Phần 2. YÊU CẦU VỀ KỸ THUẬT

Chương V. YÊU CẦU VỀ KỸ THUẬT

Yêu cầu về kỹ thuật mang tính kỹ thuật thuần túy và các yêu cầu khác liên quan đến việc cung cấp dịch vụ (trừ giá). Yêu cầu về kỹ thuật phải được nêu đầy đủ, rõ ràng và cụ thể để làm cơ sở cho nhà thầu lập E-HSDT.

Trong yêu cầu về kỹ thuật không được đưa ra các điều kiện nhằm hạn chế sự tham gia của nhà thầu hoặc nhằm tạo lợi thế cho một hoặc một số nhà thầu gây ra sự cạnh tranh không bình đẳng.

Yêu cầu về kỹ thuật bao gồm các nội dung cơ bản như sau:

1. Giới thiệu chung về dự án/dự toán mua sắm, gói thầu:

- Dự án: Thuê tấn công (Redteam) vào Trung tâm dữ liệu và Trung tâm CSKH của EVNSPC nhằm phát hiện các lỗ hổng và khắc phục
- Địa điểm thực hiện dự án: Trụ sở Tổng công ty Điện lực miền Nam, 72 Hai Bà Trưng, Phường Sài Gòn, Thành phố Hồ Chí Minh
- Quy mô dự án:

STT	Nội dung yêu cầu	Đơn vị tính	Số lượng	Yêu cầu về cung cấp dịch vụ thuộc gói thầu	Thời gian thực hiện gói thầu	Ghi chú
1	- **Dịch vụ Redteam**	Gói	01	Theo yêu cầu kỹ thuật	Trong vòng 56 ngày kể từ ngày hợp đồng có hiệu lực.	

2. Mục tiêu công việc:

- Kiểm thử xâm nhập Red Team để phát hiện các điểm yếu bảo mật tồn tại bên trong hệ thống thông tin và ứng dụng thông qua việc thực hiện: Đánh giá điểm yếu, kiểm thử xâm nhập của hệ thống CNTT của EVNSPC tại TTDL và TT CSKH.
- Cung cấp cho đội ngũ quản trị, vận hành hệ thống CNTT của SPCIT, TT CSKH thực hiện vá các lỗ hổng và quản trị, vận hành an toàn cho hệ thống CNTT. Đặc biệt cung cấp cho đội ngũ quản trị vận hành hệ thống AD evnspc.vn các điểm yếu để tránh bị tấn công, nâng quyền để chiếm quyền quản trị.
- Cung cấp báo cáo chi tiết về các lỗ hổng phát hiện được để tư vấn cho đội ngũ lập trình của SPCIT và TT CSKH các phương pháp lập trình phần mềm an toàn, cách bảo vệ mã nguồn phần mềm trước việc dịch ngược mã nguồn.

- Cung cấp cho Lãnh đạo về tình hình lộ lọt các thông tin khách hành, nhân viên, các thông tin nhạy cảm, tài liệu nội bộ của EVNSPC, thông tin tài khoản của CBCNV trên internet.

3. Yêu cầu kỹ thuật của gói thầu: đáp ứng theo yêu cầu kỹ thuật và tiêu chuẩn đánh giá chi tiết

4. Giải pháp và phương pháp luận: không

Nhà thầu chuẩn bị đề xuất giải pháp, phương pháp luận tổng quát thực hiện dịch vụ theo các nội dung quy định tại Chương này, gồm các phần như sau:

1. Giải pháp và phương pháp luận;

2. Kế hoạch công tác.

5. Quy định về kiểm tra, nghiệm thu sản phẩm: Thực hiện tốt các nội dung yêu cầu

TỔNG CÔNG TY
ĐIỆN LỰC MIỀN NAM
CÔNG TY CÔNG NGHỆ THÔNG TIN ĐIỆN LỰC MIỀN NAM

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

BIÊN CHẾ BÁO CÁO KINH TẾ KỸ THUẬT

DỰ ÁN: "Thuê tấn công (Redteam) vào Trung tâm dữ liệu và Trung tâm CSKH của EVNSPC nhằm phát hiện các lỗ hổng và khắc phục"

Dự án đầu tư "Thuê tấn công (Redteam) vào Trung tâm dữ liệu và Trung tâm CSKH của EVNSPC nhằm phát hiện các lỗ hổng và khắc phục" là dự án đầu tư sử dụng vốn Sản xuất kinh doanh, thực hiện kiểm tra tìm kiếm lỗ hổng bảo mật và mức độ bảo mật của các hệ thống CNTT của Trung tâm dữ liệu (TTDL, Data Center) và Trung tâm Chăm sóc Khách hàng (TT CSKH) với góc nhìn của hacker, giúp cho EVNSPC đánh giá và khắc phục các điểm yếu của hệ thống.

