Compromise SocialNet

Attack Tree Report

April 20, 2024

Contents

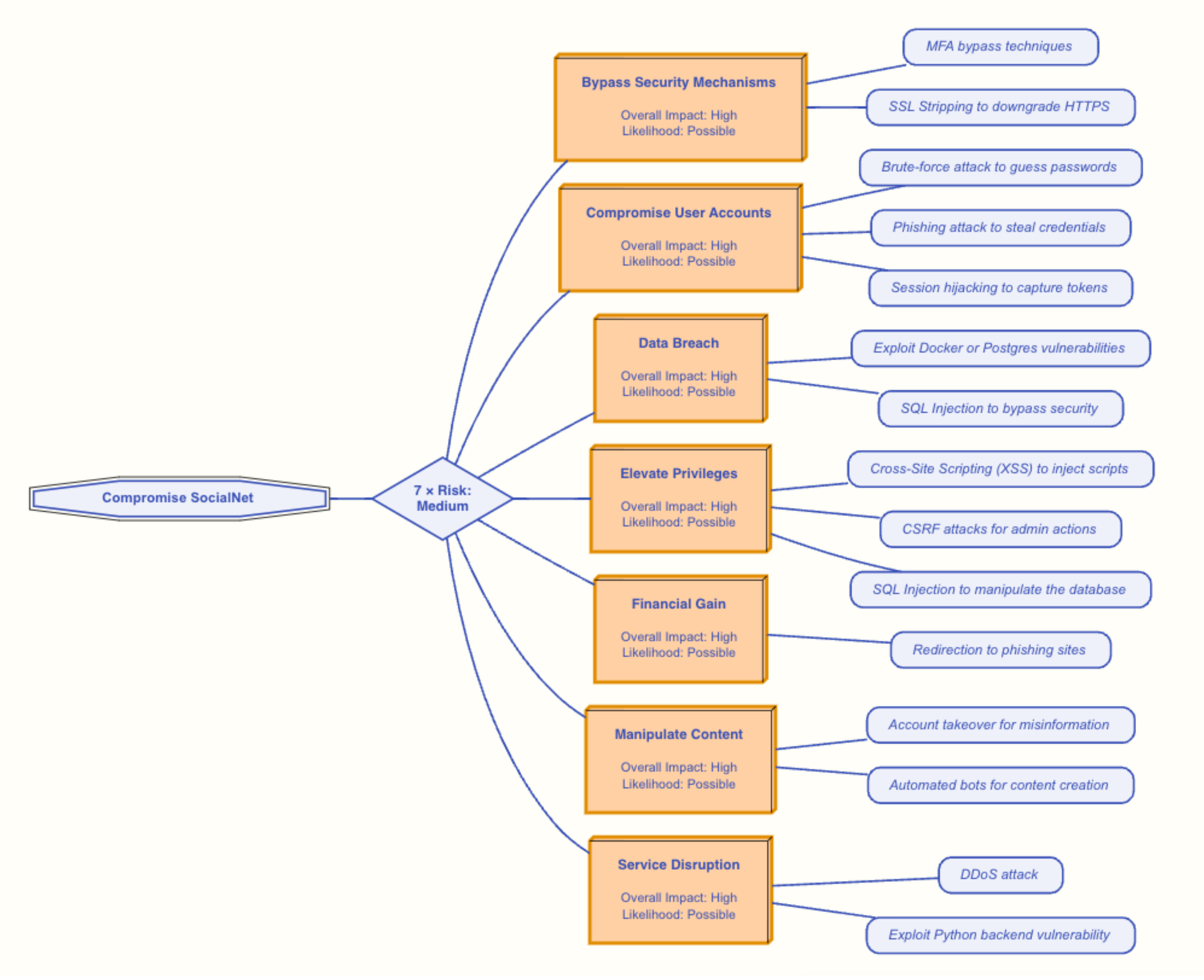
1. Summary

1.1. Attack Tree

In a scenario-driven approach an attack tree was created to evaluate possible Attack Paths for attackers reaching the following 7 identified Attack Goals in the context of Compromise SocialNet:

- Bypass Security Mechanisms
- Compromise User Accounts
- Data Breach
- Elevate Privileges
- Financial Gain
- Manipulate Content
- Service Disruption

To execute these Attack Paths, 15 Attack Vectors were identified as possible initial steps for attackers, each with different likelihood. See the Attack Goals chapter of this report for more details.


Compromise SocialNet
7 × Risk: Medium
Bypass Security Mechanisms
Overall Impact: High
Likelihood: Possible
Compromise User Accounts
Overall Impact: High
Likelihood: Possible
Data Breach
Overall Impact: High
Likelihood: Possible
Elevate Privileges
Overall Impact: High
Likelihood: Possible
Financial Gain
Overall Impact: High
Likelihood: Possible
Manipulate Content
Overall Impact: High
Likelihood: Possible
Service Disruption
Overall Impact: High
Likelihood: Possible
MFA bypass techniques
SSL Stripping to downgrade HTTPS
Brute-force attack to guess passwords
Phishing attack to steal credentials
Session hijacking to capture tokens
Exploit Docker or Postgres vulnerabilities
SQL Injection to bypass security
Cross-Site Scripting (XSS) to inject scripts
CSRF attacks for admin actions
SQL Injection to manipulate the database
Redirection to phishing sites
Account takeover for misinformation
Automated bots for content creation
DDoS attack
Exploit Python backend vulnerability

2. Attack Goals

The following sub-chapters evaluate the 7 identified Attack Goals of the Compromise SocialNet analysis showing current and simulated remaining risks along with their Attack Paths as subtrees.

