COMANDO PER LE OPERAZIONI IN RETE
UFFICIO AMMINISTRAZIONE
Sezione Gestione Finanziaria e Contratti
C . F . 9 6 4 5 1 0 6 0 5 8 4
Via Stresa 31/B – 00135 ROMA

Posta elettronica: cor@cor.difesa.it
Posta elettronica certificata: cor@postacert.difesa.it

Lettera di Ordinazione n. 172
(da citare in fattura)

Roma, 21/11/2024

Società CYBER-BEE
Via Monte Carmelo 5 – Roma
Pec: cyber-bee.srl@legalmail.it

Oggetto: GARA 144 Acquisizione e licenze SW per la raccolta dati piattaforma C2RED per le esigenze del COR DIFESA. CUP D87H240002990001 – CIG B3A454B561 - Capitolo - 7115/2 – E.F. 2024.RDO 4737570.

IDV: 1908608

Rife: Obbligazione Commerciale nr. 43/2024 del 21/11/2024.

1. Codesta Ditta è risultata essere aggiudicataria della seguente fornitura, comprensiva dei relativi costi alla sicurezza, pari a euro **100,00** come da T.D. in oggetto:

Descrizione	IMPONIBILE
Acquisizione e licenze SW per la raccolta dati piattaforma C2RED per le esigenze del COR DIFESA , come da R.T.I. in allegato.	**€. 55.000,00**
Totale imponibile	**€. 55.000,00**
IVA 22%	**€. 12.100,00**
TOTALE	**€. 67.100,00**

2. La presenta commessa, per tutto quanto non previsto nella presente, si svolgerà sotto l'osservanza del Codice dei contratti di cui al decreto legislativo 31 marzo 2023, nr. 36.
3. **Si precisa che la fattura elettronica dovrà essere obbligatoriamente emessa in data successiva all'ultimazione della fornitura/servizio** ovvero successivamente agli esiti positivi delle procedure previste ai fini dell'accertamento della conformità della fornitura/servizio (verbale di verifica conformità ove previsto) e comunque, **previa richiesta di autorizzazione al seguente indirizzo email: uam.sa.sca.cs@cor.difesa.it**; dovrà essere compilata in maniera analitica nelle modalità richieste, come sopra specificato, e dovrà indicare il numero di protocollo del presente ordinativo, il numero di **CIG e CUP, la causale come da oggetto della presente lettera** e l'annotazione "SCISSIONE DEI PAGAMENTI" (qualora in presenza di IVA da versare allo Stato). La stessa dovrà essere intestata ed inviata a: COMANDO PER LE OPERAZIONI IN RETE - Servizio Amministrativo - Via Stresa, n. 31/b – 00135 ROMA Codice Fiscale 96451060584. **Codice Ufficio ai sensi dell'articolo 3, del Decreto MEF n. 55 del 3 aprile 2013 in materia di emissione, trasmissione e ricevimento della fattura elettronica 2SR075**.
4. Il presente affidamento trova copertura finanziaria con risorse attestate sul **capitolo di bilancio 7115/2 dell'E.F. 2024** mediante apertura di credito a favore del Funzionario Delegato dell'Ufficio Generale Centro di Responsabilità Amministrativa (UGCRA).
5. La fornitura/prestazione dovrà essere effettuata a cura di codesta Ditta secondo le modalità riportate nell'Obbligazione Commerciale in riferimento e dovrà essere conclusa **entro il 12/12/2024.**
6. **Direttore Esecuzione Contrattuale: C.F. Stefano CAPPELLI – mail: roc.upa.ssi.cs@cor.difesa.it**

Il CAPO SERVIZIO AMMINISTRATIVO
Col. com. Maurizio LAMBIASE
(documento firmato digitalmente)

Firmato Digitalmente da/Signed by:
MAURIZIO LAMBIASE
RUP
In Data/On Date:
giovedì 21 novembre 2024 12:01:53

FIRMA PER ACCETTAZIONE
IL RAPPRESENTANTE LEGALE DELLA DITTA
(documento firmato digitalmente)

COMANDO PER LE OPERAZIONI IN RETE

Reparto Operazioni Cibernetiche

REQUISITO
TECNICO OPERATIVO

Relativo a

Acquisizione licenze software per avvio operativo modulo *Reconnaissance* componenente *Intel* della piattaforma C2Red.

