Examen

Tabla de contenido

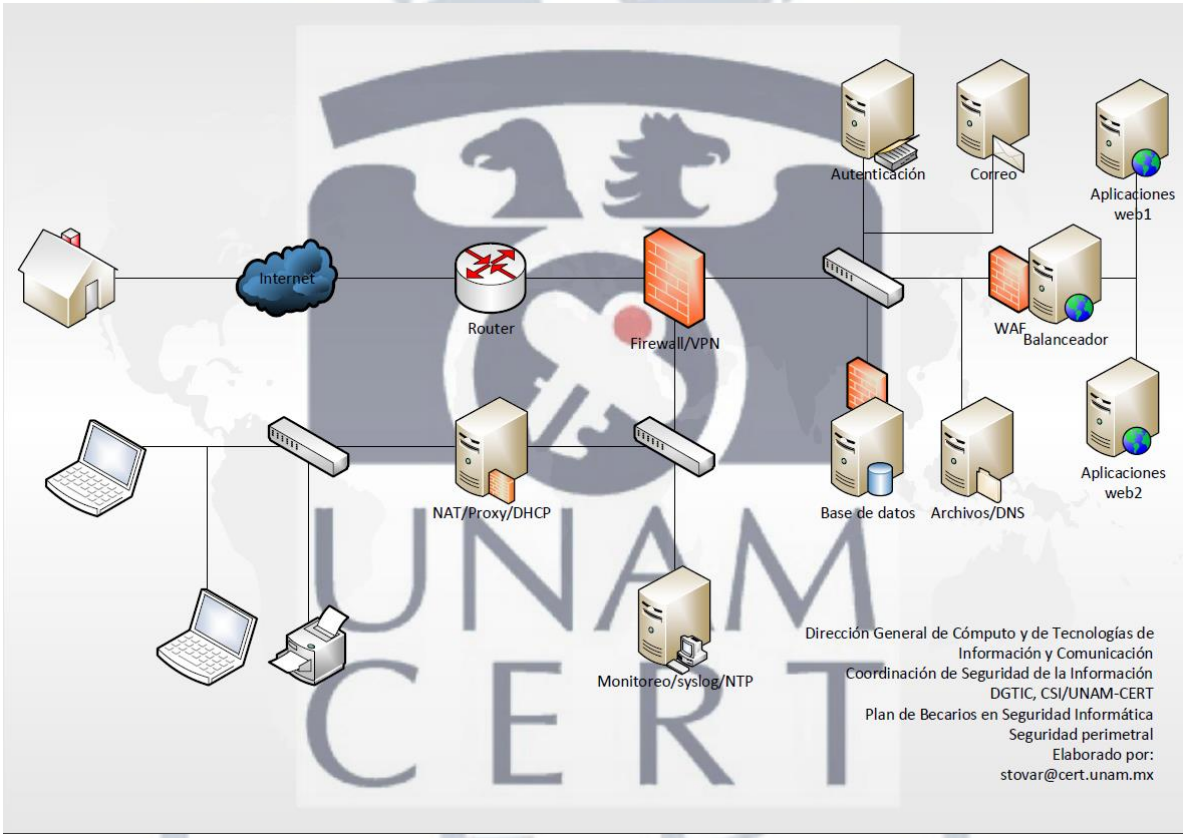
Documentos

Entregar un documento PDF que contenga un informe ejecutivo de la implementación.

Entregar un documento PDF que contenga el proceso de instalación y configuración de la infraestructura.

Práctico

Infraestructura



Servidores

Los servidores deberán tener:

- El direccionamiento de la Red interna y Red protegida es abierto, se sugiere:
  - Red pública: 192.168.X.0/24
  - Red interna: 10.10.X.0/24
  - Red protegida: 172.16.X.0/24
  - Sustituir X por el segmento
    1. Equipo: SP RLI: X -> 10 – AIDE - Wordpress
    2. Equipo: FAM: X -> 20 – Tripwire - Joomla
    3. Equipo: Krakcy: X -> 30 – Tiger – Magento/Owncloud
    4. Equipo: Los Angls (AWS): X -> 40 – OSSEC – Moodle (moosh)
    5. Equipo: La mafia del poder: X -> 50 – Samhain– MediaWiki
    6. Equipo: Sycorax: X -> 60 – Sagan – NextCloud
    7. Equipo: SIX-G9: X -> 70 – OSSEC – Drupal (drush)
- Política de firewall **restrictiva** permitiendo el acceso a:
  - Administración dependiendo de la red origen
  - Servicios dependiendo de cada servidor
  - Monitoreo (servicios)
- Instalar fail2ban, logwatch, logcheck y HIDS
  - Configurar cada servicio y enviar notificaciones a monitoreo@equipo.dominio
  - El servicio de HIDS enviará los correos de notificación a su servidor de correo y a la cuenta asignada por equipo (monitoreo@equipo.dominio).
  - Enviar correo electrónico a la cuenta de monitoreo.
- Hardening
  - Deshabilitar los servicios, cuentas de usuario, etc.
  - Sin ambiente gráfico
  - Instalación base (mínima)
- Instalar vim, curl, nmap, hping3 y tcpdump
  - Verificar que se cuenta con los comandos: nslookup, dig y mail.

Detalle

- Servidor de Autenticación (LDAP y LDAPS)
  - El servidor web (dominio:8443/int) buscará los usuarios en la base de datos de LDAP para su autenticación.
  - El servidor de autenticación tiene interfaz web de administración en el servidor de aplicaciones empleando HTTPS (restringida para la red interna)
  - Se permite la administración desde la Red interna (NAT)
  - Este servidor enviará las bitácoras del servicio de SSH, LDAP y LDAPS al servidor de syslog (Monitoreo).
  - Este servidor sincronizará la hora con el servidor NTP (Monitoreo)

- Servidor de Correo (SMTP, IMAP, POP3, SMTPS, IMAPS y POP3S)
    - Los protocolos de correo son públicos (SMTP, SMTPS, IMAPS y POP3S)
    - Los protocolos HTTPS, IMAP y POP3 estarán permitidos para la red interna
    - Interfaz web para revisar el correo electrónico en el servidor de aplicaciones (restringida para la red interna)
    - Se permite la administración desde la Red interna (NAT)
    - Este servidor enviará las bitácoras del servicio de SSH, HTTP, HTTPS, SMTP, SMTPS, IMAP, IMAPS, POP3 y POP3S al servidor de syslog (Monitoreo).
    - Este servidor sincronizará la hora con el servidor NTP (Monitoreo)

- Base de datos (MySQL y PostgreSQL) de las aplicaciones (Moodle, Joomla, Drupal, etc.)
    - Se permite la administración desde la Red interna y conexión de base de datos del servidor de aplicaciones
    - El manejador de base de datos que no será utilizado para la aplicación (Moodle, Joomla, Drupal, etc.) solamente permitirá la conexión desde un usuario de manera remota usando los comando mysql (mysql -h IP -p 3306 -u usuarioRemoto) o psql (psql -h IP -U usuarioRemoto -p 5432) desde la red interna o un cliente de VPN
    - Este servidor enviará las bitácoras del servicio de SSH, MySQL y PostgreSQL al servidor de syslog (Monitoreo).
    - Este servidor sincronizará la hora con el servidor NTP (Monitoreo)
- Balanceador
    - Será el encargado de balancear el tráfico y/o filtrar hacia los servidores de aplicaciones (2 servidores)
    - Se podrá utilizar Nginx o haproxy para realizar el balanceo de carga
    - Este servidor enviará las bitácoras del servicio de SSH, HTTP y HTTPS al servidor de syslog (Monitoreo).
    - Este servidor sincronizará la hora con el servidor NTP (Monitoreo)
- Aplicaciones (HTTP/HTTPS) – 2 servidores
    - El protocolo del servidor es público (HTTP/HTTPS)
    - WAF en modo embebido para proteger las aplicaciones
    - Se permite la administración desde la Red interna
    - El servidor web (Apache HTTPD) (dominio:8443/int) buscará los usuarios en la base de datos de LDAP para su autenticación.
    - Este servidor enviará las bitácoras del servicio de SSH, HTTP y HTTPS al servidor de syslog (Monitoreo).
    - Este servidor sincronizará la hora con el servidor NTP (Monitoreo)
- Archivos
    - Servidor FTP público (/pub)
        - Anónimo
    - Servidor FTP interno (/int)
        - Autenticación (básica o centralizada)
        - Solo se podrá ver desde la red interna