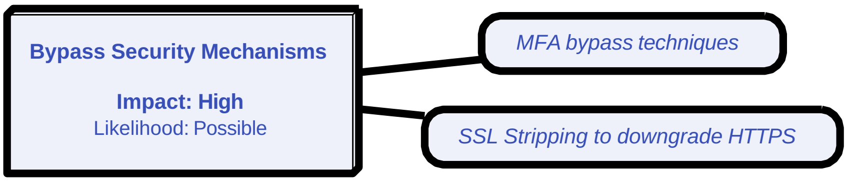
The root of the subtree represents the respective Attack Goal in the scenario under investigation. Starting from the root, the listing of possible steps with which attackers can reach the respective node is refined for level. This results in possible Attack Paths, which can be executed via different Attack Vectors (the leafs of the tree) as first steps. See the Legend chapter of this report for more details about the Value Ranges and the Color Scheme used in the tree diagrams of this report.

2.1. Bypass Security Mechanisms

Impact: High

Current Risk: Medium

The current risk (taking already implemented Security Controls into account) is medium.
The following graph represents the current subtree of the Attack Goal Bypass Security Mechanisms:

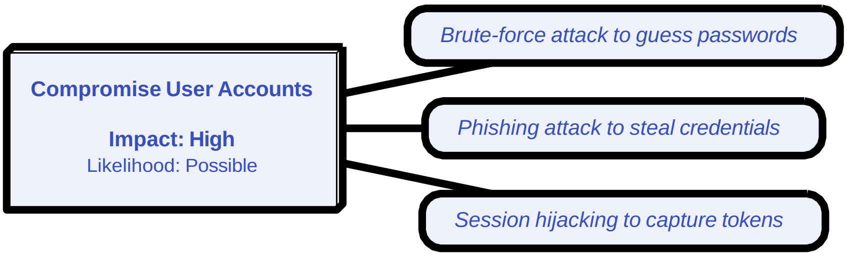


2.2. Compromise User Accounts

Impact: High

Current Risk: Medium

The current risk (taking already implemented Security Controls into account) is medium.
The following graph represents the current subtree of the Attack Goal Compromise User Accounts:

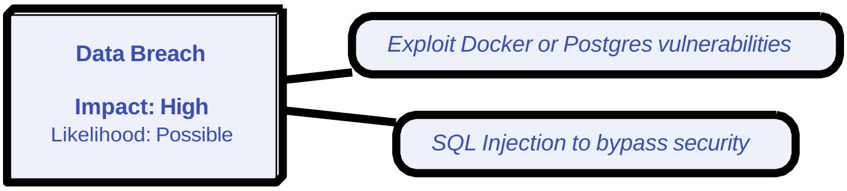

Compromise User Accounts
Impact: High
Likelihood: Possible
Brute-force attack to guess passwords
Phishing attack to steal credentials
Session hijacking to capture tokens

2.3. Data Breach

Impact: High

Current Risk: Medium

The current risk (taking already implemented Security Controls into account) is medium.
The following graph represents the current subtree of the Attack Goal Data Breach:

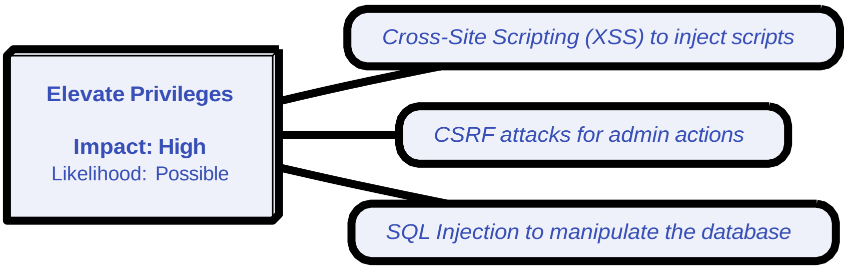

Data Breach
Impact: High
Likelihood: Possible
Exploit Docker or Postgres vulnerabilities
SQL Injection to bypass security

2.4. Elevate Privileges

Impact: High

Current Risk: Medium

The current risk (taking already implemented Security Controls into account) is medium.
The following graph represents the current subtree of the Attack Goal Elevate Privileges:

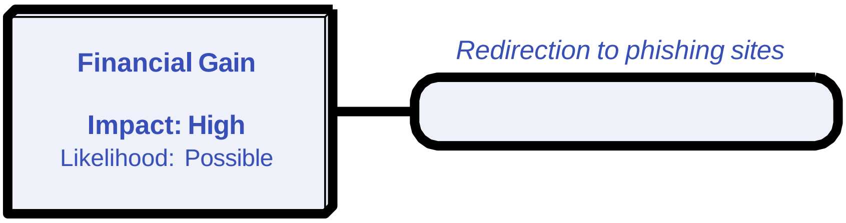

Elevate Privileges
Impact: High
Likelihood: Possible
Cross-Site Scripting (XSS) to inject scripts
CSRF attacks for admin actions
SQL Injection to manipulate the database

2.5. Financial Gain

Impact: High

Current Risk: Medium

The current risk (taking already implemented Security Controls into account) is medium.
The following graph represents the current subtree of the Attack Goal Financial Gain:

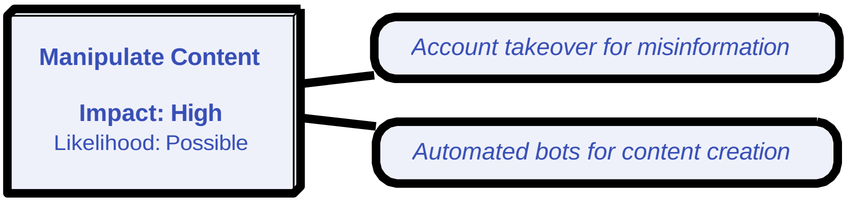


2.6. Manipulate Content

Impact: High

Current Risk: Medium

The current risk (taking already implemented Security Controls into account) is medium.
The following graph represents the current subtree of the Attack Goal Manipulate Content:

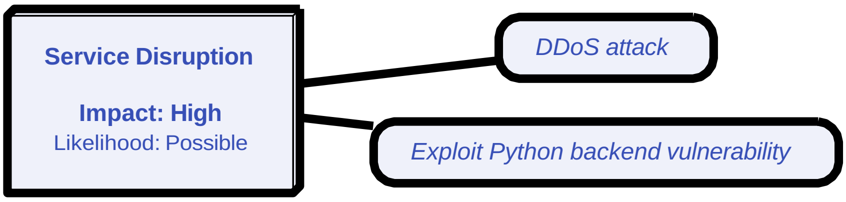

Manipulate Content
Impact: High
Likelihood: Possible
Account takeover for misinformation
Automated bots for content creation

2.7. Service Disruption

Impact: High

Current Risk: Medium

The current risk (taking already implemented Security Controls into account) is medium.
The following graph represents the current subtree of the Attack Goal Service Disruption:



3. Legend

3.1. Value Ranges

The following value ranges are used in this report:

Type	Value Range
Risk	Very High → High → Medium → Low → Very Low → Almost None
Attack Likelihood	Very Likely → Likely → Possible → Unlikely → Very Unlikely → Almost None
Threat Actor	Script Kiddie → Hacktivist → Attacker Group Outside → Social Engineer → Attacker Group Inside → Compromised Employee → Evil Admin
Attack Complexity	Very Simple → Simple → Ordinary → Complex → Very Complex
Control Kind	Architecture → Development → Operations → Business → Process
Control Effort	Very High → High → Medium → Low → Very Low
Control Status	Failed → Ignored → Discussion → Blocked → Deferred → Unsettled → Medium term → Short term → Implemented

3.2. Color Scheme

The following color scheme is used in the tree graphs (Attack paths without any security control are outlined in black):

Type	Color Scheme
Attack Likelihood	Very Likely → Likely → Possible → Unlikely → Very Unlikely → Almost None
Threat Actor	Script Kiddie → Hacktivist → Attacker Group Outside → Social Engineer → Attacker Group Inside → Compromised Employee → Evil Admin

Disclaimer

The authors conducted this attack tree analysis based on the provided information about the applications and systems that existed as of this report's date. Information security threats are continually changing, with new vulnerabilities discovered on a daily basis, and no application can ever be 100% secure no matter how much security analysis and testing is conducted. It is recommended to execute security analysis and testing on a regular basis (for example yearly) to ensure a high ongoing level of security and constantly check for new attack vectors. This report cannot and does not protect against personal or business loss as the result of use of the applications or systems or the recommendations or measures described. The authors and the attack tree toolkit developers offer no warranties, representations or legal certifications concerning the applications or systems they analyze or review and the recommendations or measures they define. By using this information you agree that the authors and the attack tree toolkit developers shall be held harmless in any event. All software includes defects: nothing in this document is intended to represent or warrant that security analysis and testing was complete and without error, nor does this document represent or warrant that the application tested is suitable to task, free of other defects than reported, fully compliant with any industry standards, or fully compatible with any operating system, hardware, or other application. This report is intended for internal, confidential use by the client. The recipient is obligated to ensure the confidential contents are kept secret. The recipient assumes responsibility for further distribution of this document. In this particular project, a timebox approach was used to define the consultant effort. This means that the authors allotted a prearranged amount of time to identify and document risks. Because of this, there is no guarantee that all possible risks are discovered. Furthermore, the security analysis applies to a snapshot of the current state at the examination time.