

# Consegna BW 3

## Consegna: Analisi Malware, analisi traffico DNS, Buffer Overflow, analisi di rete

### Sezione 1: Laboratori Malware Analysis

**Obiettivo:** Scaricare il malware indicato e condurre un'analisi completa per creare un report dettagliato.

**1. Malware da analizzare:**

- Link: [AdwereCleaner.exe](#)

**2. Attività richieste:**

- Effettuare un'analisi forense completa.
- Generare un report che includa:
  - Tecniche di propagazione.
  - Evasione dei sistemi di sicurezza.
  - Comunicazione con i server C2.

**3. Strumenti suggeriti:**

- Any.run.
  - Sandbox per test.
  - Disassemblatori (es. IDA Pro, Ghidra).
- 

### Sezione 2: Laboratori di Analisi DNS

**Obiettivo:** Analizzare il traffico DNS per identificare query sospette e risposte anomale.

**1. Attività:**

- Catturare il traffico DNS tramite strumenti come Wireshark.

- Esaminare query e risposte DNS.

## 2. Risultati attesi:

- Identificazione di query potenzialmente dannose.
- Generazione di report con i dettagli tecnici.

## 3. Riferimenti:

- [Lab Exploring DNS Traffic](#)
- 

## Sezione 3: Laboratori di Buffer Overflow

**Obiettivo:** Identificare e sfruttare vulnerabilità di tipo buffer overflow in un'applicazione.

### 1. Attività richieste:

- Determinare il punto di overflow in un'applicazione vulnerabile.
- Sviluppare un exploit funzionante.

### 2. Strumenti:

- Metasploit.
- Script Python per payload personalizzati.

### 3. Report richiesto:

- Introduzione al concetto di overflow.
- Dettagli tecnici sull'exploit creato.
- Soluzioni di mitigazione.

### 4. Riferimenti:

- [Guida al Buffer Overflow](#)
- 

## Sezione 4: Network Forensics e PCAP Analysis

**Obiettivo:** Estrarre eseguibili e identificare attività sospette da file PCAP.

### 1. Attività:

- Utilizzare Wireshark per analizzare i pacchetti.
- Estrarre file eseguibili dai dati catturati.

## 2. Risultati attesi:

- Report con dettagli sui file estratti.
- Analisi del comportamento del file.

## 3. Riferimenti:

- [Extract Executable from PCAP](#)
- 

# Sezione 5: Bonus

## Bonus 1:


- Studiare un ulteriore link fornito da Any.run e spiegare l'analisi in un breve report.
- [Link Any.run Bonus 1](#)

## Bonus 2:

- Investigare SQL injection e DNS exfiltration tramite Security Onion.
- [Lab Details](#)

## Bonus 3:

- Utilizzare Security Onion per isolare un host compromesso.
  - [Lab Using 5-Tuple](#)
- 

 **Chiavi:** [cybersecurity, malware\_analysis, penetration\_testing, forensics, ethical\_hacking]