Căn cứ theo Khoản 2 Điều 10 của 73/2019/NĐ-CP ngày 05/09/2019, hồ sơ dự án được thiết kế 01 bước.

Theo đó, Hồ sơ dự án có biên chế hồ sơ thành 03 tập như sau:

- Tập 1 : Thuyết minh Báo cáo kinh tế kỹ thuật
- **Tập 2 : Yêu cầu kỹ thuật và tiêu chí đánh giá chi tiết**

TẬP 2 – YÊU CẦU KỸ THUẬT

I. PHẠM VI CUNG CẤP:

1. Phạm vi của dự án

Stt	Hạng mục	Mô tả	Đơn vị tính	Số lượng
1	Dịch vụ Red Team	Kiểm thử xâm nhập Red Team trên các ứng dụng, thiết bị từ bên ngoài internet. Đơn vị thực hiện phải tìm kiếm, khai thác, đánh giá và tư vấn các giải pháp để bảo vệ các các thông tin nhạy cảm của EVNSPC: - Thông tin khách hàng: Dữ liệu cá nhân của khách hàng, nhân viên - Thông tin tài chính: Thông tin về tài chính, hợp đồng và các giao dịch ngân hàng. - Thông tin hệ thống: Cấu hình hệ thống, thông tin về mạng nội bộ, danh sách các thiết bị và dịch vụ đang vận hành + Hạ tầng mạng: Kiểm thử các thiết bị mạng, tường lửa, và các thành phần hạ tầng để đảm bảo chúng không có lỗ hổng bảo mật. + Hạ tầng vật lý: Kiểm tra các hệ thống vật lý như máy chủ, thiết bị lưu trữ và các thiết bị khác. - Thông tin đăng nhập: Tài khoản và mật khẩu của nhân viên, đặc biệt là những tài khoản có quyền quản trị, - Thông tin nhạy cảm khác: Thư tín nội bộ, chính sách bảo mật và các tài liệu nội bộ khác.	Gói dịch vụ	01

2. Nội dung công việc

Nhằm mô phỏng thực tế nhất các cuộc tấn công từ không gian mạng, đơn vị thực hiện phải xây dựng một quy trình kiểm thử xâm nhập dựa trên những tiêu chuẩn và tài liệu của các tổ chức bảo mật trên thế giới bao gồm MITRE ATT&CK, OWASP, PTES, OSSTMM và ISSAF.

Khi thực hiện dự án, đơn vị thực hiện phải xây dựng các kịch bản thử nghiệm xâm nhập. Công tác kiểm thử, tấn công hệ thống được kết hợp giữa các công cụ tự động và đánh giá thủ công bởi các chuyên gia.

Các công cụ sử dụng trong quá trình kiểm thử, tấn công phải được phê duyệt bởi EVNSPC. Nguồn sử dụng công cụ bao gồm: các công cụ thương mại có bản quyền của RedTeam, các công cụ mã nguồn mở, các công cụ do RedTeam phát triển.

Các hạng mục bao gồm, nhưng không giới hạn các giai đoạn sau:

Giai đoạn 1: Tấn công các dịch vụ bên ngoài internet

Mục tiêu:

- Mô hình các đối tượng tấn công từ bên ngoài internet khi không có bất kỳ thông tin đến hiểu toàn bộ dịch vụ đang public ra Internet.
- Tấn công kiểm soát càng nhiều máy chủ dịch vụ đang public càng tốt và duy trì backdoor hoặc webshell trên các máy chủ này, kết nối vào CnC để kiểm soát, duy trì truy cập

Tiêu chí cần đạt:

- Tấn công kiểm soát bất kỳ dịch vụ đang public ra Internet (RCE, Webshell, FileUpload), các lỗ hổng có thể cho phép chiếm quyền kiểm soát ứng dụng hoặc máy chủ ứng dụng.
- Tạo ra backdoor hoặc webshell trên các máy chủ dịch vụ public Internet.
- Đánh cắp thông tin trực tiếp các dữ liệu người dùng, dữ liệu khách hàng mà không cần sử dụng bất kỳ tài khoản người dùng (BlackBox 100%)
- Đánh cắp mã nguồn ứng dụng.
- Xác định khả năng phòng thủ, tự phòng vệ trước các tấn công từ bên ngoài, ngăn chặn hoặc phát hiện các kỹ thuật khai thác lỗ hổng, đánh giá hiệu quả các giải pháp phòng thủ vùng biên.

Tiêu chuẩn áp dụng: OWASP, PTES, BlackBox

Giai đoạn 2: Tấn công người dùng cuối (phi kỹ thuật và lừa đảo)

Mục tiêu:

- Xâm nhập ban đầu thành công vào hệ thống mạng của tổ chức thông qua hướng tiếp cận khai thác điểm yếu về mặt nhận thức cũng như quản lý thông tin cá nhân của người dùng cuối.

