Penetration Test Report

< Company Name>

< Date of Test>

**Student Name**

College Name

Contact Info

Tel: 1-234-567-8990

Email: [a@a.co](mailto:a@a.co)

Contents

[Executive Summary 2](#_Toc81562445)

[Summary of Results 3](#_Toc81562446)

[Attack Narrative 4](#_Toc81562447)

[Remote System Discovery 4](#_Toc81562448)

[Admin Webserver Interface Compromise 6](#_Toc81562449)

[Interactive Shell to Admin Server 8](#_Toc81562450)

[Administrative Privilege Escalation 10](#_Toc81562451)

[Java Client Attacks 11](#_Toc81562452)

[Escalation to Local Administrator 12](#_Toc81562453)

[Deep Packet Inspection Bypass 12](#_Toc81562454)

[Escalation to Domain Administrator 14](#_Toc81562455)

[Conclusion 15](#_Toc81562456)

[Recommendations 17](#_Toc81562457)

[Risk Rating 18](#_Toc81562458)

[Appendix A: Vulnerability Detail and Mitigation 19](#_Toc81562459)

[Risk Rating Scale 19](#_Toc81562460)

[Appendix B: Additional Details 23](#_Toc81562461)

# Executive Summary

<Student Name>was contracted by <Company Name>to conduct a penetration test in order to determine its exposure to a targeted attack. All activities were conducted in a manner that simulated a malicious actor engaged in a targeted attack against <Company Name>with the goals of:

* Identifying if a remote attacker could penetrate <Company Name>defenses
* Determining the impact of a security breach on:
  + Confidentiality of the company’s private data
  + Internal infrastructure and availability of <Company Name>information systems

Efforts were placed on the identification and exploitation of security weaknesses that could allow a remote attacker to gain unauthorized access to organizational data. The attacks were conducted with the level of access that a general Internet user would have. The assessment was conducted in accordance with the recommendations outlined in NIST SP 800-1151 with all tests and actions being conducted under controlled conditions.

1 [http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pd](http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf)f

