Hacking IPv6 Networks v4.0

Curso práctico de tres días

Este curso proporciona conocimientos avanzados sobre seguridad IPv6, de modo que el asistente sea capaz de evaluar y mitigar las implicancias de seguridad de IPv6 en entornos de producción. Se proporcionará al asistente explicaciones detalladas de cada tópico abarcado por este curso, de modo que pueda aprender – mediante ejercicios prácticos – como puede explotarse cada característica de IPv6 con fines maliciosos. Seguidamente, se discutirán distintas posibles alternativas para mitigar cada una de las vulnerabilidades en cuestión.
Este curso utiliza una gran cantidad de herramientas de software libre para evaluar la seguridad de redes IPv6, así como también para reproducir una cantidad de ataques basados en IPv6. Durante el curso, el asistente realizará una gran cantidad de ejercicios en un laboratorio de red (con la asistencia del docente), de modo tal que los conceptos y las técnicas aprendidos durante el curso sean afianzadas con ejercicios prácticos. El asistente deberá reproducir una gran cantidad de ataques IPv6, y luego diseñar estrategias de mitifación para las vulnerabilidades asociadas.

Audiencia y pre-requisitos

Ingenieros de Red, Administradores de Red, Administradores de Seguridad, Penetration Testers, y Profesionales de Seguridad en general.

Los asistentees deberán poseer:

- Buenos conocimientos sobre TCP/IP (IPv4, ICMP, ARP, etc.)
- Buenos conocimientos sobre elementos de red (routers, firewalls, etc.)
- Conocimientos basicos sobre la interfaz de comandos de UNIX/Linux
- Conocimientos de herramientas de deburación de redes IPv4, tales como: ping, traceroute, y analizadores de protocolos (como por ejemplo tcpdump).

Es deseable (pero *no* requerido) que los asistentes poseean conocimientos sobre IPv6.

Duración, del curso y formato

Tres dias, con hasta un 50% del curso destinado a ejercicios prácticos.

Materiales del curso

- Manual del curso (escrito por el docente) que incluye todas las diapositivas y los ejercicios presentados durante el curso.
- Una copia del laboratoio virtual utilizado durante el curso.
- Un certificado de asistencia al curso.

Consultas y reservas

Para consultas y reservas sobre capacitación y consultoia, puede contactarnos a través de estos medios:

- Email: info@si6networks.com
- Teléfono: +54 (911) 6536 4380

Precios, fechas, y otros detalles

Para consultar precios, fechas, y otras información sobre este curso, por favor visite el sitio web correspondiente, *https://www.si6networks.com/education/ipv6*.

Acerca del docente

Fernando Gont es mundialmente reconocido como experto en IPv6, brindando consultoría sobre IPv6 aledeor del mundo:

- Ha escrito mas de 20 *IETF RFCs*, muchos de ellos sobre IPv6.
- Se encuentra activamente involucrado en la estandarización de IPv6 standardization, contando con mas de *IETF Internet-Drafts* activos.
- Es autor del *SI6 Network's IPv6 toolkit*, el único paquete de herramientas portable y de software libre enfocado en IPv6.
- Ha brindado servicios de consultoría y capacitación alrededor del mundo por más de diez años.
- Puede encontrar mas información sobre Fernando Gont en su sitio web: *http://www.gont.com.ar*.

Hacking IPv6 Networks v4.0: Agenda detallada del curso

1. **Introduction to IPv6**
   - IPv4 address exhaustion
   - IPv6 service
   - IPv6 transition/deployment mechanisms
   - IPv6: current state of affairs
   - Brief comparison between IPv6 and IPv4
   - IPv6 security overview
2. **IPv6 Addressing Architecture**
   - IPv6 address types
   - IPv6 address analysis
   - Implications for address scanning attacks & possible mitigations
   - Privacy implications & possible mitigations
   - Implications for end-to-end connectivity
3. **IPv6 Header Fields**
   - IPv6 header overview
   - Basic header fields
   - Security assessment
4. **IPv6 Extension Headers (EHs)**
   - General implications of EHs
   - Security implications of specific IPv6 EHs
   - Security implications of specific IPv6 options
   - IPv6 EHs in the real world
   - Exploitation of IPv6 EHs
   - Troubleshooting IPv6 EHs
   - Network reconnaissance with IPv6 EHs
   - Recent advances
5. **IPsec**
   - Virtual Private Network (VPN) traffic leakages
6. **Internet Control Message Protocol version 6 (ICMPv6)**
   - ICMPv6 error messages
   - ICMPv6 informational messages
   - Network reconnaissance with ICMPv6
7. **Neighbor Discovery for IPv6**
   - Address resolution in IPv6
   - Address resolution messages and options
   - Neighbor Discovery cache
   - Neighbor Discovery attacks
   - Neighbor Discovery security controls
   - Evasion of Neighbor Discovery security controls
   - System configuration options
8. **Stateless Address Auto-configuration (SLAAC)**
   - SLAAC operation
   - SLAAC messages and options
   - Duplicate Address Detection (DAD)
   - Troubleshoting SLAAC
   - SLAAC attacks
   - DAD attacks
   - SLAAC security controls
   - Evasion of SLAAC security controls
   - System configuration options
9. **Dynamic Host Configuration Protocol version 6 (DHCPv6)**
   - Sample DHCPv6 traffic
   - Security implications of DHCPv6
   - DHCPv6 attacks
   - DHCPv6 security controls
10. **Multicast Listener Discovery (MLD)**
    - Sample MLD traffic
    - Security implications of MLD
    - MLD attacks
    - MLD security controls
11. **Upper-Layer Attacks**
    - TCP-based attacks
    - UDP-based attacks
    - Possible mitigations
12. **DNS Support for IPv6**
    - Network reconnaissance
    - Exploiting DNS reverse mappings
13. **IPv6 Firewalls**
    - Known limitations
    - Evasion of IPv6 firewalls
14. **Security Implications of IPv6 for IPv4-only Networks**
    - IPv6 attacks on IPv4-only networks
    - Mitigating IPv6 attacks on IPv4-only networks
15. **Transition/Co-existence Technologies**
    - Automatic tunneling mechanisms
    - Attacks on automatic tunneling mechanisms
    - Mitigations
16. **Network Reconnaissance in IPv6**
    - Host scanning in IPv6
    - Port scanning in IPv6
17. **IPv6 Deployment Considerations**
    - Designing an IPv6 address plan
    - Operating System hardening
    - Other considerations