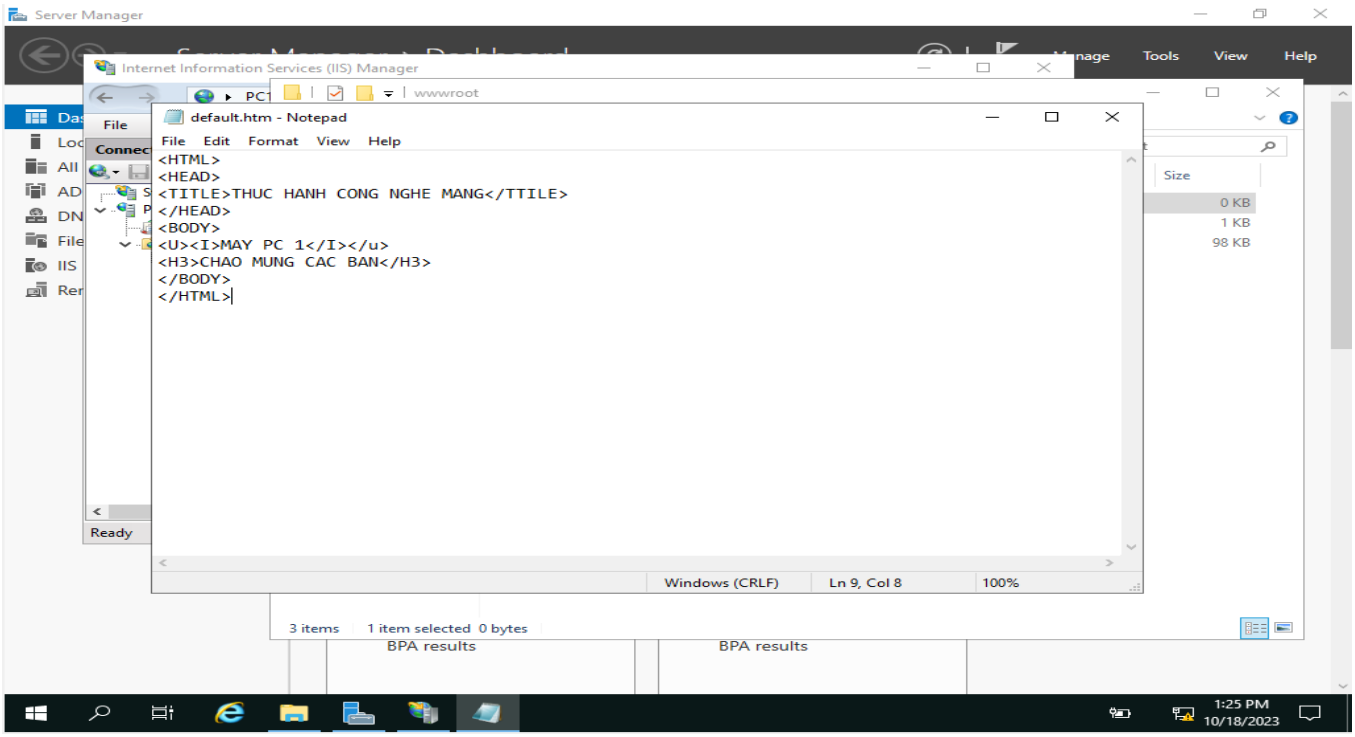
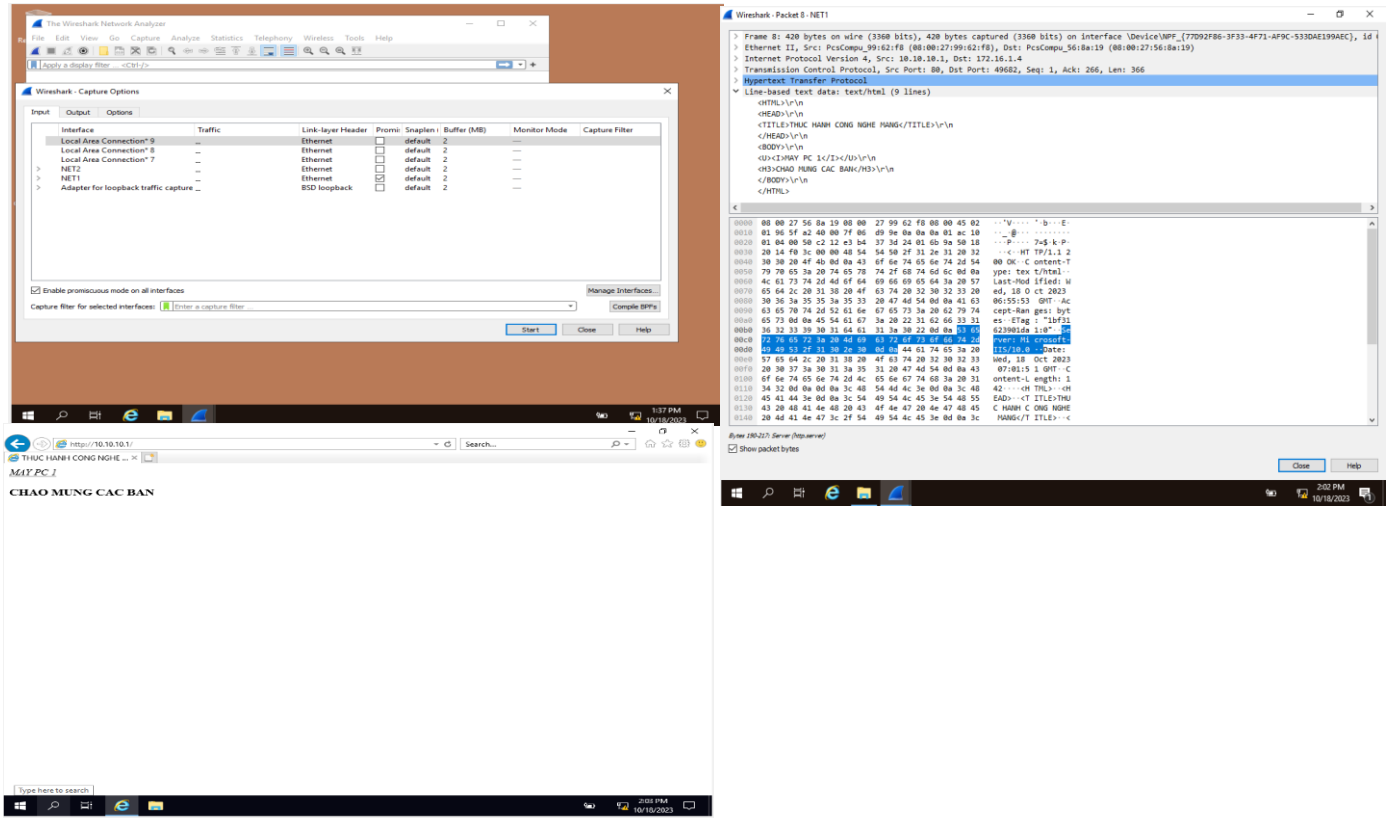
Phần 1: bảo mật dữ liệu web:

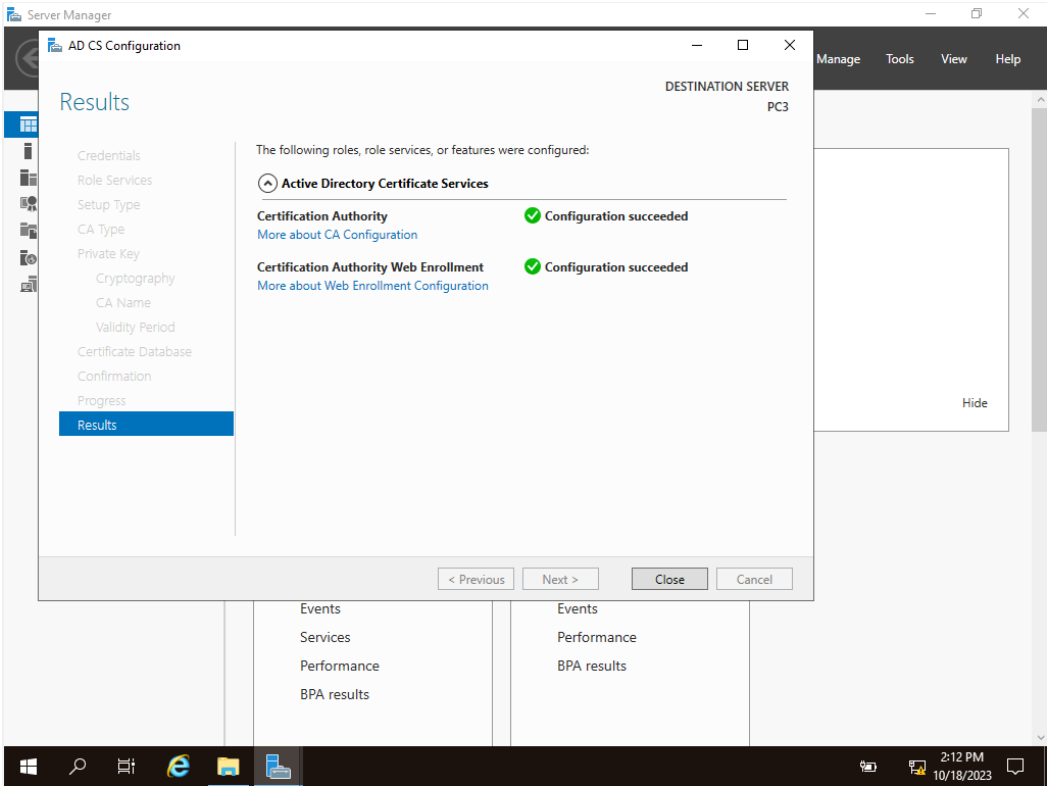
1. Cấu hình PC1 thành máy chủ Web và tạo một trang chủ đơn giản:



