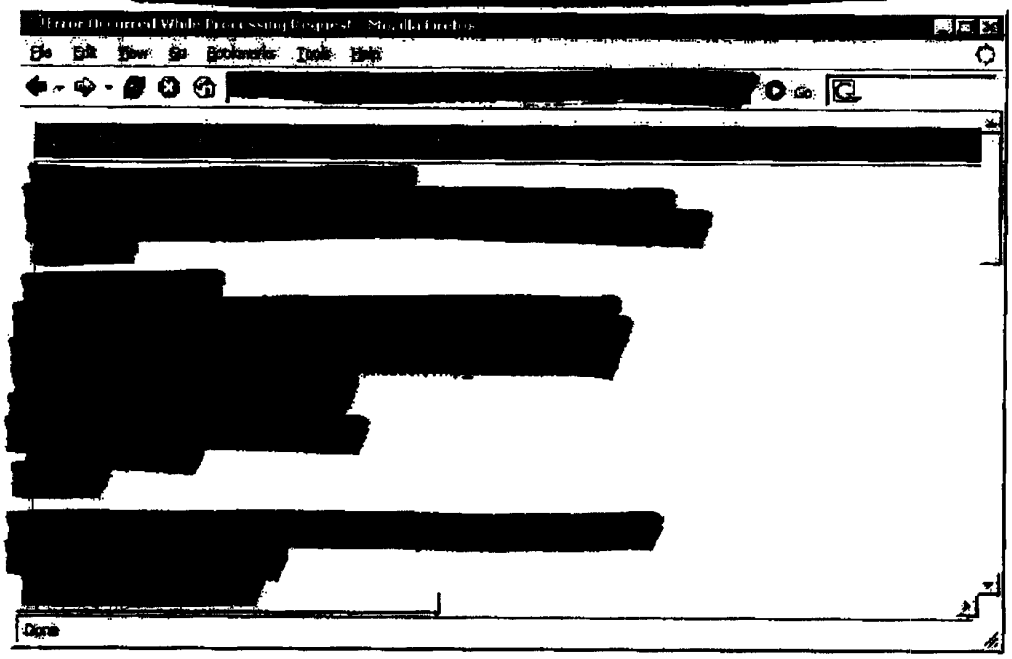
Highest Risk: Medium
Category: Web Configuration
Identifier: [redacted]
References: None

[redacted]

ID	Vulnerable IP	System Name	Impact	Likely	Risk
[redacted]			Medium	Medium	Medium

[redacted]

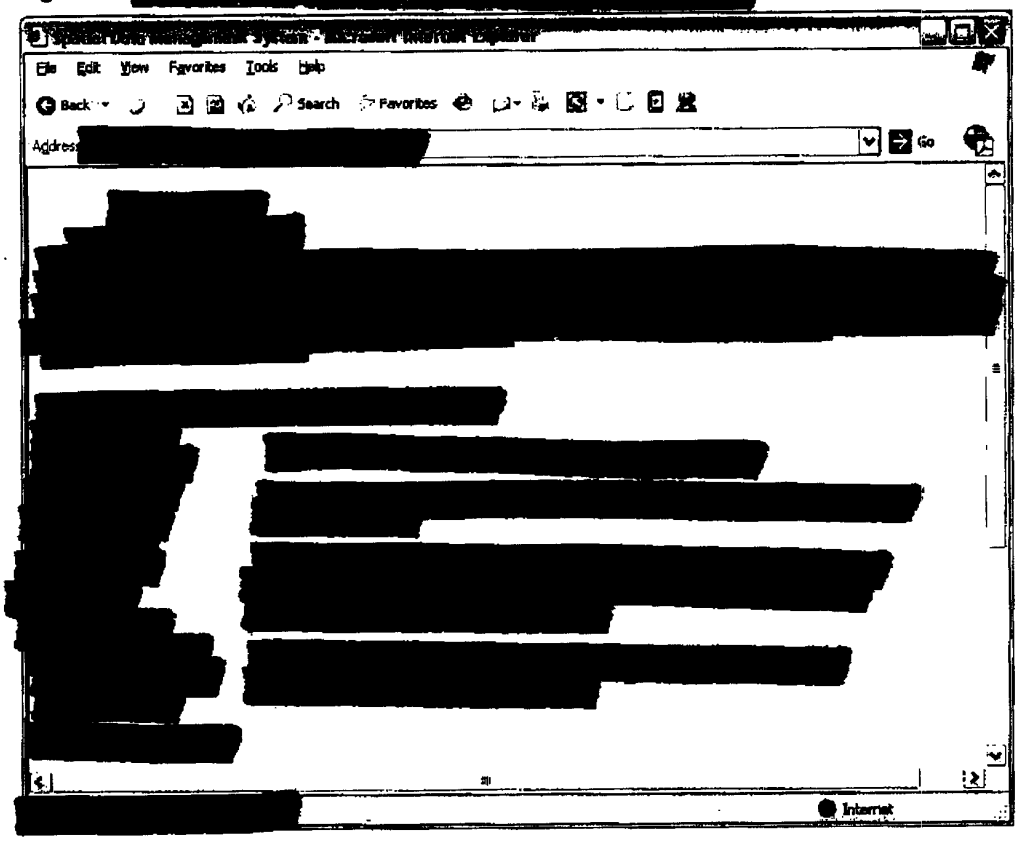
Figure 13: [redacted]



ID	Vulnerable IP	System Name	Impact	Likely	Risk
[redacted]			Medium	Medium	Medium

[redacted]

Figure 14: [redacted]



Recommendation: [redacted]

4M. [redacted]

Highest Risk: Medium
Category: OS configuration
Identifier: [redacted]
References: [redacted]

[redacted]

[redacted]

ID	Vulnerable IP	System Name	Impact	Likely	Risk
[redacted]			High	Low	Medium

[redacted]

Recommendation:

[redacted]

5M. [redacted]

Highest Risk: Medium
Category: Access Controls
Identifier: [redacted]
References: [redacted]

[redacted]

ID	Vulnerable IP	System Name	Impact	Likely	Risk
[redacted]			High	Low	Medium

[redacted]

Recommendation:

[redacted]

6M. [redacted]

Highest Risk: Medium
Category: OS configuration
Identifier: [redacted]
References: None

[redacted]

ID	Vulnerable IP	System Name	Impact	Likely	Risk
[redacted]			Medium	Medium	Medium

[redacted]

Database	Database Name	[redacted]
[redacted]		

[redacted]

Recommendation:

[redacted]

7M. [redacted]

Highest Risk: Medium
Category: Access Control
Identifier: [redacted]

References: [redacted]

[redacted]

ID	Vulnerable	System Name	Impact	Likely	Risk
[redacted]			Medium	Medium	Medium

[redacted]

Recommendation: [redacted]

8M. [redacted]

Highest Risk: Low
Category: Server configuration
Identifier: [redacted]
References: [redacted]

[redacted]

ID	Vulnerable IP	System Name	Impact	Likely	Risk
[redacted]			High	Medium	Medium

[redacted]

Recommendation: [redacted]

[redacted]

Low-Risk Vulnerabilities

1L. [redacted]

Highest Risk: Low
Category: OS configuration
Identifier: [redacted]
References: [redacted]

[redacted]

ID	Vulnerable IP	System Name	Impact	Likely	Risk
[redacted]			Low	Low	[redacted]

[redacted]

Recommendation: [redacted]

2L. [redacted]

Highest Risk:
Category: Patch maintenance
Identifier: [redacted]
References: [redacted]

[redacted]

[redacted]

ID	Vulnerable IP	System Name	Impact	Likely	Risk
[redacted]			High	Low	[redacted]

[redacted]

Recommendation:

[redacted]

3L. [redacted]

Highest Risk: Low
Category: Patch maintenance
Identifier: [redacted]
References: [redacted]

[redacted]

ID	Vulnerable IP	System Name	Impact	Likely	Risk
[redacted]				LOW	[redacted]

[redacted]

Recommendation:

[redacted]

4L. [redacted]

Highest Risk: Low
Category: Patch maintenance
Identifier: [redacted]
References: [redacted]

[redacted]

ID	Vulnerable IP	System Name	Impact	Likely	Risk
[redacted]			High	Low	[redacted]

[redacted]

Recommendation: [redacted]

5L. [redacted]

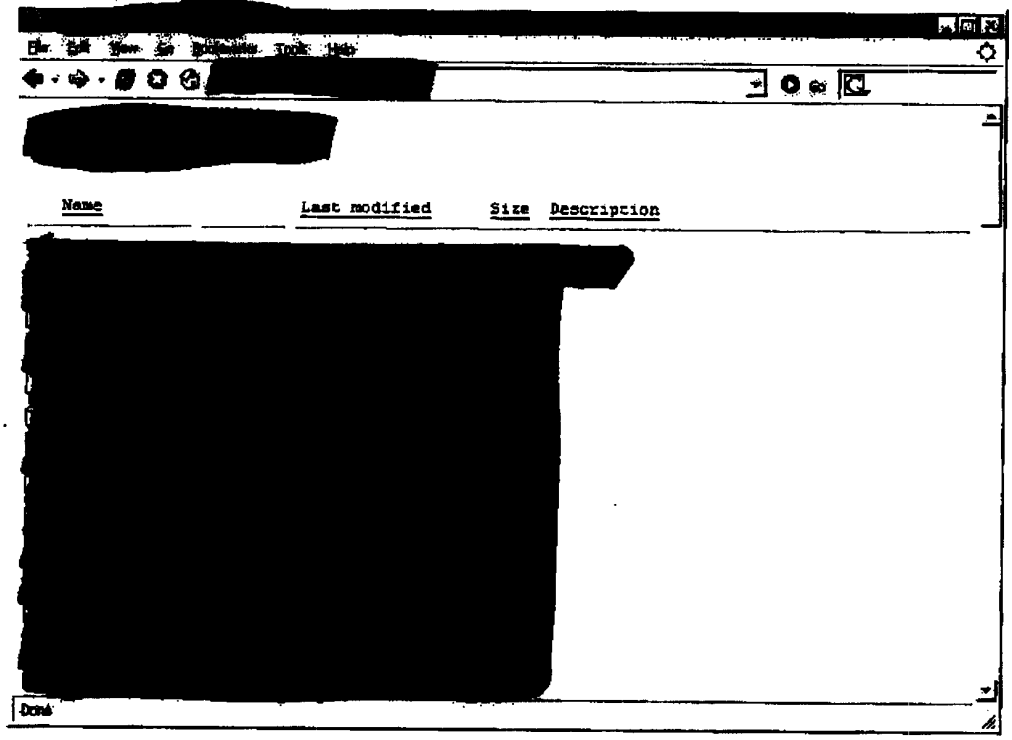
Highest Risk: Low
Category: Web server configuration
Identifier: [redacted]
References: [redacted]

[redacted]

ID	Vulnerable IP	System Name	Impact	Likely	Risk
[redacted]			Low	Low	[redacted]

[redacted]

Figure 15: [redacted]



Recommendation: [redacted]

6L. [redacted]

Highest Risk: Low
Category: Configuration
Identifier: [redacted]
References: [redacted]

ID	Vulnerable IP	System Name	Impact	Likely	Risk
[redacted]			Low	Low	[redacted]

[redacted]

- [redacted]

Recommendation: [redacted]

7L. [redacted]

Highest Risk: Low
Category: Configuration
Identifier: [redacted]
References: [redacted]

ID	Vulnerable IP	System Name	Impact	Likely	Risk
[redacted]			Low	Low	[redacted]

[redacted]

Recommendation: [redacted]

8L. [redacted]

Highest Risk: Low
Category: Unnecessary services
Identifier:
References: [redacted]

[redacted]

ID	Vulnerable IP	System Name	Impact	Likely	Risk
[redacted]			Low	Low	[redacted]
			Low	Low	

[redacted]

Recommendation:
[redacted]

9L. [redacted]

Highest Risk: Low
Category: OS configuration
Identifier:
References: [redacted]

[redacted]

ID	Vulnerable IP	System Name	Impact	Likely	Risk
[redacted]			Low	Medium	[redacted]

[redacted]

Recommendation:

[redacted]

10L. [redacted]

Highest Risk: Low
Category: Web server configuration
Identifier: [redacted]
References: [redacted]

[redacted]

ID	Vulnerable IP	System Name	Impact	Likely	Risk
[redacted]			Low	Low	[redacted]
			Low	Low	
				Low	

[redacted]

Recommendation:

[redacted]

11L. [redacted]

Highest Risk: Low
Category: Information
Identifier: [redacted]
References: [redacted]

[redacted]

ID	Vulnerable IP	System Name	Impact	Likely	Risk
[redacted]			Low	Low	[redacted]
			Low	Low	
			Low	Low	
			Low	Low	
			Low	Low	
			Low	Low	
			Low	Low	
			Low	Low	
			Low	Low	
			Low	Low	
			Low	Low	
			Low	Low	
			Low	Low	

[redacted]

Recommendation:

[redacted]