## Summary of Results

Infiltration Methods, Kill Chain and Processes

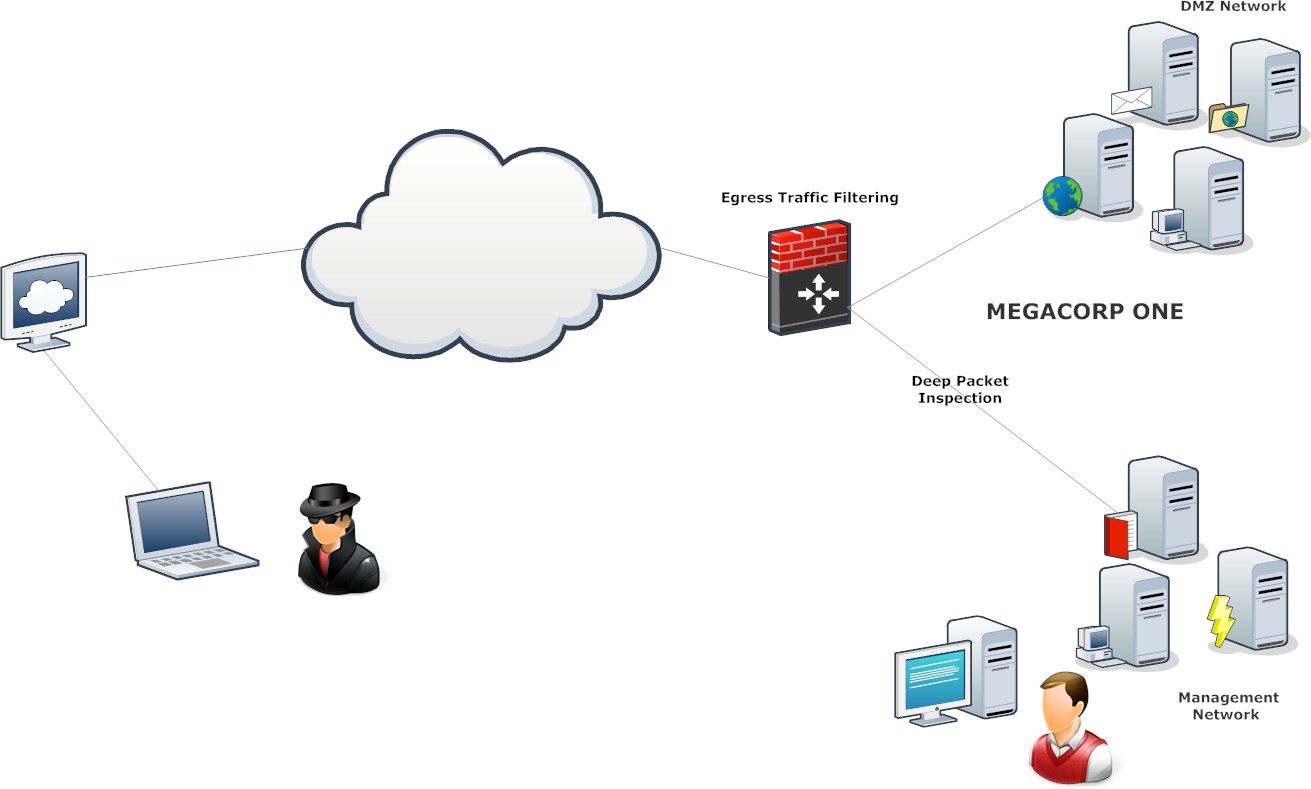
# Attack Narrative

## Remote System Discovery

**Ex: Figure 1 – Information gathering reveals three active name servers.**

It can also leak information about the network ranges owned by the organization. Please see Appendix A for more information.

