TEKNİK ŞARTNAME
(Hizmet Alımı)

Madde 1. Tanımlar

Ajans: Güney Marmara Kalkınma Ajansı

Yararlanıcı: Ajans'tan teknik destek almaya hak kazanan gerçek veya tüzel kişiler

İstekli: Bu şartnamede yer alan hizmet alımı için teklif veren gerçek veya tüzel kişiler

Yüklenici: Hizmet alımı işini üstlenecek olan gerçek veya tüzel kişiler

Madde 2. Eğitim/Danışmanlık Hizmet Alımının Genel Kapsamı

Yararlanıcı	Balıkesir Büyükşehir Belediyesi BASKİ Genel Müdürlüğü
Yeri	BASKİ Genel Müdürlüğü
Konu	Güvenli Bilişim Kullanımı Kapsamında Siber Güvenlik Eğitimi
Tarih	06.11.2023-15.11.2023
Faydalanacak Kişi Sayısı	20
Toplam Süre (Gün)	10

Madde 3. Hizmet Sağlayıcı ve Eğitmen/Danışmanda Aranan Şartlar

- Eğitim verecek olan Eğitmen aşağıda belirtilen alt konu başlıklarında daha önce eğitim vermiş olmalıdır.
- Eğitim verecek olan Eğitmen T.C. vatandaşı olacak global ölçekte kabul gören aşağıdaki sertifikaların en az ikisine sahip olacaktır. Sertifikaların geçerlilik süresinin devam ediyor olması gerekmektedir. İlgili sertifikalar işe başlamadan önce Kuruluşa sunulacaktır.

  Kabul gören sertifikalar aşağıdaki gibidir:

  - LPT (Licenced Penetration Tester)
  - GPEN (GIAC Certified Penetration Tester)
  - OSCP (Offensive Security Certified Professional)
  - OSCE (Offensive Security Certified Expert)
  - OSEP (Offensive Security Experienced Penetration Tester)
  - eCPTx (E-Learn Security Certified Penetration Tester Extreme)
  - CYSA (Cyber Security Analyst Certified)
- Eğitimler sonunda katılımcılara firma tarafından sertifika verilecektir.

Madde 4a. Talep edilen eğitim hizmetinin detaylı içeriği

ALT KONULAR (Her bir konu başlığının içeriğine ilişkin özet bilginin verilmesi istenmektedir.)	SÜRE (GÜN)	GÜNLÜK SAAT	TOPLAM SAAT
Siber Güvenlik Eğitimi **Temel Ağ Bilgisi** **Ağ Nedir, Özellikleri ve Faydaları** **Ders Örneklendirmesi (Paylaşımlar)** **Başlıca Ağ Donanımları** **LAN, VLAN ve WAN Ağlar** **Ağ Protokolü Kavramı** **OSI ve TCP/IP Referans Modelleri** **TCP ve UDP Protokolleri** **Portlar** **ARP, ICMP ve Tracert Başarım Araçları** **TCP/IP Paketleri ve İçerikleri** **RFC (Request for Comments) Kavramı** **IANA (Internet Assigned Numbers Authority)** **IP (Internet Protocol) Adresleri** **Network ID ve Host ID Kavramı** **Subnet Mask ve IP Sınıfları** **İletim Türleri ve Teknikleri** **Ağ Servisleri** **DNS (Domain Name System)** **DHCP (Dynamic Host Configuration Protocol)** **NAT (Network Address Translation)** **Domain, DNS Hiyerarşisi ve FQDN Kavramları** **VPN Kavramı ve Türleri** **Firewall (Güvenlik Duvarı) Yönetimi** **SSH ile Uzaktan Konsol ve Dosya Yönetimi** **Lokal Kullanıcı Komutları ve Yönetimi** **Disk Yönetimi ve Dosya Sistemleri (nas-das-iscsi)** **Siber Saldırı ve Savunma Yöntemleri** **Test Araçları** **Penetration Testing Tools** **NMAP - Introduction** **NMAP - Switches** **NMAP - Scan Types - Overview** **NMAP - Scan Types - TCP Connect Scans** **NMAP - Scan Types - SYN Scans** **NMAP - Scan Types - UDP Scans** **NMAP - Scan Types - NULL, FIN, Xmas Scans** **NMAP - Scan Types - ICMP Network Scanning** **NMAP - NSE Scripts - Working with the NSE** **NMAP - NSE Scripts - Searching for Scripts** **NMAP - Firewall Evasion** **NMAP - Practical & Conclusion** **NMAP - NSE Scripts – Overview** **BURPSUITE - Intro & Installation** **BURPSUITE - Getting Certified**	10		