- Từ các thông tin thu thập được cố gắng kiểm soát và chiếm quyền thành công càng nhiều máy trạm, tài khoản người dùng nội bộ, máy chủ hệ thống tiếp cận được thông qua tài khoản người dùng nội bộ của tổ chức càng nhiều càng tốt

Tiêu chí cần đạt:

Xâm nhập thành công vào tài khoản người dùng cuối.

- Thu thập nhiều nhất các tài khoản người dùng, máy tính người dùng bị tấn công chiếm quyền và các ứng dụng nội bộ, phục vụ hoạt động hằng ngày mà người dùng được phép truy cập.
- Kiểm tra khả năng vượt qua cơ chế phòng thủ (Endpoint Protection).
- Thu thập thông tin và mở rộng thành công quyền truy cập sang các hệ thống lân cận càng nhiều càng tốt

Tiêu chuẩn áp dụng: OWASP, PTES

Giai đoạn 3: Tấn công hệ thống Active Directory (AD) evnspc.vn

Mục tiêu:

- Xâm nhập và chiếm quyền kiểm soát cao nhất trong môi trường quản lý tập trung Active Directory
- Sử dụng tất cả kết quả đạt được từ 02 giai đoạn 1 và 2

Tiêu chí cần đạt

- Chiếm quyền thành công các máy chủ dịch vụ thông qua các các điểm yếu bảo mật từ các hệ thống có thể tiếp được thông qua tài khoản người dùng cuối đã được kiểm soát, thu thập, chiếm quyền truy cập.
- Mở rộng quyền kiểm soát quản trị trên diện rộng hệ thống. Duy trì quyền truy cập trên các máy chủ, hệ thống, tài khoản người dùng tiếp cận được.
- Tấn công các giải pháp bảo mật
- Vượt qua các cơ chế phòng thủ hoặc chính sách truy cập
- Thu thập được tài khoản quản trị Domain Admin
- Thu thập được giá Hash của tài khoản quản trị
- Thu thập được vé xác thực (ticket) dịch vụ
- Chiếm quyền truy cập vào máy chủ Domain Controller thông qua giao thức quản trị (RDP) hoặc khai thác lỗ hổng.

Tiêu chuẩn áp dụng: PTES, OSSTMM, ISSAF

Quá trình thực hiện bao gồm nhưng không giới hạn các giai đoạn sau:

STT	Công việc	Đơn vị thực hiện RedTeam	EVNSPC phối hợp	Kết quả

1	Khảo sát thông tin	Đơn vị RedTeam thực hiện chuẩn bị các nội dung cần khảo sát đến hệ thống	EVNSPC cung cấp thông tin liên quan đến hệ thống cần đánh giá.	Phạm vi và Kế hoạch thực hiện
2	Đánh giá lần thứ nhất	Đơn vị RedTeam thực hiện đánh giá an toàn thông tin lần thứ nhất theo các phạm vi và kế hoạch đã thống nhất.	EVNSPC theo dõi	Báo cáo các điểm yếu bao gồm, nhưng không giới hạn, các bằng chứng chứng minh, các khuyến nghị hiệu chỉnh cấu hình, lập trình cho ứng dụng, hệ thống
3	Khắc phục, vá lỗ hổng	RedTeam theo dõi quá trình khắc phục và hỗ trợ tư vấn, giải đáp thông tin.	EVNSPC thực hiện vá, khắc phục lỗ hổng, điểm yếu bảo mật do RedTeam phát hiện.	Hệ thống được vá hoặc vá tạm thời theo khuyến nghị để đảm bảo an toàn
4	Tái đánh giá	RedTeam thực hiện tái đánh giá.	EVNSPC theo dõi	Báo cáo tình trạng khắc phục các điểm yếu đã phát hiện, các điểm yếu mới phát hiện và bao gồm, nhưng không giới hạn, các bằng chứng chứng minh, các khuyến nghị hiệu chỉnh

				cấu hình, lập trình cho ứng dụng, hệ thống
5	Báo cáo kết quả đánh giá	RedTeam gửi kết quả đánh giá cho EVNSPC	EVNSPC tiếp nhận báo cáo.	Báo cáo kết quả tổng kết

3. Phạm vi kiểm thử, tấn công

- Các hệ thống public mặt ngoài internet của TTDL và TT CSKH
- Người dùng cuối của EVNSPC (tấn công phi kỹ thuật và lừa đảo)
- Hệ thống AD evnspc.vn

