POLITECNICO MILANO 1863

Prova orale – traccia 1

1. Descrivere il protocollo 802.1x
2. Descrivere il "Common Vulnerabilities and Exposures" (CVE)
3. In Microsoft Excel, descrivere la "formattazione condizionale"
4. Tradurre il seguente testo:

   What we refer to as "DNSSEC" is the third iteration of the DNSSEC specification; [RFC2065] was the first, and [RFC2535] was the second. Earlier iterations have not been deployed on a significant scale. Throughout this document, "DNSSEC" means the protocol initially defined in [RFC4033], [RFC4034], and [RFC4035].The three initial core documents generally cover different topics:

   • [RFC4033] is an overview of DNSSEC, including how it might change the resolution of DNS queries. [RFC4034] specifies the DNS resource records used in DNSSEC. It obsoletes many RFCs about earlier versions of DNSSEC. [RFC4035] covers the modifications to the DNS protocol incurred by DNSSEC. These include signing zones, serving signed zones, resolving in light of DNSSEC, and authenticating DNSSEC-signed data.At the time this set of core documents was published, someone could create a DNSSEC implementation of signing software, of a DNSSEC-aware authoritative server, and/or of a DNSSEC-aware recursive resolver from the three core documents, plus a few older RFCs specifying the cryptography used. Those two older documents are the following:

   • [RFC2536] defines how to use the DSA signature algorithm (although it refers to other documents for the details). DSA was thinly implemented and can safely be ignored by DNSSEC implementations. [RFC3110] defines how to use the RSA signature algorithm (although refers to other documents for the details). RSA is still among the most popular signing algorithms for DNSSEC.It is important to note that later RFCs update the core documents. As just one example, [RFC9077] changes how TTL values are calculated in DNSSEC processing.

POLITECNICO MILANO 1863

Prova orale – traccia 2

1. Descrivere il protocollo DHCP, soffermandosi sugli aspetti di sicurezza
2. Descrivere il concetto di "zero day" nell'ambito delle vulnerabilità
3. In Microsoft Excel, descrivere l'uso di "tabella pivot"
4. Tradurre il seguente testo:

Differences between IKEv1 and IKEv2

As with IPsec-v3, IKEv2 incorporates "lessons learned" from implementation and operational experience with IKEv1. Knowledge was gained about the barriers to IKE deployment, the scenarios in which IKE is most effective, and the requirements that needed to be added to IKE to facilitate its use with other protocols as well as in general-purpose use. The documentation for IKEv2 replaces multiple, at times contradictory, documents with a single document; it also clarifies and expands details that were underspecified or ambiguous in IKEv1.

Once an IKE negotiation is successfully completed, the peers have established two pairs of one-way (inbound and outbound) SAs. Since IKE always negotiates pairs of SAs, the term "SA" is generally used to refer to a pair of SAs (e.g., an "IKE SA" or an "IPsec SA" is in reality a pair of one-way SAs). The first SA, the IKE SA, is used to protect IKE traffic. The second SA provides IPsec protection to data traffic between the peers and/or other devices for which the peers are authorized to negotiate. It is called the IPsec SA in IKEv1 and, in the IKEv2 RFCs, it is referred to variously as a CHILD_SA, a child SA, and an IPsec SA. This document uses the term "IPsec SA". To further complicate the terminology, since IKEv1 consists of two sequential negotiations, called phases, the IKE SA is also referred to as a Phase 1 SA and the IPsec SA is referred to as a Phase 2 SA.

Changes to IKE include:

- Replaced multiple alternate exchange types with a single, shorter exchange
- Streamlined negotiation format to avoid combinatorial bloat for multiple proposals
- Protect responder from committing significant resources to the exchange until the initiator's existence and identity are confirmed
- Reliable exchanges: every request expects a response
- Protection of IKE messages based on ESP, rather than a method unique to IKE
- Add traffic selectors: distinct from peer IDs and more flexible
- Support of EAP-based authentication methods and asymmetric authentication (i.e., initiator and responder can use different authentication methods)

DOMANDE POLITECNICO DI MILANO - AVVISO DI SELEZIONE PUBBLICA PER N. 1 NETWORK ENGINEER - PROVA SCRITTA - BUSTA 1

1) [massimo 7 punti] Si descriva il funzionamento del protocollo DNS, soffemandosi sui messaggi scambiati tra client e server. Si descrivano gli aspetti di sicurezza.

