CREST Assessors Panel

CREST Registered Penetration Tester

Syllabus Version 2.0

Issued by	CREST Assessors Panel
Document Reference	SYL_CRT_v2.0
Version Number	2.0
Status	Public Release
Issue Date	2023-07-07

Table of Contents

Version History

Version	Date	Authors & Notes	Status
2.0	July 7, 2023	CREST Assessors Panel	Public Release

1 Introduction

The technical syllabus identifies at a high level the technical skills and knowledge that CREST expects candidates to possess for the CREST Registered Penetration Tester (CRT) examination.

CREST Registered Penetration Tester (CRT)

The CREST Registered Penetration Tester (CRT) examination tests candidates' knowledge in assessing operating systems and common network services for the intermediate level below that of the main Certified level qualifications. The CRT examination also includes an intermediate level of web application security testing and methods to identify common web application security vulnerabilities.

The examination covers a common set of core skills and knowledge; the candidate must demonstrate that they can perform an infrastructure and web application vulnerability scan using commonly available tools; and interpret the results. Success combined with valid CPSA certification will confer CREST Registered Penetration Tester (CRT) status to the individual.

2 Certification Examination Structure

CREST Registered Penetration Tester (CRT)

The Certified Examination has one component: a practical assault course assessment. The practical assessment tests candidates' hands-on penetration testing methodology and skills against reference networks, hosts and applications.

The Notes for Candidates (CRT) document for the Certification Examinations provides further information regarding the Certification Examinations in general and the skill areas that will be assessed within the practical assault course.

3 Syllabus Structure

The syllabus is divided into topics, each of which is subdivided into specific skill areas.

For each skill area, CREST has indicated where and how the area will be assessed: for the CREST Registered Penetration Tester (CRT), all skills will be assessed by a practical assault course.

Appendix A - Core Technical Skills (PT002)

ID	Skill ID	Skill	Details	Assault Course
A1	PT002.01	Using Tools and Interpreting Outputs	Can use a variety of tools during a penetration test, selecting the most appropriate tool to meet a particular requirement. Can interpret and understand the output of tools, including those used for port scanning, vulnerability scanning, enumeration, exploitation and traffic capture.	Yes
A2	PT002.05	OS Fingerprinting	Understands active and passive operating system fingerprinting techniques and can demonstrate their use during a penetration test.	Yes

Appendix B - Internet Information Gathering and Reconnaissance (PT003)

ID	Skill ID	Skill	Details	Assault Course
B1	PT003.02	DNS	Understands the Domain Name Service (DNS) including queries and responses, zone transfers, and the structure and purpose of records, including: • SOA • NS • MX • A • AAAA • CNAME • PTR • TXT (including use in DMARC policies) • HINFO • SVR Can demonstrate how a DNS server can be queried to obtain the information detailed in these records. Can demonstrate how a DNS server can be queried to reveal other information that might reveal target systems or indicate the presence of security vulnerabilities. Can identify the presence of dangling DNS entries and understands the associated security vulnerabilities (e.g. susceptibility to subdomain takeover). Passive DNS monitoring.	Yes

Appendix C - Networks (PT004)

ID	Skill ID	Skill	Details	Assault Course
C1	PT004.01	Network Connections	Can use common network connections that could be required during a penetration test: • Ethernet (copper and fibre) • Wifi (IEEE 802.11.a,b,g,n,ac,ax) • Ethernet VLANs	Yes
C2	PT004.04	VLAN Tagging	Understands VLAN tagging (IEEE 802.1Q). Understands the security implications of VLAN tagging. Can connect a specific VLAN given the VLAN ID from both Linux and Windows systems. Can identify and analyse VLAN tagged traffic on a network.	Yes
C3	PT004.05	IPv4	Basic understanding of how the IPv4 protocol works. Ability to configure interfaces with IP addresses both statically and using DHCP. Can perform host discovery using ARP and ICMP. Ability to understand and configure IP routing. Ability to perform standard penetration testing activities including network mapping, port scanning, and service exploitation. Awareness of common protocols that use IPv4 e.g. ICMP, IGMP, TCP, UDP. Awareness of IPsec.	Yes

