*Raggruppamento Carabinieri Investigazioni Scientifiche*

# CAPITOLATO TECNICO

**Anno 2019**

per la fornitura di:

**CORSO DI HACKING, INTRUSION DETECTION, INCIDENT HANDLING & NETWORK FORENSICS**

**nell'ambito del Progetto n. 47.6.3 "CORSI SULLE VALUTAZIONI STATISTICHE DELLE PROVE FORENSI E SUL CONTRASTO ALLE MINACCE DI RETE MEDIANTE TECNICHE DI HACKING ", cofinanziato dall'UE nell'ambito del Fondo Sicurezza Interna 2014-2020 – Obiettivo specifico 6 "Rischi e Crisi" – Obiettivo Nazionale 3 "Formazione"**

# PARTE I

## CAPO I – GENERALITÀ

Il presente capitolato si riferisce alla fornitura di 1 (uno) corso specialistico, strutturato in 2 fasi (primo e secondo livello) in lingua italiana e/o inglese per massimo 25 persone da svolgere presso la sede del Raggruppamento CC Investigazioni Scientifiche (RaCIS), Caserma "MOVM Salvo d'Acquisto", viale Tor di Quinto 119, 00191, Roma.

Scopo del corso è fornire un'aggiornata ed esaustiva preparazione tecnica ai partecipanti che consenta loro di padroneggiare i vari aspetti dell'hacking e dell'incident handling al fine di individuare e bloccare attacchi informatici nonché condurre indagini tecniche di polizia giudiziaria sull'accaduto atte ad identificarne i responsabili.

Fornitura

La fornitura in oggetto dovrà prevedere un corso di formazione della durata di due settimane (una settimana per ciascuna fase) da effettuarsi sempre presso la stessa sede per un numero massimo di 25 frequentatori per ciascuna fase tramite l'ausilio di personal computer portatili collegati tra loro in rete.

L'ente di formazione dovrà avere pregressa esperienza nell'erogazione corsi per le forze militari nazionali e internazionali nelle materie oggetto dello specifico lotto del bando di gara con particolare riguardo ai vari aspetti dell'hacking.

La fornitura dovrà rispettare tutte le vigenti normative relative a tutti i requisiti di sicurezza.

Scenario di riferimento

L'Arma dei Carabinieri intende avviare un progetto finalizzato alla realizzazione di una formazione specifica in materia di *hacking* e *cyber forensics* rivolto agli operatori specializzati del Ra.C.I.S., R.O.S., S.I.T. e Comandi Provinciali CC (Assistenti e Analisti di Laboratorio Informatico del Ra.C.I.S., Investigatori Tecnici del R.O.S., Operatori Indagini Telematiche delle S.I.T. e dei Nuclei Investigativi) al fine di elevare la loro competenza tecnica in ambito reti e Internet.

L'iniziativa prevede l'effettuazione delle seguenti attività: 1 corso strutturato in 2 fasi di una settimana ciascuna, di cui la prima, propedeutica alla seconda, tratta delle reti e degli incidenti informatici su tali sistemi, mentre la seconda va in dettaglio sulle tecniche di attacco e sugli strumenti di rilevazione e tracciamento degli stessi.

Mediante procedura di gara, sarà individuato un unico soggetto esterno che dovrà provvedere all'organizzazione dei citati moduli didattici del corso presso la sede del Ra.C.I.S.

Per il corso dovrà essere redatto un elenco di docenti con chiara esperienza nel settore, da presentare, unitamente ai *curricula* degli interessati, nell'offerta tecnica e che verranno valutati da apposita Commissione giudicatrice nominata dal Comando Generale.

## CAPO II – REQUISITI TECNICI DI BASE

Per requisiti tecnici di base s'intendono tutte le caratteristiche che il servizio deve possedere per essere considerato idoneo alla fornitura.

Di seguito sono indicati i requisiti di base per i servizi connessi.

Soluzioni equivalenti, rispetto ai requisiti indicati nelle specifiche tecniche, saranno prese in considerazione purché tali proposte, a pena di inammissibilità, siano provate tramite comparazione con mezzi appropriati (non ammissibili autocertificazioni), al fine di accertare la corretta equipollenza con le caratteristiche richieste in sede di Capitolato Tecnico.

