

## Bài: 6.3 System Hacking - Lab Image Steganography, xóa chính sách kiểm kê trên windows & xóa nhật ký

Xem bài học trên website để ủng hộ Kteam: [6.3 System Hacking - Lab Image Steganography, xóa chính sách kiểm kê trên windows & xóa nhật ký](#)

Mọi vấn đề về lỗi website làm ảnh hưởng đến bạn hoặc thắc mắc, mong muốn khóa học mới, nhằm hỗ trợ cải thiện Website. Các bạn vui lòng phản hồi đến Fanpage [How Kteam](#) nhé!

### Lab 6-6: Image Steganography

#### Image Steganography sử dụng QuickStego

1. Mở ứng dụng **QuickStego**

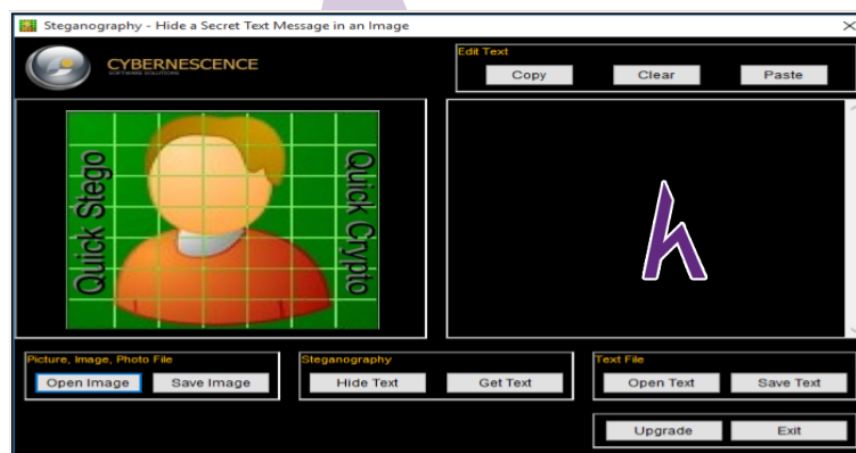


Figure 6-57 QuickStego Application for Image Steganography

2. Upload một ảnh. Ảnh này được đặt tên là **Cover** bởi vì nó sẽ ẩn văn bản.
3. Nhập văn bản hay upload tệp văn bản.
4. Nhấn nút **Hide Text**.
5. Lưu ảnh. Ảnh này chứa thông tin ẩn được đặt tên là **Stego Object**.

### Steganalysis

**Steganalysis** là bản phân tích những thông tin đáng ngờ, sử dụng kỹ thuật steganography để phát hiện và phục hồi thông tin ẩn. Steganalysis sẽ thăm dò hình ảnh chứa dữ liệu mã hóa.

**Steganalysis** phải đối mặt những thử thách về độ chính xác, hiệu quả và mẫu vật bị nhiễu trong khi phát hiện dữ liệu mã hóa.

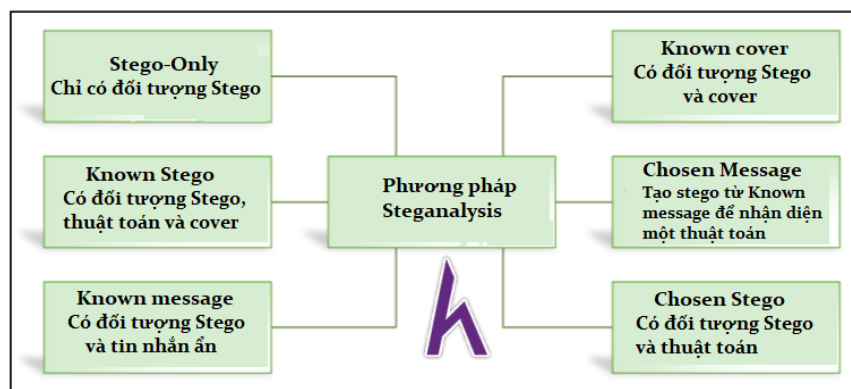


Figure 6-63 Steganalysis Methods

## Che dấu vết

Sau khi tiếp cận mục tiêu, tăng đặc quyền, thực thi ứng dụng, bước tiếp theo là xóa bỏ dấu vết. Trong công đoạn này, kẻ tấn công phải xóa nhật ký hoạt động, tin nhắn error và các bằng chứng khác để tránh bị phát hiện tấn công.