Edizione Luglio 2024

1. Premessa

La *reconnaissance* è la prima fase di un'operazione cyber di *red teaming/penetration testing* (grafica e descrizione delle fasi della *Unified Kill Chain* nelle successive **Fig. 1** e **Fig. 2** – riferimento https://www.unifiedkillchain.com/assets/The-Unified-Kill-Chain.pdf) ed ha l'obiettivo di raccogliere quante più informazioni possibili (*information gathering*) sul *target* selezionato (anche utilizzando tecniche di *Social Engineering*) e consiste nell'identificare la superficie d'attacco di quest'ultimo per pianificare e condurre le successive fasi dell'operazione.

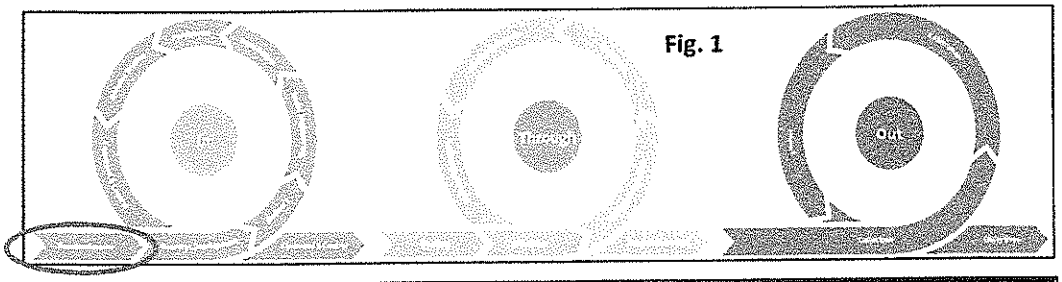

Fig. 1

The Unified Kill Chain		
1	Reconnaissance	Researching, identifying and selecting targets using active or passive reconnaissance.
2	Resource Development	Preparatory activities aimed at setting up the infrastructure required for the attack.
3	Delivery	Techniques resulting in the transmission of a weaponized object to the targeted environment.
4	Social Engineering	Techniques aimed at the manipulation of people to perform unsafe actions.
5	Exploitation	Techniques to exploit vulnerabilities in systems that may, amongst others, result in code execution.
6	Persistence	Any access, action or change to a system that gives an attacker persistent presence on the system.
7	Defense Evasion	Techniques an attacker may specifically use for evading detection or avoiding other defenses.
8	Command & Control	Techniques that allow attackers to communicate with controlled systems within a target network.
9	Pivoting	Tunneling traffic through a controlled system to other systems that are not directly accessible.
10	Discovery	Techniques that allow an attacker to gain knowledge about a system and its network environment.
11	Privilege Escalation	The result of techniques that provide an attacker with higher permissions on a system or network.
12	Execution	Techniques that result in execution of attacker-controlled code on a local or remote system.
13	Credential Access	Techniques resulting in the access of, or control over, system, service or domain credentials.
14	Lateral Movement	Techniques that enable an adversary to horizontally access and control other remote systems.
15	Collection	Techniques used to identify and gather data from a target network prior to exfiltration.
16	Exfiltration	Techniques that result or aid in an attacker removing data from a target network.
17	Impact	Techniques aimed at manipulating, interrupting or destroying the target system or data.
18	Objectives	Socio-technical objectives of an attack that are intended to achieve a strategic goal.

Fig. 2

Le informazioni da raccogliere possono essere di natura "non tecnica" (*Soft Information*), quando riconducibili all'Organizzazione *target* e/o relativi dipendenti, o di natura "tecnica" (*Hard Information*), quando relative all'Infrastruttura del *target*.

Le tecniche di indagine possono essere di tipo "passivo" (*footprinting*), quando non vi è interazione con il *target*, ovvero di tipo "attivo" (*scanning*), nel caso di interazione.

