****

Executive Report

{{ project.name }}

{{ report\_date }}

# Contacts and Resources

{{ client.name }} Points of Contact

| **Name** | **Role** | **Email** |
| --- | --- | --- |
| {%tr for poc in client.contacts %} | | |
| {{ poc.name }} | {{ poc.job\_title }} | {{ poc.email }} |
| {%tr endfor %} | | |

Red Team

| **Name** | **Role** | **Email** | **Phone** |
| --- | --- | --- | --- |
| {%tr for member in team %} | | | |
| {{ member.name }} | {{ member.role }} | {{ member.email }} | {{ member.phone }} |
| {%tr endfor %} | | | |

Domain Names Used for Assessment Activities

| **Domain Name** | **Role** |
| --- | --- |
| {%tr for domain in infrastructure.domains %} | |
| {{ domain.domain }} | {{ domain.activity }} |
| {%tr endfor %} | |

Servers Used for Assessment Activities

| **IP Address** | **Purpose** | **Role** |
| --- | --- | --- |
| {%tr for server\_server in infrastructure.servers %} | | |
| {{ server\_server.ip\_address }} | {{ server\_server.activity }} | {{ server\_server.role }} |
| {%tr endfor %} | | |
| {%tr for server\_cloud in infrastructure.cloud %} | | |
| {{ server\_cloud.ip\_address }} | {{ server\_cloud.activity }} | {{ server\_cloud.role }} |
| {%tr endfor %} | | |

# Executive Summary

**<Company>** Red Team performed a Red Team engagement on the **<UPDATE ME>** environment.

The engagement performed by the **<Company>** Red Team employed real-world adversary techniques to target the systems under test. The sequence of activities in this approach **<UPDATE ME - STEP 1>**, **<UPDATE ME - STEP 2>**, **<UPDATE ME – STEP 3>**, and **<UPDATE ME – STEP 4>** in order to perform goal specific operational impacts. A summary of goals and objectives achieved by **<Company>** Red Team include the following:

| **Goals & Objectives** | | |
| --- | --- | --- |
|  | **Completed** | **Objectives** |
|  | {%tr for obj in objectives %} |
| {{ obj.percent\_complete }} | {{ obj.objective }} |
|  | {%tr endfor %} |

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

| **Observations** | |
| --- | --- |
|  | Observation 1 |
| Observation 2 |
| Observation 3 |

**<Company>** Red Team does not primarily focus on penetration testing, however, security vulnerabilities are often found while engaging on a system. As vulnerabilities are found, **<Company>** Red Team may exploit these vulnerabilities to further their main objectives.

| **Summary of Findings** | |
| --- | --- |
| {%tr for finding in findings %} | |
| {% cellbg finding.severity\_color %}{{ finding.severity }} | {{ finding.title }} |
| {%tr endfor %} | |

| **Mitre ATT&CK Heat Map** | |
| --- | --- |
|  | |

**<Company>** Red Team has provided specific recommendations for reducing the risks imposed by these issues in the “Observations and Recommendations” and “Findings” sections of this report. **<Company>** Red Team appreciates the opportunity to support {{ client.name }} with its computer security. We look forward to assisting **<Company>** internal staff and {{ client.name }}in future endeavors.

erabilities

Table of Contents

[Contacts and Resources 2](#_heading=h.gjdgxs)

[Executive Summary 3](#_heading=h.30j0zll)

[Methodology and Goals 5](#_heading=h.3znysh7)

[Scenarios and Scope 6](#_heading=h.2et92p0)

[Scenario 6](#_heading=h.tyjcwt)

[Scope 7](#_heading=h.3dy6vkm)

[Attack Narrative 7](#_heading=h.1t3h5sf)

[Critical Step 1 7](#_heading=h.4d34og8)

[Critical Step 2 7](#_heading=h.2s8eyo1)

[Observations and Recommendations 8](#_heading=h.17dp8vu)

[Detailed Findings 9](#_heading=h.3rdcrjn)

[Mitre ATT&CK Killchain 12](#_heading=h.qk2vhz4foo5r)