BURPSUITE - Overview of Features **BURPSUITE - Engage Dark Mode** **BURPSUITE - Proxy** **BURPSUITE - Target Definition** **BURPSUITE - Repeater** **BURPSUITE - Intruder** **BURPSUITE - Sequncer** **BURPSUITE - Decoder and Comparer** **BURPSUITE - Extender** **BurpSuite Extensions - Ek Kaynak** **BURPSUITE - Scanner & Collaborator Client** **BURPSUITE - Extra Credit** **BURP SUITE: THE BASICS - Burp Suite Edition'ları** **BURP SUITE: THE BASICS - Burp Community Özellikleri** **BURP SUITE: THE BASICS - Installation** **BURP SUITE: THE BASICS - The Dashboard** **BURP SUITE: THE BASICS - Navigation & Shortcut** **BURP SUITE: THE BASICS - Options** **BURP SUITE: THE BASICS - Burp Proxy** **BURP SUITE: THE BASICS - FoxyProxy** **BURP SUITE: THE BASICS - Proxying HTTPS** **BURP SUITE: THE BASICS - Burp Suite Browser** **BURP SUITE: THE BASICS - Scoping & Targeting** **BURP SUITE: THE BASICS - Site Map & Issue Definitions** **BURP SUITE: THE BASICS - Example Attack** **METASPLOIT: INTRODUCTION - Intro** **METASPLOIT: INTRODUCTION - Main Components** **METASPLOIT: INTRODUCTION - Msfconsole** **METASPLOIT: INTRODUCTION - Working with Modules** **METASPLOIT: INTRODUCTION - Kapanış** **METASPLOIT - Initializing** **METASPLOIT - Commands** **METASPLOIT - Modules** **METASPLOIT - Shell** **METASPLOIT - Meterpreter** **METASPLOIT - Pivoting (+Proxychains)** **NESSUS - Introduction** **NESSUS - Installation** **NESSUS - Scans** **NESSUS - Scanning** **NESSUS - Web Application Tests** **HYDRA - Introduction** **HYDRA - Using** **HTTP IN DETAIL - HTTP** **HTTP IN DETAIL - Requests & Responses** **HTTP IN DETAIL - HTTP Methods** **HTTP IN DETAIL - HTTP Status Codes** **HTTP IN DETAIL - Headers** **HTTP IN DETAIL - Cookies** **HTTP IN DETAIL - Making Requests** **Aplication Based** **WEB FUNDAMENTALS - Web Sitelerini Nasıl Yükleriz?** **WEB FUNDAMENTALS - Request ve Response'lar** **WEB FUNDAMENTALS - Cookie'ler**			

