

Chương V. YÊU CẦU VỀ KỸ THUẬT

Mục 1. Yêu cầu về kỹ thuật

1.1. Giới thiệu chung về dự toán mua sắm

- Tên dự toán: Trang bị phần mềm phục vụ kiểm thử xâm nhập và giả lập tấn công APT.

- Đơn vị mua sắm: Công ty Công nghệ Thông tin VNPT – Chi nhánh Tập đoàn Bưu chính Viễn thông Việt Nam.

- Nguồn vốn: Chi phí SXKD của Trung tâm ATTT.

- Thời gian thực hiện: 2025 - 2026.

- Địa điểm thực hiện: Thành phố Hà Nội.

- Quy mô mua sắm:

TT	Danh mục	Mô tả	Đơn vị tính	Số lượng
1	Phần mềm kiểm thử xâm nhập và giả lập tấn công APT	Bản quyền 01 năm sử dụng phần mềm kiểm thử xâm nhập và giả lập tấn công APT, có các chức năng chính: - Kiểm định đánh giá, kiểm tra những nguy cơ mất an ninh an toàn mạng, máy tính - Giả lập tấn công có chủ đích; các cuộc tấn công phức tạp gây rủi ro cho các cơ quan, tổ chức	License	01

1.2. Yêu cầu kỹ thuật của hàng hoá

STT	Yêu cầu kỹ thuật
I	Nhóm tính năng kiểm thử xâm nhập
1	Phần mềm phải có khả năng thu thập thông tin mạng và xây dựng hồ sơ hệ thống.
2	Phần mềm phải có khả năng xác định hệ điều hành, thiết bị, dịch vụ và ứng dụng.
3	Phần mềm phải có khả năng thu thập thông tin xác thực và băm.
4	Phần mềm phải có khả năng sử dụng các thông tin định danh đã thu thập được như một phần của bài kiểm tra tấn công.

STT	Yêu cầu kỹ thuật
5	Phần mềm phải có khả năng kiểm soát hệ thống thông qua lỗi xác thực yếu theo cách thủ công hoặc tự động
6	Phần mềm phải có khả năng hỗ trợ chức năng xác minh các lỗi đã khắc phục để kiểm tra lại các lỗ hổng được tìm thấy, đánh giá hiệu quả khắc phục.
7	Phần mềm phải có khả năng nhập kết quả từ nhiều chương trình dò quét lỗ hổng mạng và xác nhận kết quả về khả năng khai thác.
8	Phần mềm phải hỗ trợ REST API.
9	Phần mềm phải có khả năng nằm giữa người dùng và các trang web thực tế để chụp bắt thông tin trao đổi.
10	Phần mềm phải có khả năng tự động ghi lại người dùng trong bài kiểm tra nhận thức.
11	Phần mềm phải hỗ trợ khả năng báo cáo toàn diện và có thể tùy chỉnh.
II	Nhóm tính năng giả lập tấn công APT.
1	Phần mềm phải có chức năng tạo payload, có hỗ trợ các cơ chế vượt qua các giải pháp antivirus hoặc EDR.
2	Beacon hỗ trợ thực thi các tập lệnh PowerShell scripts, logs keystrokes, takes screenshots, downloads và chuyển tiếp phiên sang các payload khác.
3	Phần mềm phải hỗ trợ nhập vào một C2 profile để trông giống như một tác nhân khác. Sử dụng HTTP, HTTPS và DNS để đi ra ngoài mạng và chống lại việc bị chặn. Sử dụng các named pipe để điều khiển agent, peer-to-peer, qua giao thức SMB.
4	Phần mềm phải hỗ trợ thiết lập máy chủ C2
5	Phần mềm phải hỗ trợ sửa đổi các chỉ báo mạng để hòa hợp với lưu lượng truy cập bình thường hoặc che giấu các hoạt động của nó bằng cách mô phỏng các loại phần mềm độc hại khác nhau.
6	Phần mềm phải hỗ trợ hoạt động nhóm, trong đó các thành viên trong nhóm có thể cùng đăng nhập được vào một phiên máy chủ, nhờ đó các thành viên trong nhóm có thể chia sẻ thông tin với nhau như các host, dữ liệu thu thập được.
7	Phần mềm phải hỗ trợ encode dữ liệu trong lưu lượng trao đổi giữa beacon và server.
8	Phần mềm phải hỗ trợ Beacon Object Files (BOFs)
9	Phần mềm phải hỗ trợ thực hiện và có khả năng tinh chỉnh hoạt động của kỹ thuật Process Injection.
10	Phần mềm phải hỗ trợ thực hiện kỹ thuật "Sleep" cho beacon
11	Phần mềm phải có thể hỗ trợ ghi nhật ký tất cả các hoạt động.

1.3. Các yêu cầu khác:

TT	Nội dung yêu cầu	
1	Dịch vụ hỗ trợ kỹ thuật	Nhà thầu cam kết dịch vụ hỗ trợ kỹ thuật 24/7 tối thiểu 12 tháng kể từ thời điểm nghiệm thu đưa vào sử dụng.
2	Điều kiện hợp đồng	Nhà thầu cam kết đáp ứng các quy định tại Chương VI. Điều kiện chung của hợp đồng và Chương VII. Điều kiện cụ thể của hợp đồng;

Lưu ý: Tài liệu chứng minh Yêu cầu kỹ thuật của hàng hóa:

Ngoài việc giới thiệu và trình bày tổng thể, chi tiết về hàng hóa và dịch vụ, nhà thầu phải trả lời mức độ đáp ứng các yêu cầu kỹ thuật theo mẫu sau đây:

TT	Yêu cầu	Mức độ đáp ứng (chọn Đạt/Không Đạt)	Dẫn chứng trong E-HSDT
[Yêu cầu trong E-HSMT]	Yêu cầu: [đưa phần mô tả yêu cầu từ E-HSMT]		Chỉ dẫn tới dẫn chứng trong E-HSDT

Nhà thầu phải nêu rõ đã giải thích/dẫn chứng tại phần nào, mục nào, tài liệu nào của E-HSDT đáp ứng yêu cầu kỹ thuật gì trong E-HSMT, để bên mời thầu dễ dàng tham chiếu khi xem xét E-HSDT.

Trường hợp nhà thầu chỉ dẫn, dẫn chiếu không đúng, hoặc thông tin trong E-HSDT được trích dẫn không chính xác, và thông tin trong E-HSDT không được tìm thấy trên các địa chỉ chính thức của hãng sản xuất sản phẩm dự thầu đáp ứng yêu cầu kỹ thuật trong E-HSMT thì yêu cầu đó coi như trả lời không hợp lệ và chấm không đạt.

Cung cấp tài liệu kỹ thuật (catalogue, datasheet, hướng dẫn sử dụng...) để chứng minh tuyên bố đáp ứng, cũng như nêu rõ nguồn gốc của các tài liệu này. Trong trường hợp tài liệu kỹ thuật nhà thầu cung cấp có nội dung khác với tài liệu kỹ thuật trên website chính thức của Hãng sản xuất thì bên mời thầu sẽ căn cứ theo tài liệu kỹ thuật trên website chính thức của Hãng sản xuất để đánh giá về khả năng đáp ứng yêu cầu kỹ thuật của hàng hóa chào thầu.

Mục 2. Bản vẽ

Không có bản vẽ

Mục 3. Kiểm tra và thử nghiệm

Theo Chương VII. Điều kiện cụ thể của hợp đồng - Mục E_ĐKC 21.1.