I requisiti tecnici di base saranno accertati, durante la valutazione dell'offerta tecnica, da apposita Commissione giudicatrice, nominata dal Comando Generale, con un controllo sui documenti consegnati dalle ditte accorrenti, con le modalità indicate.

I requisiti tecnici di base saranno inoltre oggetto di verifica di conformità a cura di apposita Commissione nominata dal Comando Generale.

### II.1 1^ FASE – PACCHETTO FORMATIVO APPROFONDITO DI INTRUSION DETECTION

Il pacchetto formativo approfondito di *Intrusion Detection* deve prevedere una giornata introduttiva di valutazione dei discenti in relazione al protocollo TCP/IP. Elementi come la struttura dei pacchetti, il modello a strati del TCP/IP, la struttura dei *frame*, l'utilizzo pratico di *Wireshark* e *tcpdump* per una comune analisi di un flusso di rete devono risultare evidenti per tutti e qualora così non fosse bisognerà provvedere all'allineamento delle conoscenze.

Successivamente si andrà avanti con gli strati *link* e IP sia in IPv4 che IPv6 e si toccheranno gli argomenti del *packet fragmentation* in entrambi i casi. Tutti i citati strati dovranno essere studiati sia praticamente che teoricamente dalla prospettiva di chi attacca la rete e di chi la difende. Questo implica l'impiego di esercizi pratici sulla rete mediante *software* come ad esempio *Wireshark* e *tcpdump*.

Appresi i concetti appena descritti si potrà passare all'uso avanzato dei mezzi di filtraggio e recupero dei pacchetti e dei frame sui canali TCP/IP, per poi apprendere come costruire pacchetti al fine di testare la reazione di IDS/IPS e sfruttarne eventuali vulnerabilità.

Si potrà quindi passare allo studio dei maggiori protocolli di livello applicazione (es. DNS, HTTP(S), SMTP, ecc) per studiarne le più comuni vulnerabilità e debolezze.

Con la base di studio svolta potranno essere considerati esercizi pratici su Snort per la rilevazione delle caratteristiche dei flussi e su Bro per la *patterns analysis* dei flussi di rete per la rilevazione di eventi e attività di rete.

Le caratteristiche minime della 1^ Fase del corso sono quindi di seguito elencate.

a. **Finalità.**

   La 1^ Fase del corso dovrà essere orientata a porre gli operatori nelle migliori condizioni per impiegare operativamente i concetti appresi durante il corso nell'ambito delle indagini informatiche e telematiche di polizia giudiziaria.

b. **Programma.**

   Programma di riferimento di seguito.

c. **Durata della 1^ Fase del corso.**

   La 1^ Fase del corso dovrà avere una durata di almeno una settimana (6 gg), suddivisa approssimativamente a metà fra le lezioni teoriche e le lezioni pratiche per almeno 4h al mattino e 3h al pomeriggio.

d. **Località e date della 1^ Fase del corso.**

   La 1^ Fase del corso sarà tenuta presso la sede del Ra.C.I.S. in date e luogo da concordare con l'Amministrazione.

e. **Numero di frequentatori e requisiti istruttori.**

   Il numero massimo di frequentatori alla 1^ Fase del corso sarà 25.

   I *curricula* degli istruttori del pacchetto formativo dovranno essere presentati nell'offerta tecnica per la successiva valutazione da parte di apposita Commissione giudicatrice nominata dal Comando Generale. Nel dettaglio, la Commissione giudicatrice procederà alla verifica delle pubblicazioni scientifiche e/o esperienze pregresse dei docenti elencati nei *curricula*, con particolare riguardo a quelle strettamente inerenti all'argomento del corso.

f. **Lingua.**

   La 1^ Fase del corso dovrà essere tenuto in lingua italiana e/o inglese.

g. **Materiale didattico**

   Tutte le lezioni svolte dai docenti dovranno essere fornite in formato digitale (documentazione con estensione doc, pdf e analoghi ovvero video/audio da poter riprodurre coi comuni software "multimedia player") sia ai discenti che al Raggruppamento Carabinieri Investigazioni Scientifiche (RaCIS) **entro 15gg dal termine delle lezioni** su supporto multimediale; dalla visione del materiale didattico, oltre al contenuto di dettaglio di ciascuna lezione, si dovrà evincere il tipo di insegnamento impartito da ciascun docente.

h. **Attestati.**

   Ai frequentatori della 1^ Fase del corso sarà rilasciato, a cura della Ditta/Società fornitrice, un attestato di partecipazione alla medesima.

i. **Esami di certificazione.**

   I frequentatori della 1^ Fase del corso parteciperanno agli esami di certificazione inerenti al programma di studio, il cui costo sarà incluso in quello del corso.