WEB FUNDAMENTALS - CTF **OWASP JUICE SHOP - Giriş** **OWASP JUICE SHOP - Walking Through** **OWASP JUICE SHOP - Injection** **OWASP JUICE SHOP - Broken Authentication** **OWASP JUICE SHOP - Sensitive Data Exposure** **OWASP JUICE SHOP - Broken Access Control** **OWASP JUICE SHOP - XSS** **OWASP JUICE SHOP - Score Board** **VULNVERSITY - Reconnaissance w/ Nmap** **VULNVERSITY - Directory Discovery w/ GoBuster** **VULNVERSITY - Shell Upload** **VULNVERSITY - Linux PrevEsc** **Network-Based Vulnerabiliteies** **INTRODUCTORY NETWORKING - OSI Referans Modeli** **INTRODUCTORY NETWORKING - Encapsulation** **INTRODUCTORY NETWORKING - TCP/IP Modeli** **INTRODUCTORY NETWORKING – Ping** **INTRODUCTORY NETWORKING - Traceroute** **INTRODUCTORY NETWORKING - Whois** **INTRODUCTORY NETWORKING - Dig** **INTRODUCTORY NETWORKING - Kapanış** **NETWORK SERVICES - Intro** **NETWORK SERVICES - SMB Hakkında** **NETWORK SERVICES - SMB Enumeration** **NETWORK SERVICES - SMB Exploiting** **NETWORK SERVICES - Telnet Hakkında** **NETWORK SERVICES - Telnet Enumeration** **NETWORK SERVICES - Telnet Exploiting** **NETWORK SERVICES - FTP Hakkında** **NETWORK SERVICES - FTP Enumeration** **NETWORK SERVICES - FTP Exploiting** **NETWORK SERVICES - Kapanış** **NETWORK SERVICES 2 - Intro** **NETWORK SERVICES 2 - NFS Hakkında** **NETWORK SERVICES 2 - NFS Enumeration** **NETWORK SERVICES 2 - NFS Exploiting w/ Root Squash PrivEsc** **NETWORK SERVICES 2 - SMTP Hakkında** **NETWORK SERVICES 2 - SMTP Enumeration** **NETWORK SERVICES 2 - SMTP Exploiting** **NETWORK SERVICES 2 - MySQL Hakkında** **NETWORK SERVICES 2 - MySQL Enumeration** **NETWORK SERVICES 2 - MySQL Exploiting** **NETWORK SERVICES 2 - Kapanış** **KENOBI - Samba Enumeration** **KENOBI - FTP Exploiting** **KENOBI - Linux PrivEsc w/ Path Variables + SUID** **Local Host Vulnerabilities** **ACTIVE DIRECTORY BASICS - Fiziksel AD** **ACTIVE DIRECTORY BASICS - Forest Yapısı** **ACTIVE DIRECTORY BASICS - Users & Groups** **ACTIVE DIRECTORY BASICS - Trusts & Policies**			

ACTIVE DIRECTORY BASICS - AD DS & Authentication **ACTIVE DIRECTORY BASICS - AD Azure** **ACTIVE DIRECTORY BASICS - PowerShell & PowerView** **PowerShell & PowerView Cheatsheets** **ACTIVE DIRECTORY BASICS - Kapanış** **ATTACKTIVE DIRECTORY - Setups (Impacket, Bloodhound & Neo4j)** **ATTACKTIVE DIRECTORY - AD Enumeration** **ATTACKTIVE DIRECTORY - Domain User Enumeration** **ATTACKTIVE DIRECTORY - Kerberos Exploiting** **Kerberos Hakkında - Ek Kaynak** **ATTACKTIVE DIRECTORY - SMB Map & Decoding** **ATTACKTIVE DIRECTORY - Domain PrivEsc** **ATTACKING KERBEROS - Terminoloji** **ATTACKING KERBEROS - AD User Enumeration** **ATTACKING KERBEROS - Ticket Harvesting & Password Spraying** **ATTACKING KERBEROS - Kerberoasting Attack** **ATTACKING KERBEROS - AS-REP Roasting Attack** **ATTACKING KERBEROS - Pass the Ticket Attack** **ATTACKING KERBEROS - Golden/Silver Ticket Attacks** **ATTACKING KERBEROS - Kerberos Backdoors** **ATTACKING KERBEROS - Kapanış** **POST EXPLOITATION BASICS - Enumeration w/ Powerview** **POST EXPLOITATION BASICS - Enumeration w/ Bloodhound** **POST EXPLOITATION BASICS - Dumping w/ Mimikatz** **POST EXPLOITATION BASICS - Golden Ticket w/ Mimikatz** **POST EXPLOITATION BASICS - Enumeration w/ Server Manager** **POST EXPLOITATION BASICS - Persistence Backdoor** **POST EXPLOITATION BASICS - Kapanış** **----------** **UPLOAD VULNERABILITIES - Intro II** **UPLOAD VULNERABILITIES - General Methodology** **UPLOAD VULNERABILITIES - Overwriting Existing Files** **UPLOAD VULNERABILITIES - Remote Code Execution (Web)** **UPLOAD VULNERABILITIES - Filtering** **File Upload** **UPLOAD VULNERABILITIES - Bypassing Client-Side Filtering** **cURL** **UPLOAD VULNERABILITIES - Bypassing Server-Side Filtering: File Extensions** **UPLOAD VULNERABILITIES - Bypassing Server-Side Filtering: Magic Numbers** **UPLOAD VULNERABILITIES - Example Methodology** **UPLOAD VULNERABILITIES - Challenge** **UPLOAD VULNERABILITIES - Kapanış** **Etik Hacking, Penetrasyon Testi ve Lab Kurulumları**			