La combinazione tra la natura delle informazioni da raccogliere con le tecniche d'indagine copre tutte le tipologie di attività conseguibili durante la fase di *reconnaissance* (**Fig. 3**).

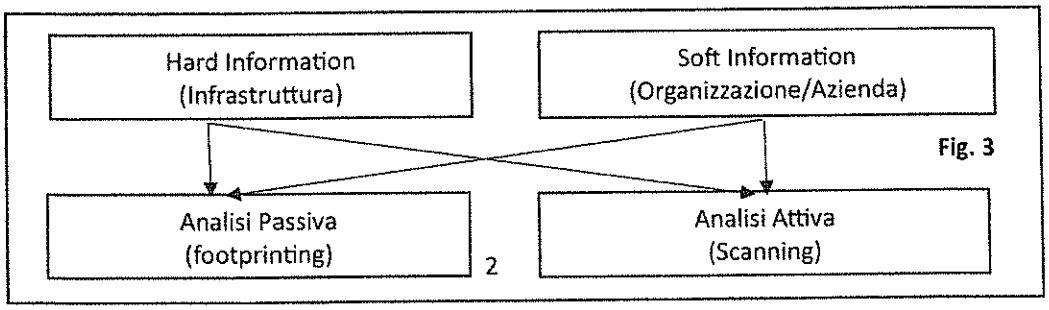

Fig. 3

Nel dettaglio:

a. l'*Information gathering* di tipo *Soft Information* – Analisi Passiva consiste nell'acquisire informazioni su qualsiasi figura aziendale (esempi: dirigenti ed impiegati, indirizzo delle sedi, etc.) da fonti aperte, tramite tecniche di Osint e Social Media Osint. Dette informazioni sono importanti anche per abilitare le tecniche di *Social Engineering*.

b. l'*Information gathering* di tipo *Soft Information* – Analisi Attiva consiste ancora nell'acquisire informazioni su qualsiasi figura aziendale, tramite interazione con il *target* e sfruttando tecniche di *Social Engineering* (*phishing, pretexting*, false notifiche, richieste di documentazione, *dumpster diving*, etc.).

c. l'*Information gathering* di tipo *Hard Information* – Analisi Passiva consiste nell'acquisire informazioni sull'infrastruttura del *target* (esempi: intervalli di indirizzi IP, *Domain Name System*, server di posta elettronica, numeri telefonici, etc.) da fonti aperte, tramite tecniche di Osint, per mappare la dimensione della superficie d'attacco (pubblica) del *target*;

d. l'*Information gathering* di tipo *Hard Information* – Analisi Attiva consiste sempre nell'acquisire informazioni sull'infrastruttura del *target*, tramite interazione ed interrogazione dei sistemi del *target* e l'utilizzo di appositi strumenti, per ottenere informazioni sui servizi di rete disponibili e versione, porte di rete aperte, sistemi operativi, domini e sottodomini, tecnologie e *content management system* delle pagine dei siti web del *target*, etc.

La raccolta informativa con tecniche di indagine di tipo passivo è svolta utilizzando strumenti di ricognizione on-line con accesso a *data base* più o meno pubblici, di massima tutti a servizio e che non prevedono pertanto interazione diretta con il *target*. La finalità dell'indagine di tipo passivo è di acquisire il maggior numero di informazioni, rimanendo occulti nei confronti del *target*.

La raccolta informativa con tecniche di indagine di tipo attivo è svolta utilizzando strumenti e programmi manuali o automatici, interagendo direttamente con i sistemi ed il personale dell'organizzazione *target*. La finalità dell'indagine di tipo attivo è di acquisire il maggior numero di informazioni, agendo con maggior rischio e conseguente possibile rilevamento da parte delle difese del *target*.