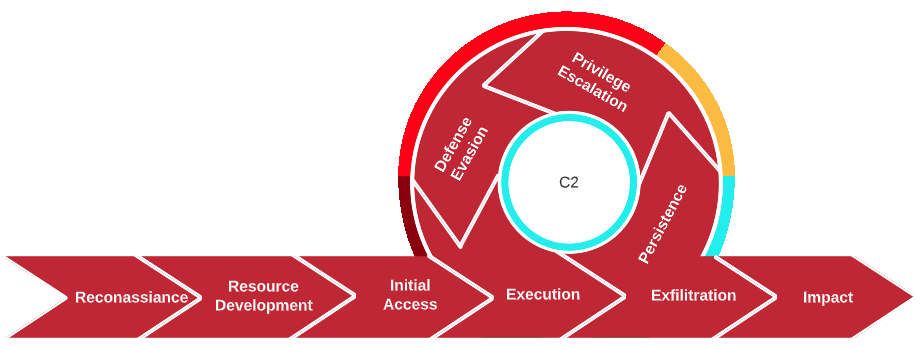
[Tactics, Techniques, and Procedures 13](#_heading=h.ecuvj8ptfg15)

[Timeline 15](#_heading=h.26in1rg)

[Conclusion 15](#_heading=h.lnxbz9)

# Methodology and Goals

Red Team engagements performed by **<Company>** Red Team employ real-world adversary techniques to target the systems under test. **<Company>** Red Team 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 **<UPDATE ME>** environment. Vetted tools, methodologies, and operator experience were employed to prevent unintentional disruption, degradation or denial of service to the **<UPDATE ME>** environment.



|  | **Goals and Objectives** | |
| --- | --- | --- |
|  | {%tr for obj in objectives %} |
| {{ obj.objective }} |
| {%tr endfor %} |

# Scenarios and Scope

## Scenario

The Red Team engagement was based on the **<UPDATE ME - Full Engagement / Assumed Breach / Custom Breach>** Model utilizing external command and control. **<UPDATE ME – Go into details of the scenario, where did we start? Any assumptions made? Quick high level draft of what happened in each phase.>** The approach of the **<UPDATE ME - Full Engagement / Assumed Breach / Custom Breach >** Model allows the test to **<UPDATE ME>**.

## Scope

The scope identified by {{ client.name }} is to:

{% for index in scope %}

{{p index.description\_rt }}

{% endfor %}

# Attack Narrative

The following section outlines the sequence of events and highlights the key points during the engagement. Critical steps are key points in an engagement that allow a Red Team operator to further an engagement to completion. As Observations and Recommendations provide details to help resolve incidents, Critical Steps should be further investigated as these are key turning points in an engagement.

## Critical Step 1

| **<UPDATE ME>** | **<APPLY GLYPH HERE>** |
| --- | --- |

## Critical Step 2

| **<UPDATE ME>** | **<APPLY GLYPH HERE>** |
| --- | --- |

# Observations 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 | |
| --- | --- |
|  | **<UPDATE ME>** |
| Recommendation | |
|  | **<UPDATE ME>** |
| Validation | |
|  | **<UPDATE ME>** |

| Observation 2 | |
| --- | --- |
|  | **<UPDATE ME>** |
| Recommendation | |
|  | **<UPDATE ME>** |
| Validation | |
|  | **<UPDATE ME>** |

# Detailed Findings

Detailed findings provide **<Company>** with vulnerabilities found during an investigation. Each finding will provide the CVSS score, affected hosts, a detailed description and solution, as well as evidence to help engineers recreate the vulnerability.

| {%tr for finding in findings %} | |
| --- | --- |
| {% if finding.severity == ‘Critical’ %} | |
| **Critical Finding** – {{ finding.title }} | |
|  | **CVSS Score:** {{ finding.cvss\_score }} |
| **Affected Hosts:**  {{p finding.affected\_entities\_rt }} |
| **Description:**  {{p finding.description\_rt }}  **Impact:**  {{p finding.impact\_rt }} |
| **Replication Steps:**  {{p finding.replication\_steps\_rt }} |
| **Host Detection Techniques:**  {{p finding.host\_detection\_techniques\_rt}} |
| **Solution:**  {{p finding.recommendation\_rt }} |
| {% endif %} | |
| {%tr endfor %} | |

| {%tr for finding in findings %} | |
| --- | --- |
| {% if finding.severity == ‘High’ %} | |
| **High Finding** – {{ finding.title }} | |
|  | **CVSS Score:** {{ finding.cvss\_score }} |
| **Affected Hosts:**  {{p finding.affected\_entities\_rt }} |
| **Description:**  {{p finding.description\_rt }}  **Impact:**  {{p finding.impact\_rt }} |
| **Replication Steps:**  {{p finding.replication\_steps\_rt }} |
| **Host Detection Techniques:**  {{p finding.host\_detection\_techniques\_rt}} |
| **Solution:**  {{p finding.recommendation\_rt }} |
| {% endif %} | |
| {%tr endfor %} | |