II. CÁC YÊU CẦU:

STT	Nội dung yêu cầu	
	Mô tả	**Yêu cầu**
I	**Thời gian thực hiện dịch vụ**	
1	Thời gian thực hiện dịch vụ	8 tuần
II.	**Năng lực nhà thầu**	
1	Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng	Nhà thầu phải có "Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng" về dịch vụ được cấp là Dịch vụ tư vấn an toàn thông tin mạng và Dịch vụ kiểm tra, đánh giá an toàn thông tin mạng
2	Chứng nhận ISO 27001	Nhà thầu được cấp các chứng nhận ISO 9001 và ISO 27001 còn hiệu lực hoặc tương đương
3	Kinh nghiệm thực hiện kiểm thử xâm nhập, đánh giá an toàn thông tin	Đã có kinh nghiệm thực hiện kiểm thử xâm nhập, đánh giá an toàn thông tin (Từ năm 2020 đến thời điểm đóng thầu)
III	**Nhân sự thực hiện dự án**	
1	Trưởng dự án	+ Số lượng: tối thiểu 01
		+ Kinh nghiệm: tối thiểu 10 năm trong lĩnh vực ATTT; đã tham gia ít nhất 1 dự án redteam hoặc đánh giá ATTT
		+ Tốt nghiệp từ đại học trở lên một trong các chuyên ngành công nghệ thông tin, an toàn thông tin, điện tử, viễn thông, tin học, toán tin, khoa học máy tính, kỹ thuật máy tính, hệ thống thông tin, mạng máy tính và truyền thông

		+ có chứng chỉ về quản lý dự án PMP hoặc tương đương
2	Trưởng nhóm làm việc	+ Số lượng: tối thiểu 01
		+ Kinh nghiệm: tối thiểu 05 năm trong lĩnh vực ATTT; đã tham gia ít nhất 1 dự án redteam hoặc đánh giá ATTT
		+ Tốt nghiệp từ đại học trở lên một trong các chuyên ngành công nghệ thông tin, an toàn thông tin, điện tử, viễn thông, tin học, toán tin, khoa học máy tính, kỹ thuật máy tính, hệ thống thông tin, mạng máy tính và truyền thông
		+ có ít nhất một trong các chứng chỉ về đánh giá an toàn thông tin hệ thống như CompTIA Security+, ISC2 Certified in Cybersecurity (CC), CISA (ISACA), GSEC (SANS) trở lên hoặc tương đương
		+ có ít nhất một trong các chứng chỉ về kiểm thử xâm nhập như eJPT (INE), CompTIA PenTest+, CEH (EC-Council) , OSCP (OffSec) trở lên hoặc tương đương
3	Chuyên viên kiểm thử xâm nhập	+ Số lượng: tối thiểu 05
		+ Kinh nghiệm: tối thiểu 01 năm trong lĩnh vực ATTT; đã tham gia ít nhất 1 dự án redteam hoặc đánh giá ATTT
		+ Tốt nghiệp từ đại học trở lên một trong các chuyên ngành công nghệ thông tin, an toàn thông tin, điện tử, viễn thông, tin học, toán tin, khoa học máy tính, kỹ thuật máy tính, hệ thống thông tin, mạng máy tính và truyền thông
		+ có ít nhất một trong các chứng chỉ về kiểm thử xâm nhập như eJPT (INE), CompTIA PenTest+, CEH (EC-Council) , OSCP (OffSec) trở lên hoặc tương đương
4	Chuyên viên đánh giá an toàn thông tin	+ Số lượng: tối thiểu 03
		+ Kinh nghiệm: tối thiểu 01 năm trong lĩnh vực ATTT; đã tham gia ít nhất 1 dự án redteam hoặc đánh giá ATTT
		+ Tốt nghiệp từ đại học trở lên một trong các chuyên ngành công nghệ thông tin, an toàn thông tin, điện tử, viễn thông, tin học, toán tin,

		khoa học máy tính, kỹ thuật máy tính, hệ thống thông tin, mạng máy tính và truyền thông
		+ có ít nhất một trong các chứng chỉ về đánh giá an toàn thông tin hệ thống như CompTIA Security+, ISC2 Certified in Cybersecurity (CC), CISA (ISACA), GSEC (SANS) trở lên hoặc tương đương
IV	**Yêu cầu kỹ thuật**	
1	Phương pháp luận	Có phương pháp luận thực hiện trong đó mô tả phương thức, kỹ thuật tấn công nhằm đạt được mục tiêu, phát hiện được các điểm yếu bảo mật trong hệ thống CNTT, bao gồm nhưng không giới hạn như sau: - Reconnaissance - Resource Development - Initial Access - Execution - Persistence - Privilege Escalation - Defense Evasion - Credential Access - Discovery - Lateral Movement - Collection - Exfiltration - Impact Nhà thầu mô tả quy trình thực hiện Red Team, trong đó nêu rõ phương án quản lý, giảm thiểu rủi ro. Nhà thầu cam kết không sử dụng các phương thức, kỹ thuật tấn công có thể gây nguy hại, gián đoạn hoạt động của hệ thống CNTT như tấn công DoS hay DDoS, …
2	Phạm vi và hình thức	Phạm vi: Trung tâm Dữ liệu và Trung tâm CSKH của EVNSPC Hình thức: - tấn công hệ thống từ bên ngoài internet trên bất kỳ dịch vụ với cách thức của hacker (redteam) khai thác lỗ hổng và đi sâu vào hệ thống bằng cách khai thác các lỗ hổng đã phát hiện - lừa đảo người dùng (phishing) để chiếm tài