ID	Skill ID	Skill	Details	Assault Course
C4	PT004.10	Network Mapping	Can demonstrate the mapping of a network using a range of tools, such as traceroute, traceroute and ping, and by querying active searches, such as DNS and SNMP servers. Can present the map as a logical network diagram, detailing all discovered subnets and interfaces, including routers, switches, hosts and other devices. Can accurately identify all hosts on a target network that meet a defined set of criteria, e.g. to identify all FTP servers or Cisco routers.	Yes
C5	PT004.12	Network Devices	Analysing the configuration of the following types of network equipment: • Routers • Switches • Firewalls	Yes
C6	PT004.13	Network Filtering	Understands network traffic filtering and where this may occur in a network. Understands the devices and technology that implement traffic filtering, such as firewalls, and can advise on their configuration. Can demonstrate methods by which traffic filters can be bypassed.	Yes
C7	PT004.14	Traffic Analysis	Can intercept and monitor network traffic, capturing it to disk in a format required by analysis tools (e.g. PCAP). Understands and can demonstrate how network traffic can be analysed to recover user account credentials and detect vulnerabilities that may lead to the compromise of a target device. Can analyse network traffic stored in PCAP files.	Yes

ID	Skill ID	Skill	Details	Assault Course
C8	PT004.16	TCP	Understands how TCP works and its relationship with IP protocols and higher level protocols. Understands different TCP connection states. Understands and can demonstrate active techniques for discovery of TCP services on a network, such as: • SYN and Connect scanning • FIN/NULL and XMAS scanning	Yes
C9	PT004.17	UDP	Understands how UDP works and its relationship with IP protocols and higher level protocols. Understands different UDP connection states. Understands and can demonstrate active techniques for discovery of UDP services on a network.	Yes
C10	PT004.22	Service Identification	Can identify the network services offered by a host by banner inspection. Can state the purpose of an identified network service and determine its type and version. Understands the methods associated with unknown service identification, enumeration and validation. Evaluation of unknown services and protocols.	Yes
C11	PT004.23	Host Discovery	Can identify targets on common networks using active and passive fingerprinting techniques and can demonstrate their use.	Yes

Appendix D - Network Services (PT005)

ID	Skill ID	Skill	Details	Assault Course
D1	PT005.02	Unencrypted Services	Understands how unencrypted services can be exploited. Can identify unencrypted services on the network and capture sensitive data. Is aware of common unencrypted services including: • Telnet • FTP • SNMP • HTTP	Yes
D2	PT005.03	TLS / SSL	Understands the use of TLS and SSL in protecting data in transit. Is aware of SSL and TLS protocols and their common weaknesses. Understands the components of cipher suites and their roles. Understands the role of certificates in SSL and TLS. Can identify insecure configurations.	Yes

ID	Skill ID	Skill	Details	Assault Course
D3	PT005.06	Name Resolution Services	Understands and can demonstrate the use of the following name resolution services: • DNS • NetBIOS / WINS • WINS • LLMNR • mDNS Understands the security attributes of the above protocols and technologies. Can demonstrate how these services can be exploited to gain access to a device or derive further information about the target network. Understands the Domain Name Service (DNS) including queries and responses, zone transfers, and the structure and purpose of records, including: • SOA • NS • MX • A • AAAA • CNAME • PTR • TXT (including use in DMARC policies) • HINFO • SVR	Yes

ID	Skill ID	Skill	Details	Assault Course
D4	PT005.08	Management Services	Understands and can demonstrate the use of the following network management services: • Telnet • Cisco Reverse Telnet • SSH • HTTP • Remote Powershell • WMI • WinRM • RDP • VNC • X Understands the security attributes of the above protocols and technologies. Can demonstrate how these services can be exploited to gain access to a device or derive further information about the target network.	Yes
D5	PT005.09	Desktop Access	Is aware of common protocols used to provide remote access to desktop services including: • RDP • VNC • XDMCP • X Understands the security attributes of the above protocols and technologies. Can demonstrate how these services can be exploited to gain access to a device or derive further information about the target network.	Yes
D6	PT005.10	IPsec	Enumeration and fingerprinting of devices running IPsec services.	Yes
D7	PT005.11	FTP	Understands FTP and can demonstrate how a poorly configured FTP server can be exploited, e.g. the downloading of arbitrary files, the uploading and over-writing of files, and the modification of file system permissions. Understands the security implications of anonymous FTP access Understands FTP access control.	Yes