2. Caratteristiche tecniche della funzionalità di *footprinting* del Modulo di *Reconnaissance*

La piattaforma C2RED abilita alla *reconnaissance* passiva (*footprinting*) con un insieme di micro-servizi dedicati alle specifiche sorgenti di *intelligence* esterne/interne. Ad oggi **le sorgenti di *intelligence*, accessibili solo dopo aver sottoscritto un abbonamento con il *provider* del relativo servizio**, per le quali sono già stati sviluppati ed integrati nella piattaforma i relativi connettori, **sono i seguenti: *HaveIBeenPwned, Dehashed, LeakLookUp, Shodan, AlienVault, CiscoUmbrella, CrowdStrike, WealeakInfo, GhostProject, HunterIO, IPInfo, MISP, PassiveTotal, RocketReach, VirusTotal, ZoomEye, Censys*. Ulteriori sorgenti dati, oltre quelle già implementate nella piattaforma, saranno in futuro integrate nel modulo di *reconnaissance*, per incrementarne l'efficacia.**

L'architettura di *reconnaissance* passiva include, inoltre, una sorgente di rumore in grado di aggiungere richieste fittizie a quelle legittime. È possibile definire quante ricerche fittizie aggiungere alle richieste legittime. La sorgente di rumore può essere caricata con *target* in base alla tematica ricercata.

In **Fig. 4**, si riporta, lo schema di massima dell'architettura del modulo di *reconnaissance*, evidenziando (riquadri colore rosso) le funzionalità di *footprinting* descritte nel presente paragrafo.