		khoản/ cài đặt malware phục vụ khai thác sâu vào hệ thống - nâng quyền tấn công vào hệ thống AD evnspc.vn
3	Tiêu chuẩn kiểm thử, tấn công xâm nhập	Nhà thầu có quy trình kiểm thử xâm nhập dựa trên những tiêu chuẩn và tài liệu của các tổ chức bảo mật trên thế giới bao gồm MITRE ATT&CK, OWASP, PTES, OSSTMM và ISSAF
4	Công cụ thực hiện	Nhà thầu liệt kê các công cụ được sử dụng để thực hiện kiểm tra, khai thác trong phạm vi gói thầu, tối thiểu bao gồm: tên công cụ, nhà phát triển, chức năng. Sử dụng các công cụ: - phần mềm thương mại có bản quyền của nhà thầu - phần mềm nhà thầu tự xây dựng (có hồ sơ chứng minh) - phần mềm open source Trong đó, đảm bảo có tối thiểu các công cụ sau:
		+ Công cụ có khả năng cung cấp Công cụ quản lý lỗ hổng bảo mật cho phép cập nhật thông tin lỗ hổng theo thời gian thực khi được yêu cầu. Các lỗ hổng được quản lý theo trạng thái (mới phát hiện, đã khắc phục, …), và phải cung cấp ít nhất mô tả, cách thức khai thác, tham số, điều kiện khai thác, mức độ nghiêm trọng, bằng chứng, …
		+ Công cụ cung cấp kho lỗ hổng CVE, thông tin lộ lọt, cho phép tìm kiếm nguồn thông tin lộ lọt (tài khoản, mật khẩu), thông tin bề mặt tấn công của đối tượng đánh giá, thông tin các nhóm APT có nêu rõ các kỹ thuật tấn công theo MITRE và các lỗ hổng CVE liên quan đến hạ tầng công nghệ thông tin của chủ đầu tư.
		+ Công cụ cung cấp kho mã khai thác lỗ hổng, cho phép quản lý, kiểm tra các mã khai thác công khai và hỗ trợ xây dựng mã khai thác mới bằng AI. Đồng thời cung cấp khả năng chủ động thực hiện dò quét, khai thác lỗ hổng từ bên ngoài, có tính năng trợ lý ảo cho phép

		tìm kiếm thông tin lỗ hổng, mã khai thác bằng ngôn ngữ tự nhiên.
		Nhà thầu cam kết cung cấp kết quả demo công cụ để đánh giá tính năng và khả năng ảnh hưởng đến hệ thống CNTT.
5	Các giai đoạn thực hiện	Bao gồm nhưng không giới hạn: GĐ 1: tấn công khai thác các dịch vụ bên ngoài internet. Nhà thầu tấn công các dịch vụ public ngoài internet của EVNSPC (bao gồm Data Center và TT CSKH) để khai thác lỗ hổng và chiếm quyền điều khiển các máy chủ
		GĐ 2: tấn công lừa đảo (phising) người dùng Nhà thầu thực hiện chiến dịch phising người dùng để đánh cắp tài khoản
		GĐ 3: nâng quyền tấn công vào hệ thống AD evnspc.vn Nhà thầu thực hiện nâng quyền từ các kết quả có được ở các giai đoạn trước (GĐ 1 và GĐ 2) để tấn công vào hệ thống AD evnspc.vn
6	Khắc phục lỗ hổng	Nhà thầu thực hiện báo cáo bao gồm nhưng không giới hạn, các nội dung: + mức độ nghiêm trọng theo CVSS + mức độ ảnh hưởng của lỗ hổng đến hệ thống + khuyến nghị cần khắc phục, hỗ trợ khắc phục các lỗ hổng đối với các lỗ hổng trên thiết bị, phần mềm do CĐT trang bị
		Nhà thầu thực hiện báo cáo bao gồm nhưng không giới hạn, các nội dung: + mức độ nghiêm trọng theo CVSS + mức độ ảnh hưởng của lỗ hổng đến hệ thống + khuyến nghị cần khắc phục, tư vấn phương pháp lập trình an toàn để phòng chống các lỗ hổng đối với các lỗ hổng phần mềm do CĐT xây dựng
7	Tái đánh giá	Nhà thầu tái đánh giá các lỗ hổng EVNSPC đã khắc phục