ID	Skill ID	Skill	Details	Assault Course
D8	PT005.12	TFTP	Understands TFTP and can demonstrate how a poorly configured TFTP server can be exploited, e.g. the downloading of arbitrary files. the uploading over-writing of files. Understands and can exploit TFTP within a Cisco environment.	Yes
D9	PT005.13	SNMP	Understands the difference between versions 1, 2c, and 3. Can enumerate information from targets including: • users • processes • network configuration Understands the MIB structure pertaining to the identification of security vulnerabilities. Understands the security attributes of SNMP. Can demonstrate how these services can be exploited to gain access to a device or derive further information about the target network. Understands how to extract and replace configuration files of Cisco devices.	Yes
D10	PT005.14	SSH	Understands SSH and its associated security attributes, including the different versions of the protocol, version fingerprinting and how the service can be used to provide a number of remote access services. Can demonstrate how trust relationships can lead to the compromise of a server, allow a user to escalate privileges and/or gain further access to a host, e.g. through the use, creation or modification of -- /.ssh/authorized_keys files. Understands authentication mechanisms used by SSH.	Yes

ID	Skill ID	Skill	Details	Assault Course
D11	PT005.15	NFS	Understands NFS and its associated security attributes and can demonstrate how exports can be identified. Can demonstrate how a poorly configured NFS service can lead to the compromise of a server, allow a user to escalate privileges and/or gain further access to a host, e.g. through the creation of SUID-root files, the modification of files and file system permissions, and UID/GID manipulation. Understands the concepts of root squashing, nosuid and noexec options Understands how NFS exports can be restricted at both a host and file level	Yes
D12	PT005.16	SMB	Is aware of common SMB implementations including: • Windows File Shares • Samba Can identify and analyse accessible SMB shares.	Yes
D13	PT005.17	LDAP	Is aware of common LDAP implementations including: • Windows Active Directory • OpenLDAP Can enumerate LDAP directories and extract arbitrary data including: • usernames and groups • target system names	Yes
D14	PT005.18	Berkeley R* Services	Understands the Berkeley r-services and their associated security attributes and can demonstrate how trust relationships can: • lead to the compromise of a server allow • a user to escalate privileges and/or gain further access to a host, e.g. through the use, creation or modification of .rhosts and/or /etc/hosts.equiv files. Can perform user enumeration using the rwho and rusers services.	Yes

ID	Skill ID	Skill	Details	Assault Course
D15	PT005.19	X	Understands X and its associated security attributes, and can demonstrate how insecure sessions can be exploited, e.g.. by obtaining screen shots, capturing keystrokes and injecting commands into open terminals. Understands X authentication mechanisms. Understands the difference between host based and user based access control.	Yes
D16	PT005.20	Finger	Understands how finger daemon derives the information that it returns, and hence how it can be abused. Enumeration of usernames.	Yes
D17	PT005.21	RPC Services	Can perform RPC service enumeration. Is aware of common RPC services. Is aware of and can exploit recent or commonly-found RPC service vulnerabilities.	Yes
D18	PT005.22	NTP	Understands the function of NTP and the importance of it for logging and authentication. Can extract information about the target network from NTP services.	Yes
D19	PT005.25	SMTP and Mail Servers	Understands and can demonstrate valid username discovery via EXPN and VRFY. Awareness of recent vulnerabilities in mail server applications (e.g. Postfix and Exchange) and the ability to exploit them if possible Understands mail relaying.	Yes

Appendix E - Microsoft Windows Security Assessment (PT006)

ID	Skill ID	Skill	Details	Assault Course
E1	PT007.01	Windows Reconnaissance	Can identify Windows hosts on a target network. Can identify forests, domains, domain controllers, domain members and workgroups. Can enumerate accessible Windows shares. Can identify and analyse internal browse lists.	Yes
E2	PT007.02	Windows Network Enumeration	Can perform user and group enumeration on target systems and domains, using various protocols and methods including: • NetBIOS • LDAP • SNMP • RID Cycling Can obtain other information, such as password policies.	Yes
E3	PT007.04	Active Directory Enumeration	Can enumerate information from Active Directory including: • Users • Groups • Computers • Trusts • Service Principle Names	Yes