Những kĩ thuật thường được dùng để che dấu vết là:

- Vô hiệu hóa kiểm kê
- Xóa nhật kí
- Điều chỉnh nhật kí

## Vô hiệu hóa kiểm kê

Đây là phương pháp tiếp cận tốt nhất để đề phòng cơ chế bảo mật phát hiện và cảnh báo mục tiêu sự đột nhập từ bên ngoài. **Vô hiệu hóa kiểm kê** cũng là kĩ thuật tốt nhất để xóa dấu vết và đề phòng phát hiện hoặc để lại rất ít bằng chứng.

Khi bạn vô hiệu hóa kiểm kê trên hệ thống mục tiêu, nó không chỉ ngăn ghi lại nhật kí hoạt động mà còn hạn chế sự phát hiện. Chức năng kiểm kê được kích hoạt để theo dõi hoạt động. Khi kiểm kê bị vô hiệu hóa, mục tiêu sẽ không thể ghi lại nhật kí những hoạt động quan trọng, không chỉ là bằng chứng tấn công mà còn bao gồm những thông tin nguồn của kẻ tấn công.

Nhập dòng lệnh sau để liệt kê các categories được kiểm kê:

```
C:\Windows\System32>auditpol /list /category /v
```

Để kiểm tra chính sách kiểm kê tất cả category, nhập dòng lệnh sau:

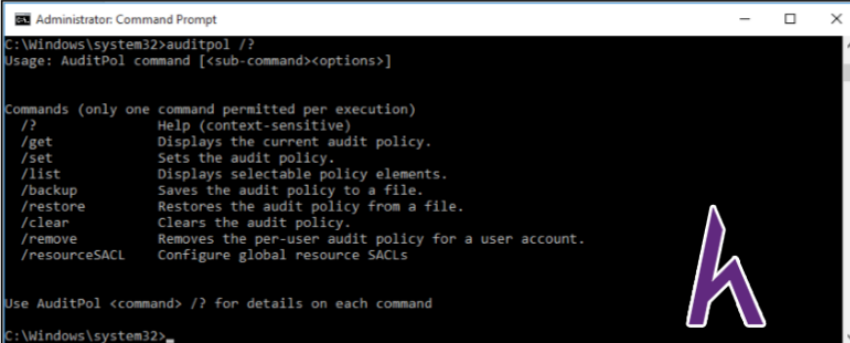
```
C:\Windows\system32>auditpol /get /category: *
```

## Lab 6-7: Xóa chính sách kiểm kê trên Windows

### Kích hoạt và xóa chính sách kiểm kê

Để kiểm tra những lựa chọn sẵn có của dòng lệnh, nhập

```
C:\Windows\system32> auditpol /?
```



```
Administrator: Command Prompt
C:\Windows\system32>auditpol /?
Usage: AuditPol command [<sub-command><options>]

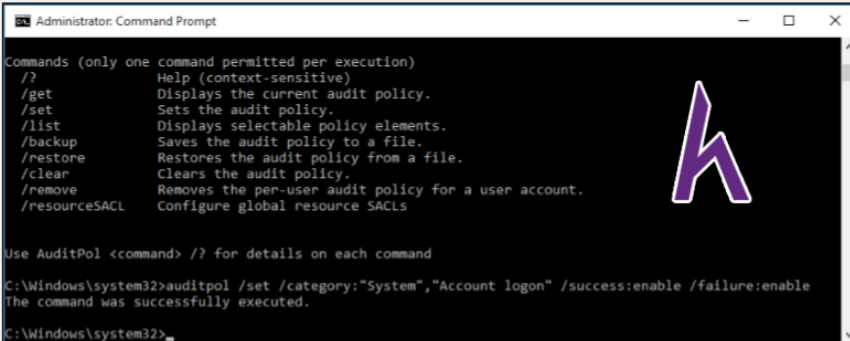
Commands (only one command permitted per execution)
/?          Help (context-sensitive)
/get        Displays the current audit policy.
/set        Sets the audit policy.
/list       Displays selectable policy elements.
/backup     Saves the audit policy to a file.
/restore    Restores the audit policy from a file.
/clear      Clears the audit policy.
/remove     Removes the per-user audit policy for a user account.
/resourceSACL  Configure global resource SACLs

Use AuditPol <command> /? for details on each command
C:\Windows\system32>
```