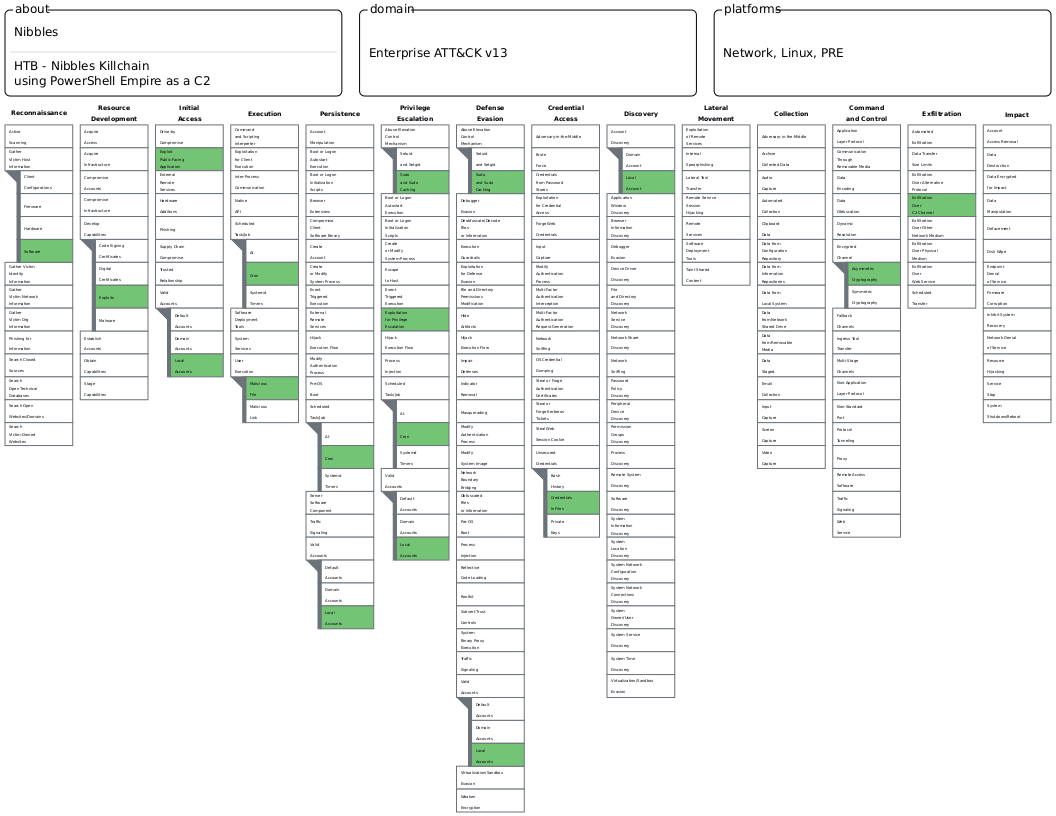
| {%tr for finding in findings %} | |
| --- | --- |
| {% if finding.severity == ‘Medium’ %} | |
| **Medium Finding** – {{ finding.title }} | |
|  | **CVSS Score:** {{ finding.cvss\_score }} |
| **Affected Hosts:**  {{p finding.affected\_entities\_rt }} |
| **Description:**  {{p finding.description\_rt }}  **Impact:**  {{p finding.impact\_rt }} |
| **Replication Steps:**  {{p finding.replication\_steps\_rt }} |
| **Host Detection Techniques:**  {{p finding.host\_detection\_techniques\_rt}} |
| **Solution:**  {{p finding.recommendation\_rt }} |
| {% endif %} | |
| {%tr endfor %} | |

| {%tr for finding in findings %} | |
| --- | --- |
| {% if finding.severity == ‘Low’ %} | |
| **Low Finding** – {{ finding.title }} | |
|  | **CVSS Score:** {{ finding.cvss\_score }} |
| **Affected Hosts:**  {{p finding.affected\_entities\_rt }} |
| **Description:**  {{p finding.description\_rt }}  **Impact:**  {{p finding.impact\_rt }} |
| **Replication Steps:**  {{p finding.replication\_steps\_rt }} |
| **Host Detection Techniques:**  {{p finding.host\_detection\_techniques\_rt}} |
| **Solution:**  {{p finding.recommendation\_rt }} |
| {% endif %} | |
| {%tr endfor %} | |

| {%tr for finding in findings %} | |
| --- | --- |
| {% if finding.severity == ‘Informational’ %} | |
| **Informational Finding** – {{ finding.title }} | |
|  | **CVSS Score:** {{ finding.cvss\_score }} |
| **Affected Hosts:**  {{p finding.affected\_entities\_rt }} |
| **Description:**  {{p finding.description\_rt }}  **Impact:**  {{p finding.impact\_rt }} |
| **Replication Steps:**  {{p finding.replication\_steps\_rt }} |
| **Host Detection Techniques:**  {{p finding.host\_detection\_techniques\_rt}} |
| **Solution:**  {{p finding.recommendation\_rt }} |
| {% endif %} | |
| {%tr endfor %} | |