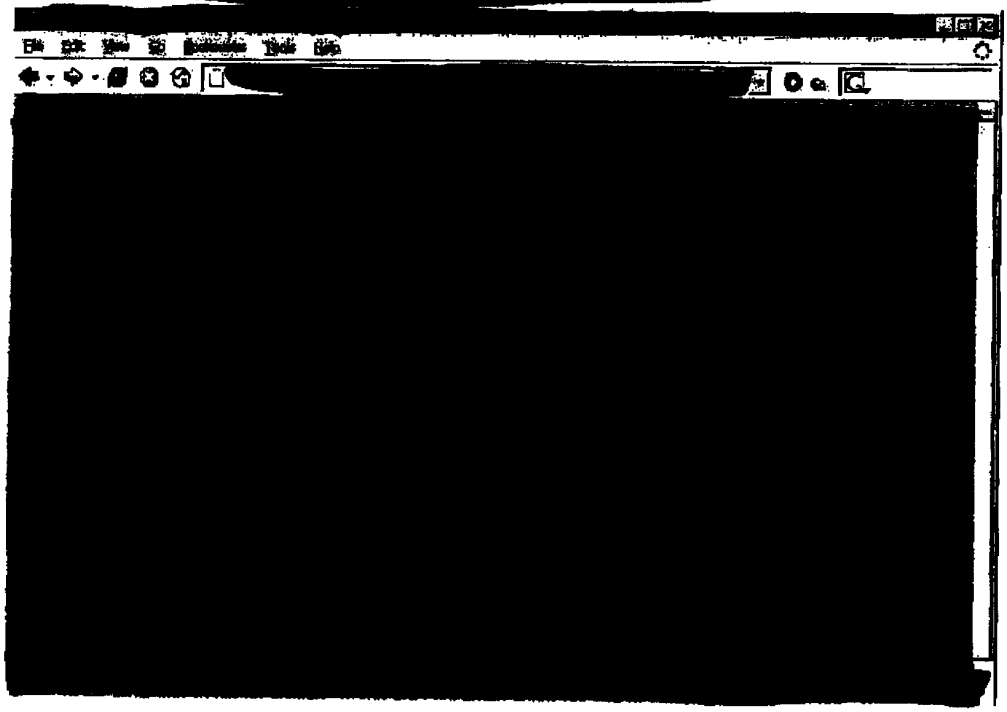
Penetration

[redacted]

Initial view of the BLM network

[redacted]

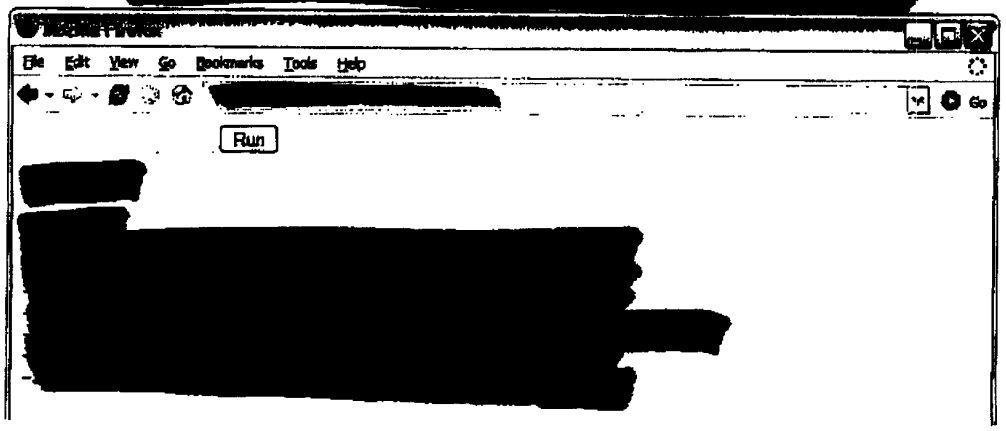
Figure 16: [redacted]

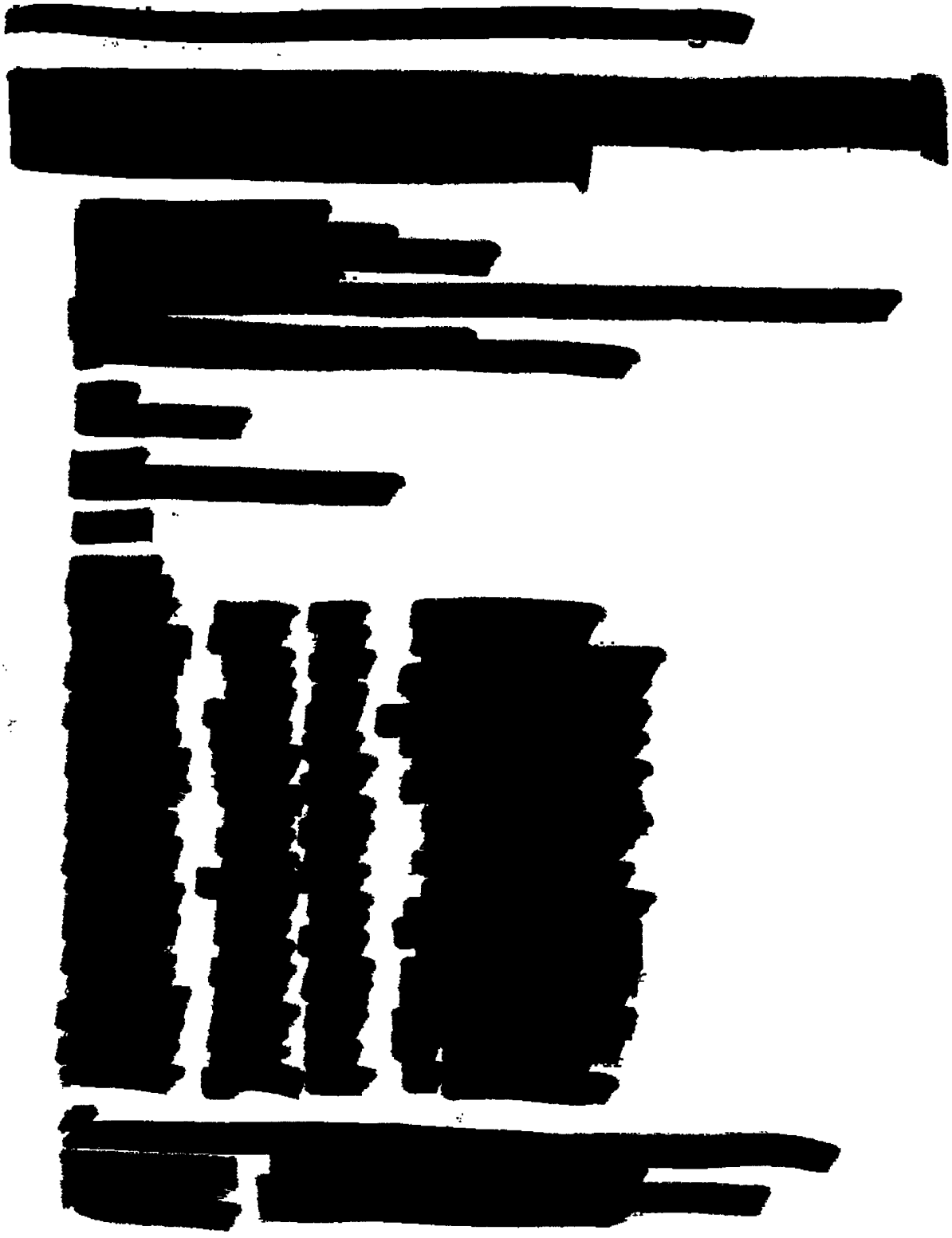


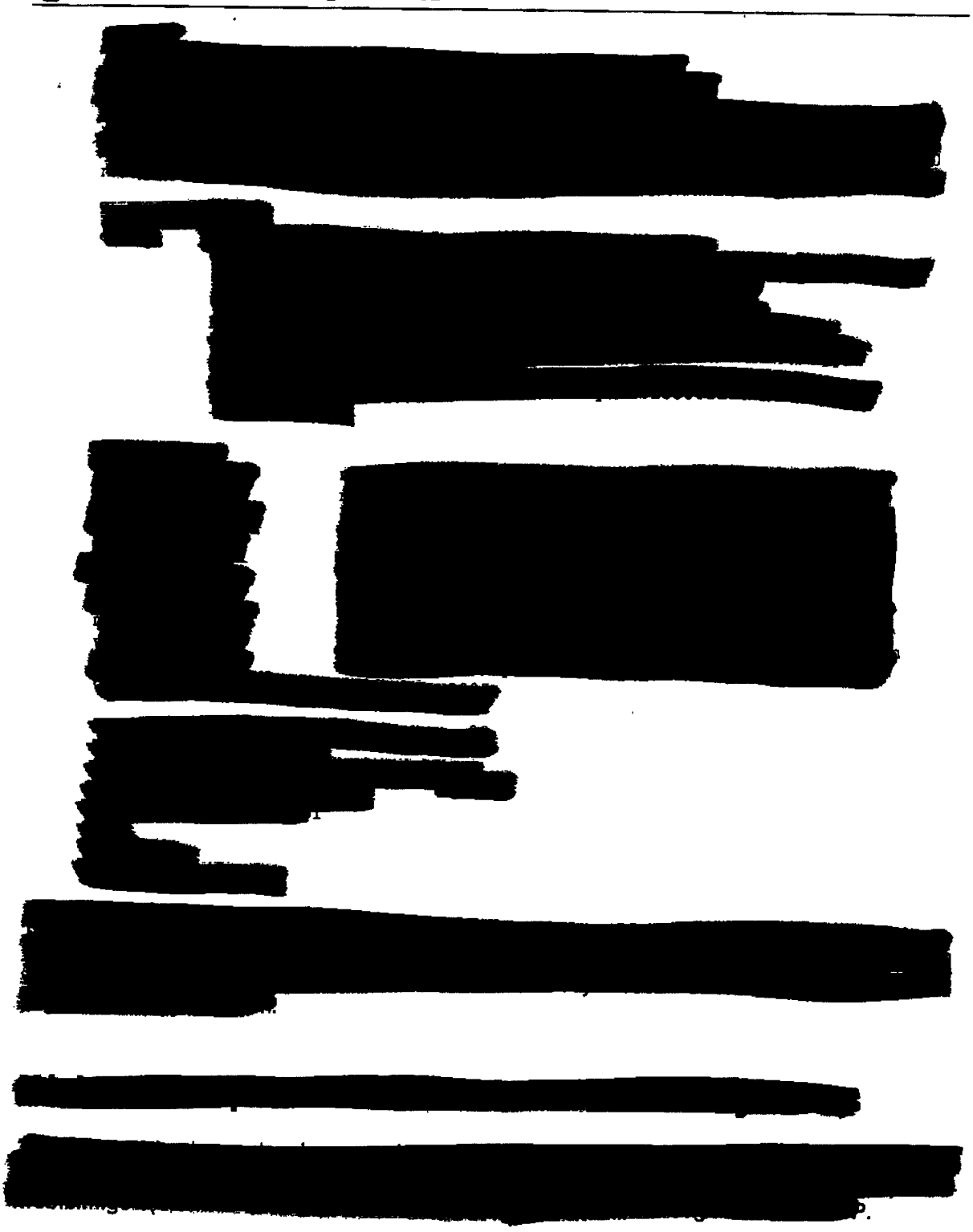
[redacted]

[redacted]

Figure 17: [redacted]







