Carrier Digit

کـــاریـــارارقـــام

مشاوره، تحقیقات، طرح و اجرای شبکه های ارتباطی

و برگزارکننده دوره های آموزشی

RHCSS

Red hat Certified Security Specialist

مدت(ساعت): ۶۰ | پیش نیاز: RHCE | اعتبار دهنده: LINUX

معرفی دوره :

دوره RHCSS برای بالابردن امنیت در سرویس های لینوکس میباشد. همچنین بحث Cryptography نیز در مورد SSL و GPG مورد بحث قرار میگیرد. نحوه دسترسی امن به سرویس ها نیز جزء سر فصلهای این دوره میباشد. دانشجو پس از سپری کردن آن میتواند سرویس های خود را تحت شبکه امن نماید و از دسترسیهای غیر مجاز تا حد زیادی جلوگیری نماید.

این دوره ترکیبی از دوره ذیل میباشد:

RH333 Red Hat Enterprise Security: Network Service

و RH429 Red Hat Enterprise SELinux Policy Administration

RH423 به صورت دوره ای جداگانه آموزش داده می شود،

پس از گذراندن سه دوره فوق می توانید مدرک RHCSS را دریافت نمایید.

امتیازات دوره :

- اعطای مدرک فارسی و انگلیسی با مجوز رسمی از :
  - سازمان مدیریت و برنامه ریزی کشور (معاونت توسعه مدیریت و سرمایه انسانی رئیس جمهوری سابق)
  - مجوز از اداره کل نظام مدیریت امنیت اطلاعات (نما)
  - شورای عالی انفورماتیک
  - قابلیت ترجمه وتایید قوه قضاییه وامور خارجه
- بهره گیری از لابراتوارسخت افزاری ونرم افزاری مجهز
- بهره گیری از اساتید مجرب و تأیید شده با سابقه حضور در پروژه‌های ملی

اهداف دوره :

- آشنایی و آگاهی کامل از مباحث امنیتی سیستم عامل .
- توانایی تشخیص و اعمال موارد امنیتی مورد نیاز در سرویس های قابل ارائه توسط سیستم عامل ردهت لینوکس .

مخاطبان دوره :

- مدیران، کارشناسان، دانشجویان فعال در حوزه فناوری اطلاعات

محتوای دوره :

3. Cryptography
- Overview of cryptographic techniques
- Management of SSL certificates
- Using GnuPG

4. Logging and NTP
- Time synchronization with NTP
- Logging: syslog and its weaknesses
- Protecting log servers

Course Outline :

RHS333 Red Hat Enterprise Security: Network Services

1. The Threat Model and Protection Methods
- Internet threat model and the attacker's plan
- System security and service availability
- An overview of protection mechanisms

2. Basic Service Security
- SELinux
- Host-based access control
- Firewalls using Netfilter and iptables
- TCP wrappers
- xinetd and service limits

« مالکیت مادی و معنوی این مستند منحصراً متعلق به کاریار ارقام است »

لطفا در باز نشر این مستند نام پدیدآورنده لحاظ گردد.

تهران : خیابان ملاصدرا، بعد از خیابان شیخ بهائی ، ساختمان فردوس ، پلاک ۲۴۲ تلفن مستقیم آموزش: ۸۸۰۶۲۲۰۳، ۸ فاکس: ۸۸۰۶۵۲۲۲

Accredited by CARRIER DIGIT Computer Software LLC

EC-Council

Course Outline :	محتوای دوره :

5. BIND and DNS Security
- BIND vulnerabilities
- DNS Security: attacks on DNS
- Access control lists
- Transaction signatures
- Restricting zone transfers and recursive queries
- DNS Topologies
- Bogus servers and blackholes
- Views
- Monitoring and logging
- Dynamic DNS security

6. Network Authentication: RPC, NIS, and Kerberos
- Vulnerabilities
- Network-managed users and account management
- RPC and NIS security issues
- Improving NIS security
- Using Kerberos authentication
- Debugging Kerberized Services
- Kerberos Cross-Realm Trust
- Kerberos EncryptionOpenSSH

