Purple team bootcamp

Post-System Compromise Operations and Techniques

Prepared By:
Kazim Ali Obad

Supervisor:
Anmar Mohammed

Mohammed baqer

2026/2/11

scholarkazim

Table of Contents

scholarkazim

Compromise Operations

System Compromise:

When a system is compromised by an attacker, they bypass the traditional security measures like IDS (Intrusion Detection System), IPS (Intrusion Prevention System), and firewalls. Once these defenses are evaded, the attacker establishes a connection between their system and the compromised one.

اختراق النظام:

عندما يتعرض النظام للاختراق من قبل مهاجم، يقوم المهاجم بتجاوز التدابير الأمنية التقليدية مثل IDS)نظام كشف التسلل(، IPS(نظام منع التسلل)، والجدران النارية. بعد أن يتجاوز هذه الدفاعات، يقوم المهاجم بإنشاء اتصال بين جهازه والنظام المخترق.

Creating a Connection:

After compromising the system, the attacker sets up a **Command and Control (C2) Server**, through which they can send commands, exfiltrate data, and control the system remotely.

إنشاء الاتصال:

بعد اختراق النظام، يقوم المهاجم بإنشاء **خادم للتحكم والقيادة(C2)** ، من خلاله يمكنه إرسال الأوامر، وسحب البيانات، والتحكم في النظام عن بُعد.

2. DNS Tunneling

What is DNS Tunneling?

DNS Tunneling is a technique used by attackers to evade detection by embedding malicious data within DNS queries. DNS queries are typically allowed through firewalls and IDS/IPS systems, making it an ideal method for data exfiltration.

scholarkazim

ما هو أنفاقDNS ؟

أنفاق DNS هي تقنية يستخدمها المهاجمون لتجنب الكشف من خلال تضمين البيانات الضارة داخل استعلامات DNS. استعلامات DNS عادة ما يتم السماح بها من خلال الجدران النارية وأنظمة IDS/IPS، مما يجعلها طريقة مثالية لاستخراج البيانات.

How It Works:

The attacker encodes data into DNS queries, which are then sent to a DNS server controlled by the attacker. This method allows the attacker to bypass security measures and exfiltrate sensitive data.

كيف يعمل؟

يقوم المهاجم بتشفير البيانات في استعلاماتDNS ، ثم يرسلها إلى خادم DNS يتحكم فيه. هذه الطريقة تسمح للمهاجم بتجاوز التدابير الأمنية وسحب البيانات الحساسة.

3. Command and Control (C2) Server

Role of C2 Server:

The C2 server is the heart of an attacker's ability to control a compromised system. Once the connection between the victim and the attacker is established, the C2 server acts as the intermediary, allowing the attacker to issue commands, extract files, and continue the attack.

دور خادم:C2

خادم C2 هو قلب قدرة المهاجم على التحكم في النظام المخترق. بمجرد إنشاء الاتصال بين الضحية والمهاجم، يعمل خادم C2 كوسيط، مما يسمح للمهاجم بإصدار الأوامر، واستخراج الملفات، ومواصلة الهجوم.

scholarkazim

4. DNS Resolution and Data Exfiltration

DNS Queries:

When a user types a domain name like "google.com", the system resolves it to an IP address. However, in a compromise scenario, an attacker can send DNS queries containing encoded malicious data, such as passwords or sensitive files.

استعلامات DNS:

عندما يكتب المستخدم اسم نطاق مثل"google.com" ، يقوم النظام بحل النطاق إلى عنوان IP. ولكن في حالة الاختراق، يمكن للمهاجم إرسال استعلامات DNS تحتوي على بيانات ضارة مشفرة، مثل كلمات السر أو الملفات الحساسة.

DNS Tunneling for Data Exfiltration:

Attackers use DNS tunneling to bypass traditional security and exfiltrate data without triggering alarms. They encode data like passwords or documents into DNS queries, which appear as normal DNS traffic.

أنفاق DNS لاستخراج البيانات:

يستخدم المهاجمون أنفاق DNS لتجاوز الأمان التقليدي واستخراج البيانات دون تفعيل الإنذارات. يشفرون البيانات مثل كلمات السر أو المستندات في استعلاماتDNS ، التي تظهر كحركة مرور DNS عادية.

5. RITA (Real Intelligence Threat Analytics)

What is RITA?

RITA is a tool used for network traffic analysis. It specifically looks for **C2 Servers** and other indicators of compromise (IOCs). By analyzing **ZEEK logs**, RITA helps to detect suspicious communication patterns and unauthorized access attempts.

scholarkazim

ما هي ريتا؟

ريتا هي أداة تستخدم لتحليل حركة مرور الشبكة. وهي تبحث بشكل محدد عن **خوادم C2** وغيرها من مؤشرات الاختراق .(IOCs) من خلال تحليل **سجلاتZEEK** ، تساعد ريتا في اكتشاف أنماط الاتصال المشبوهة ومحاولات الوصول غير المصرح بها.