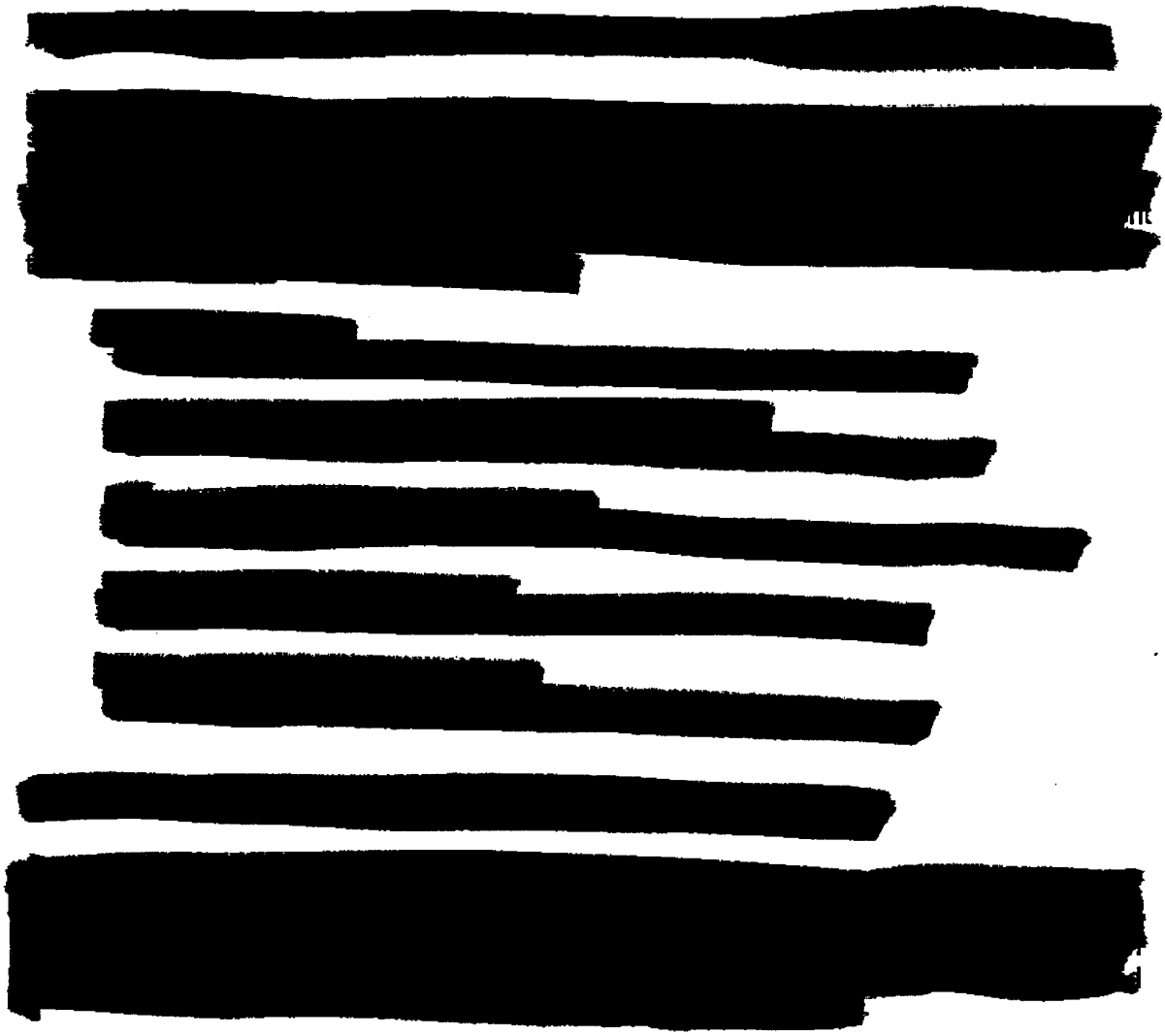
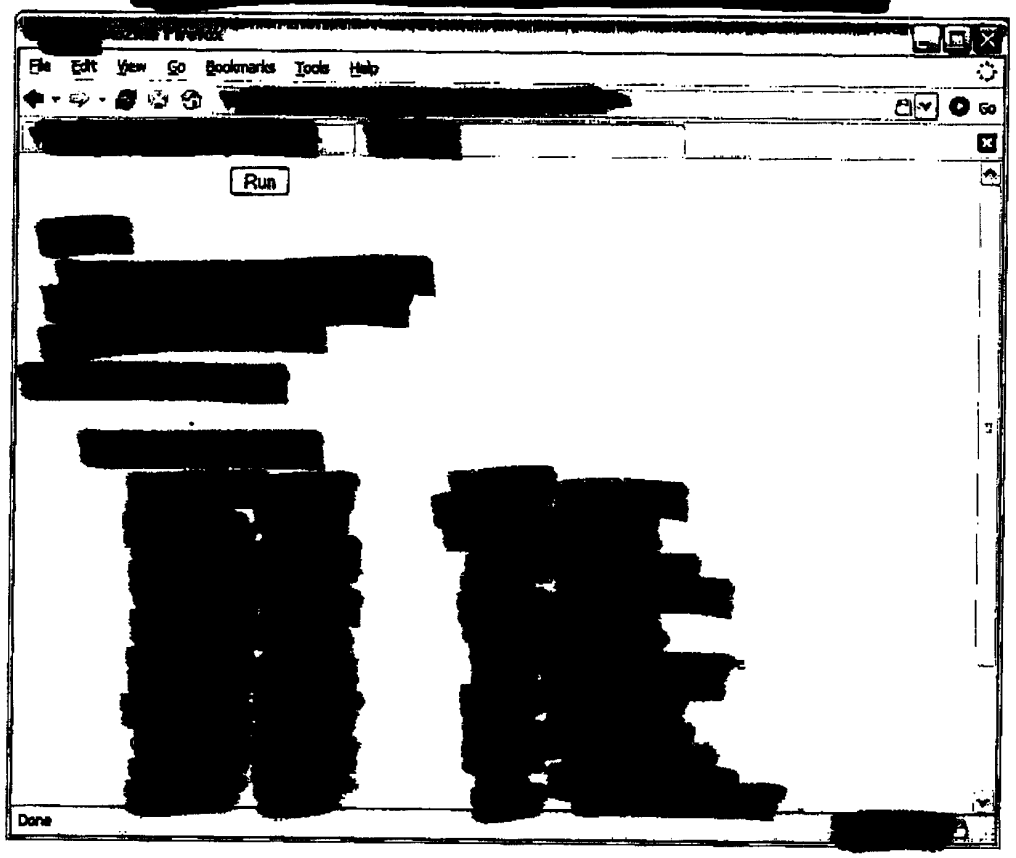
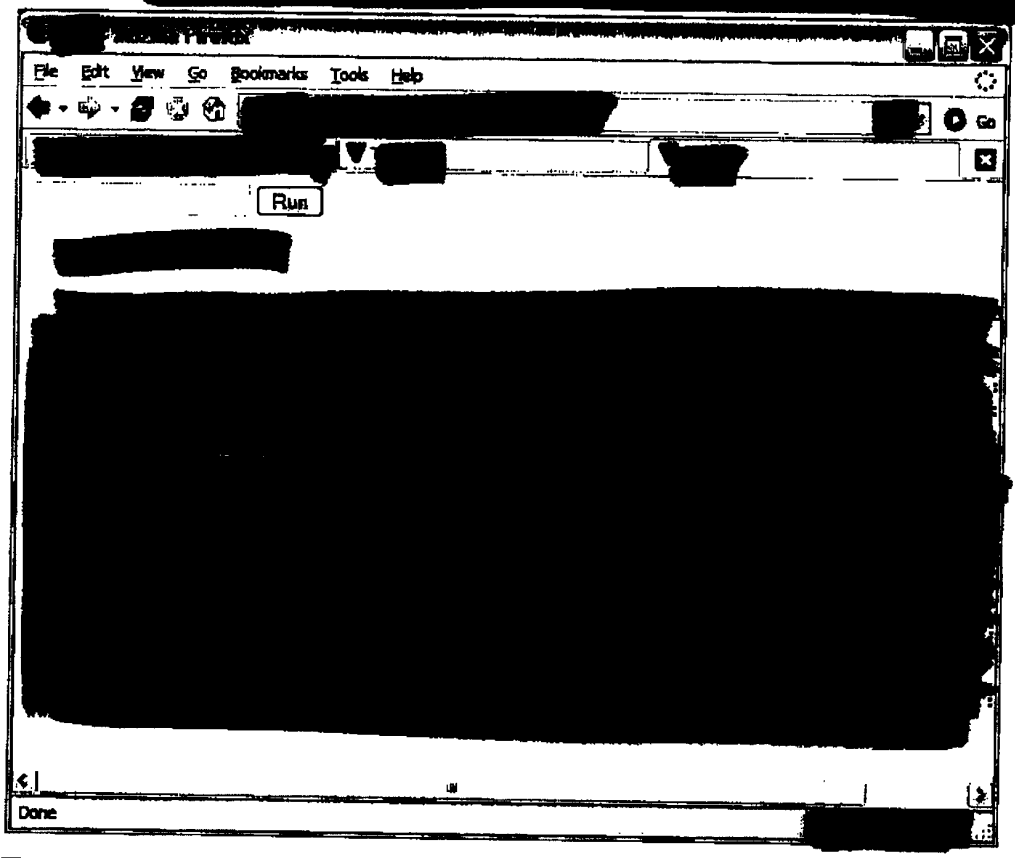


Figure 18: [redacted]



[redacted]

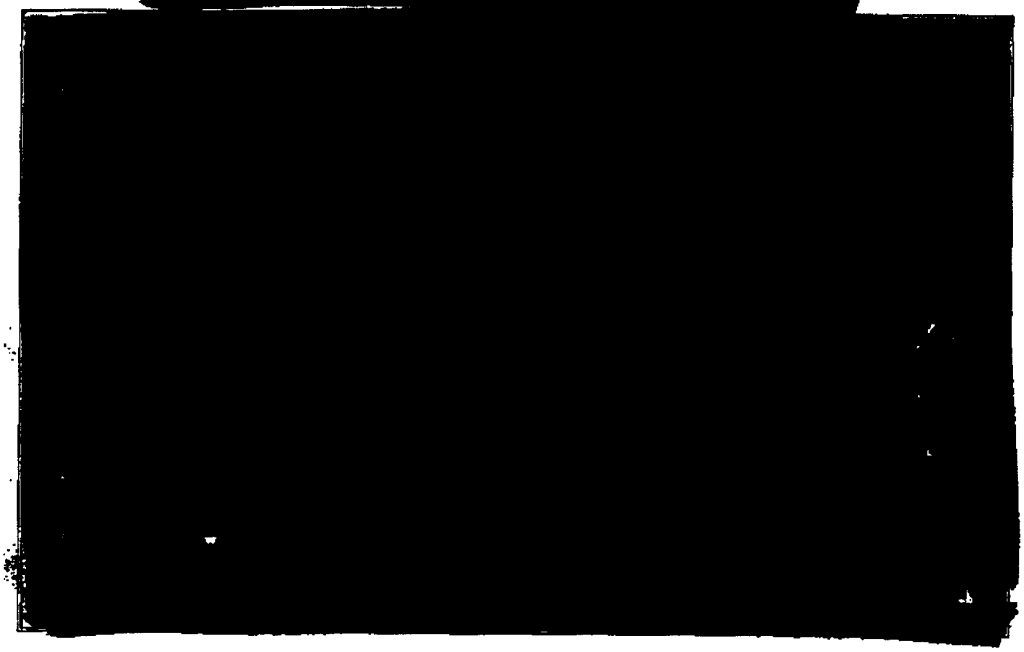
Figure 19: [redacted]



[redacted]

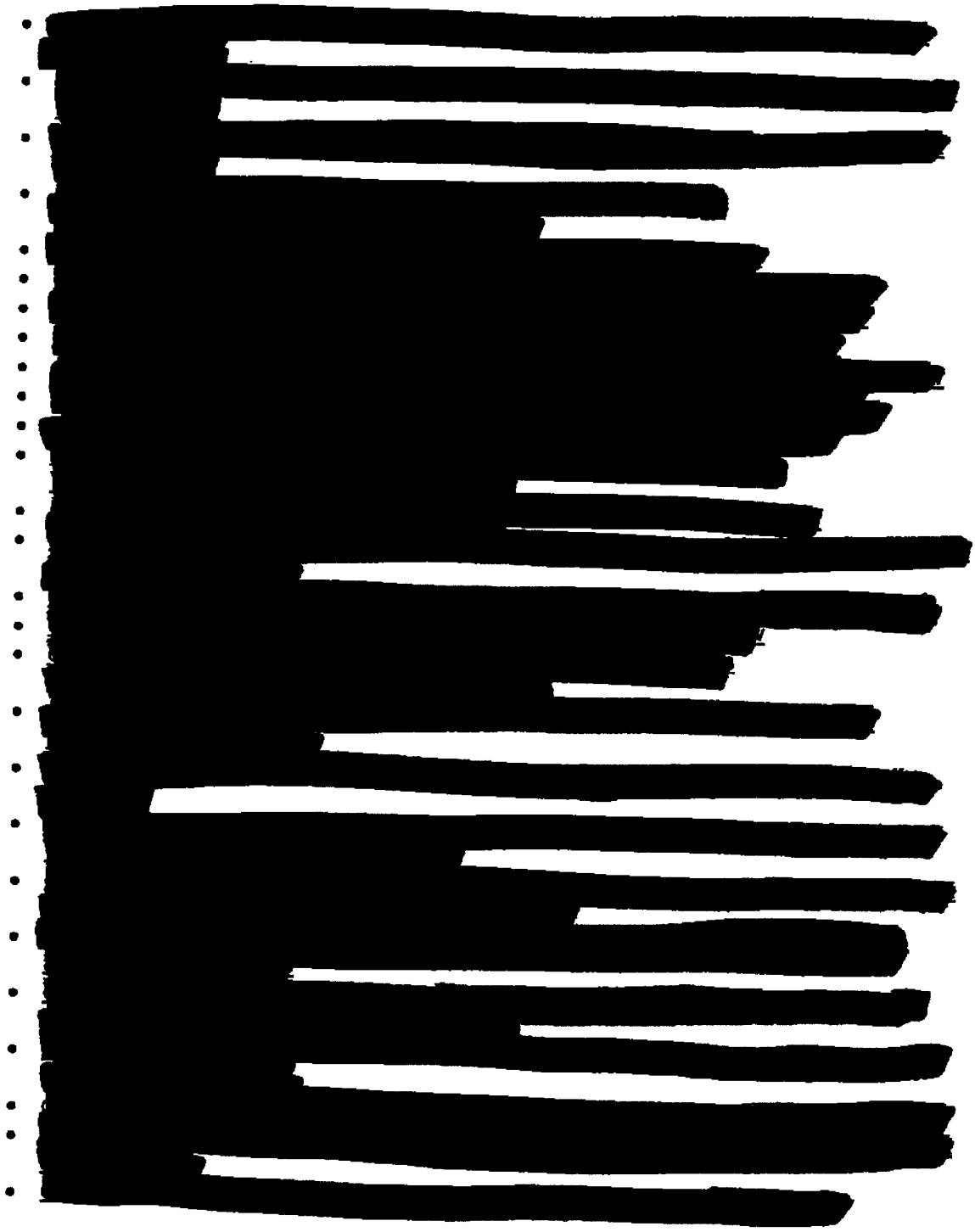
[redacted]

Figure 20: [redacted]



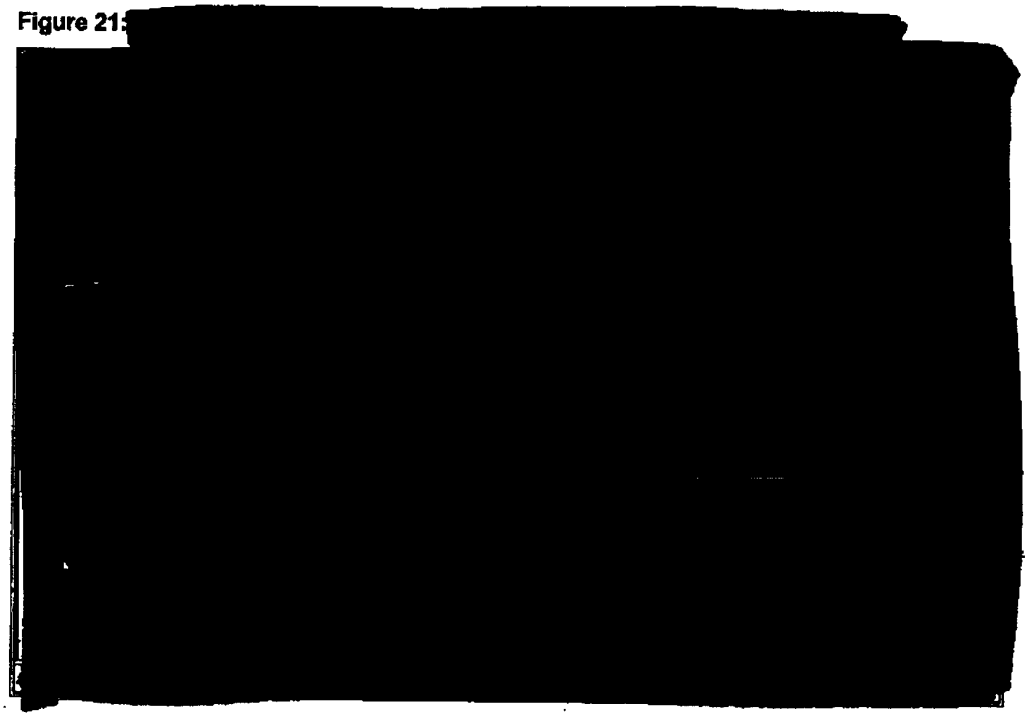
[redacted]