  - Se permite la administración desde la Red interna
  - Este servidor enviará las bitácoras del servicio de SSH, FTP y STFP al servidor de syslog (Monitoreo).
  - Este servidor sincronizará la hora con el servidor NTP (Monitoreo)
- DNS
  - Permitir recursión
  - Crear registros por cada equipo y/o servicio
  - Este servidor enviará las bitácoras del servicio de SSH y DNS al servidor de syslog (Monitoreo).
  - Este servidor sincronizará la hora con el servidor NTP (Monitoreo)
- Firewall (pfSense) - VPN
  - Transparente
  - Política restrictiva
  - Permitir la conexión a los servicios desde la Red interna hacia la Red protegida (DMZ)
  - Permitir la conexión a los servicios desde la Red externa (Internet) hacia la Red protegida (DMZ)
    - Aplicaciones del servidor de archivos (/pub)
    - Aplicaciones (HTTPS)
    - Correo (SMTP, SMTPS, IMAPS y POP3S)
  - Se permite la administración desde la Red interna
  - Implementar la VPN para la administración de los equipos y permitir el acceso de la red interna
  - Este servidor enviará las bitácoras de las reglas del firewall al servidor de syslog (Monitoreo).
  - Este servidor sincronizará la hora con el servidor NTP (Monitoreo)
- Firewall - VPN (OpenVPN)
  - Configurar OpenVPN en el firewall pfSense
  - Permitirá la conexión de los usuarios desde una Red externa a la Red interna a través del NAT.
  - Crear las reglas necesarias para su uso
  - Permitirá consultar los servicios de la Red protegida
  - Se permite la administración desde la Red interna y cliente Linux (SSH) y Windows (RDP)
- Router
  - Se permite la administración desde la Red interna
- Monitoreo (Nagios) – Syslog - NTP
  - Instalar y configurar el servicio de syslog para recibir las bitácoras de los servicios de los servidores de correo, aplicaciones, NAT, base de datos, etc. Las bitácoras deberán estar organizadas por equipo/servicio. Por ejemplo, servidorweb1/ssh, servidorweb1/http, servidorweb1/https, servidorweb2/ssh, servidorweb2/http y

servidorweb2/https. Todas las bitácoras estarán dentro del directorio /opt/bitácoras
    - servidorAuth/ssh
      servidorAuth/ldap
      servidorAuth/ldaps
    - servidorweb1/ssh
      servidorweb1/http
      servidorweb1/https
      servidorweb1/waf
    - servidorweb2/ssh
      servidorweb2/http
      servidorweb2/https
      servidorweb2/waf
    - Etcétera
  - Realizar la configuración de syslog en todos los servidores
  - Instalar y configurar el servicio de NTP que se sincronizará con el NTP del CENAM. Todos los servidores sincronizaran la hora con este servidor.
  - Monitoreo de:
    - Equipos
      - ping
    - Servicios
      - HTTP[S], SSH, [S]FTP, SMTP[S], IMAP[S], POP3[S], LDAP[S], Proxy, VPN, MySQL, PostgreSQL, syslog, NTP, etc.
  - [Gráficas]
  - [Mapa]
  - Envío de notificaciones por correo electrónico a la cuenta monitoreo en el servidor de correo y a la cuenta asignada por equipo
  - Se permite la administración desde la Red interna
- NAT (netfilter)
  - Traducción de direcciones IP
  - Restricción de los clientes de la Red interna a los servicios de la Red protegida
    - Todos los clientes Linux y Windows tienen acceso a correo, aplicaciones y FTP (/int)
    - Algunos clientes Linux y Windows tienen acceso a la administración de todos los equipos de la Red protegida
  - Se permite la administración desde la Red interna
  - Red interna
    - Cliente Linux
    - Cliente Windows
  - Este servidor enviará las bitácoras de las reglas del firewall al servidor de syslog (Monitoreo).
  - Este servidor sincronizará la hora con el servidor NTP (Monitoreo)
- Proxy (Squid, SquidGuard, e2guardian) – servicio en NAT

- Autenticación para navegar en Internet (básica o centralizada (LDAP/LDAPS))
- Inspección de SSL
- Listas negras
- Filtrado de contenido
- Se permite la administración desde la Red interna

- DHCP – servicio en NAT
  - Asignar direcciones IP a través de la MAC
  - Especificar un rango
  - Especificar la dirección IP del DNS de la red protegida