**PROGRAMMA DI RIFERIMENTO**

TCP/IP

- Packet headers and data?
- TCP/IP communications model
- Data encapsulation/de-encapsulation

Uso di Wireshark

- Stream reassembly con Wireshark
- Visualizzare e analizzare i pacchetti con Wireshark
- Filtraggio dei pacchetti

Uso di tcpdump

- Stream reassembly con tcpdump
- Visualizzare e analizzare i pacchetti con tcpdump
- Filtraggio dei pacchetti

Strati del TCP/IP

- Network Access/Link Layer: Layer 2
- Introduction to 802.x link layer
- Address resolution protocol
- ARP spoofing

IP Layer: Layer 3

- IPv4
  - Checksums e Fragmentation: problemi di sicurezza e integrità;
- IPv6
  - Confronto con IPv4
  - Metodo di indirizzamento IPv6
  - Il protocollo Neighbor discovery
  - Extension headers

TCP:

- Come stimolare risposte anomale del TCP
- Riassemblare i pacchetti nel TCP e metodi per influenzare gli IDS/IPS

UDP:

- Come stimolare risposte anomale del UDP

ICMP:

- Teoria e pratica di impiego del ICMP
- Problemi di sicurezza con ICMP
- Il mapping
- Uso normale e malevolo del ICMP

DNS

- Teoria e pratica del DNS su Internet
- La risoluzione degli indirizzi
- Caching
- DNSSEC
- Problemi di sicurezza con i DNS

Protocolli:

- SMB/CIFS
- MSRPC

HTTP(2)/TLS

SMTP

- STARTTLS
- Esempi pratici di attacco

## II.2 2^ FASE – PACCHETTO FORMATIVO APPROFONDITO DI HACKER TOOLS, TECHNIQUES & INCIDENT HANDLING/FORENSICS

Questo pacchetto formativo, basandosi sugli strumenti concettuali e pratici della 1^ Fase del corso precedente, dovrà permettere al discente di capire come muoversi al verificarsi di un incidente informatico in ambiente di rete, sia che rappresenti un reato che una mera violazione delle regole di gestione del sistema stesso.

Ci dovrà essere quindi una completa introduzione al processo di gestione dell'incidente informatico attraverso i classici passi di preparazione, identificazione, contenimento, eradicazione, recupero e feedback sulle contromisure da preparare per il futuro. Ci dovranno essere inoltre molti casi pratici di studio (meglio se reali) per comprendere cosa voglia dire identificare un attacco informatico e identificare l'attaccante. Questo dovrà essere correlato al lavoro di forensics che viene fatto per trattare il caso in dibattimento e nelle indagini di polizia giudiziaria qualora si configurassero reati.

Dopo l'introduzione dovranno essere passati in rassegna i principali strumenti hacker per la preparazione e lo svolgimento di un attacco informatico. Dall'analisi delle informazioni di rete, a quella dei firewall, al cracking delle protezioni di reti wireless, modem e router fino all'aggiramento degli IDS ed al social engineering. Fattore di merito è lo svolgimento di sessioni pratiche che dovranno aver luogo nella rete locale isolata destinata alla lezione e mai presso le reti interne dell'Arma dei Carabinieri.

Dovranno essere studiate le tecniche di sniffing orientate ai metodi di penetrazione delle protezioni di rete e l'uso delle debolezze di sistema delle macchine e dei sistemi operativi impiegati al fine di guadagnare il controllo delle risorse. Di qui si dovrebbe proseguire con le più comuni tecniche di cracking e di impiego delle backdoor dei software.

