Red teaming: A Pentest case study

pentest
INFORMATION SECURITY ASSURANCE

The scenario: A global technology organisation wanted to see if it was possible for an attacker to take control of their network and steal sensitive product designs.

The goal: Gain domain level administrative rights.

The result: We were able to achieve the goal within the time frame set.

Here's how we achieved the goal

Escalate privilege

An out of date operating system introduced several vulnerabilities which could be exploited using freely available exploit code in order to escalate privileges to the local SYSTEM user.

OSINT

Openly available information sources were used to map out the staff hierarchy and departments, including those that worked in the IT department.

Physical security

Attempted entry to physical site was aborted due to increased security presence.

User password hashes

With the higher level of privilege, it was possible to dump the operating system user password hashes.

However, due to the passwords being of adequate length and complexity, these could not be cracked to reveal their plaintext.

Web applications

A number of web app vulnerabilities were discovered during the research stage, these were targeted in an attempt to bypass perimeter defences.

Remote file include (RFI)

An RFI flaw allowed for arbitrary code to be executed on the underlying server, which was used to gain command shell control over the system.

SQL injection

SQL injection vulnerability allowed us to retrieve contents of a user table in the database. Passwords were stored as MD5 hashes but could be cracked to reveal plaintext passwords.

File upload

Insufficient controls around file uploads on a public-facing website allowed for arbitrary code to be uploaded and executed on the remote system.

File permissions meant that execution was not possible.

Java deserialisation

It was possible to provide a serialised Java object to a Java application which was subsequently deserialised and executed on the remote system.

Goal achieved

Privileged credentials allowed us to gain access to the Domain Controller servers for the network, resulting in a complete compromise of all systems and data.

Spear phishing attack

A phishing email was sent to the IT Administrators, asking for IT support on the systems being monitoring.

This encouraged the IT Administrator to authenticate to these systems using a Domain Admin user account, therefore allowing us to capture credentials due to the previous compromise of internal servers.

Public disclosure

Passwords gained from public disclosures used to gain access to the accounts of two members of staff (password reuse).

Office 365

Office 365 was used throughout the organisation. This was identified as a potential source of valuable information.

SharePoint access

Credentials obtained are used to attempt log in to office 365 and SharePoint systems.

Password re-use and lack of multi-factor authentication mean SharePoint was compromised.

Documents in SharePoint reveal creds, IP addresses and connection details of VPN servers.

Outlook access

Credentials obtained through phishing are successfully used to compromise internal users Outlook accounts.

No valuable information is found.

Internal infrastructure

The internal infrastructure contained a number of networks, VPNs and servers. If we could compromise these they would potentially lead us to our goal.

Internal servers

Passwords from SQL injection used to attempt access to corporate VPN. Due to password reuse this is successful and gave us access to the corporate network.

The credentials disclosed via SharePoint are used to compromise multiple internal servers and workstations. These were monitored over time in an attempt to capture user logins.

Domain admin credentials were not available on the servers compromised within the limited time frame of the engagement

VPN compromise

Passwords obtained from public disclosure were used to gain access to corporate VPN. Due to password reuse this is successful and gave us access to the corporate network.

Password re-use

Credentials obtained from USB drop were used in an attempt to gain admin access to internal networks.

User privilege levels are too low.

Internal network

The breached web server appeared to be in a DMZ (demilitarized zone).

Due to its segregated nature, lateral movement was not possible.

Phishing

A phishing attack was launched, mimicking a genuine Office 365 password reset email. A fake login page was also created to allow our team to steal any details submitted.

A number of employees fell for the scam and entered their details.

USB drop

A USB containing keylogger malware was dropped outside company premises in the hope someone would find it and plug it into a company workstation.

An unsuspecting employee plugged in the device and provided us with login credentials.

Could a malicious threat actor gain access to your "crown jewels"?

Our red team engagements simulate the actions of a real-world cyber-attack, helping you to uncover organisational vulnerabilities which could be used to compromise sensitive data, to put your securtity defences to the test and to ensure your most important assets are as secure as possible.

Want to find out more about our information security testing services? Visit us at **www.pentest.co.uk**, call us on **+44 (0)161 233 0100** or email us via **contact@pentest.co.uk**