Figure 6-65 Auditpol Utility Options

Nhập dòng lệnh sau để kích hoạt kiểm kê cho hệ thống và tài khoản đăng nhập:

```
C:\Windows\system32>auditpol /set /category:"System","Account logon" /success:enable /failure:enable
```

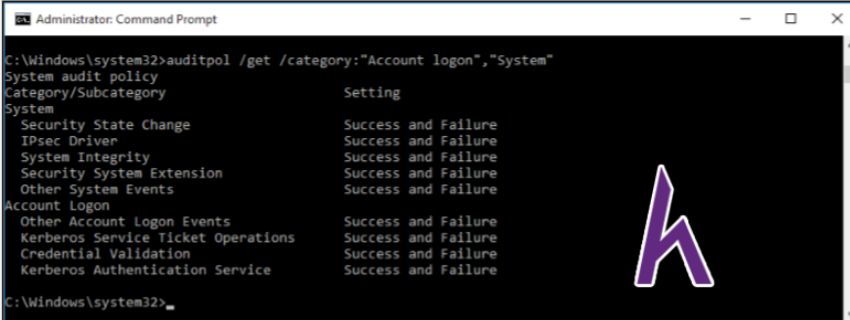


```
Administrator: Command Prompt
C:\Windows\system32>auditpol /set /category:"System","Account logon" /success:enable /failure:enable
The command was successfully executed.
C:\Windows\system32>
```

Figure 6-66 Enabling Audit Policy for System and Account login

Kiểm tra xem kiểm kê đã được kích hoạt chưa, nhập

```
C:\Windows\system32>auditpol /get /category:"Account logon","System"
```



```
Administrator: Command Prompt
C:\Windows\system32>auditpol /get /category:"Account logon","System"
System audit policy
Category/Subcategory      Setting
System
  Security State Change    Success and Failure
  IPsec Driver              Success and Failure
  System Integrity          Success and Failure
  Security System Extension Success and Failure
  Other System Events       Success and Failure
Account Logon
  Other Account Logon Events Success and Failure
  Kerberos Service Ticket Operations Success and Failure
  Credential Validation     Success and Failure
  Kerberos Authentication Service Success and Failure
C:\Windows\system32>
```

Figure 6-67 Verifying Enabled Audit Policies

Để xóa chính sách kiểm kê, nhập dòng lệnh

```
C:\Windows\system32>auditpol /clear
```

**Are you sure?** Nhấn **Y** (nhấn **N** hay để hủy hay bất cứ nào nút nào để tiếp tục).

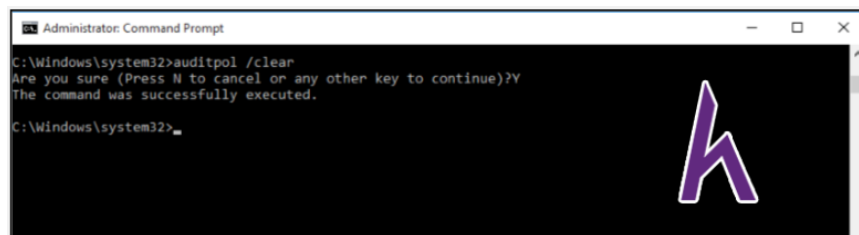


Figure 6-68 Clearing Audit policies

Để kiểm tra kiểm kê, nhập

```
C:\Windows\system32>auditpol /get /category:"Account logon","System"
```