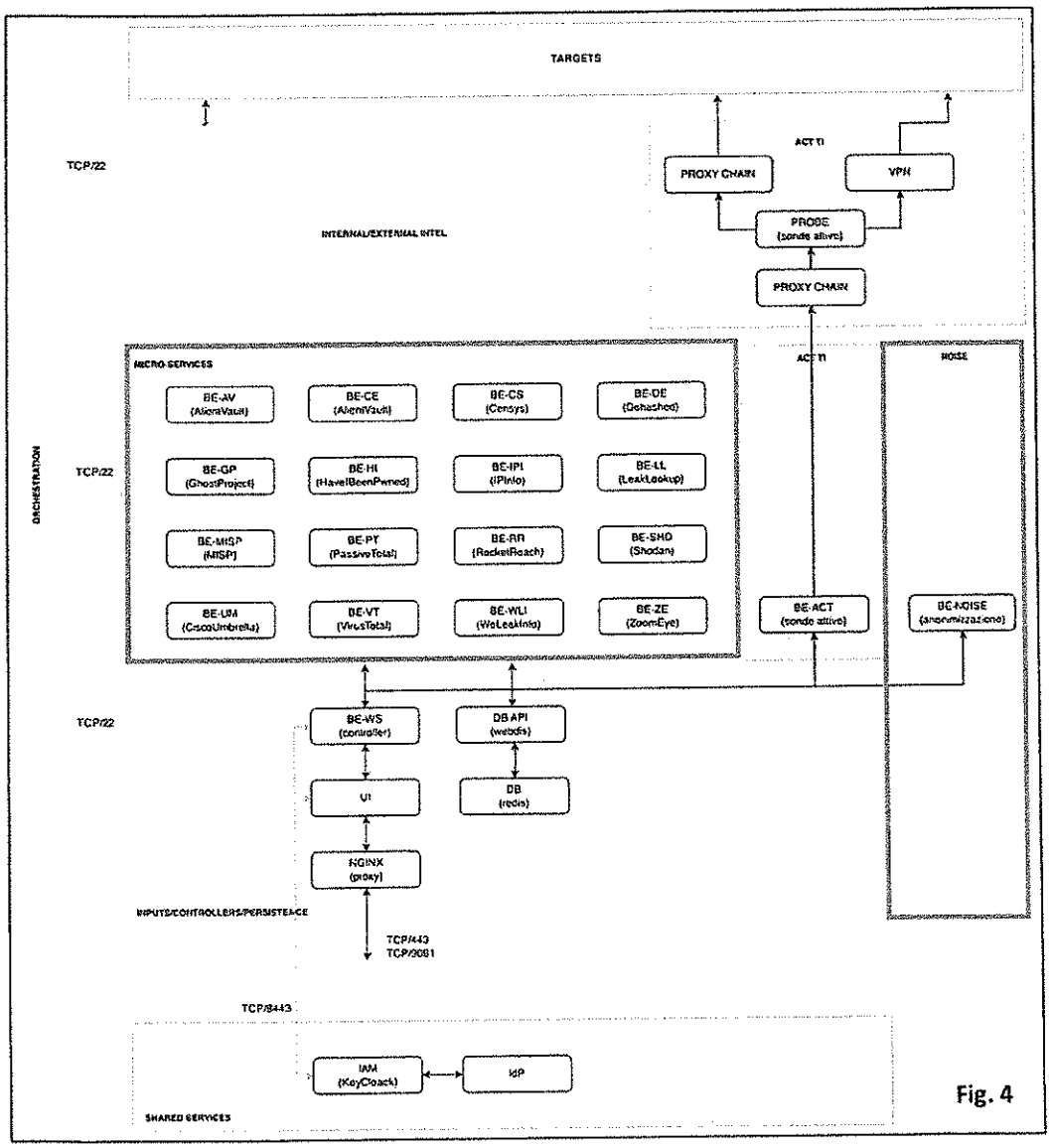

Fig. 4

3. Caratteristiche tecniche della funzionalità di *scanning* del Modulo di *Reconnaissance*

La piattaforma permette l'esecuzione di operazioni di *reconnaissance* attiva (*scanning*) attraverso delle sonde esterne. Quest'ultime vengono create dall'orchestratore infrastrutturale ed applicativo inserito in C2Red.

Sulle sonde sono installati i seguenti *tool* per abilitare alla raccolta informativa: aiodnsbrute, dirb, dnsenum, host, masscan, nikto, nmap, nslookup, smbmap, sqlmap, traceroute, whois, wpscan, zmap.

La comunicazione tra *back-end* di *reconnaissance*/sonde esterne è realizzata tramite connessioni SSH mascherate da catene di proxy e meccanismi di *port-knocking* protetti con chiavi GPG. La comunicazione tra sonde e *target* è protetta, in base all'esigenza, da catene di proxy (con meccanismi di *port-knocking*) e/o VPN dinamici.

Le sonde attive e le catene di proxy sono da implementare su ambienti cloud acquistabili da *service provider* quali AWS, DigitalOcean, Vultr, Linode, OVHCloud, etc. Medesima esigenza è richiesta per i servizi VPN.

In **Fig. 5**, si riporta, lo schema di massima dell'architettura del modulo di *reconnaissance*, evidenziando (riquadri colore verde) le funzionalità di *scanning* e anonimizzazione descritte nel presente paragrafo.