ID	Skill ID	Skill	Details	Assault Course
E4	PT006.05	Windows Passwords	Understands password policies, including complexity requirements and lock-out. Understands how to avoid causing a denial of service by locking-out accounts. Understands Windows password hashing algorithms, the merits of each algorithm, and their associated security attributes. Understands how passwords are stored and protected and can demonstrate how they can be recovered. Understands and can demonstrate off-line password cracking using dictionary and brute- force attacks, including the use of rainbow tables.	Yes
E5	PT007.06	Windows Processes	Can identify running processes and exploit vulnerabilities to escalate privileges. Understands and can exploit DLL loading mechanisms to escalate privileges.	Yes
E6	PT006.07	Windows File Permissions	Understands and can demonstrate the manipulation of file system permissions on Windows operating systems. Understands how insecure file system permissions can be exploited to escalate privileges and/or gain further access to a host. Can identify files with insecure or "unusual" permissions that can be exploited.	Yes
E7	PT006.08	Registry	Understands and can demonstrate the detection and manipulation of weak registry ACLs. Can extract data from registry keys.	Yes
E8	PT006.09	Windows Remote Exploitation	Understands and can demonstrate the remote exploitation of Windows operating system and third-party software application vulnerabilities.	Yes

ID	Skill ID	Skill	Details	Assault Course
E9	PT006.11	Windows Local Exploitation	Understands and can demonstrate the local exploitation of Windows operating system and third-party software application vulnerabilities. Understands and can demonstrate local privilege escalation techniques, e.g. through the manipulation of insecure file system or service permissions	Yes
E10	PT006.13	Windows Post Exploitation	Understands and can perform common post exploitation activities, including: • obtaining password hashes, both from the local SAM and cached credentials or obtaining locally stored clear-text passwords cracking • password hashes obtaining patch • levels • deriving a list of missing security patches • reverting to a previous state • lateral and horizontal movement	Yes
E11	PT006.14	Windows Patch Management	Understands common windows patch management strategies, including: • SMS • SUS • WSUS	Yes
E12	PT006.15	Windows Desktop Lockdown	Understands and can demonstrate techniques to break out of a locked down Windows desktop or Citrix environment. Can perform privilege escalation techniques from a desktop environment.	Yes
E13	PT006.17	Common Windows Applications	Knowledge of significant vulnerabilities in common windows applications for which there is public exploit code available.	Yes

Appendix F - Linux / UNIX Security Assessment (PT007)

ID	Skill ID	Skill	Details	Assault Course
F1	PT007.01	Linux / UNIX Reconnaissance	Can identify Linux / UNIX hosts on a network.	Yes
F2	PT007.02	Linux / UNIX Network Enumeration	Can demonstrate and explain the enumeration of data from a variety of common network services on various platforms including: • Filesystems or resources shared remotely, such as NFS and SMB • SMTP • SSH • Telnet • SNMP Is aware of legacy user enumeration techniques such as rusers, rwho and finger. Can enumerate RPC services and identify those with known security vulnerabilities.	Yes

ID	Skill ID	Skill	Details	Assault Course
F3	PT007.03	Linux / UNIX Passwords	Understands users, groups and password policies, including complexity requirements and lock out. Understands how to avoid causing a denial of service by locking out accounts. Understands the format of the passwd, shadow, group and gshadow files. Understands UNIX password hashing algorithms and their associated security attributes. Understands how passwords are stored and protected and can demonstrate how they can be recovered. Understands and can demonstrate off-line password cracking using dictionary and brute force attacks. Can demonstrate the recovery of password hashes when given physical access to a Linux / UNIX host.	Yes
F4	PT007.04	Linux / UNIX File Permissions	Understands and can demonstrate the manipulation of file system permission on Linux and UNIX operating systems. Understands how insecure file system permissions can be exploited to escalate privileges and/or gain further access to a host. Can find "interesting' files on an operating system, e.g. those with insecure or "unusual" permissions, or containing user account passwords.	Yes
F5	PT007.05	Linux / UNIX Processes	Can identify running processes on Linux / UNIX hosts and exploit vulnerabilities to escalate privileges. Understands and can exploit shared library loading mechanisms to escalate privileges.	Yes

ID	Skill ID	Skill	Details	Assault Course
F6	PT007.06	Linux / UNIX Remote Exploitation	Understands and can demonstrate the remote exploitation of Linux and UNIX systems including: • Solaris • Linux • FreeBSD • OpenBSD	Yes
F7	PT007.07	Linux / UNIX Local Exploitation	Understands and can demonstrate the local exploitation of Solaris, Linux and *BSD operating system vulnerabilities. Understands and can demonstrate Local privilege escalation techniques, e.g. through the manipulation of insecure file system permissions.	Yes
F8	PT007.08	Linux / UNIX Post Exploitation	Understands and can demonstrate common post-exploitation activities, including: • obtaining locally stored clear-text passwords • password recovery (exfiltration and cracking) • lateral movement • checking OS and third party software application patch levels • deriving a list of missing security patches • reversion of OS and software components to previous state	Yes