2. Cài đặt Wireshark để bắt gói tin trên máy trung gian (PC3):

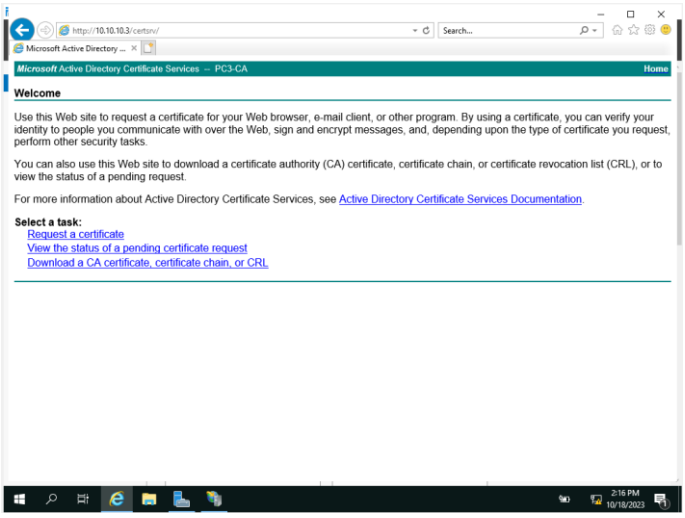


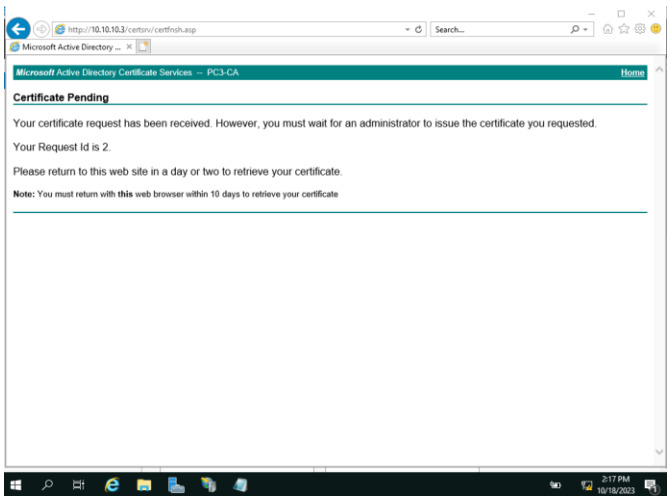
3. Cấu hình PC3 thành Certificate Authority (CA) để cung cấp dịch vụ chứng thực chìa khóa công khai.