**Ex: Figure 2 – A misconfigured name server allows a full and unrestricted DNS zone transfer.**



**Figure 3 - Target Network**

## Admin Webserver Interface Compromise

**Figure 4 – Enumeration of host partially discloses the webserver’s folder structure.**

**Figure 5 – Access to the “admin” folder is password-protected.**

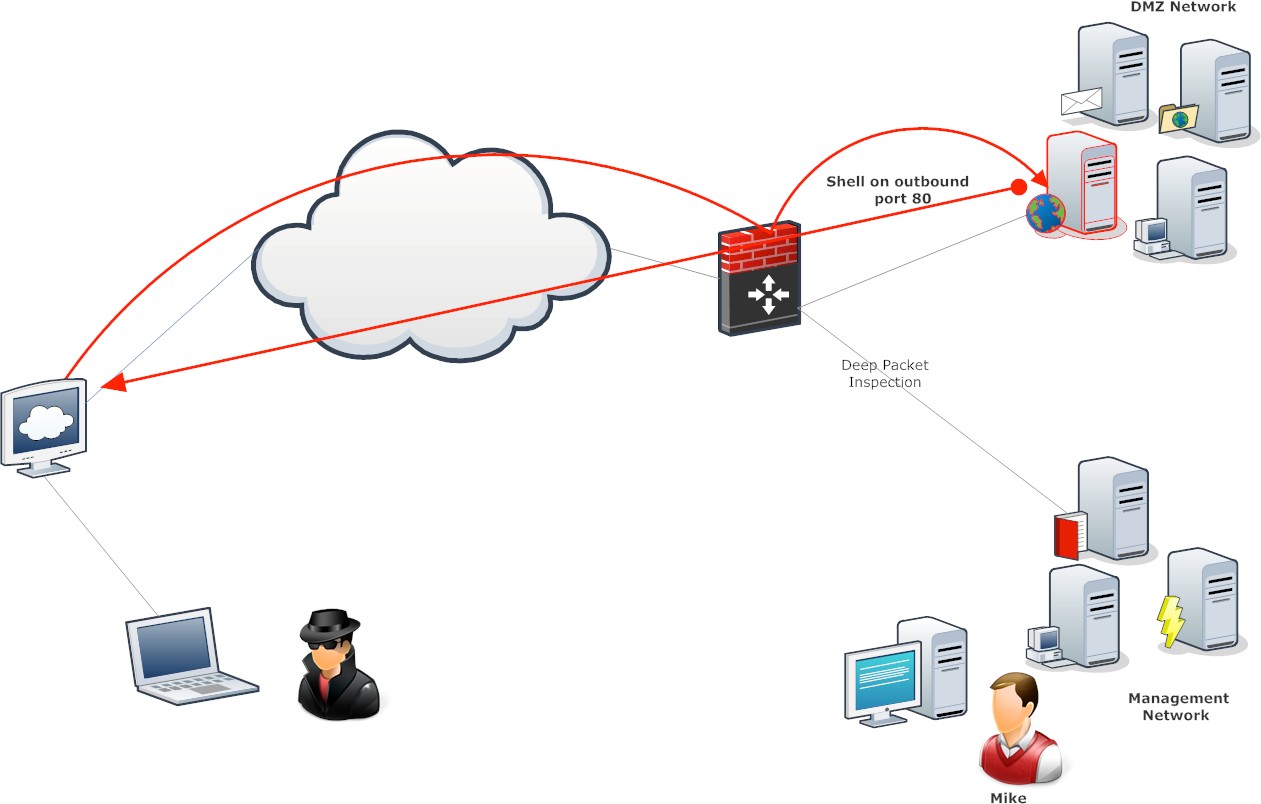
**Figure 6 –It is possible to discover the administrative password for the “admin” folder.**