# Mitre ATT&CK Killchain

**<Company>** Red Team will map threats to the Mitre ATT&CK killchain. This allows business decisions to be made in alignment with cost and effective results. Each Tactic, and their Technique, have been outlined below, detailing the killchain. Some Tactics may not apply, their Techniques will not be provided:



* <https://mitre-attack.github.io/attack-navigator/>
* **<LINK TO A NAVIGATOR JSON FILE>**

## 

## Tactics, Techniques, and Procedures

TA0043 - Reconnaissance

[T1592.002 - Gather Victim Host Information: Software](https://attack.mitre.org/techniques/T1592/002/)

TA0042 - Resource Development

[T1587.004 - Develop Capabilities: Exploits](https://attack.mitre.org/techniques/T1587/004/)

TA0001 - Initial Access

[T1190 - Exploiting Public-Facing Applications](https://attack.mitre.org/techniques/T1190/)

[T1078.003 - Valid Accounts: Local Accounts](https://attack.mitre.org/techniques/T1078/003/)

TA0002 - Execution

[T1053.003 - Scheduled Task/Job: Cron](https://attack.mitre.org/techniques/T1053/003/)

[T1204.002 - User Execution: Malicious File](https://attack.mitre.org/techniques/T1204/002/)

TA0003 - Persistence

[T1053.003 - Scheduled Task/Job: Cron](https://attack.mitre.org/techniques/T1053/003/)

[T1078.003 - Valid Accounts: Local Accounts](https://attack.mitre.org/techniques/T1078/003/)

TA0004 - Privilege Escalation

[T1548.003 - Abuse Elevation Control Mechanism: Sudo and Sudo Caching](https://attack.mitre.org/techniques/T1548/003/)

[T1068 - Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068/)

[T1053.003 - Scheduled Task/Job: Cron](https://attack.mitre.org/techniques/T1053/003/)

[T1078.003 - Valid Accounts: Local Accounts](https://attack.mitre.org/techniques/T1078/003/)

TA0005 - Defense Evasion

[T1548.003 - Abuse Elevation Control Mechanism: Sudo and Sudo Caching](https://attack.mitre.org/techniques/T1548/003/)

[T1078.003 - Valid Accounts: Local Accounts](https://attack.mitre.org/techniques/T1078/003/)

TA0006 - Credential Access

[T1552.001 - Unsecured Credentials: Credentials In Files](https://attack.mitre.org/techniques/T1552/001/)

TA0007 - Discovery

[T1087.001 - Account Discovery: Local Account](https://attack.mitre.org/techniques/T1087/001/)

TA0008 - Lateral Movement

TA0009 - Collection

TA0011 - Command and Control

[T1573.002 - Encrypted Channel: Asymmetrical Cryptography](https://attack.mitre.org/techniques/T1573/002/)

TA0010 - Exfiltration

[T1041 - Exfiltration Over C2 Channel](https://attack.mitre.org/techniques/T1041/)

TA0040 - Impact

# Timeline

The timeline provides insight into the Red Team engagement. All timestamps are within UTC and converted from their respectable Host via C2 logs, host logs, GhostWriter, and Vectr.

# Conclusion

**<Company>** Red Team performed a Red Team engagement at the request of {{ client.name }} to determine the full impact of a **<UPDATE ME>**. The **<Company>** Red Team identified **<UPDATE ME>**. **<Company>** Red Team assesses that an external threat can successfully **<UPDATE ME>** 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. **<Company>** Red Team used a **<UPDATE ME = “publicly available attack framework”|”privately built tool”>** 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 a .NET TCP Client deployed, lack of antivirus or minimal configuration of an antivirus, and disaster recovery taking longer than allowed for most Enterprise customers. **<Company>** Red Team operators demonstrated that an adversary with compromised Developer credentials could potentially compromise the O11 environment 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 **<Company>** platform will be improved as a result of the efforts.