

<<Report Title>>

<CLIENT NAME>

<Insert Date>

Executive Summary

I♥REDTEAMS, INC performed a Red Team engagement on <CLIENT NAME> domain from <DATES>.

The engagement performed by I♥REDTEAMS, INC employed real-world adversary techniques to target the systems under test. The sequence of activities in this approach involves open source intelligence (OSINT) collection, enumeration, exploitation, and attack in order to perform goal specific operational impacts.

The goals included:

* Goal 1
* Goal 2
* Goal 3
* Goal 4

Although Red Team engagements are focused on security weaknesses, several positive observations were made:

* Observation A
* Observation B
* Observation C
* Observation D

Specific observations for this assessment are outlined in the “Observations and Recommendations” section of this report. The following list is a brief summary of these observations:

* Observation A
* Observation B
* Observation C
* Observation D

A summary of goals and objectives achieved by I♥REDTEAMS, INC include the following:

* Goal 1 results
* Goal 2 results
* Goal 3 results
* Goal 4 results

I♥REDTEAMS, INC has provided specific recommendations for reducing the risks imposed by these issues in the “Observations and Recommendations” section of this report.

I♥REDTEAMS, INC appreciates the opportunity to support <CLIENT NAME> with its computer security. We look forward to assisting you and the <CLIENT NAME> IT Staff in future endeavors.

TABLE OF CONTENTS

Section Page

1 Methodology and Goals 1-1

2 Scenario and Scope 2-1

2.1 Scenario 2-1

2.2 Scope 2-1

3 Attack Narrative 3-1

3.1 Critical Step #1 3-1

3.2 Critical Step #2 3-2

3.3 Critical Step #3 3-2

4 Observatsions and Recommendations 4-1

4.1 Observation #1 4-1

4.2 Observation #2 4-1

4.3 Observation #3 4-2

5 Conclusion 5-2

# Methodology and Goals

Red Team engagements performed by I♥REDTEAMS, INC employ real-world adversary techniques to target the systems under test. I♥REDTEAMS, INC uses a red team model emulating real adversary tools, techniques and procedures (TTPs) driven by attack scenarios and goals. Unlike a traditional penetration test, the red team model allows for the testing of the entire security scope of an organization to include people, processes and technology.

The three major Red Team phases were used during the engagement to accurately emulate a realistic threat. Get In, Stay In, and Act. The sequence of activities in this approach involves open source intelligence (OSINT) collection, enumeration, exploitation, and attack. Information gathered during OSINT collection is used in conjunction with passive and active enumeration. Enumeration information typically yields details about specific hardware, services, and software running on remote machines. The next phase involves analyzing all accumulated information to identify potential attack vectors. If a weakness can be exploited, operators attempt to obtain additional access into the network or system and to collect sensitive system information to create effects and demonstrate impact to the customer. Vetted tools, methodologies, and operator experience were employed to prevent unintentional disruption, degradation or denial of service to the customer.

The goals included:

* Goal 1
* Goal 2
* Goal 3
* Goal 4

# Scenario and Scope

## Scenario

The Red Team engagement was based on the Assumed Breach Model utilizing external command and control. A coordinated phishing attack was used to begin the test and involved the support of a trusted agent. The coordinated phish was followed by a phishing attack against real-world users who did not have any knowledge of the engagement. The approach of the Assumed Breach Model allows the test to begin quickly and later use access gained from the phishing attack to validate actions.

## Scope

The scope identified by <CLIENT NAME> is to include the subnet: 111.222.333.444/24.

Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text

### MISCELLANEOUS

Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text

* List Bullet
* List Bullet
* List Bullet

#### Miscellaneous

Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text

# Attack Narrative

The following section outlines the sequence of events and highlights the key points during the engagement.





Figure 1: <DESCRIPTION>

## Critical Step #1

Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text

|  |
| --- |
| Text  Description automatically generatedFigure 1: <DESCRIPTION> |
|  |

## Critical Step #2

Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text

|  |
| --- |
| Text  Description automatically generatedFigure 2: <DESCRIPTION> |
|  |

## Critical Step #3

Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text

|  |
| --- |
| Text  Description automatically generatedFigure 3: <DESCRIPTION> |
|  |

|  |
| --- |
|  |

# Observatsions and Recommendations

The following section is intended to discuss specific scenarios that contributed to the compromise. The observations might be individually exploitable, an element of the overall compromise, or serve as a condition that directly impacts the ability to move laterally, escalate privileges, or persist.

## Observation #1

Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text

### Recommendations (Optional)

Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text

### Validation (Optional)

Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text

## Observation #2

Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text

### Recommendations (Optional)

Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text

### Validation (Optional)

Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text

## Observation #3

Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text

### Recommendations (Optional)

Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text

### Validation (Optional)

Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text

# Conclusion

I♥REDTEAMS, INC performed a Red Team engagement at the request of <CLIENT NAME> to determine the full impact of a realistic threat. The I♥REDTEAMS, INC team identified several exploitable vulnerabilities that were leveraged to establish a foothold, escalate privileges, expand access across the domain, and move proprietary information out of the network. I♥REDTEAMS, INC assesses that an external threat can successfully compromise <CLIENT NAME> systems based on the path demonstrated during the assessment. No highly specialized exploits or tools were used or required to perform any of the actions described within this report. I♥REDTEAMS, INC used a publicly available attack framework for nearly all exploitation activities. The technical skill level required to conduct individual actions ranges from low to intermediate. The required technical capability and level of access that was achieved by chaining these vulnerabilities is a cause for concern. Critical exposures and observations include <observation>, <observation>, and <observation>. I♥REDTEAMS, INC operators demonstrated that an adversary with an organized phishing campaign could potentially compromise the <CLIENT NAME> domain and remotely collect sensitive data or observe, disrupt or deny business operations.

Overall, the Red Team was able to accomplish threat objectives and it is our hope that the security posture of <CLIENT NAME> systems will be improved as a result of the efforts.