- [redacted]
- [redacted]



[redacted]

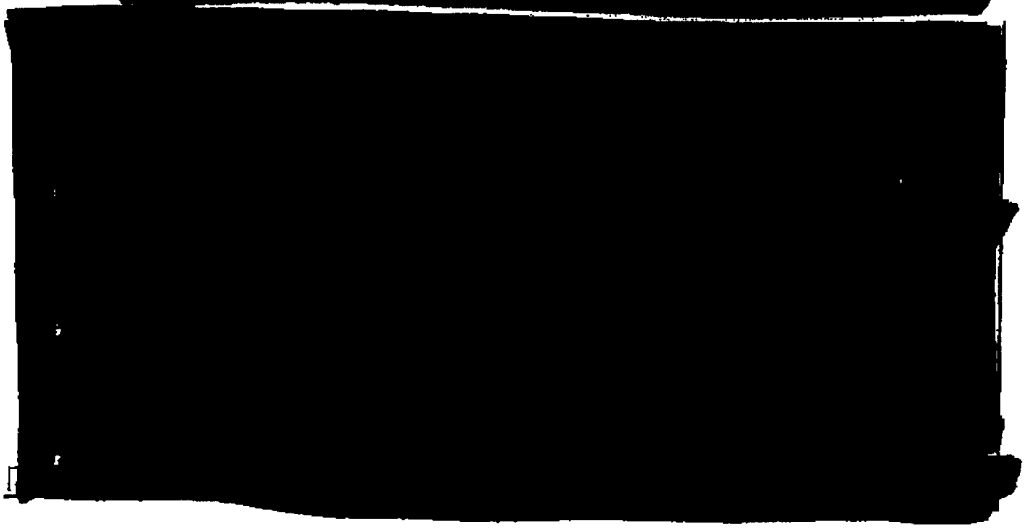
Figure 21: [redacted]



[redacted]

[redacted]

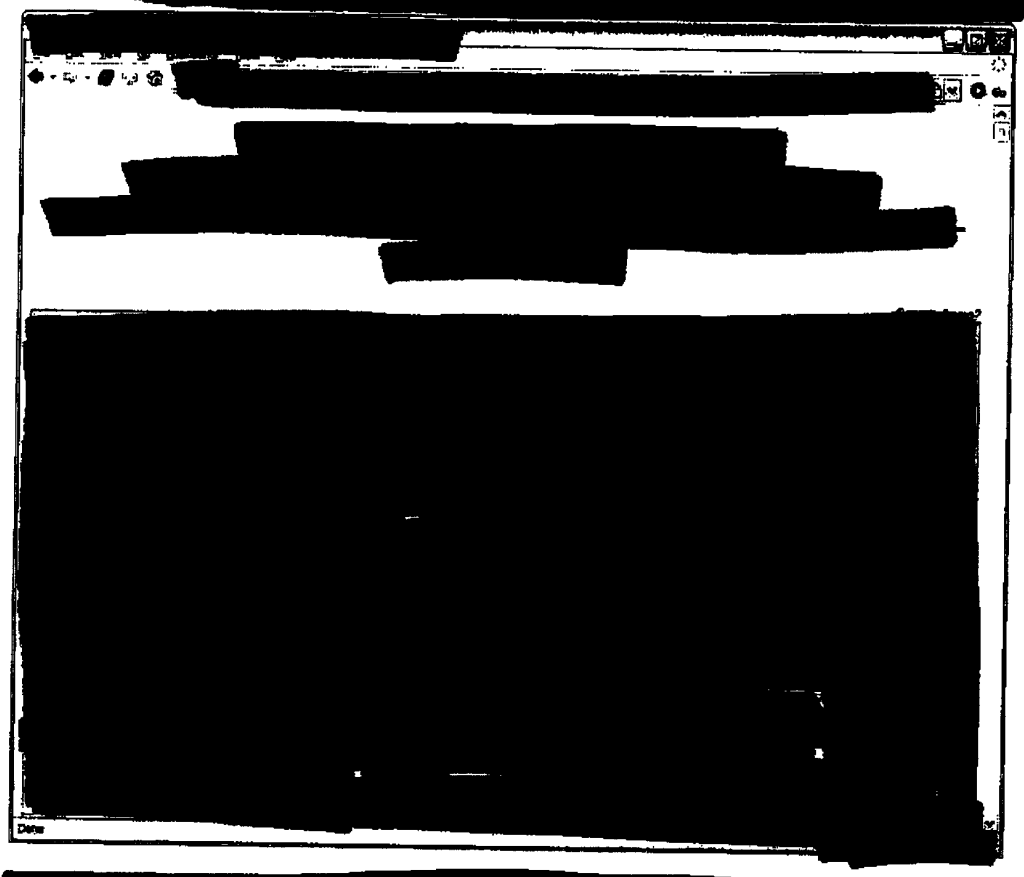
Figure 22: [redacted]



[redacted]

[redacted]

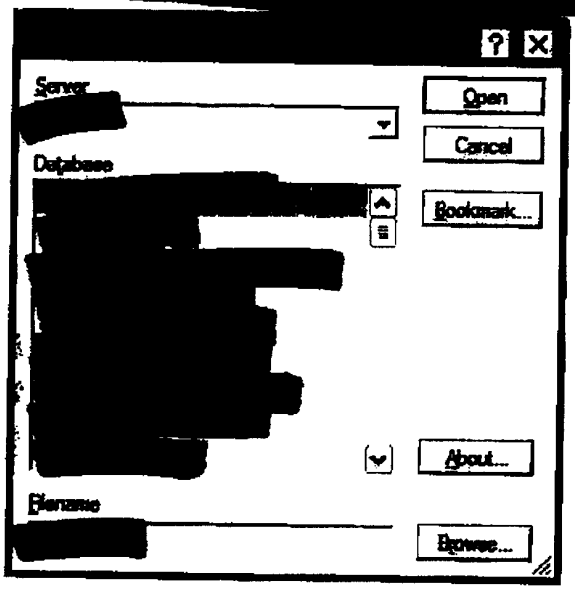
Figure 23: [redacted]



[redacted]

[redacted]

Figure 24: [redacted]



[redacted]

[redacted]

Figure 25: [redacted]

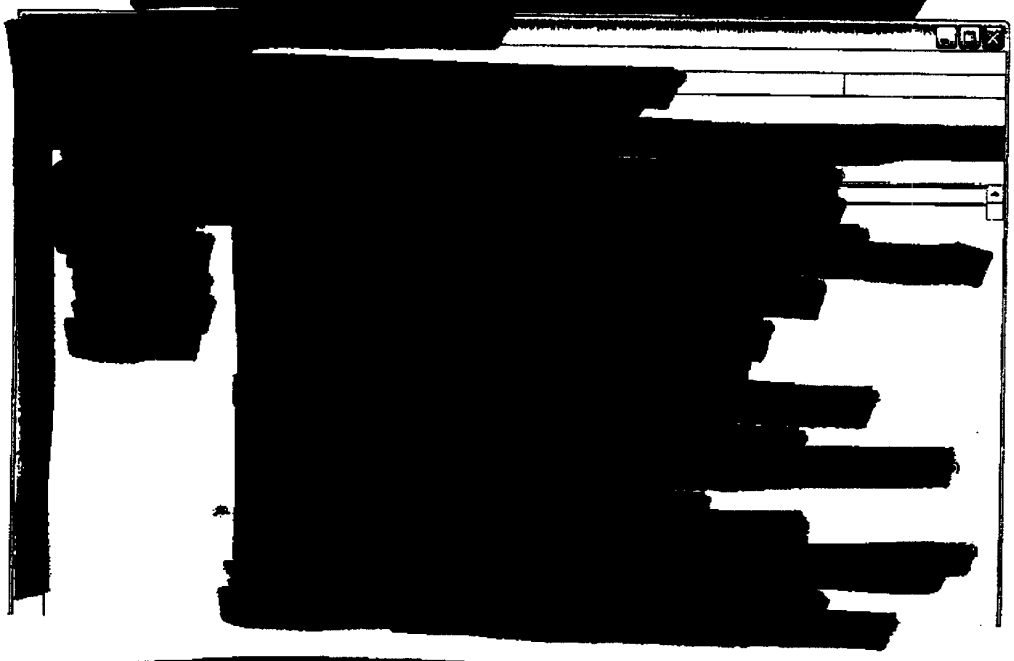
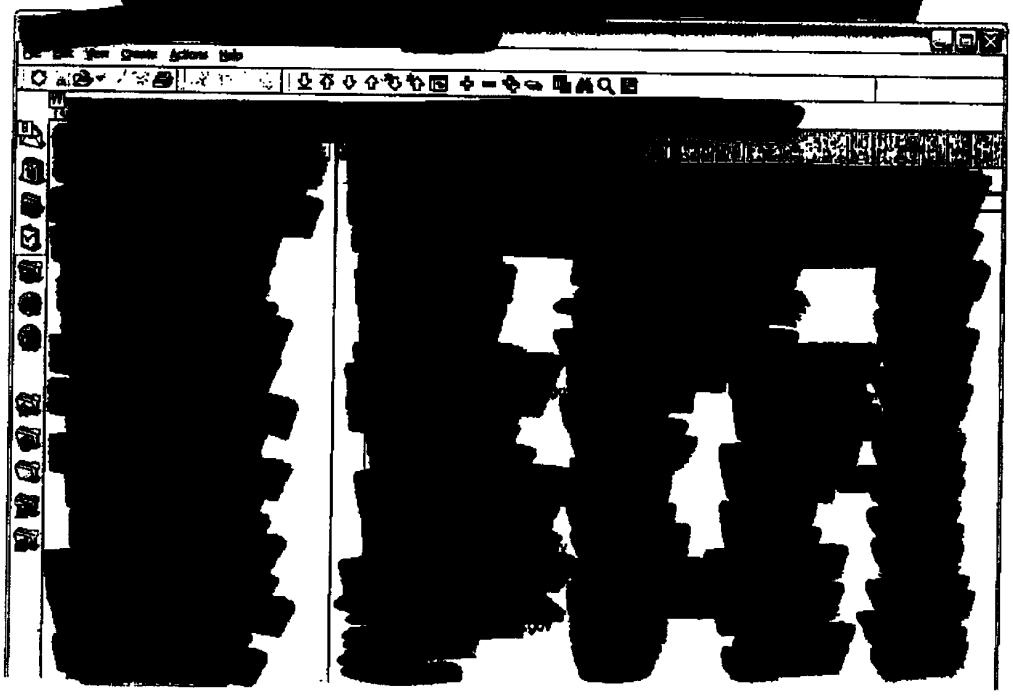
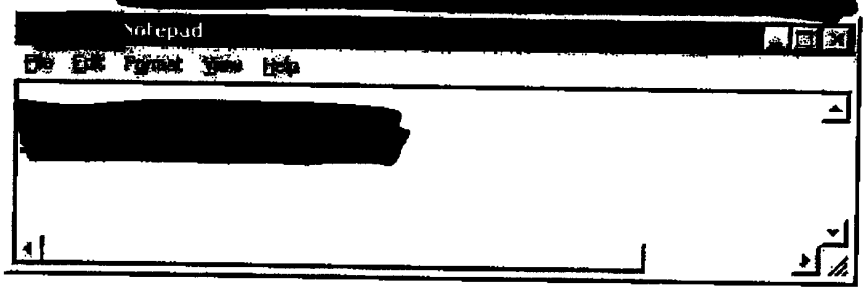


Figure 26 [redacted]



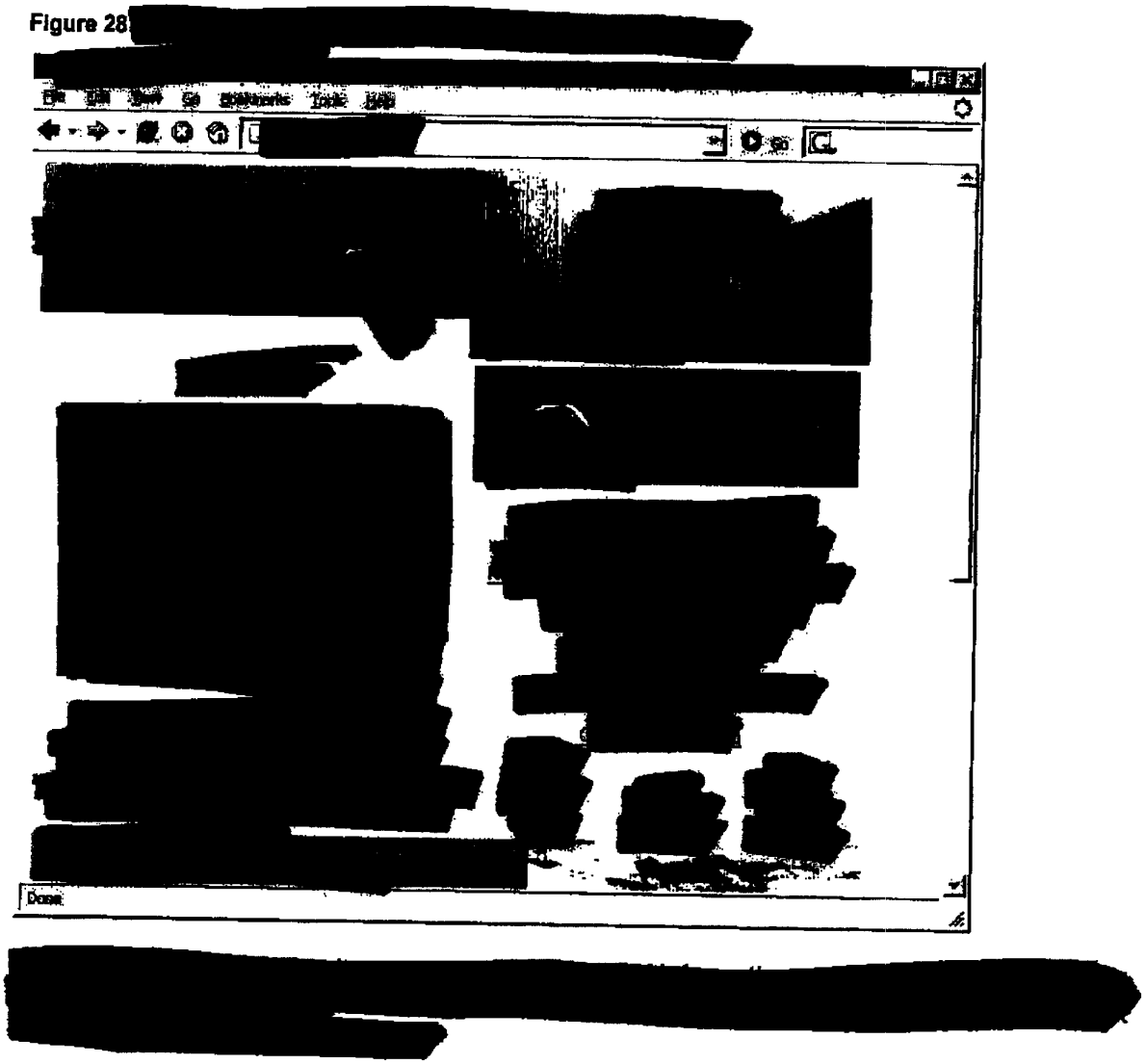
[redacted]