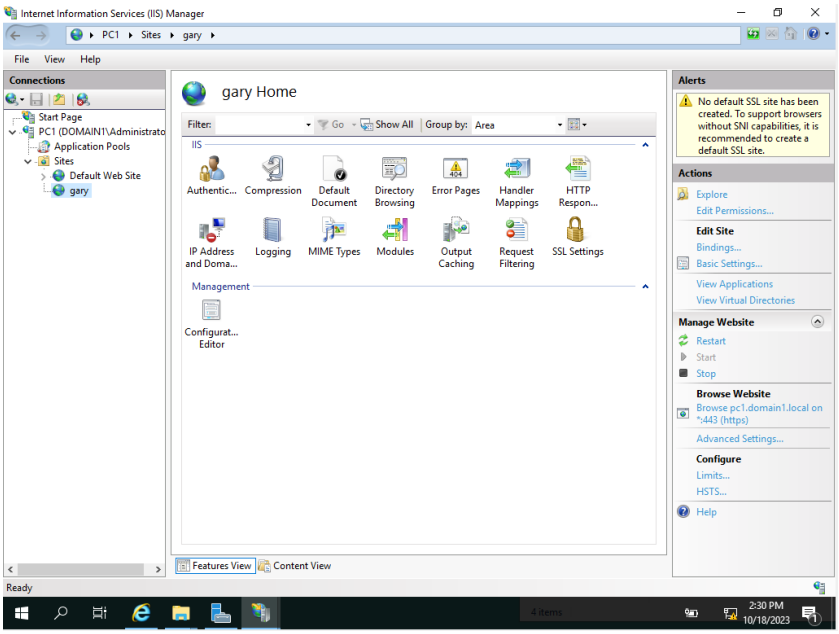
4. Cấu hình PC1 sử dụng HTTP bảo mật (HTTPS).

Bước 1: Đăng ký chứng thực:

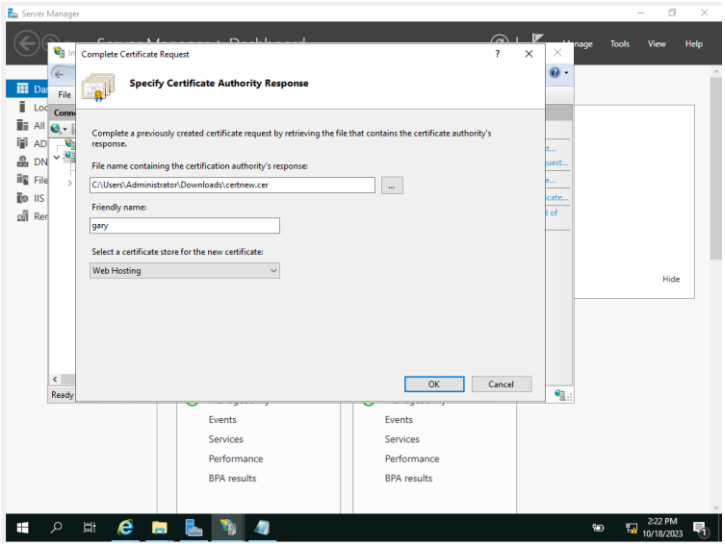


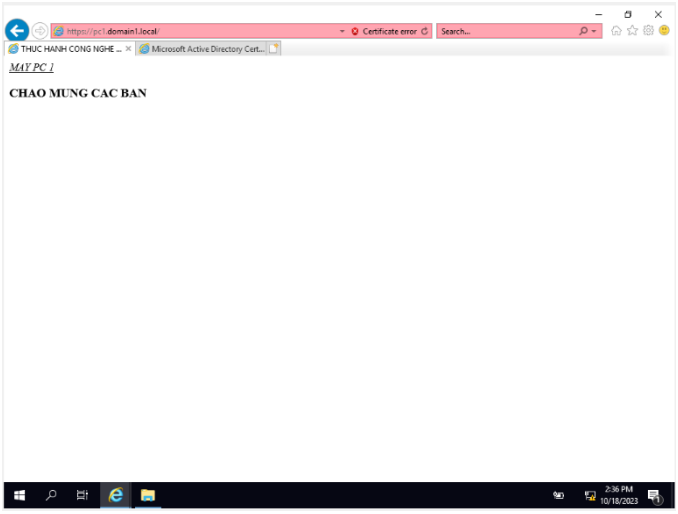


Bước 2: Tạo trang web bảo mật:



Bước 3: Thêm máy chủ CA vào danh sách tin tưởng:

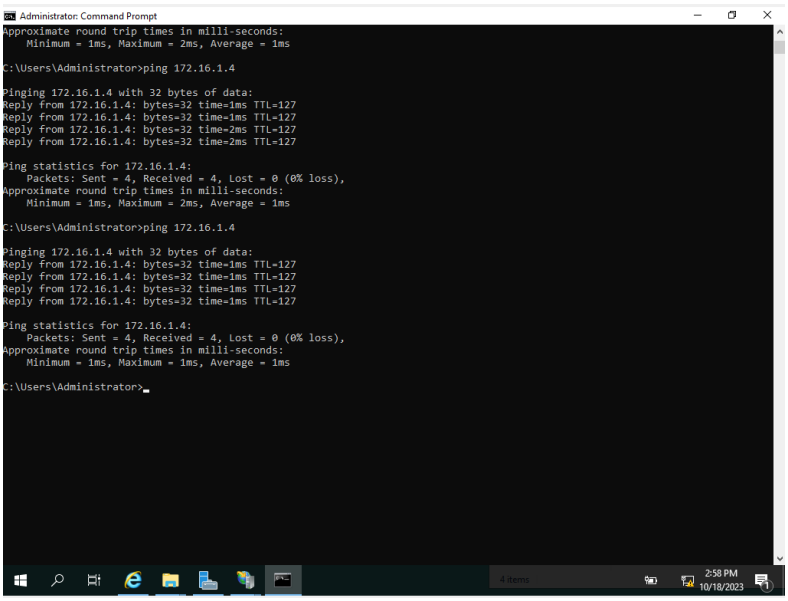


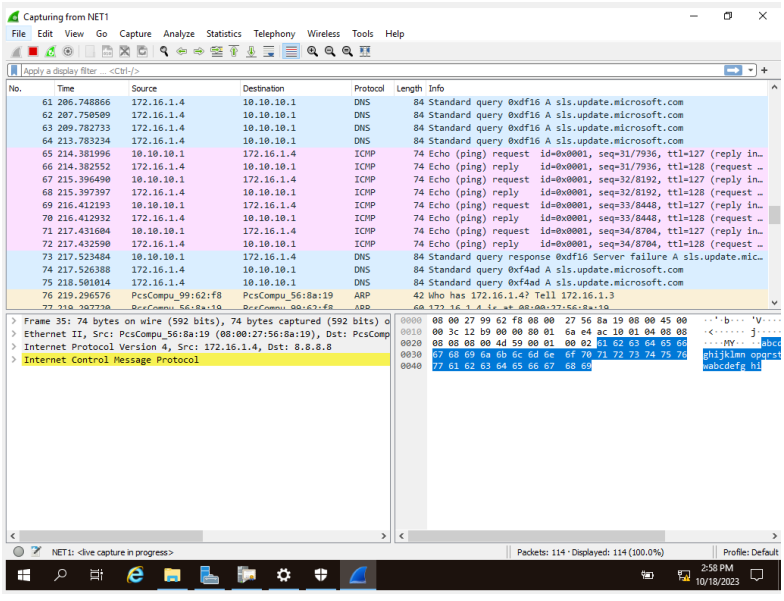


Phần 2: bảo mật dữ liệu trong mạng doanh nghiệp:

5. Tiến hành gia nhập domain1.local trên PC4.

6. Thực hiện lại câu 2, thay duyệt web bằng ICMP (PC1 ping PC2) → Thấy được loại gói tin là ICMP (không được mã hóa)





7. Cấu hình bảo mật mã hóa các gói tin ICMP trong mạng sử dụng mã hóa Kerberos.

8. Khởi động lại Máy PC1, sau đó khởi động lại máy PC4. Thực hiện lại câu 6 và kiểm tra kết quả.