Hack ve Hacker Kavramı **Penetrasyon Testi Metodolojisi** **Cyber Kill Chain (Siber Ölüm Zinciri) Nedir?** **VMware ile Kali Kurulumu** **Kali'de Root Olmak** **Kali'de Shell Değişimi** **Kali'de XFCE Özelleştirmeleri** **Kali'de Encryption'lı Diski Genişletme** **Alias, Git, Path ve Repo Kullanımları** **Pentest Faz: 1** **Arama Operatörleri ile Google Dorking** **Shodan Nedir, Nasıl Kullanılır?** **WayBack Machine Nedir, Neden Kullanılır?** **Domain Enumeration Nedir, Nasıl Yapılır?** **Shell Komutları ile Domain ve DNS Enumeration** **SubDomain'leri Tespit Etme** **DNS Zone Transfer Kontrolü** **Reverse IP Lookup ile Host'taki Web Sayfalarının Tespiti** **Web Sitesinde Kullanılan Teknolojilerinin Tespiti** **Web Sitelerinde Dosya-Dizin Tespiti ve Wordlist Kavramı** **Photon ve Raccoon ile Tümleşik Tespitler** **OSINT Kavramı ve E-Mail Hesapları (Personel) Tespiti** **Potansiyel Profil Tespitleri** **Maltego ile Tümleşik OSINT** **Proxy ve VPN Kavramı** **OpenVPN ile VPN Kullanımı** **TOR ile Anonim Olmak (Gizlenmek)** **Deep Web, Dark Web Kavramları ve Arasındaki Farklılıklar** **TOR Browser Kurulumu** **Deep Web'te Surf ve İçerikler** **Lab Kurulumu** **Metasploitable 3 (Windows Server 2008 R2) Kurulumu** **Metasploitable 3 İndirme Linkleri** **Kioptrix 1 (Linux RedHat Server) Kurulumu** **LAB Çalışma Alanı İpuçları** **LAB Network Ayarları** **Pentest Faz 2** **Netdiscover ve ARP-Scan ile Host Discovery** **Nmap, Komut ve Parametreleri (Nmap Cheat Sheet)** **Nmap Kullanımı ile Port, Servis ve OS Tespiti** **NSE (Nmap Script Engine) Yardım Alımı** **NSE ile NetBIOS Discovery** **NSE ile SMB Enumeration** **NSE ile MySQL, Postgres, Oracle, Msql Enumeration** **NSE ile SSH Enumeration** **NSE ile HTTP Enumeration** **NSE ile Güvenlik Açığı ve CVE Tespiti (Vuln, Vulners)** **Nmap Vulscan ile Güvenlik Açığı ve CVE Tespiti** **Legion (Nmap GUI) ile Tümleşik Tarama** **Lab Güncelleme - W2K8 Lisans Süresini Uzatma** **Nessus ile Güvenlik Açığı Tespiti**			