Le caratteristiche minime della 2^ Fase del corso sono di seguito elencate.

a. **Finalità.**

   La 2^ Fase del corso dovrà essere orientata a porre gli operatori nelle migliori condizioni per impiegare operativamente i concetti appresi durante il corso nell'ambito delle indagini informatiche e telematiche di polizia giudiziaria.

b. **Programma.**

   Programma di riferimento di seguito.

c. **Durata della 2^ Fase del corso.**

   La 2^ Fase del corso dovrà avere una durata di almeno una settimana (6 gg), suddivisa approssimativamente a metà fra le lezioni teoriche e le lezioni pratiche per almeno 4h al mattino e 3h al pomeriggio.

d. **Località e date della 2^ Fase del corso.**

   La 2^ Fase del corso sarà tenuta presso la sede del Ra.C.I.S. in date e luogo da concordare con l'Amministrazione.

e. **Numero di frequentatori e requisiti istruttori.**

   Il numero massimo di frequentatori alla 2^ Fase del corso sarà 25.

   I *curricula* degli istruttori del pacchetto formativo dovranno essere presentati nell'offerta tecnica per la successiva valutazione da parte di apposita Commissione giudicatrice nominata dal Comando Generale. Nel dettaglio, la Commissione giudicatrice procederà alla verifica delle pubblicazioni scientifiche e/o esperienze pregresse dei docenti elencati nei *curricula*, con particolare riguardo a quelle strettamente inerenti all'argomento del corso.

**f. Lingua.**

La 2^ Fase del corso dovrà essere tenuta in lingua italiana e/o inglese.

**g. Materiale didattico**

Tutte le lezioni svolte dai docenti dovranno essere fornite in formato digitale (documentazione con estensione doc, pdf e analoghi ovvero video/audio da poter riprodurre coi comuni software "multimedia player") sia ai discenti che al Raggruppamento Carabinieri Investigazioni Scientifiche (RaCIS) **entro 15gg dal termine di ciascuna fase del corso** su supporto multimediale; dalla visione del materiale didattico, oltre al contenuto di dettaglio di ciascuna lezione e delle ore erogate, si dovrà evincere il tipo di insegnamento impartito da ciascun docente.

**h. Attestati.**

Ai frequentatori della 2^ Fase del corso sarà rilasciato, a cura della Ditta/Società fornitrice, un attestato di partecipazione alla medesima.

**i. Esami di certificazione.**

I frequentatori della 2^ Fase del corso parteciperanno agli esami di certificazione inerenti al programma di studio, il cui costo sarà incluso in quello del corso.

**PROGRAMMA DI RIFERIMENTO:**

Preparazione

- Kit di emergenza per la gestione degli incidenti informatici
- Come gestire e organizzate un team di pronta risposta
- Come gestire e organizzare un sistema contro gli incidenti informatici

Identificazione

- Rilevare l'incidente
- La catena di custodia
- Rilevazione dei soggetti attivi e ostili
- Aspetti forensi: identificazione di reati

Contenimento, Congelamento e Repertamento

- Documentazione cartacea video e audio
- Organizzazione di una quarantena
- Come sospendere i servizi del Sistema
- Copia forense dello stato del sistema
- Congelamento dello stato del sistema

Eliminazione

- Valutazione della compromissione dei backup
- Riattivazione del Sistema operativo
- Eventuale denuncia e indagini di polizia giudiziaria

Recupero e feedback

- Riattivazione dei servizi del sistema
- Piani di monitoraggio
- Metodi aggiornati di gestione degli attacchi
- Modifiche delle politiche di sicurezza

Tecniche di rilevazione dati e tracciamento dalle reti

- Using Whois lookups, ARIN, RIPE and APNIC
- Domain Name System harvesting
- Analisi di post, website e databases
- Recon-ng
- Pushpin
- Identificazione e uso di account compromessi

Scanning di rete

- wireless LAN insicure
- telefoni e modem insicuri
- Port scanning: base, stealth e blind scanning
- Rilevazione delle regole dei firewall
- Vulnerability scanning con Nessus e altri strumenti
- CGI scanning - Nikto
- Powershell Empire
- Bloodhound
- Rubber Duckie attacks
- Analisi comportamentale degli utenti di rete

Elusione degli Intrusion Detection System (IDS)

- Elusione IDS a livello rete
- Elusione IDS a livello applicazione
- Web Attack IDS
- Tecniche di offuscamento