<http://phpsqlitecms.net/>

## Interactive Shell to Admin Server

**Figure 10 –**

1. [http://www.exploit-db.com/exploits/2432](http://www.exploit-db.com/exploits/24320/)0/



**Figure 12 - Web Server Compromise**

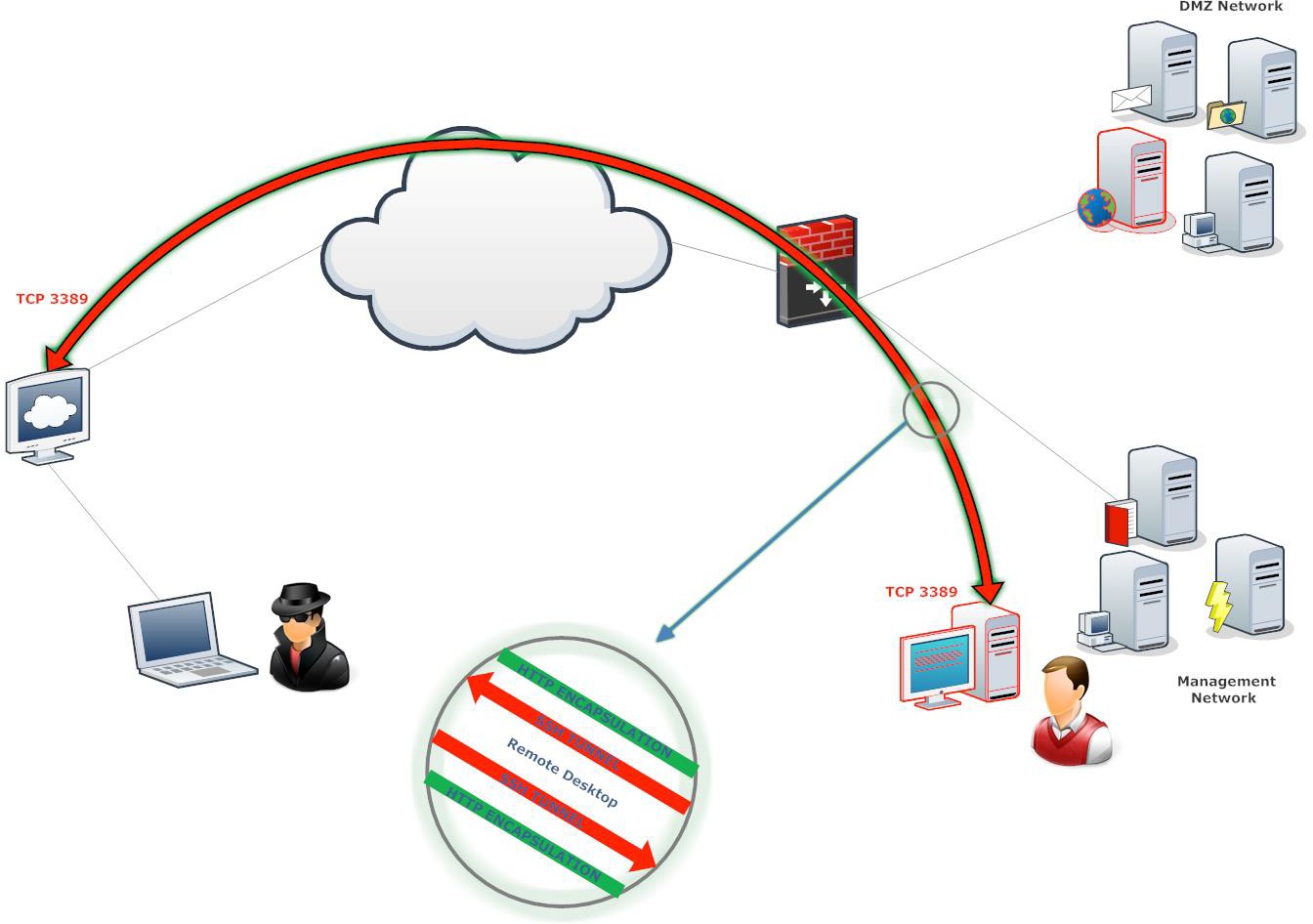
## Administrative Privilege Escalation

1. [http://www.exploit-db.com/exploits/1841](http://www.exploit-db.com/exploits/18411/)1/

## Java Client Attacks

## Escalation to Local Administrator

## Deep Packet Inspection Bypass



**Figure 25 – Compromise of the <Company Name>network has reached into the network management subnet**

## Escalation to Domain Administrator

# Conclusion

<Company Name>suffered a series of control failures, which led to a complete compromise of critical company assets. These failures would have had a dramatic effect on <Company Name>operations if a malicious party had exploited them. Current policies concerning password reuse and deployed access controls are not adequate to mitigate the impact of the discovered vulnerabilities.

The specific goals of the penetration test were stated as:

* Identifying if a remote attacker could penetrate <Company Name>defenses
* Determining the impact of a security breach on:
  + Confidentiality of the company’s information
  + Internal infrastructure and availability of <Company Name>information systems

These goals of the penetration test were met. A targeted attack against <Company Name>can result in a complete compromise of organizational assets. Multiple issues that would typically be considered minor were leveraged in concert, resulting in a total compromise of the <Company Name>information systems. It is important to note that this collapse of the entire <Company Name>security infrastructure can be greatly attributed to insufficient access controls at both the network boundary and host levels. Appropriate efforts should be undertaken to introduce effective network segmentation, which could help mitigate the effect of cascading security failures throughout the <Company Name>infrastructure.

## Recommendations

Due to the impact to the overall organization as uncovered by this penetration test, appropriate resources should be allocated to ensure that remediation efforts are accomplished in a timely manner. While a comprehensive list of items that should be implemented is beyond the scope of this engagement, some high level items are important to mention.

<Student Name>recommends the following:

1. Example Remediation.

## Risk Rating

The overall risk identified to <Company Name>as a result of the penetration test is **\_\_\_**

# Appendix A: Vulnerability Detail and Mitigation

## Risk Rating Scale

In accordance with NIST SP 800-30, exploited vulnerabilities are ranked based upon likelihood and impact to determine overall risk.

**Default or Weak Credentials**

|  |  |
| --- | --- |
| **Rating:** |  |
| **Description:** |  |
| **Impact:** |  |
| **Remediation:** |  |

**Password Reuse**

|  |  |
| --- | --- |
| **Rating:** |  |
| **Description:** |  |
| **Impact:** |  |
| **Remediation:** |  |

**Shared Local Administrator Password**

|  |  |
| --- | --- |
| **Rating:** |  |
| **Description:** |  |
| **Impact:** |  |
| **Remediation:** |  |

**Patch Management**

|  |  |
| --- | --- |
| **Rating:** |  |
| **Description:** |  |
| **Impact:** |  |
| **Remediation:** |  |

**DNS Zone Transfer**

|  |  |
| --- | --- |
| **Rating:** |  |
| **Description:** |  |
| **Impact:** |  |
| **Remediation:** |  |

**Default Apache Files**

|  |  |
| --- | --- |
| **Rating:** |  |
| **Description:** |  |
| **Impact:** |  |
| **Remediation:** |  |

# Appendix B: Additional Details