Figure 27 [redacted]



[redacted]

Figure 28 [redacted]



[redacted]

Figure 29: [redacted]

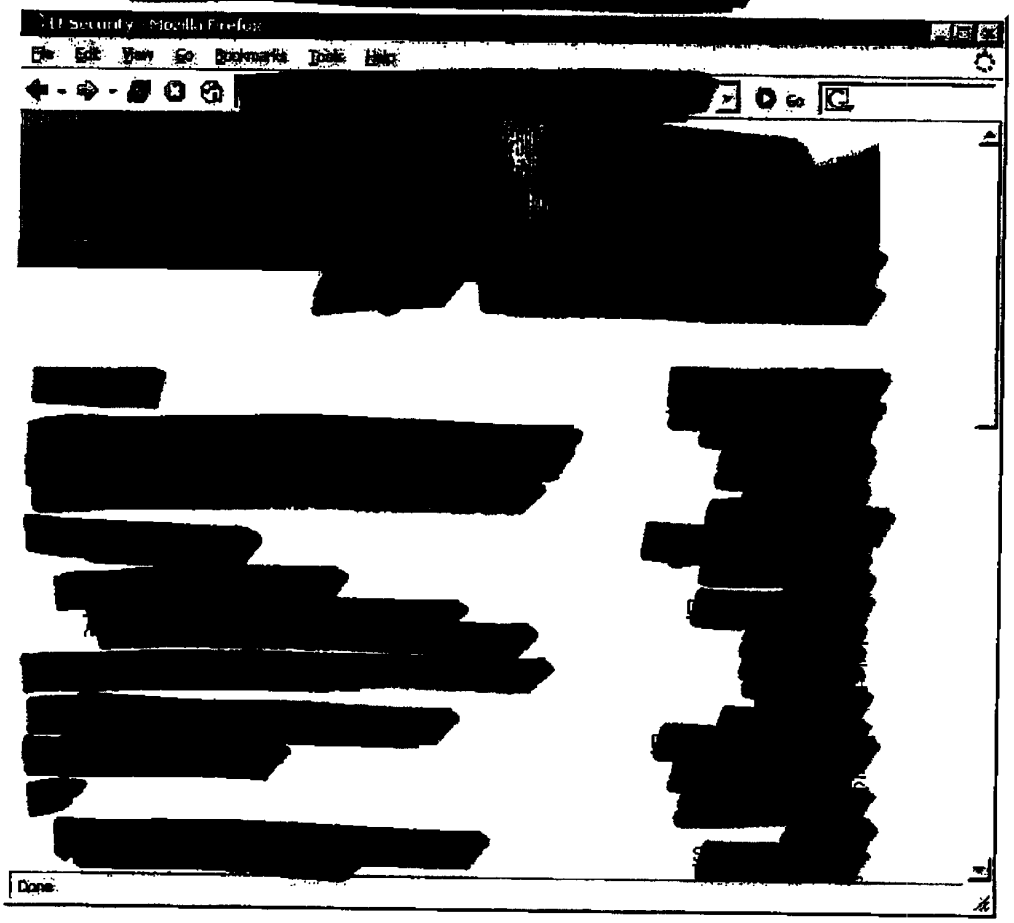


Figure 30: Nessus security vulnerability reports accessible on Intranet site

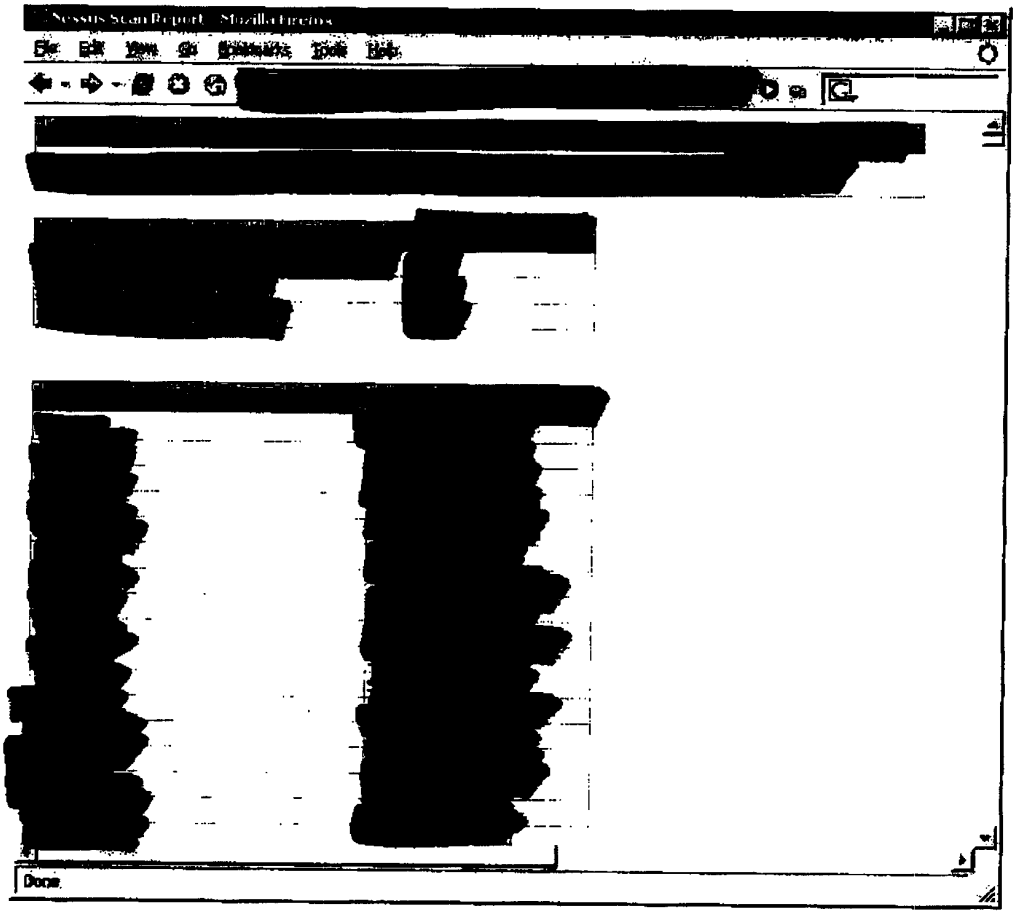
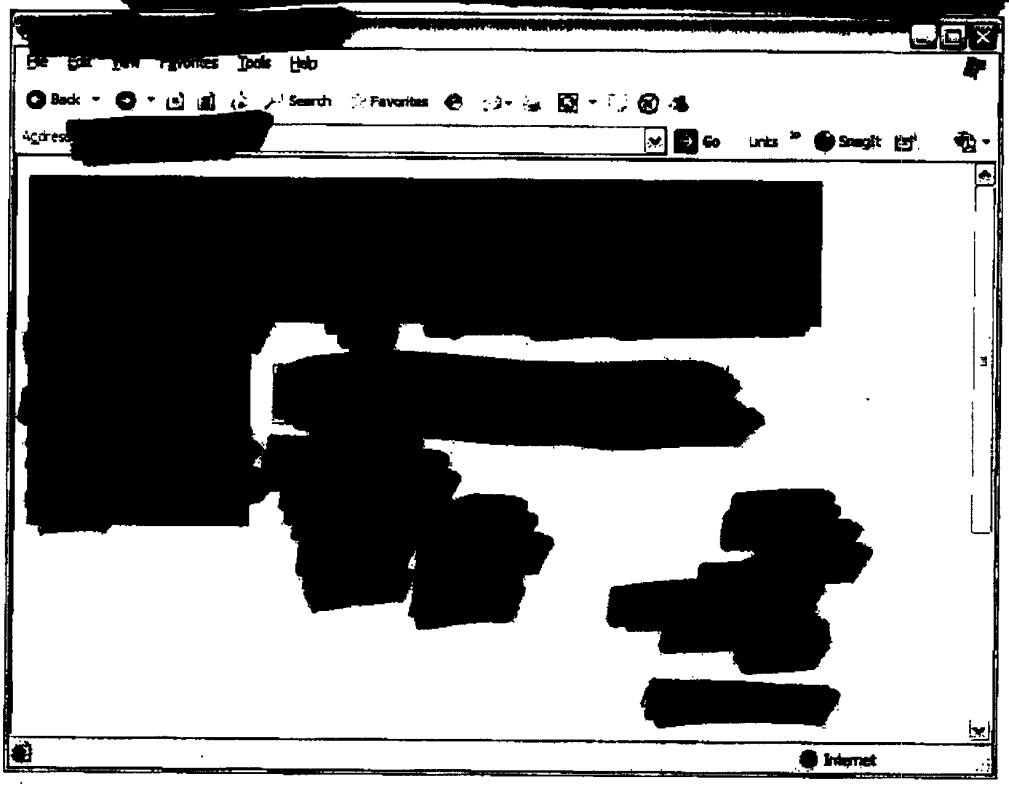
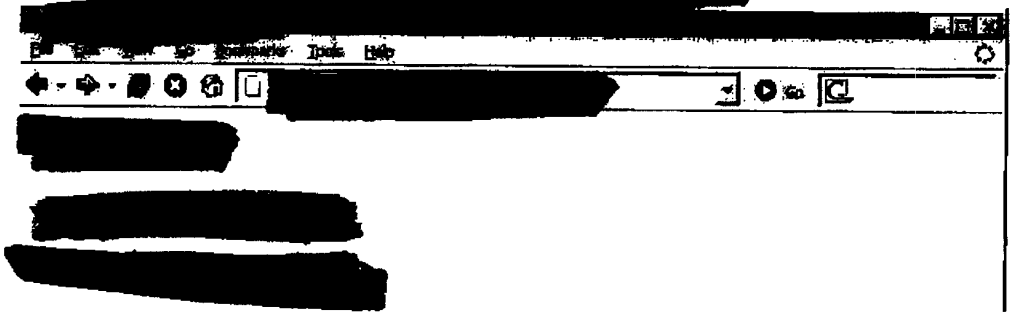


Figure 31: [redacted]



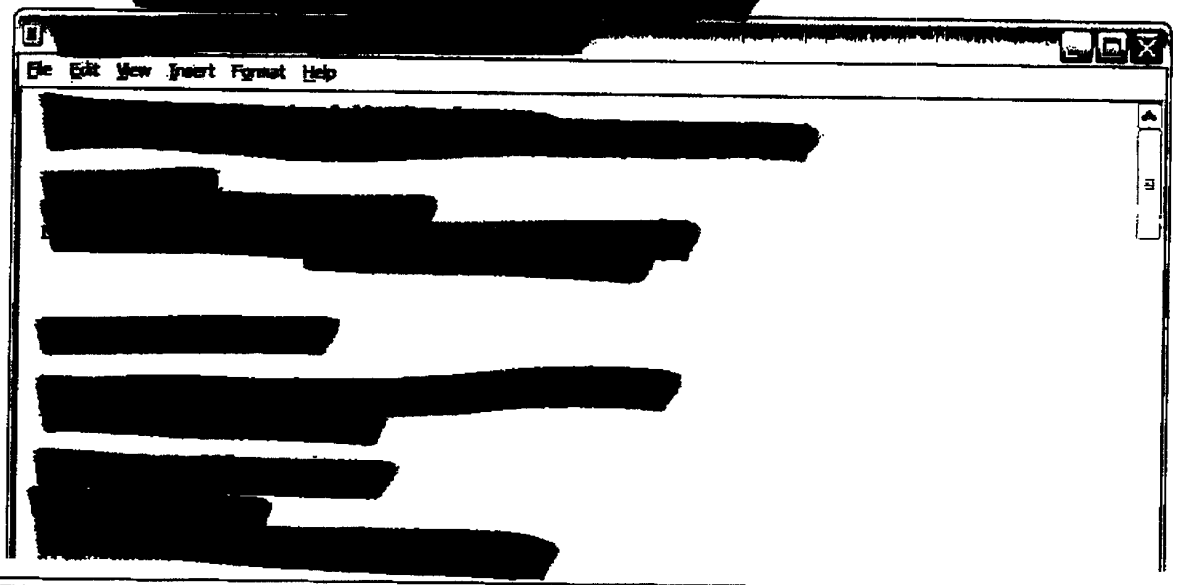
[redacted]