2) [massimo 7 punti] Si descrivano i più comuni protocolli per l'implementazione di Virtual Private Network (VPN), confrontandoli tra loro.

3) [massimo 16 punti] Nel contesto di un Ateneo di grandi dimensioni, esteso su molteplici sedi connesse tra loro, si consideri l'esigenza di implementare un sistema Security Information and Event Management (SIEM) per l'infrastruttura in uso, in particolare per raccogliere e correlare i log dei client e dei server gestiti centralmente, del sistema di Network access Control (NAC), del traffico gestito dai firewall, dai proxy e dei log di sistema degli apparati in ambito.
1) Descrivere in dettaglio una proposta di architettura del sistema, tenendo presente l'esigenza di garantire:
I.la configurazione/gestione centralizzata dell'infrastruttura
II.la possibilità di estensione del sistema realizzato e la facilità di manutenzione
III.l'alta affidabilità del sistema
2) Descrivere come il sistema possa supportare la rilevazione e la gestione degli incident di sicurezza, fornendone un esempio.
3) Descrivere gli aspetti di integrità del dato.

DOMANDE POLITECNICO DI MILANO - AVVISO DI SELEZIONE PUBBLICA PER N. 1 NETWORK ENGINEER - PROVA SCRITTA - BUSTA 2

---

1) [massimo 7 punti] Si descriva il funzionamento di un Proxy server per la navigazione web, confrontando le possibili architetture e gli aspetti di alta affidabilità.

---

2) [massimo 7 punti] Si descriva un possibile approccio alla valutazione e prioritizzazione delle segnalazioni di vulnerabilità di sicurezza.

---

3) [massimo 16 punti] Nel contesto di un Ateneo di grandi dimensioni, esteso su molteplici sedi connesse tra loro, si consideri l'esigenza di monitorare efficacemente l'infrastruttura di rete in tutti i suoi componenti e servizi.
1) Descrivere in dettaglio una proposta di architettura del sistema di monitoraggio, tenendo presente l'esigenza di garantire:
I.la configurazione/gestione centralizzata di tale infrastruttura
II.la possibilità di estensione del sistema realizzato e la facilità di manutenzione
III. l'alta affidabilità del sistema
2) Descrivere quali protocolli e metriche si ritiene opportuno utilizzare per il monitoraggio.
3) Descrivere gli aspetti di hardening da tenere in considerazione per la sicurezza del sistema di monitoraggio

DOMANDE POLITECNICO DI MILANO - AVVISO DI SELEZIONE PUBBLICA PER N. 1 NETWORK ENGINEER - PROVA SCRITTA - BUSTA 3

1) [massimo 7 punti] Monitoraggio di performance e log di rete: si descrivano i più comuni protocolli e le metriche che si ritengono essere più significative.

2) [massimo 7 punti] Si descrivano lo scopo ed una possibile architettura per un Security Information and Event Management (SIEM), analizzando in particolare gli aspetti di integrità e immutabilità del dato.

3) [massimo 16 punti] Nel contesto di un Ateneo di grandi dimensioni, esteso su molteplici sedi connesse tra loro, si consideri l'esigenza di erogare a molteplici categorie di utenti censiti nell'anagrafica del sistema informativo (docenti, personale tecnico ed amministrativo, studenti) servizi di DNS, DHCP e AAA (autenticazione, autorizzazione e accounting) alle reti client, compresi i dispositivi di eventuali ospiti temporanei. In particolare:
1) Descrivere in dettaglio una proposta di architettura del sistema, tenendo presente l'esigenza di garantire:
I.la configurazione/gestione centralizzata dell'infrastruttura
II.la possibilità di estensione del sistema realizzato e la facilità di manutenzione
2) Dettagliare la modalità di autenticazione degli utenti per l'accesso alla rete.
3) Descrivere i principali aspetti di sicurezza del protocollo DNS.