Greenbone ile Güvenlik Açığı Tespiti **Pentest Faz 3** **Remote Shell Kavramı ve Türleri** **Netcat ile Bind Shell Örneği** **Metasploit Kavramları ve Komutları** **Metasploit Veritabanı (DB) İlk Ayarlamaları** **Metasploit'te Yardım Alımı** **Metasploit'te Arama (Search) Kullanımı** **Metasploit'te Modül Kullanımı ve Ayarları** **Metasploit'te Nmap Kullanımı** **Exploit Saldırıları** **Nmap ve Metasploit ile MS17-010 Açığı Kontrolü** **MS17-010 Açığına Exploit Saldırısı** **Meterpreter Komutları (Meterpreter Cheat Sheet)** **Meterpreter ile Hedefte Sistem Keşfi** **Meterpreter ile Hedefte Dosya Dizin Yönetimi** **Exploit Araştırması (Spesifik Hedef için)** **ManageEngine'e Exploit Saldırısı - Windows** **ElasticSearch'e Exploit Saldırısı - Windows** **Apache Axis2'ye Exploit Saldırısı - Windows** **Samba'ya Exploit Saldırısı (ve Staged, Non-Staged Payload'lar) - Linux** **Java JMX'e Exploit Saldırısı - Windows** **Exploit Veritabanları ve Kaynakları** **Searchsploit ile Exploit-DB Kullanımı** **Manuel Exploit ile Apache'ye Saldırı - Linux** **Manuel Exploit ile Samba'ya Saldırı - Linux** **Burute Force ve Exploit Saldırıları** **Dictionary Attack ve Wordlist'ler Hk.** **Lokal Wordlist'ler** **Nmap ile Dictionary Attack (SSH)** **Metasploit ile Dictionary Attack (SSH)** **Medusa ile Dictionary Attack (SSH)** **Ncrack ile Dictionary Attack (SSH)** **Hydra ile Dictionary Attack (SSH)** **SSH Komutları ve Kullanımı** **RDP'ye Dictionary Attack ve RDesktop** **MySQL'e Dictionary Attack ve Null Password** **MySQL Komutları, Kullanımı ve DBDump** **Hash Cracking** **Wordpress Login'e Dictionary Attack** **ManageEngine Login'e Dictionary Attack** **SMB'ye Dictionary Attack + Exploit + Hash Crack** **GlassFish'e Dictionary Attack + Exploit** **Man in the Middler Saldırısı – bu eğitimde ve diğerlerinde sorunların karşı tedbirleri alınması** **Ortadaki Adam (Man-in-the-Middle) Kavramı** **Wireshark Kullanımı ve Paket Filtreleme** **ARP Hakkında Ön Bilgilendirme** **ARP Poisoning (ARP Zehirleme) Saldırısı** **ARP Poisoning'in Kavranması ve IP Forwarding**			

HTTP Packet Sniffing **HTTPS, SSL Strip ve HSTS Hk.** **DNS Spoofing Saldırısı** **DHCP Spoofing (Rogue Server) Saldırısı** **DHCP Starvation Saldırısı** **Pentest Faz 4** **Windows'ta Local Exploit Tespiti** **Linux'ta Local (Kernel) Exploit Tespiti** **Linux'a Dosya Çekerek Kernel Exploit Tespiti** **Metasploit Çoklu Oturum Yönetimi** **Metasploit ile Local Exploit Tespiti** **Hedefte Local Enumeration (Otomatik)** **Privilege Escalation Saldırıları** **Windows'ta Yetki Yükseltme (Otomatik)** **Windows'ta Yetki Yükseltme (Manuel)** **Linux'ta Yetki Yükseltme (Manuel)** **Linux Hash Dump ve Crack** **Windows Hash Dump ve Crack** **Migration (Göç) İşlemi** **Meterpreter Scriptleri ve Şifrelerin Elde Edilmesi** **Hedefte Keylogger Çalıştırma** **Hedefin Ekran Görüntüsünü Alma** **Apt (Advanced Persistent Threat) Saldırıları** **Manuel Payload'lar Oluşturma (Backdoor)** **Backdoor'u Sistem Açılışına Yerleştirme** **Backdoor'u Görev Zamanlayıcıya Yerleştirme** **Unquoted Service Path ile Kullanıcı Ekleme** **Registry ile Kullanıcı Girişi Gizleme** **Registry ile Açılışa Exe Yerleştirme** **Registry ile Remote Desktop'ı Aktif Etme** **Metasploit ile Remote Desktop'ı Aktif Etme** **Metasploit ile Açılışa Exe Yerleştirme** **Lab 2 Kurulumu** **Lokal Domain ve Active Directory Kavramları** **İndirmeler (Microsoft Evaluation Center)** **Windows Server 2019 Domain Controller Kurulumu** **Domain Kurulumu ve Active Directory Ayarları** **Windows 10 Client 1 Kurulumu** **Client 1 Ayarları ve Domain'e Join Etme** **Windows 10 Client 2 Kurulumu** **Client 2 Ayarları ve Domain'e Join Etme** **Kurumsal Düzen - Gerçek Dünya** **Antivirüs Kurulumları** **Group Policy Kavramı ve Kullanımı** **Aktif Directory / Domain Atak Vektörleri** **LM, NT Hash, NTLMv1/2 Kavramlarının Pekiştirilmesi** **LLMNR/NBT-NS Poisoning ve NTLMv2 Capture**			