7. Network File System
- Overview of NFS versions 2, 3, and 4
- Security in NFS versions 2 and 3
- Improvements in security in NFS4
- Troubleshooting NFS4
- Client-side mount options

8. OpenSSH
- Vulnerabilities
- Server configuration and the SSH protocols
- Authentication and access control
- Client-side security
- Protecting private keys
- Port-forwarding and X11-forwarding issues

9. Electronic Mail with Sendmail
- Vulnerabilities
- Server topologies
- Email encryption
- Access control and STARTTLS
- Anti-spam mechanisms

10. Postfix
- Vulnerabilities
- Security and Postfix design
- Configuring SASL/TLS

11. FTP
- Vulnerabilities
- The FTP protocol and FTP servers
- Logging
- Anonymous FTP
- Access control

12. Apache security
- Vulnerabilities
- Access control
- Authentication: files, passwords, Kerberos
- Security implications of common configuration options
- CGI security
- Server side includes
- suEXEC

13. Intrusion Detection and Recovery
- Intrusion risks
- Security policy
- Detecting possible intrusions
- Monitoring network traffic and open ports
- Detecting modified files
- Investigating and verifying detected intrusions
- Recovering from, reporting, and documenting intrusions

RH-429 SELinux Policy Management & Policy Writing
SELinux Policy Writing
- Specify an enforcement mode
- Specify a particular policy
- Update a system to use the latest SELinux packages
- Create and implement a custom policy module to support a given service, including:

- Port bindings
- File and directory access
- Type transitions
- Default file types
- Booleans
- Type Aliases

Targeted Policy System Maintenance
- Specify an enforcement mode
- Specify a particular policy
- Modify an existing policy including:

- Port bindings
- File and directory access
- Type transitions
- Default file types
- Booleans

Accredited by CARRIER DIGIT Computer Software LLC

« مالکیت مادی و معنوی این مستند منحصراً متعلق به کاریار ارقام است »
لطفا در باز نشر این مستند نام پدیدآورنده لحاظ گردد.

EC-Council

تهران : خیابان ملاصدرا، بعد از خیابان شیخ بهائی ، ساختمان فردوس ، پلاک ۲۴۲ تلفن مستقیم آموزش: ۸۸۰۶۲۲۰۳، ۸ فاکس: ۸۸۰۶۵۲۲۲

Course Outline :	محتوای دوره :
5. BIND and DNS Security • BIND vulnerabilities • DNS Security: attacks on DNS • Access control lists • Transaction signatures • Restricting zone transfers and recursive queries • DNS Topologies • Bogus servers and blackholes • Views • Monitoring and logging • Dynamic DNS security **6. Network Authentication: RPC, NIS, and Kerberos** • Vulnerabilities • Network-managed users and account management • RPC and NIS security issues • Improving NIS security • Using Kerberos authentication • Debugging Kerberized Services • Kerberos Cross-Realm Trust • Kerberos EncryptionOpenSSH **7. Network File System** • Overview of NFS versions 2, 3, and 4 • Security in NFS versions 2 and 3 • Improvements in security in NFS4 • Troubleshooting NFS4 • Client-side mount options **8. OpenSSH** • Vulnerabilities • Server configuration and the SSH protocols • Authentication and access control • Client-side security • Protecting private keys • Port-forwarding and X11-forwarding issues	**9. Electronic Mail with Sendmail** • Vulnerabilities • Server topologies • Email encryption • Access control and STARTTLS • Anti-spam mechanisms **10. Postfix** • Vulnerabilities • Security and Postfix design • Configuring SASL/TLS **11. FTP** • Vulnerabilities • The FTP protocol and FTP servers • Logging • Anonymous FTP • Access control **12. Apache security** • Vulnerabilities • Access control • Authentication: files, passwords, Kerberos • Security implications of common configuration options • CGI security • Server side includes • suEXEC **13. Intrusion Detection and Recovery** • Intrusion risks • Security policy • Detecting possible intrusions • Monitoring network traffic and open ports • Detecting modified files • Investigating and verifying detected intrusions • Recovering from, reporting, and documenting intrusions