Figure 32: [redacted]



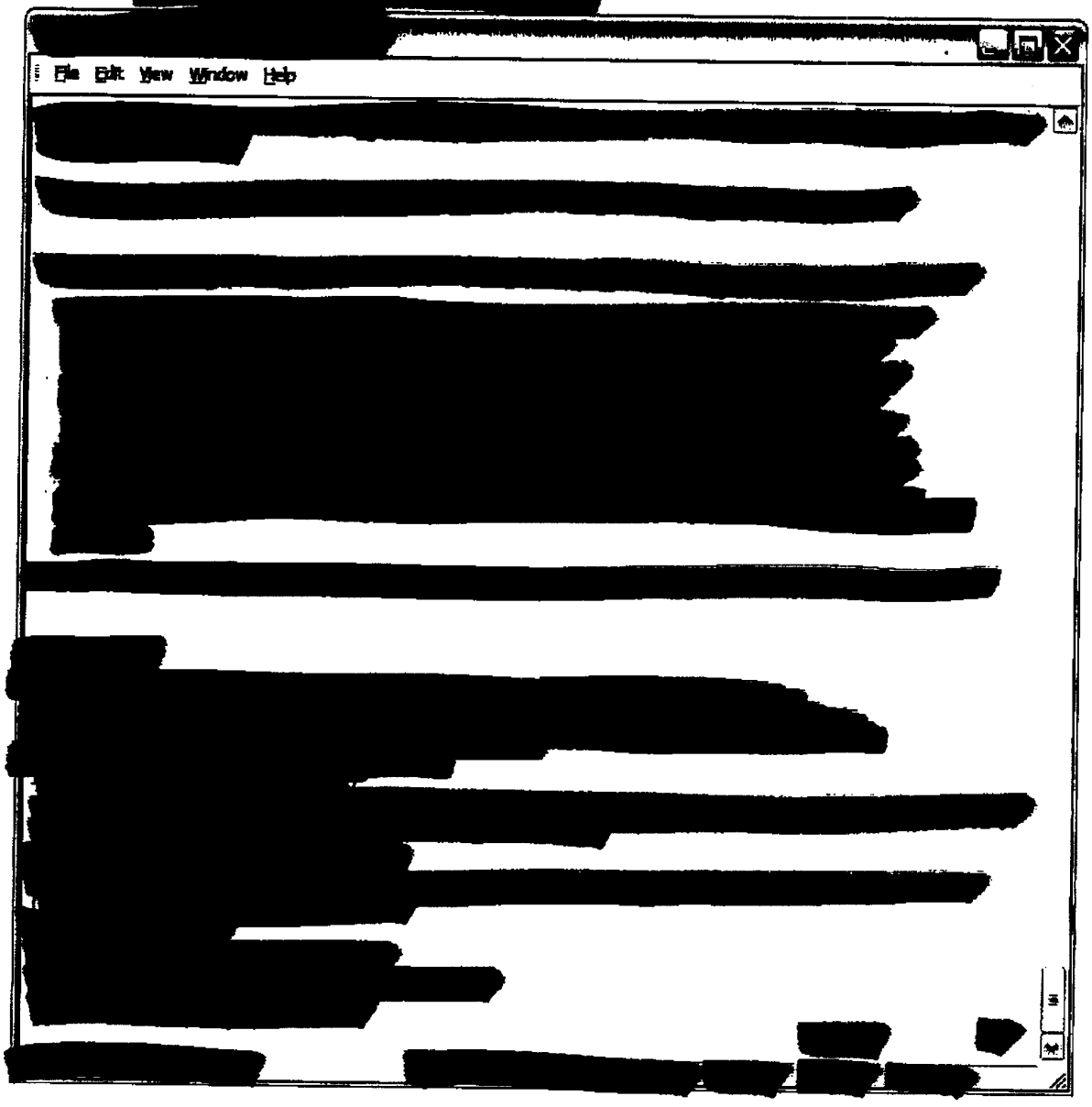
[redacted]

Figure 33: [redacted]



[redacted]

Figure 34: [redacted]



[redacted]

Figure 35: [redacted]

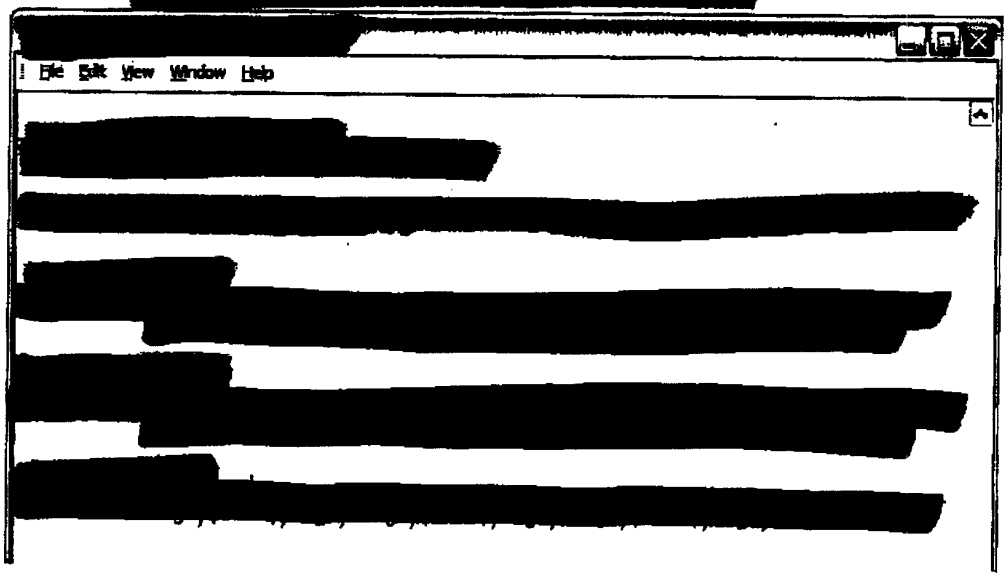
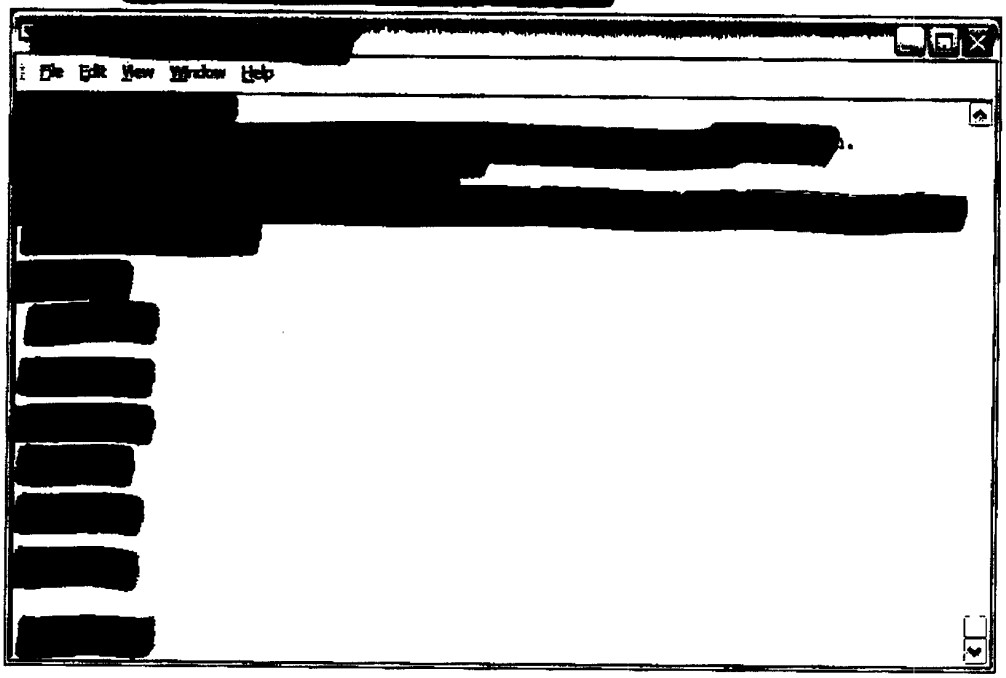
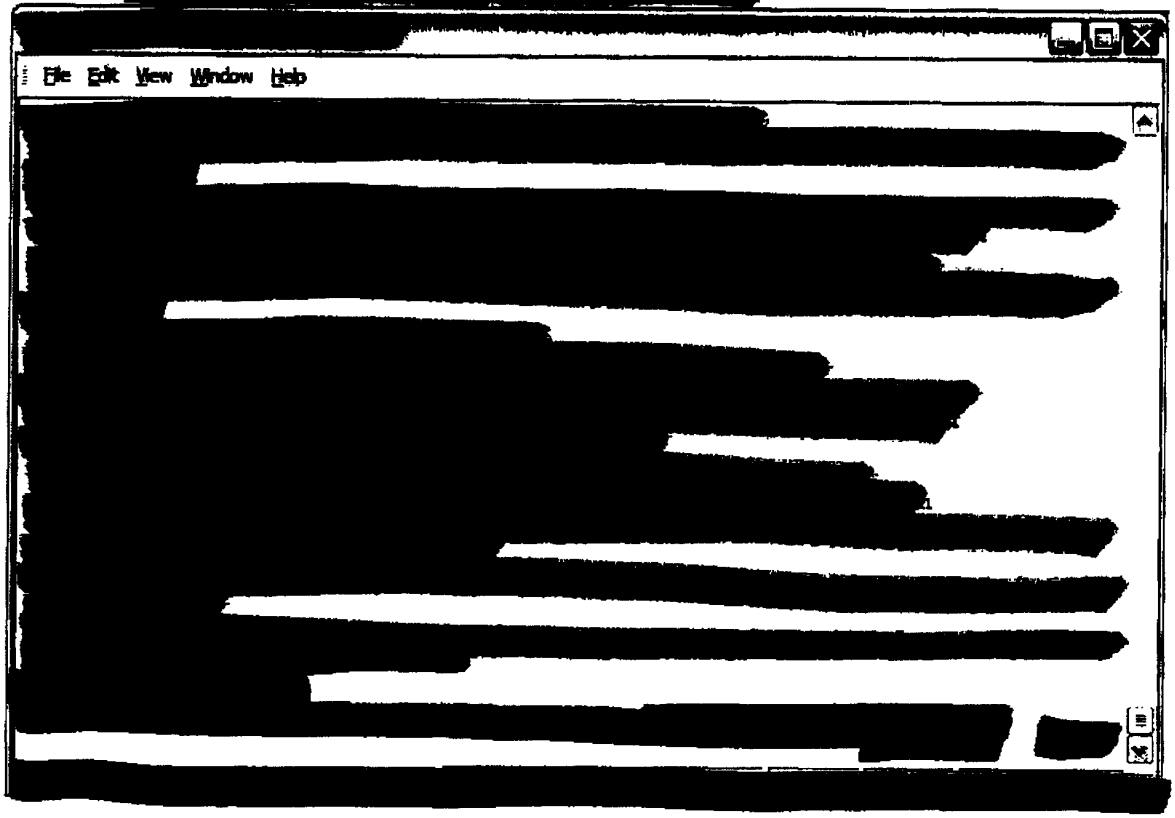


Figure 36: [redacted]



[redacted]

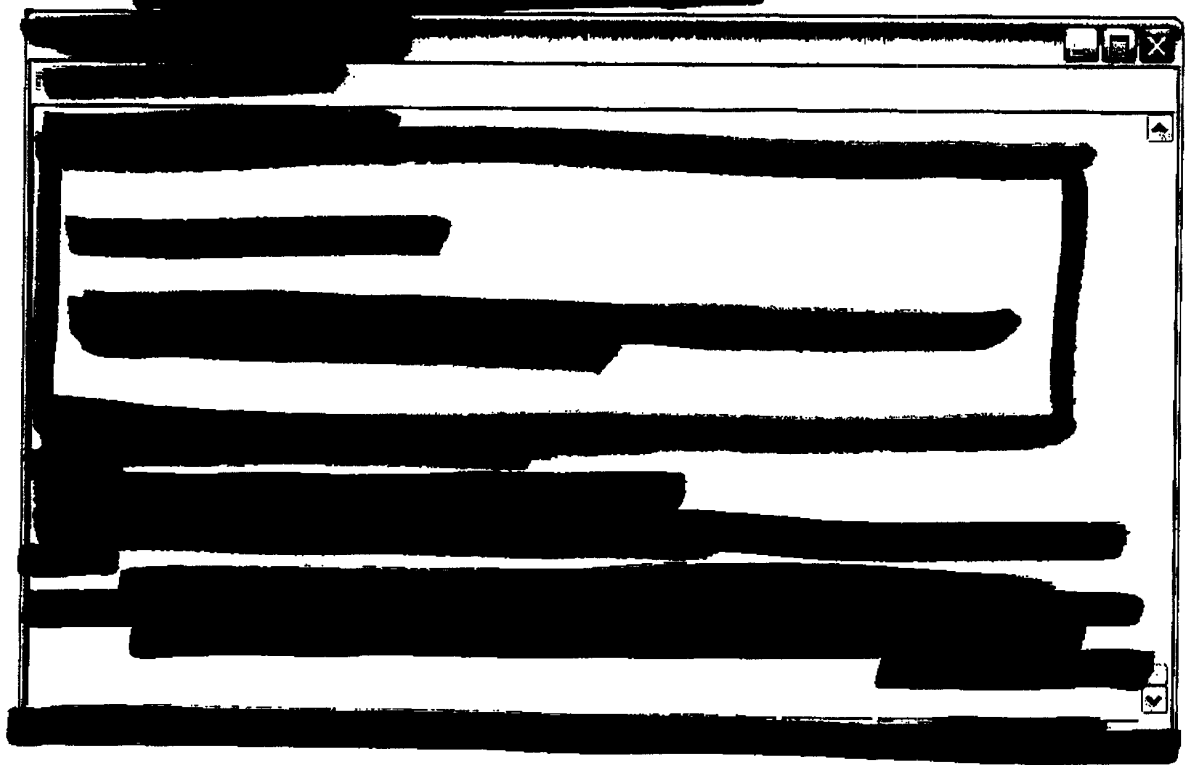
Figure 37[redacted]