8	Báo cáo	Nhà thầu báo cáo kết quả bao gồm, nhưng không giới hạn: + báo cáo tổng quan phục vụ lãnh đạo + báo cáo kỹ thuật chi tiết các thức khai thác, kèm bằng chứng chứng minh + báo cáo đánh giá tổng quan năng lực đảm bảo ATTT của hệ thống và giải pháp khắc phục (nếu có)

III. TIÊU CHÍ ĐÁNH GIÁ:

1. Phương pháp đánh giá

- **Phương pháp đánh giá: ĐẠT / KHÔNG ĐẠT**

2. Các yêu cầu :

STT	Nội dung yêu cầu		Mức độ đáp ứng		
	Mô tả	Yêu cầu	Đạt	Chấp nhận được	Không đạt
I	**Thời gian thực hiện dịch vụ**				
1	Thời gian thực hiện dịch vụ	8 tuần	<=08 tuần		> 08 tuần
II.	**Năng lực nhà thầu**				
1	Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng	Nhà thầu phải có "Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng" về dịch vụ được cấp là Dịch vụ tư vấn an toàn thông tin mạng và Dịch vụ kiểm tra, đánh giá an toàn thông tin mạng	Như yêu cầu		Không như yêu cầu
2	Chứng nhận ISO 27001	Nhà thầu được cấp các chứng nhận ISO 9001 và ISO 27001 còn hiệu lực hoặc tương đương	Như yêu cầu		Không như yêu cầu
3	Kinh nghiệm thực hiện kiểm thử xâm nhập, đánh giá an toàn thông tin	Đã có kinh nghiệm thực hiện kiểm thử xâm nhập, đánh giá an toàn thông tin (Từ năm 2020 đến thời điểm đóng thầu)	Như yêu cầu		Không như yêu cầu
III	**Nhân sự thực hiện dự án**				
1	Trưởng dự án	+ Số lượng: tối thiểu 01	>= 01 người		< 01 người

		+ Kinh nghiệm: tối thiểu 10 năm trong lĩnh vực ATTT; đã tham gia ít nhất 1 dự án redteam hoặc đánh giá ATTT	Như yêu cầu		Không như yêu cầu
		+ Tốt nghiệp từ đại học trở lên một trong các chuyên ngành công nghệ thông tin, an toàn thông tin, điện tử, viễn thông, tin học, toán tin, khoa học máy tính, kỹ thuật máy tính, hệ thống thông tin, mạng máy tính và truyền thông	Như yêu cầu		Không như yêu cầu
		+ có chứng chỉ về quản lý dự án PMP hoặc tương đương	Như yêu cầu		Không như yêu cầu
2	Trưởng nhóm làm việc	+ Số lượng: tối thiểu 01	>= 01 người		< 01 người
		+ Kinh nghiệm: tối thiểu 05 năm trong lĩnh vực ATTT; đã tham gia ít nhất 1 dự án redteam hoặc đánh giá ATTT	>=05 năm		< 05 năm
		+ Tốt nghiệp từ đại học trở lên một trong các chuyên ngành công nghệ thông tin, an toàn thông tin, điện tử, viễn thông, tin học, toán tin, khoa học máy tính, kỹ thuật máy tính, hệ thống thông tin, mạng máy tính và truyền thông	Như yêu cầu		Không như yêu cầu

		+ có ít nhất một trong các chứng chỉ về đánh giá an toàn thông tin hệ thống như CompTIA Security+, ISC2 Certified in Cybersecurity (CC), CISA (ISACA), GSEC (SANS) trở lên hoặc tương đương	Như yêu cầu		Không như yêu cầu
		+ có ít nhất một trong các chứng chỉ về kiểm thử xâm nhập như eJPT (INE), CompTIA PenTest+, CEH (EC-Council) , OSCP (OffSec) trở lên hoặc tương đương	Như yêu cầu		Không như yêu cầu
3	Chuyên viên kiểm thử xâm nhập	+ Số lượng: tối thiểu 05	>= 05 người		< 05 người
		+ Kinh nghiệm: tối thiểu 01 năm trong lĩnh vực ATTT; đã tham gia ít nhất 1 dự án redteam hoặc đánh giá ATTT	>=01 năm		< 01 năm
		+ Tốt nghiệp từ đại học trở lên một trong các chuyên ngành công nghệ thông tin, an toàn thông tin, điện tử, viễn thông, tin học, toán tin, khoa học máy tính, kỹ thuật máy tính, hệ thống thông tin, mạng máy tính và truyền thông	Như yêu cầu		Không như yêu cầu
		+ có ít nhất một trong các chứng chỉ về kiểm thử xâm nhập như eJPT (INE), CompTIA PenTest+,	Như yêu cầu		Không như yêu cầu