Attacchi a livello rete

- Session hijacking: da Telnet a SSL e SSH
- Monkey-in-the-middle attacks
- Passive sniffing

Raccolta e analisi pacchetti

- Active sniffing: ARP cache poisoning e DNS injection
- Bettercap
- Responder
- LLMNR poisoning
- WPAD Attacks
- MITMf
- DNS cache poisoning: redirezione del traffico su Internet
- Netcat
- IP address spoofing

Attacchi a livello applicazione e Sistema operativo

- Dettagli sul Buffer overflows
- The Metasploit exploitation framework
- Format string attacks
- AV and application whitelisting bypass techniques

Password Cracking

- Worm
- Password cracking con John the Ripper
- Hashcat
- Rainbow Tables
- Password spraying

Attacchi alle Web Application

- Account harvesting
- SQL Injection: back-end databases
- Session Cloning: Grabbing web sessions
- Cross-Site Scripting

Denial-of-Service Attacks

- Distributed Denial of Service
- Local Denial of Service

## CAPO III – REQUISITI TECNICI OPZIONALI

Per requisiti tecnici opzionali s'intendono tutte le caratteristiche migliorative delle prestazioni di base che il servizio può possedere e che costituiscono oggetto di eventuale punteggio incrementale per la valutazione dell'offerta.

Di seguito sono indicati i requisiti opzionali che sono oggetto di valutazione.

Soluzioni equivalenti, rispetto ai requisiti indicati nelle specifiche tecniche, saranno prese in considerazione purché tali proposte, a pena di inammissibilità, siano provate tramite comparazione con mezzi appropriati (non ammissibili autocertificazioni), al fine di accertare la corretta equipollenza con le caratteristiche richieste in sede di Capitolato Tecnico.

I requisiti tecnici opzionali saranno accertati, durante la valutazione dell'offerta tecnica, da apposita Commissione giudicatrice, nominata dal Comando Generale, con un controllo sui documenti consegnati dalle ditte accorrenti, con le modalità indicate.

I requisiti tecnici opzionali saranno inoltre oggetto di verifica di conformità a cura di apposita Commissione giudicatrice, nominata dal Comando Generale.

### III.1. 1^ FASE – PACCHETTO FORMATIVO APPROFONDITO DI INTRUSION DETECTION

| CRITERIO N. | REQUISITO | SPIEGAZIONE |
|---|---|---|
| **1** | **Esercitazioni pratiche** | Esercitazioni pratiche in relazione a ogni singolo argomento |
| **2** | **Software per la didattica da pre-installare** | Software (in particolare il VMwave) sul luogo della didattica, installato prima delle lezioni sui PC e quindi già disponibile sulle postazioni impiegate dai discenti. |
| **3** | **Coursebook con materiale didattico attinente la fase del corso** | Fornitura di Coursebook attinente la fase del corso come ausilio alla didattica |
| **4** | **Files audio MP3 con i contenuti della didattica** | Fornitura di files audio MP3 con le lezioni complete come ausili alla didattica |
| **5** | **Modulo sulle attività di rete** | Modulo relativo alle attività sulla rete di seguito elencate:<br>- Configurare una rete per la raccolta e filtraggio dei pacchetti<br>- Installazione e strategie di IDS/IPS<br>- Esempi di Hardware per la cattura del traffico dati<br>- Principali funzioni di un IDS<br>- Gestione dei flussi di rete con Snort e Bro<br>- Esempi pratici di IDS e IPS |
| **6** | **Modulo file pcaps** | Modulo relativo ai file pcaps su:<br>- Analisi dei file pcaps e gestione dei file pcaps di grosse dimensioni |

| | | |
|---|---|---|
| **7** | **Modulo traffico criptato e tunnel** | Modulo relativo al traffico criptato e tunnel su:<br>- DNS tunnel software dnscat2<br>- Tunneling software The Onion Router (TOR) |
| **8** | **Esame di certificazione** | Esame di certificazione riconosciuto a livello internazionale sugli argomenti del corso |