[redacted]

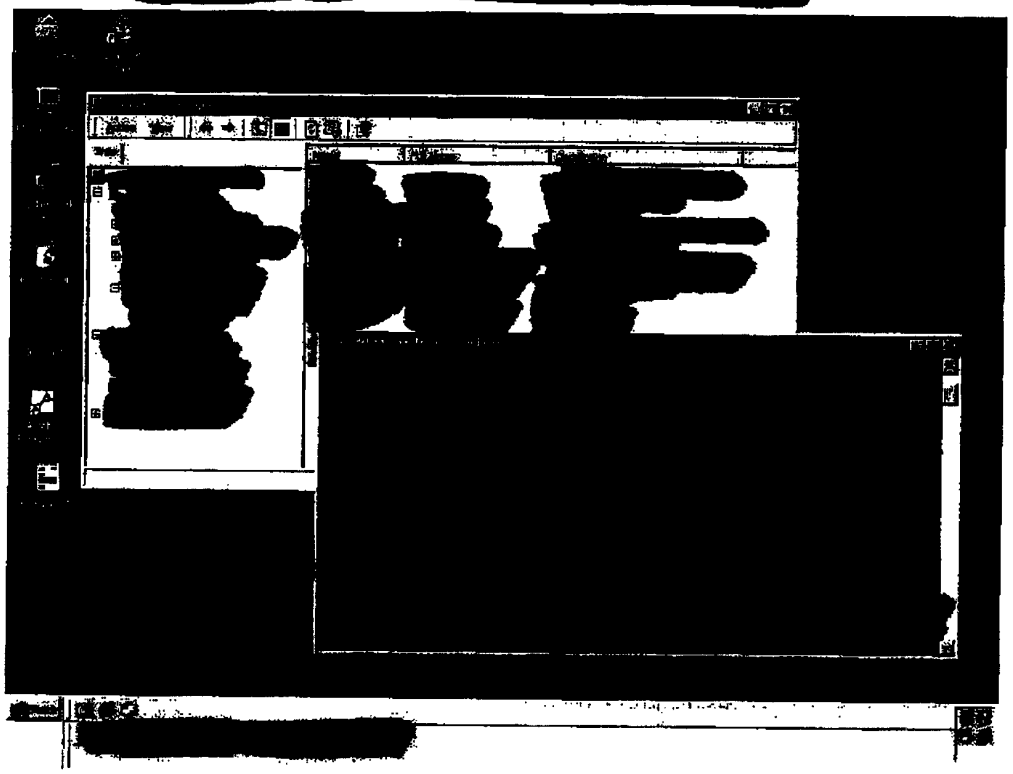
[redacted]

Figure 38: [redacted]



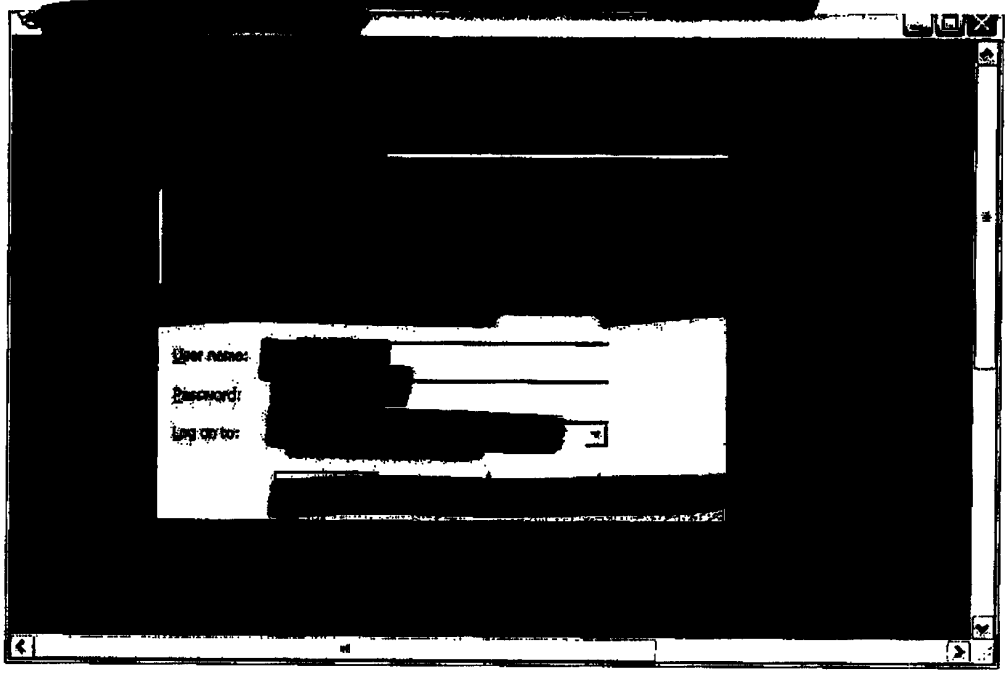
[redacted]

Figure 39: [redacted]



[redacted]

Figure 40:



[redacted]

Figure 41: [redacted]

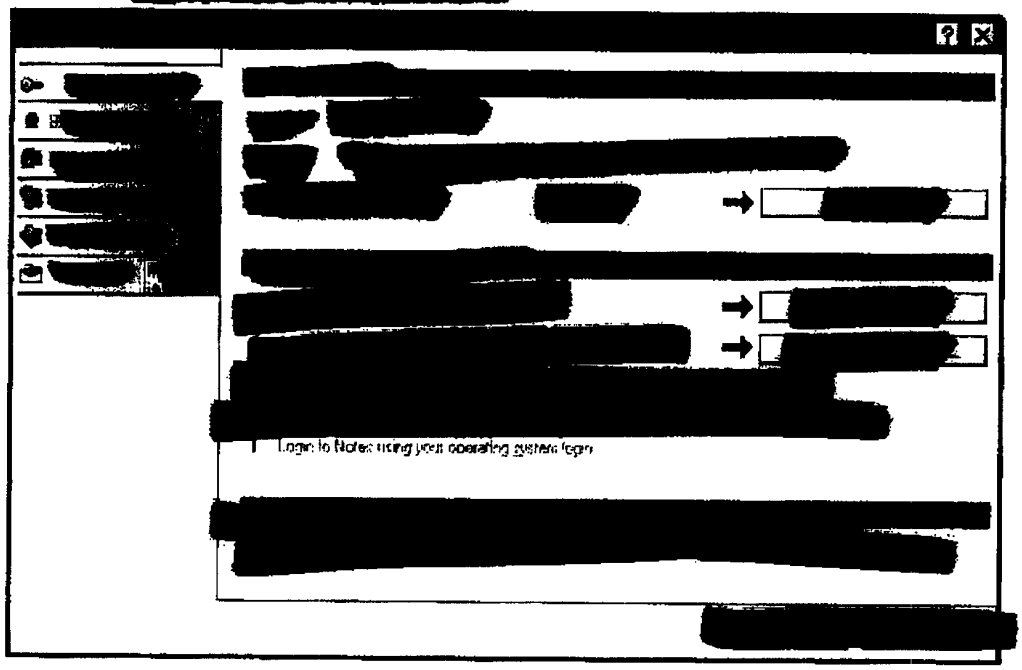


Figure 42: [redacted]

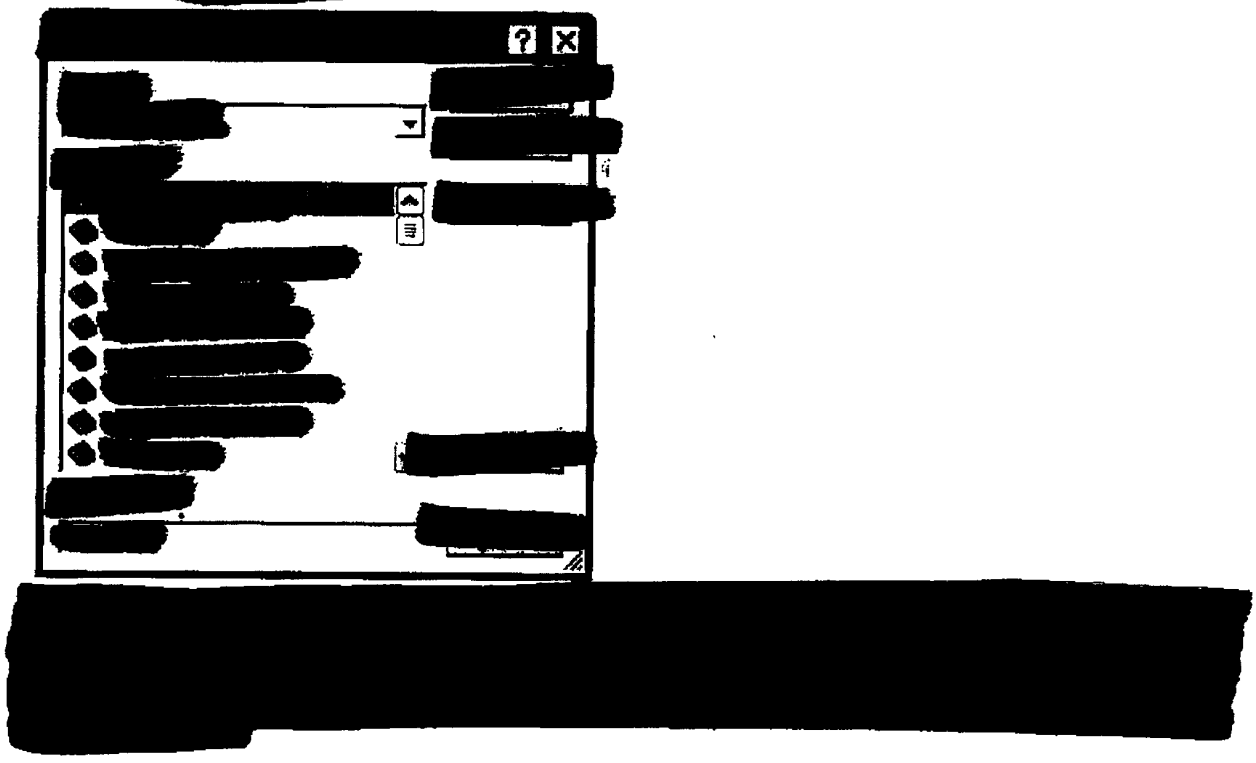
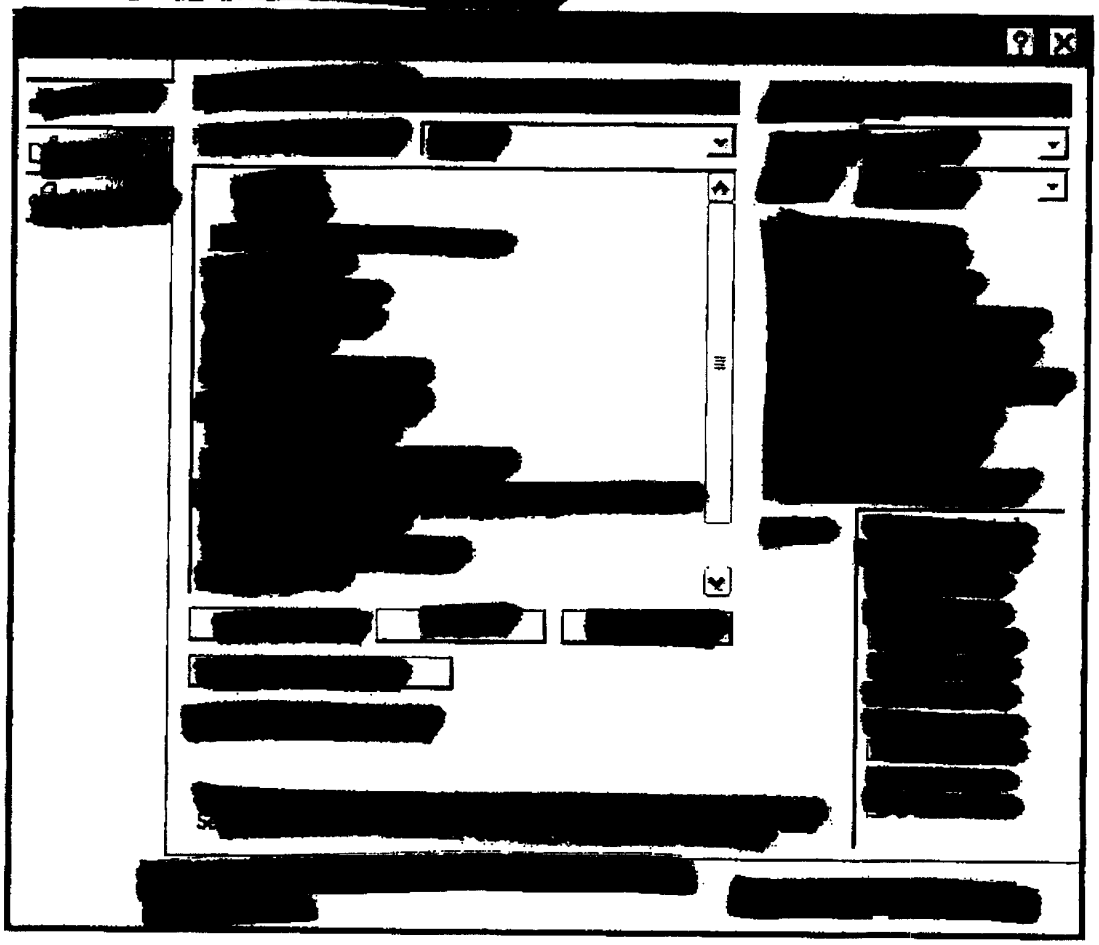
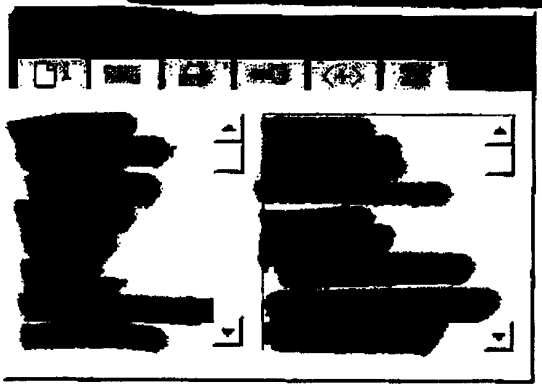