		CEH (EC-Council) , OSCP (OffSec) trở lên hoặc tương đương			
4	Chuyên viên đánh giá an toàn thông tin	+ Số lượng: tối thiểu 03	>= 03 người		< 03 người
		+ Kinh nghiệm: tối thiểu 01 năm trong lĩnh vực ATTT; đã tham gia ít nhất 1 dự án redteam hoặc đánh giá ATTT	>=01 năm		< 01 năm
		+ Tốt nghiệp từ đại học trở lên một trong các chuyên ngành công nghệ thông tin, an toàn thông tin, điện tử, viễn thông, tin học, toán tin, khoa học máy tính, kỹ thuật máy tính, hệ thống thông tin, mạng máy tính và truyền thông	Như yêu cầu		Không như yêu cầu
		+ có ít nhất một trong các chứng chỉ về đánh giá an toàn thông tin hệ thống như CompTIA Security+, ISC2 Certified in Cybersecurity (CC), CISA (ISACA), GSEC (SANS) trở lên hoặc tương đương	Như yêu cầu		Không như yêu cầu
IV	**Yêu cầu kỹ thuật**				

1	Phương pháp luận	Có phương pháp luận thực hiện trong đó mô tả phương thức, kỹ thuật tấn công nhằm đạt được mục tiêu, phát hiện được các điểm yếu bảo mật trong hệ thống CNTT, bao gồm nhưng không giới hạn như sau: - Reconnaissance - Resource Development - Initial Access - Execution - Persistence - Privilege Escalation - Defense Evasion - Credential Access - Discovery - Lateral Movement - Collection - Exfiltration - Impact Nhà thầu mô tả quy trình thực hiện Red Team, trong đó nêu rõ phương án quản lý, giảm thiểu rủi ro. Nhà thầu cam kết không sử dụng các phương thức, kỹ thuật tấn công có thể gây nguy hại, gián đoạn hoạt động của hệ thống CNTT như tấn công DoS hay DDoS, …	Nhà thầu cam kết thực hiện trong hồ sơ		Nhà thầu không cam kết thực hiện trong hồ sơ

2	Phạm vi và hình thức	Phạm vi: Trung tâm Dữ liệu và Trung tâm CSKH của EVNSPC Hình thức: - tấn công hệ thống từ bên ngoài internet trên bất kỳ dịch vụ với cách thức của hacker (redteam) khai thác lỗ hổng và đi sâu vào hệ thống bằng cách khai thác các lỗ hổng đã phát hiện - lừa đảo người dùng (phishing) để chiếm tài khoản/ cài đặt malware phục vụ khai thác sâu vào hệ thống - nâng quyền tấn công vào hệ thống AD evnspc.vn	Nhà thầu cam kết thực hiện trong hồ sơ		Nhà thầu không cam kết thực hiện trong hồ sơ
3	Tiêu chuẩn kiểm thử, tấn công xâm nhập	Nhà thầu có quy trình kiểm thử xâm nhập dựa trên những tiêu chuẩn và tài liệu của các tổ chức bảo mật trên thế giới bao gồm MITRE ATT&CK, OWASP, PTES, OSSTMM và ISSAF	Nhà thầu cam kết thực hiện trong hồ sơ		Nhà thầu không cam kết thực hiện trong hồ sơ
4	Công cụ thực hiện	Nhà thầu liệt kê các công cụ được sử dụng để thực hiện kiểm tra, khai thác trong phạm vi gói thầu, tối thiểu bao gồm: tên công cụ, nhà phát triển, chức năng. Sử dụng các công cụ: - phần mềm thương mại có bản quyền của nhà thầu	Như yêu cầu Nhà thầu liệt kê công cụ trong hồ sơ		Không như yêu cầu Nhà thầu không liệt kê công cụ trong hồ sơ

		- phần mềm nhà thầu tự xây dựng (có hồ sơ chứng minh) - phần mềm open source Trong đó, đảm bảo có tối thiểu các công cụ sau:			
		+ Công cụ có khả năng cung cấp Công cụ quản lý lỗ hổng bảo mật cho phép cập nhật thông tin lỗ hổng theo thời gian thực khi được yêu cầu. Các lỗ hổng được quản lý theo trạng thái (mới phát hiện, đã khắc phục, …), và phải cung cấp ít nhất mô tả, cách thức khai thác, tham số, điều kiện khai thác, mức độ nghiêm trọng, bằng chứng, …	Như yêu cầu Nhà thầu liệt kê công cụ trong hồ sơ		Không như yêu cầu Nhà thầu không liệt kê công cụ trong hồ sơ
		+ Công cụ cung cấp kho lỗ hổng CVE, thông tin lộ lọt, cho phép tìm kiếm nguồn thông tin lộ lọt (tài khoản, mật khẩu), thông tin bề mặt tấn công của đối tượng đánh giá, thông tin các nhóm APT có nêu rõ các kỹ thuật tấn công theo MITRE và các lỗ hổng CVE liên quan đến hạ tầng công nghệ thông tin của chủ đầu tư.	Như yêu cầu Nhà thầu liệt kê công cụ trong hồ sơ		Không như yêu cầu Nhà thầu không liệt kê công cụ trong hồ sơ