## III.2. 2^ FASE – PACCHETTO FORMATIVO APPROFONDITO DI HACKER TOOLS, TECHNIQUES & INCIDENT HANDLING/FORENSICS

| CRITERIO N. | REQUISITO | SPIEGAZIONE |
|---|---|---|
| **9** | **Esercitazioni pratiche** | Esercitazioni pratiche in relazione a ogni singolo argomento |
| **10** | **Software per la didattica da pre-installare** | Software (in particolare il VMwave) sul luogo della didattica, installato prima delle lezioni sui PC e quindi già disponibile sulle postazioni impiegate dai discenti. |
| **11** | **Slides (almeno 1000) di istruzioni/note attinenti la fase del corso** | Slides (almeno 1000) di istruzioni/note attinenti la fase del corso utili per la didattica |
| **12** | **Files audio MP3 con i contenuti della didattica** | Fornitura di files audio MP3 con le lezioni complete come ausili alla didattica |
| **13** | **Modulo Denial-of-Service Attacks** | Modulo relative Denial-of-Service Attacks su:<br>- Distributed Denial of Service<br>- Local Denial of Service |
| **14** | **Modulo superamento delle difese** | Modulo relativo alla superamento delle difese, rimanendo internamente ad un sistema "ostile"<br>- Backdoors: Poison Ivy, VNC, Ghost RAT, e altro<br>- Trojan horse backdoors<br>- Rootkits<br>- Kernel-level Rootkits |
| **15** | **Modulo eliminazione delle "tracce"** | Modulo relative all'eliminazione delle "tracce" su<br>- Camuffare directory e file<br>- Log file editing su Windows e Unix<br>- Accounting entry: UTMP, WTMP, shell histories, etc.<br>- Canali sotto copertura su HTTP, ICMP, TCP, e altri protocolli<br>- Sniffing backdoors<br>- Steganography |
| **16** | **Esame di certificazione** | Esame di certificazione riconosciuto a livello internazionale sugli argomenti del corso |

# CAPO V – DISPOSIZIONI TECNICO-AMMINISTRATIVE

Tutti i costi finalizzati alla formazione del personale presso la sede del RaCIS, compresi gli spostamenti dei docenti, sono a carico dell'ente di formazione.

A seguito della sottoscrizione del contratto, il fornitore dovrà **erogare il corso di formazione entro 45gg. solari** a decorrere dal giorno successivo alla ricezione della comunicazione, a mezzo P.E.C., dell'avvenuta registrazione del contratto presso gli organi di controllo, comunicando al RaCIS l'inizio delle attività (a mezzo PEC) con almeno **15gg solari di preavviso**. Il corso potrà essere erogato solo a seguito di specifica autorizzazione del RaCIS.

## CAPO VI – DESTINAZIONE FINALE DI EVENTUALI CAMPIONI O MATERIALI

Eventuali campioni o materiali forniti dalla ditta aggiudicataria, sia in fase di gara che durante il corso che nella successiva verifica di conformità, resteranno nelle disponibilità del RaCIS.

## CAPO VII – VERIFICA DI CONFORMITA'

Durante il corso di formazione si procederà a condurre verifiche di conformità al termine di ciascuna delle due fasi del corso per constatare il corretto svolgimento delle attività formative; tali accertamenti verranno effettuati da una Commissione nominata dal Comando Generale che procederà alla verifica della corrispondenza di ciascuna fase formativa ai requisiti tecnici e al completo svolgimento del corso sulla base della documentazione fornita all'Amministrazione che verrà verificata tramite riscontro diretto dei corsisti.
Il costo delle operazioni di verifica di conformità è a carico dell'Ente fornitore.

## CAPO VIII – PAGAMENTI

Il pagamento a favore del/della R.T.I. fornitore/Società fornitrice avverrà in due rate, del tutto equivalenti, rispettivamente al termine di ciascuna delle due fasi del corso, dopo la favorevole verifica di conformità.
La fattura relativa dovrà essere emessa solo a seguito dell'avvenuta favorevole verifica di conformità.

## CAPO IX – DUVRI
## (Documento Unico di Valutazione dei Rischi da Interferenze)

Non sussiste l'obbligo di redazione del DUVRI e l'importo dei relativi oneri della sicurezza è pari a zero in quanto non sono previste interferenze e contatti rischiosi tra il personale della ditta appaltatrice della fornitura ed il personale dell'Arma dei Carabinieri e di imprese eventualmente operanti con contratti differenti nella medesima sede di esecuzione della prestazione.