SMB İletişimini Kesme ve NTLMv2 Capture **NTLMv2 Hash Cracking** **SMBv2 Signing Kullanım Tespiti** **SMB Relay Saldırısı ve NTLM Hash Capture** **NTLM Hash Cracking** **Tüm Ağda ve Uzaktan (Remote) Hash Dump** **Önbelleklenmiş (CDLC) Şifre Hash'lerini Elde Etme** **Cached Domain Logon Hash'lerinin Kırılması** **Psexec ile Shell Alımı - Defender VS TrendMicro** **Fake SMB Server Saldırısı** **SMB Relay Saldırısı ile NC Shell Alımı** **Pass the hash saldırırları - lateral Movement** **Şifre Püskürtme (Password Spraying) Saldırısı** **Tüm Network'e Pass-the-Hash (PTH) Saldırısı** **PTH Saldırısı ile Hash Dump** **PTH Saldırısı ile Paylaşım ve Kullanıcı Yetki Tespiti** **PTH Saldırısı ile Dosya Download-Upload** **PTH Saldırısı ile Dosya Çalıştırma** **PTH Saldırısı ile RDP Kullanımı** **PTH Saldırısı ile Domain'i Ele Geçirme** **Antivirüs Atlatmaları ve Trojan Saldırıları** **Veil Framework Kurulumu** **Trojan'ler Hazırlama** **Trojan'leri Online Test Etme ve No Distribute Hk.** **Embed File Hazırlama** **Embed Trojan Hazırlama** **Trojan'e RTLO (U+202E) Uygulama** **Trend Micro'lu Windows 10'da Test** **Otomatik Embed Trojan Hazırlama** **Trend Micro'lu Windows 10'da Test II** **Antivirüs Modları ve Davranışları Hakkında** **Relay ve Pivoting Saldırıları** **Pivoting'in Kavranması** **Port Yönlendirme ile İzinsiz Hedefe Erişim** **Lab Güncelleme - Yeni Network Oluşturma** **Bilinmeyen Diğer Ağların ve Hedeflerin Tespiti** **Pentest Faz 5** **Route ve Port Yönlendirmelerinin Silinmesi** **Registry Girdilerinin Temizlenmesi** **Powershell Geçmişini Silme** **Run Geçmişinin Temizlenmesi** **Temp'in Temizlenmesi** **Geri Döndürülemez Olarak Silme** **Kayıtların (Log'ların) Yok Edilmesi** **Raporlama ve Dokümantasyon** **Dokümantasyon ve Raporlama Süreçleri** **Statement of Work (SOW)** **Master Service Agreement (MSA)** **Non-Disclosure Agreement (NDA)**			