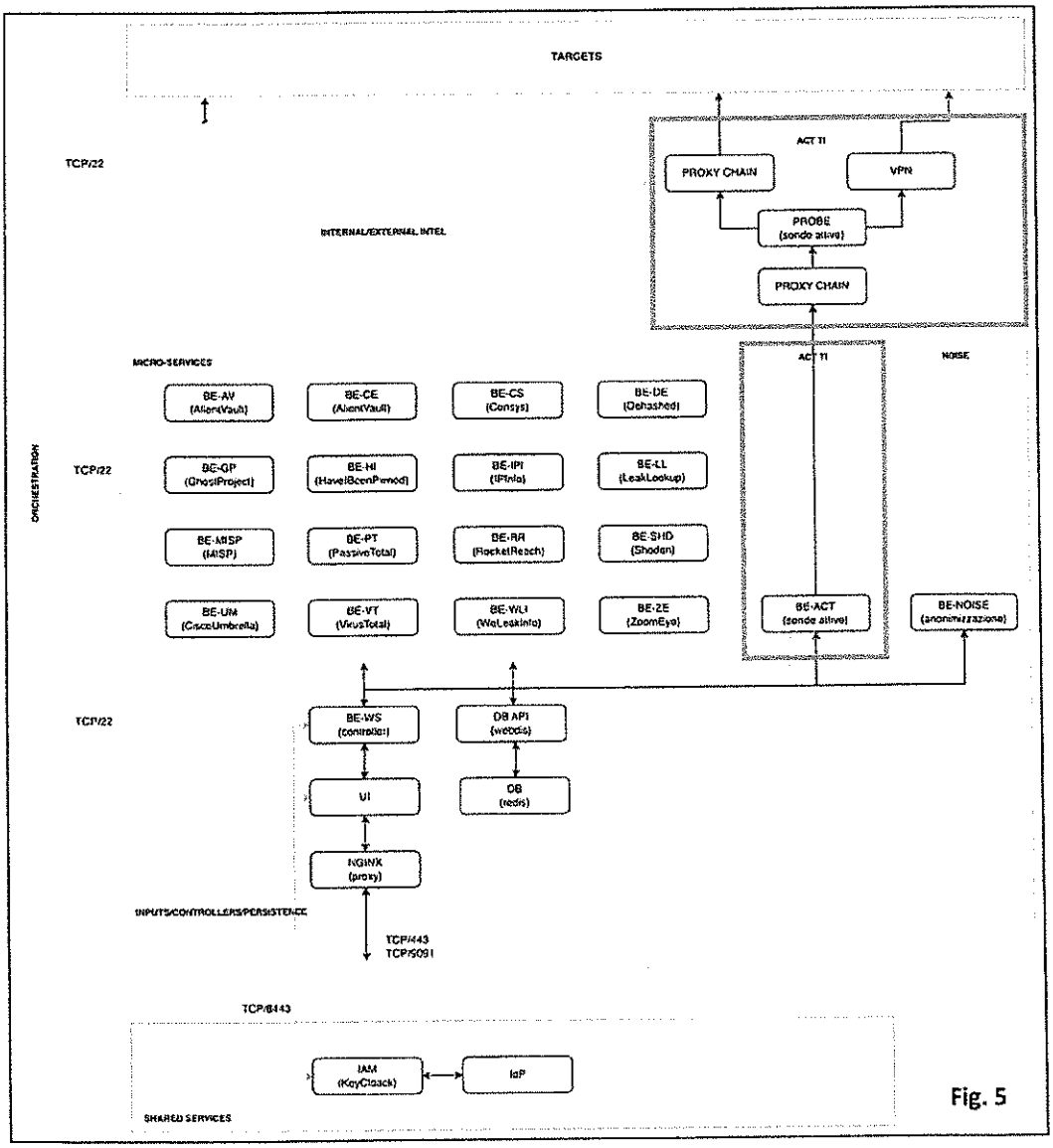

Fig. 5

4. Elenco dei servizi di *footprinting*

Sulla base di quanto ad oggi preventivabile accedendo alle pagine di *marketplace* dei servizi riportati nel precedente **para. 2**, si riporta di seguito la **tabella 1** riepilogativa dei prodotti da acquisire

Futuri sviluppi della piattaforma e, quindi, l'integrazione di altri micro-servizi, allo stato dell'arte valutati significativi per la conduzione delle attività di *reconnaissance* passiva, quali EPIEOS, PIMEYE, TINEYE, NETCRAFT, VIEWDNSINFO, NETLAS, HACKERTARGET, SINT INDUSTRIES, EMAIL TARCKER, PIPL, INTELLIGENCE X, incrementeranno ulteriormente, presumibilmente dal 2025/2026, l'esigenza attuale.

Elenco dei servizi *da acquisire per la durata di 1 anno* *(i successivi rinnovi avverranno attraverso atti separati)*	
Nome Servizio	Numero licenze
CENSYS	1
DEHASHED	1
HAVEIBEENPWNED	1
GHOST PROJECT	1
IPINFO	1
LEAKLOOKUP	1
ROCKET REACH	1
SHODAN	1
VIRUS TOTAL	1
WELEAKINFO	1
ZOOMEYE	1
HUNTERIO	1
PASSIVE TOTAL	1
CISCO UMBRELLA	1
CROWD STRIKE	1
VPN/Cloud Service	1

cyber-bee

DETTAGLIO ANALITICO RDO 4737570

Software	Qt	Costo Unitario	Costo totale
Falcon Adversary Intelligence 12 months	1	55.000,00 €	55.000,00 €

LUCA GABRIELLI
CYBER-BEE S.R.L.