		+ Công cụ cung cấp kho mã khai thác lỗ hổng, cho phép quản lý, kiểm tra các mã khai thác công khai và hỗ trợ xây dựng mã khai thác mới bằng AI. Đồng thời cung cấp khả năng chủ động thực hiện dò quét, khai thác lỗ hổng từ bên ngoài, có tính năng trợ lý ảo cho phép tìm kiếm thông tin lỗ hổng, mã khai thác bằng ngôn ngữ tự nhiên.	Như yêu cầu Nhà thầu liệt kê công cụ trong hồ sơ		Không như yêu cầu Nhà thầu không liệt kê công cụ trong hồ sơ
		Nhà thầu cam kết cung cấp kết quả demo công cụ để đánh giá tính năng và khả năng ảnh hưởng đến hệ thống CNTT.	Như yêu cầu Nhà thầu liệt kê công cụ trong hồ sơ		Không như yêu cầu Nhà thầu không liệt kê công cụ trong hồ sơ
5	Các giai đoạn thực hiện	Bao gồm nhưng không giới hạn:			
		GĐ 1: tấn công khai thác các dịch vụ bên ngoài internet. Nhà thầu tấn công các dịch vụ public ngoài internet của EVNSPC (bao gồm Data Center và TT CSKH) để khai thác lỗ hổng và chiếm quyền điều khiển các máy chủ	Nhà thầu cam kết thực hiện trong hồ sơ		Nhà thầu không cam kết thực hiện trong hồ sơ

		GĐ 2: tấn công lừa đảo (phising) người dùng Nhà thầu thực hiện chiến dịch phising người dùng để đánh cắp tài khoản	Nhà thầu cam kết thực hiện trong hồ sơ		Nhà thầu không cam kết thực hiện trong hồ sơ
		GĐ 3: nâng quyền tấn công vào hệ thống AD evnspc.vn Nhà thầu thực hiện nâng quyền từ các kết quả có được ở các giai đoạn trước (GĐ 1 và GĐ 2) để tấn công vào hệ thống AD evnspc.vn	Nhà thầu cam kết thực hiện trong hồ sơ		Nhà thầu không cam kết thực hiện trong hồ sơ
6	Khắc phục lỗ hổng	Nhà thầu thực hiện báo cáo bao gồm nhưng không giới hạn, các nội dung: + mức độ nghiêm trọng theo CVSS + mức độ ảnh hưởng của lỗ hổng đến hệ thống + khuyến nghị cần khắc phục, hỗ trợ khắc phục các lỗ hổng đối với các lỗ hổng trên thiết bị, phần mềm do CĐT trang bị	Nhà thầu cam kết thực hiện trong hồ sơ		Nhà thầu không cam kết thực hiện trong hồ sơ

		Nhà thầu thực hiện báo cáo bao gồm nhưng không giới hạn, các nội dung: + mức độ nghiêm trọng theo CVSS + mức độ ảnh hưởng của lỗ hổng đến hệ thống + khuyến nghị cần khắc phục, tư vấn phương pháp lập trình an toàn để phòng chống các lỗ hổng đối với các lỗ hổng phần mềm do CĐT xây dựng	Nhà thầu cam kết thực hiện trong hồ sơ		Nhà thầu không cam kết thực hiện trong hồ sơ
7	Tái đánh giá	Nhà thầu tái đánh giá các lỗ hổng EVNSPC đã khắc phục	Nhà thầu cam kết thực hiện trong hồ sơ		Nhà thầu không cam kết thực hiện trong hồ sơ
8	Báo cáo	Nhà thầu báo cáo kết quả bao gồm, nhưng không giới hạn: + báo cáo tổng quan phục vụ lãnh đạo + báo cáo kỹ thuật chi tiết các thức khai thác, kèm bằng chứng chứng minh + báo cáo đánh giá tổng quan năng lực đảm bảo ATTT của hệ thống và giải pháp khắc phục (nếu có)	Nhà thầu cam kết thực hiện trong hồ sơ		Nhà thầu không cam kết thực hiện trong hồ sơ