Rules of Engagement (ROE) **Findings Report (FR)** **Örnek Penetrasyon Testi Raporları** **Kurumda canlı olarak yapılacak olan pentestin raporlanması** **Wifi Saldırıları (Atak Vektörleri) Eğitimi** **WiFi TEKNOLOJİLERİ - Standart, Hız ve Menziller** **WiFi TEKNOLOJİLERİ - Frekans Bantları ve Arasındaki Farklılıklar** **WiFi TEKNOLOJİLERİ - Parazitler** **WiFi TEKNOLOJİLERİ - WiFi Kanalları ve Kanal Çakışmaları** **WiFi TEKNOLOJİLERİ - Kanalların Tespiti için Uygulamalar** **HAZIRLIKLAR - WiFi Adaptörünün Kali'ye Tanıtılması** **HAZIRLIKLAR - Saldırılar Öncesi MAC Adresi Değiştirme** **WiFi DOS SALDIRILARI - Aircrack-ng Aracı Hk** **WiFi DOS SALDIRILARI - Monitör Moda Geçiş** **WiFi DOS SALDIRILARI - Etraftaki SSID ve MAC'lerin Tespiti** **WiFi DOS SALDIRILARI - Packet Injection ve AP'e Bağlı Kullanıcıları Görme** **WiFi DOS SALDIRILARI - AP'e Deauth ile DOS Saldırısı** **WiFi DOS SALDIRILARI - Spesifik Kullanıcıya DOS Saldırısı** **WiFi DOS SALDIRILARI - Gizli SSID'lerin İsimlerini Öğrenme** **WiFi BRUTEFORCE SALDIRILARI - WPA-WPA2 Parolasını Elde Etme** **WiFi BRUTEFORCE SALDIRILARI - WPA-WPA2 Parolasını Kırma** **WiFi MITM SALDIRILARI - Evil Twin ve Captive Portal Saldırıları Hk** **WiFi MITM SALDIRILARI - Açıklama** **WiFi MITM SALDIRILARI - WiFi Spoofing Saldırısı** **WiFi MITM SALDIRILARI - Evil Twin ve Captive Portal Saldırısı** **WiFi MITM SALDIRILARI - PHP Script ile Login Bilgilerini Ayıklama** **WiFi MITM SALDIRILARI - Deauth Saldırısı için Bilgilendirme** **WiFi MITM SALDIRILARI - Script Injection** **WiFi MITM SALDIRILARI - Beacon (SSID) Flood Saldırısı** **WiFi MITM SALDIRILARI - Jammer Saldırısı** **WiFi GÜVENLİĞİ - MFP (Management Frame Protection) Önlemi** **WiFi GÜVENLİĞİ - Diğer Önlemler** **WiFi GÜVENLİĞİ - Kayıtlı WiFi Şifresinin Elde Edilmesi** **WiFi GÜVENLİĞİ - Kayıtlı WLAN Profillerinin Silinmesi** **Yukarıdaki yer alan maddelerin başımaza gelmemesi için alınması gereken tedbirler** **Linux Eğitimleri** **GNU Linux'u Kavramı** **Kavramları Pekiştirme** **Linux Dizin Yapısı (Directory Structure)** **Masaüstü Ortamlarına Genel Bakış** **Dizin Yapısına Genel Bakış**			

Linux Açılış Süreci ve Çalışma Seviyeleri **Terminal ve Kısayolları** **Terminal Özelleştirme** **Komutlar ve Shell, Yardım Alma Komutları, Bilgi Alma Komutları, İçerik Komutları, Dosya ve Dizin Komutları, Alıştırma - Pekiştirme, Arşiv Komutları, Komut Operatörleri, Bash Shell Dosyaları, History Kullanımı** **Paket Yönetim Sistemleri (Package Managers)** **Repo Yönetimi** **SSH ile Uzaktan Konsol ve Dosya Yönetimi** **Linux Performans İyileştirme (Performance Tweaks)** **Linux Güvenlik Güçlendirme (Security Hardening)** **Unutulan Parolayı Resetleme (Şifre Kırma)** **Yetkiler ve Kurulum Yönetimi** **Dosya ve Dizin Erişim Yetkileri** **Sayısal İfadelerle Erişim Yetkileri** **Lokal Kullanıcı Komutları ve Yönetimi** **Paket Komutları, Kurulumları ve Yönetimi** **Sistem Güncelleme** **Sistemsel ve Networksel Yönetimler, Komutlar, Kurulumlar** **Süreç Yönetimi ve Komutları** **Servis Yönetimi ve Run Level'ları Anlama** **Disk Yönetimi ve Dosya Sistemleri** **Network Yönetimi ve Kalıcı Statik Route Ekleme** **Görev Yönetimi ve Zamanlanmış Görevler Oluşturma** **Bash Script'leri ve Script Yazma**			