How RITA Helps in Detection:

RITA analyzes traffic logs to identify potential security threats such as **beaconing**, **data exfiltration**, and **DNS Tunneling**. It allows analysts to detect and respond to advanced persistent threats (APTs).

كيف تساعد ريتا في الكشف؟

تقوم ريتا بتحليل سجلات حركة المرور لتحديد التهديدات الأمنية المحتملة مثل **الإشارة المتكررة، استخراج البيانات، و أنفاق DNS**. وتسمح للمحللين بالكشف عن والرد على التهديدات المستمرة المتقدمة.(APTs)

6. (IOCs)

What is an IOC?

An **Indicator of Compromise (IOC)** is evidence that indicates a system has been compromised. It helps investigators track the attacker's steps. For instance, compromised servers or suspicious files can be identified as IOCs.

ما هو الـIOC ؟

مؤشر الاختراق هو دليل يُظهر أن النظام قد تم اختراقه. يساعد المحققين في تتبع خطوات المهاجم. على سبيل المثال، يمكن تحديد الخوادم المخترقة أو الملفات المشبوهة كمؤشرات للاختراق.

scholarkazim

The Role of IOCs in Cybersecurity

IOCs provide valuable information to help security teams identify a compromise and investigate it further. This is the key to tracking malicious activity in an organization.

دور الـ IOCs في الأمن السيبراني

توفر الـ IOCs معلومات قيمة تساعد فرق الأمان في تحديد الاختراق والتحقيق فيه بشكل أكبر. هذا هو المفتاح لتتبع الأنشطة الخبيثة في المنظمة.

7. ZEEK Logs and Security Analysis

What are ZEEK Logs?

ZEEK logs are captured network traffic that provide detailed information about network activity. They are crucial for detecting suspicious behavior.

ما هي سجلات ZEEK ؟

سجلات ZEEK هي حركة مرور الشبكة الملتقطة التي توفر معلومات مفصلة حول النشاط الشبكي. وهي ضرورية لاكتشاف السلوك المشبوه.

Summarizing Logs with ZEEK

ZEEK doesn't show raw packet data like Wireshark. Instead, it summarizes the logs, making it easier to focus on the relevant security data.

تلخيص السجلات باستخدام ZEEK

لا تعرض ZEEK البيانات الخام مثل Wireshark. بدلاً من ذلك، تقوم بتلخيص السجلات، مما يجعل من الأسهل التركيز على بيانات الأمان ذات الصلة.

Scholarkazim

RITA's Role in Analyzing ZEEK Logs

RITA is used to analyze **ZEEK logs** to identify potential **C2 servers** and suspicious traffic patterns, such as **beaconing** or **data exfiltration**.

دور ريتا في تحليل سجلاتZEEK

تُستخدم ريتا لتحليل **سجلات ZEEK** لتحديد الخوادم **C2** المحتملة وأنماط الحركة المشبوهة مثل **الإشارة المتكررة** أو **استخراج البيانات**

8. Beaconing and C2 Servers

What is Beaconing?

Beaconing refers to a technique where the attacker's system continuously checks for a connection to the compromised system, often every few seconds. This behavior is often used to maintain persistence.

ما هي الإشارة المتكررة؟

الإشارة المتكررة تشير إلى تقنية حيث يتحقق نظام المهاجم بشكل مستمر من وجود اتصال بالنظام المخترق، غالبًا كل بضع ثوانٍ. يتم استخدام هذا السلوك غالبًا للحفاظ على الوصول المستمر.

How RITA Detects C2 Servers and Beaconing

RITA can detect beaconing patterns by checking for regular connections between the compromised system and the C2 server. If beaconing is found, it indicates that the system has been compromised.

كيف تكشف ريتا عن خوادم C2 والإشارة المتكررة

يمكن لريتا اكتشاف أنماط الإشارة المتكررة عن طريق التحقق من وجود اتصالات منتظمة بين النظام المخترق وخادم C2. إذا تم العثور على إشارة متكررة، فهذا يشير إلى أن النظام قد تم اختراقه.

scholarkazim

9. DNS Tunneling for Data Exfiltration

What is DNS Tunneling?

DNS Tunneling is a method where malicious data is encoded in DNS queries, allowing attackers to exfiltrate data by hiding it in DNS traffic, which is usually allowed through firewalls.

ما هو أنفاقDNS ؟

أنفاق DNS هي طريقة حيث يتم تشفير البيانات الضارة في استعلاماتDNS ، مما يسمح للمهاجمين باستخراج البيانات من خلال إخفائها في حركة مرورDNS ، التي يتم السماح بها عادةً عبر الجدران النارية.

Using RITA to Detect DNS Tunneling

RITA helps detect **DNS tunneling** by analyzing DNS queries and looking for unusual patterns that indicate hidden data transmission.

استخدام ريتا لاكتشاف أنفاقDNS

تساعد ريتا في اكتشاف **أنفاق DNS** عن طريق تحليل استعلامات DNS والبحث عن أنماط غير عادية تشير إلى نقل بيانات مخفية.

scholarkazim