Figure 43: [redacted]



[redacted]

Figure 44: [redacted]



[redacted]

Figure 45: [redacted]

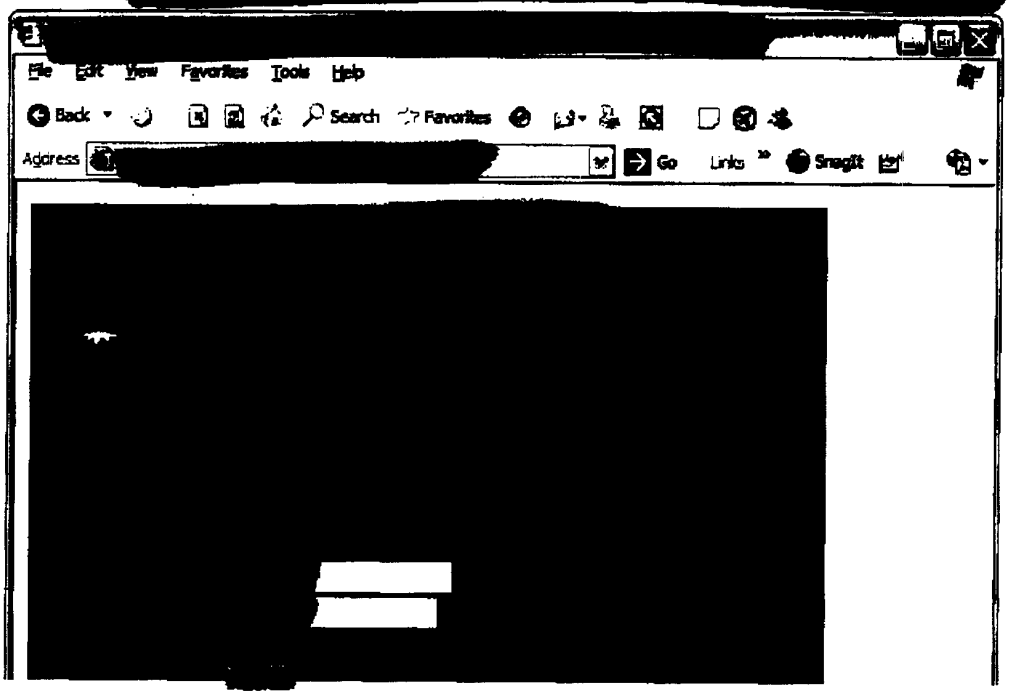
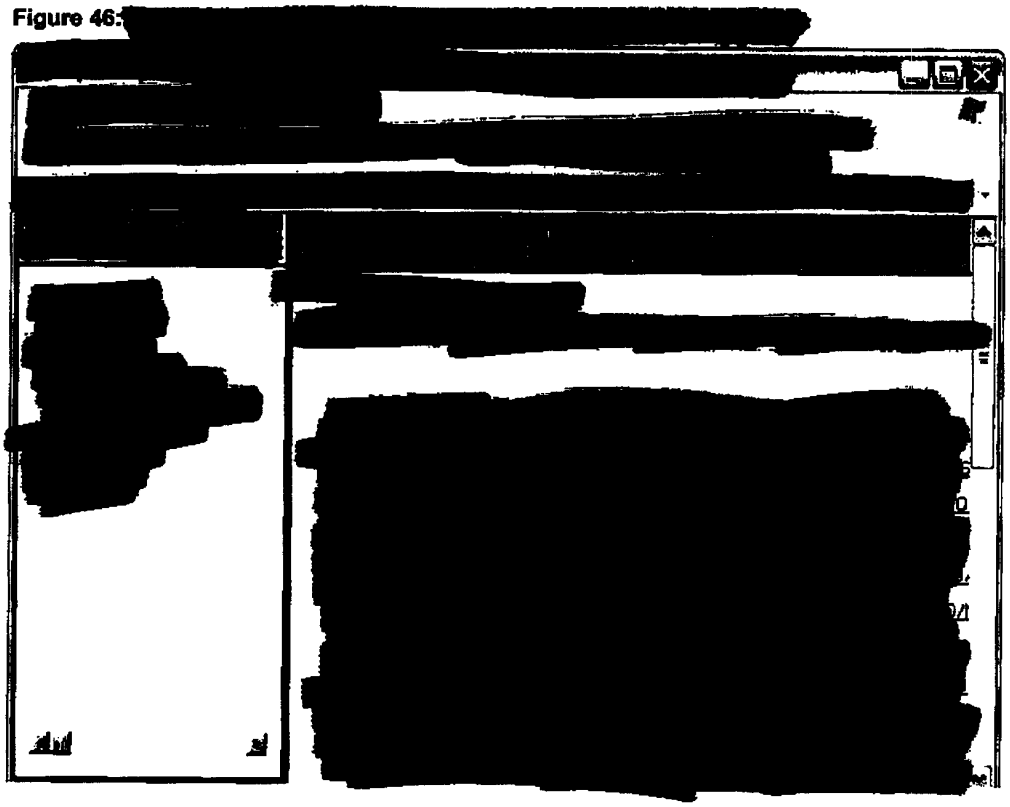


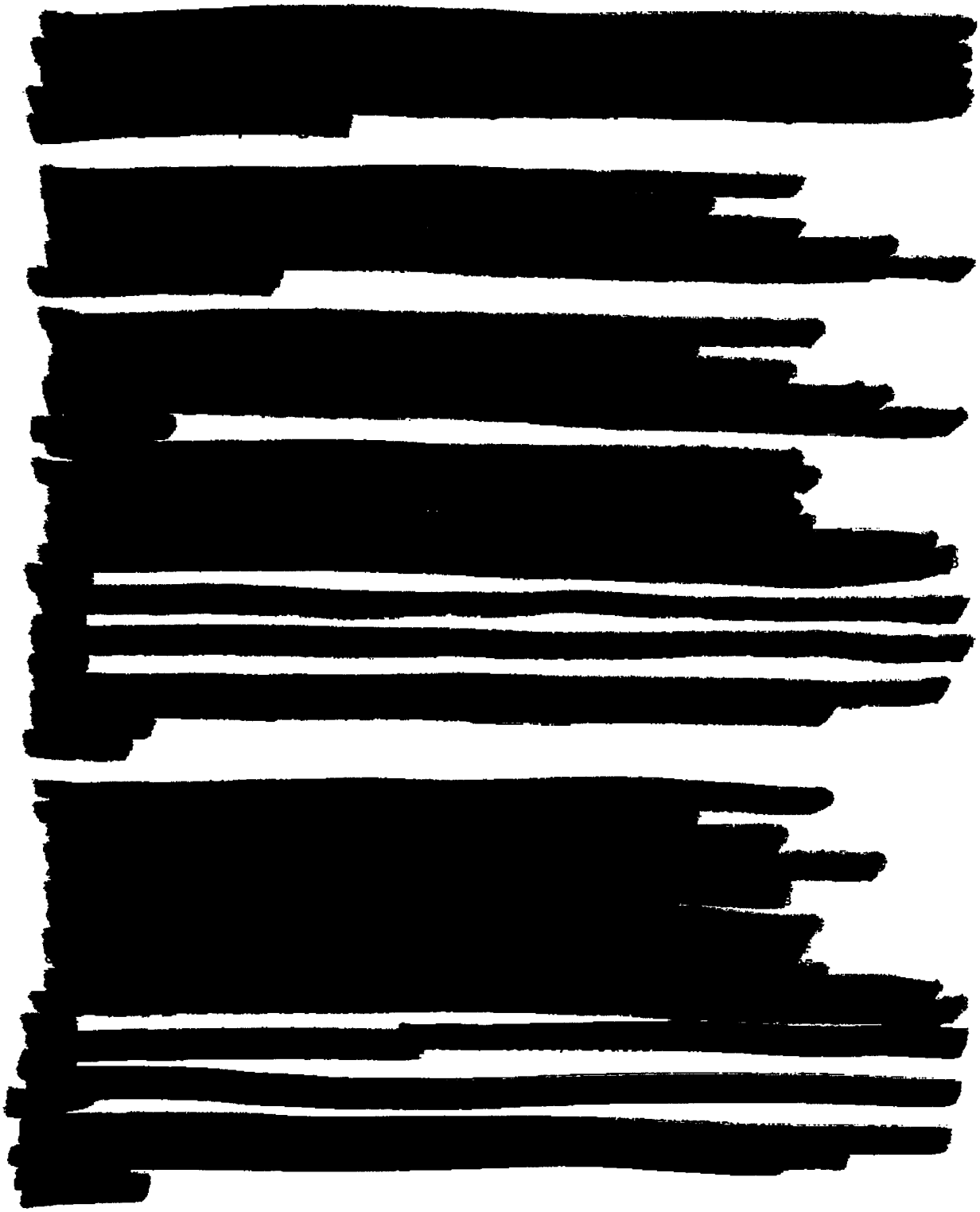
Figure 46: [redacted]



[redacted]

Name	IP Address	Services Accessed
[redacted]		

[redacted]



Tactical Recommendations

Review access controls on [redacted]

The access controls on the [redacted] should be reviewed to ensure only [redacted] that should be accessible from [redacted] can be reached.

Modify vulnerable [redacted] applications

The vulnerable [redacted] on the [redacted] server should be modified to remove [redacted] vulnerabilities. In addition, both of the [redacted] applications that allow [redacted] should be modified as soon as possible to remove the vulnerability.

Implement practices to avoid [redacted] and [redacted]

Follow the recommendations provided to avoid [redacted] and [redacted] issues in custom application code.

Review accessibility to certain data

The ability to access data such as security vulnerability reports, system core files, and backups of system configuration files should be reviewed and modified to ensure this type of data is not accessible to unauthorized users.

Change [redacted] passwords

All of the [redacted] identified in this report should be changed to strong passwords that comply with the DOI/BLM password standards. The processes used to create and change these passwords should be changed to ensure that only strong passwords may be used.

Discontinue support for [redacted] passwords

The use of [redacted] passwords should be discontinued.

Harden [redacted] and [redacted] server configurations

The configuration of [redacted] and [redacted] should be hardened according to security best practices. The [redacted] server should be configured to run in a [redacted] environment with no [redacted] allowed on any server files or [redacted] content from the [redacted] server id. The [redacted] server should be run as a [redacted] with [redacted] disabled. These [redacted] should not have the ability to write to any directories that allow [redacted] or [redacted] to limit the ability to gain access to the system through [redacted] server.

Strengthen [redacted]

All [redacted] systems should reside in an [redacted] The systems in this network should have access [redacted] that are [redacted] No access to [redacted] should be allowed from these systems. The systems should also be provided access [redacted] to those [redacted] required to function.

Improve [redacted] onfiguration of security tools

The security tools in place should be evaluated to determine if they are working effectively in the BLM environment. These systems should be replaced or appropriate changes made to improve [redacted]

Strategic Recommendations and Best Practices

In addition to the tactical recommendations set out in the above section, it is recommended that the following strategic recommendations be considered also. Many of these may already be in place.

Incorporate Security into Application Development Cycle

Security must be incorporated into the application development cycle to help reduce application security vulnerabilities. Security input should be provided in the requirements phase. Security standards and coding practices should be incorporated into the development process. Quality assurance testing should also perform basic security testing using security tools to catch common security vulnerabilities. Finally, an application security assessment should be performed by security professionals to identify any hidden vulnerabilities before a critical application is exposed to the public.

Conduct Regular Network Audits and Regular Penetration Tests

Information systems are always in flux with new attacks being discovered every day. Without auditing, it is not possible to objectively determine what the current state of security is. A penetration test can assist with a view of the network as seen by an attacker. Formal onsite assessments can provide a view of system security from an insider's perspective. This can greatly assist in obtaining true defense in depth.

Implement [redacted]

[redacted] s a critical part of any successful security policy. Were the [redacted] Were appropriate actions taken? If this test did not result in a security "fire-drill" consider conducting one. ISS recommends that BLM deploy [redacted] and [redacted] [redacted] where lacking to minimize exposure to current and unknown threats. BLM should also evaluate if it is in its interests to manage its own [redacted] or if it should be outsourced to a Managed Service Services (MSS) organization.

Always adopt a "defense in depth" Security Strategy

Employ a multi-layer "defense in depth" approach to security:

- **Perimeter** access control such as firewalls, routers, and VPN technology
- **Network** Intrusion Protection Systems (IPS) on both external and internal networks.
- **Host** Intrusion Protection for critical servers and applications. Hardened Operating systems.
- **Application** security such as access control lists and user credentials.
- **Data** level security such as compartmentalization, encryption, and classification.

Adopt Risk Management Approach

Using a risk management approach ensures that BLM is making the best business decisions about security. In a nutshell, risk management involves:

- Ranking information assets by value
- Ranking the probability of threats for each asset
- Evaluating the countermeasures for each threat
- Deciding how to handle the risk from each threat
  - Reduce the risk by applying countermeasures
  - Transfer the risk by purchasing insurance
  - Accept the risk (i.e. put the annual loss estimate for the risk in the budget)

Formal Security Policy Development

Employ and enforce a security policy that educates all levels of the organization on expectations and responsibilities with respect to security. This policy should address issues such as anti-virus protection, Intrusion Protection and acceptable use.

Appendix A: [redacted]

Appendix B: Security Reference Information