Madde 4b. Talep edilen danışmanlık hizmetinin detaylı içeriği

ALT KONULAR (Her bir konu başlığının içeriğine ilişkin özet bilginin verilmesi istenmektedir.)	**SÜRE (GÜN)**	**GÜNLÜK SAAT**	**TOPLAM SAAT**
Konu 1:			
Konu 2:			
Konu 3:			

Madde 5. Teklif Verme Tarihi ve Yeri

5.1. Son teklif verme tarihi _*(boş bırakınız)*_ saat 17.00'dır.

5.2. Teklifler Ajans'a elden, posta, faks veya eposta yoluyla ulaştırılabilir. Bu tarihten sonra isteklilerden gelecek teklifler değerlendirmeye alınmayacaktır.

Madde 6. Teklife Dair Hususlar

6.1. Fiyat KDV hariç olarak verilecektir.

6.2. Fiyat teklifleri eğitim/danışmanlık ücreti, yol, konaklama dâhil olacak şekilde verilmelidir. Yükleniciye, verecekleri fiyat teklifi dışında ilave bir ödeme yapılmayacaktır.

6.3. Teknik desteği verecek olan eğitmen/danışmanın bu şartnamede aranan özellikleri taşıdığını gösteren belgeler (Özgeçmiş, diploma, sertifika vb.) teklife eklenmelidir.

6.4. Yüklenici, teknik destek süresince kullanacağı materyalleri hazırlamak ve öncesinde Yararlanıcıya iletmekle sorumludur. Ajans'ın bu konuda hiçbir yükümlülüğü yoktur.

6.5. Yararlanıcının katılım sertifikası talep etmesi durumunda sertifikanın sağlanması Yüklenici sorumluluğundadır.

6.6. Teknik desteğin süresince gereken çalışma materyalleri ile eğitim, çalıştay gibi çalışmaların organizasyonuna ait harcamalar/gereklilikler Yararlanıcı tarafından sağlanacaktır.

6.7. Teknik desteğin verimli geçmesi ve aksaklık yaşanmaması için Yüklenici ile Yararlanıcı irtibatta olmak ve faaliyet planını en uygulanabilir şekilde hazırlamakla yükümlüdür.

Madde 7. Nihai Rapor ve Ödeme

7.1. Teknik destek faaliyetinin, sözleşme bitiş tarihini müteakip yararlanıcı, en geç otuz gün içerisinde nihai raporunu ajansa sunar. Nihai raporun onaylanmasını müteakip Yüklenici de sunması gereken evrakları Ajansa sunduğu takdirde 30 (otuz) gün içinde Yüklenicinin bildireceği banka hesabına hizmet bedeli transfer edilmek suretiyle ödenecektir. Nihai rapor sunulup onaylanmadan ödemeler yapılmayacaktır.

7.2. Yüklenici, sözleşme kapsamındaki hizmetlerin tamamlanmasından sonra, ödeme almak için aşağıda yer alan evrakları Ajansa sunması gerekmektedir:

a) Yüklenici tüzel kişiyse Fatura, gerçek kişiyse harcama pusulası,
b) Banka hesap bilgileri,
c) Sözleşme damga vergisi ödeme dekontu (sözleşme imzalandıktan sonra 15 (on beş) gün içerisinde ödenmelidir),
d) Katılımcı listeleri,
e) Eğitim/danışmanlık hizmetinde kullanılan sunumlar/dokümanları içeren flaş bellek