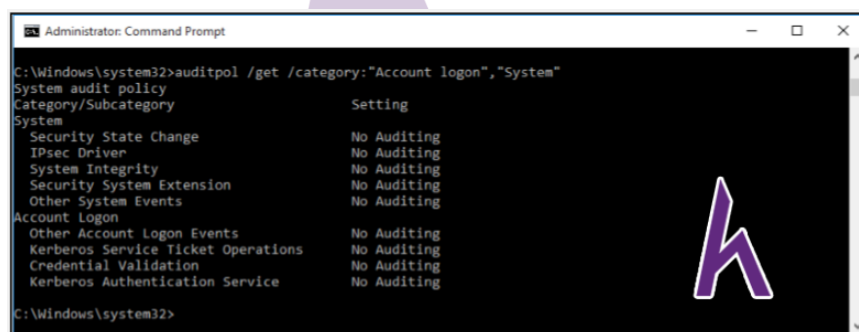


Figure 6-69 Verifying Cleared Audit Policy

## Xóa nhật kí

Một kĩ thuật che giấu khác là xóa nhật kí. Nhật kí có thể bị xóa bằng công cụ dòng lệnh cũng như xóa thủ công bằng Control Panel trên nền tảng Windows.

## Lab 6-8: Xóa nhật kí trên Windows

### Xóa nhật kí thủ công trên nền tảng Windows

1. Vào **Control Panel**
2. Nhấn chọn **System and Security**
3. Click vào **Event Viewer**
4. Chọn **Windows Log**.

Ở đây bạn sẽ thấy nhiều loại nhật kí, như ứng dụng, bảo mật, thiết lập, hệ thống và hoạt động chuyển tiếp. Bạn có thể nhập, xuất và xóa nhật kí bằng **Action Section** trong bảng bên phải.

## Lab 6-9: Xóa nhật kí trên Linux

### Xóa nhật kí thủ công trên nền tảng Linux

1. Vào **Kali Linux Machine**.

2. Mở thư mục **/var**

3. Đến folder **Logs**.

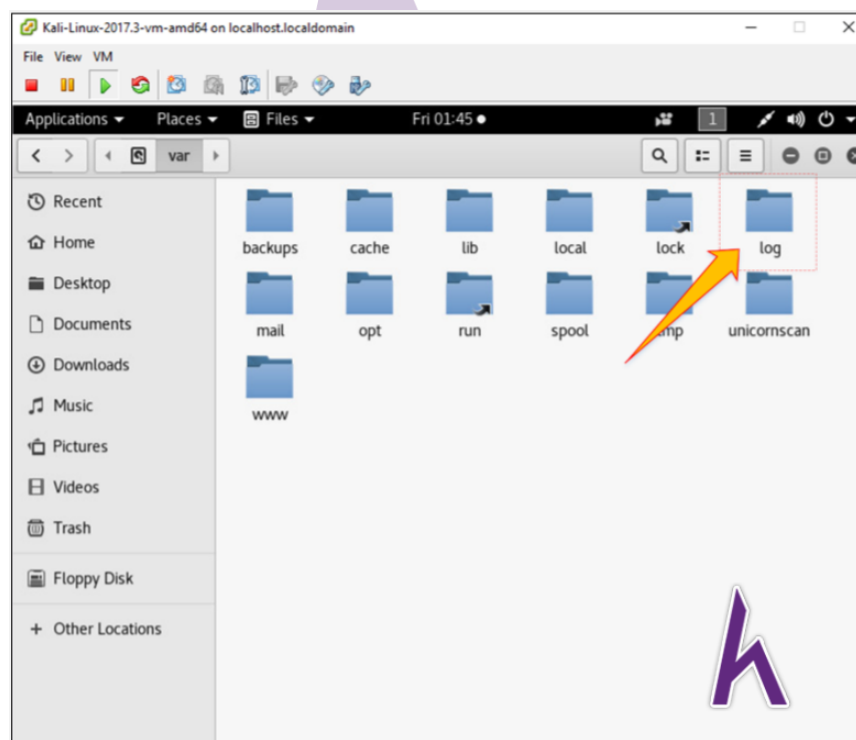


Figure 6-76 /var directory

4. Chọn bất kì một tệp nhật kí.

5. Mở tệp nhật kí bất kì; bạn có thể xóa tất cả hay bất kì mục nhập nào ở đây.

### Mindmap