Appendix G - Web Technologies (PT008)

ID	Skill ID	Skill	Details	Assault Course
G1	PT008.01	Web Servers	Can identify web servers on a target network and can remotely determine their type and version. Understands the various mechanisms web servers use for hosting applications, including: • virtual hosts • multiple ports • application specific URLs Understands and can demonstrate the remote exploitation of web servers. Understands the concepts of web proxies. Understands the purpose, operation, limitation and security attributes of web proxy servers.	Yes
G2	PT008.02	Web Application Frameworks	Can identify common application frameworks and technologies, including: • .NET • J2EE • Coldfusion • Ruby on Rails • NodeJS • Django • Flask Is aware of and can exploit vulnerabilities in common application frameworks and technologies.	Yes
G3	PT008.03	Common Web Applications	Can identify common web applications and exploit well-known vulnerabilities.	Yes

ID	Skill ID	Skill	Details	Assault Course
G4	PT008.04	Web Protocols	Understands and can demonstrate the use of web protocols, including: • HTTP • HTTPS – WebSockets Understands all HTTP methods and response codes. Understands HTTP header fields relating to security features.	Yes
G5	PT008.05	Mark Up Languages	Understands common web mark up languages, including: • HTML • XHTML • XML	Yes
G6	PT008.09	Web Application Reconnaissance	Can use spidering tools and understands their relevance in a web application test for discovering linked content. Understands and can demonstrate forced browsing techniques to discover default or unlinked content. Can identify functionality within client-side code.	Yes
G7	PT008.11	Information Gathering	Can gather information from a web site and application mark up or application code, including: • hidden form fields • database connection strings • user account credentials • developer comments • external and/or authenticated-only URLs. Can gather information about a web site and application from the error messages it generates.	Yes

ID	Skill ID	Skill	Details	Assault Course
G8	PT008.12	Web Authentication	Understands common authentication mechanisms and their security issues, including: • HTML Form Fields • kerberos • NTLM • OpenID Connect • SAML Understands common authentication vulnerabilities, including: • Transport of credentials over an unencrypted channel • Username enumeration • Brute force password attacks • Authentication bypass • Insecure password reset features • Insufficient logout/ timeout functionality • Vulnerable CAPTCHA controls Race • Conditions • Lack of MFA	Yes
G9	PT008.13	Web Authorisation	Understands common pitfalls associated with the design and implementation of application authorisation mechanisms.	Yes
G10	PT008.14	Input Validation	The importance of input validation as part of a defensive coding strategy. How input validation can be implemented and the differences between allow list, deny list and data sanitisation. Understands the need for server side validation and the flaws associated with client-side validation.	Yes
G11	PT008.16	Cross Site Scripting	Understands cross site scripting (XSS) and can demonstrate the launching of a successful XSS attack. Understands the difference between persistent, reflected and DOM based XSS. Can use XSS to perform arbitrary JavaScript execution to obtain sensitive information from other users.	Yes

ID	Skill ID	Skill	Details	Assault Course
G12	PT008.17	SQL Injection	Determine the existence of an SQL injection condition in a web application. Determine the existence of a blind SQL injection condition in a web application. Can exploit SQL injection to execute arbitrary SQL commands in a database.	Yes
G13	PT008.22	Mail Injection	Can demonstrate the ability to identify, explain and prove the existence of the following types of mail related injection in a web application: • SMTP injection • IMAP injection	Yes
G14	PT008.24	OS Command Injection	Can demonstrate the ability to identify, explain and prove the existence of OS command injection in a web application.	Yes
G15	PT008.25	Sessions	Can identify the session control mechanism used within a web application. Can identify the session ID in a web application. Understands the security implications of session IDs exposed in URLs. Can harvest and analyse a number of session identifiers for weaknesses.	Yes
G16	PT008.26	Cookies	Understands how cookies work in a web application. Understands cookie attributes and how they can affect the security of a web application.	Yes
G17	PT008.28	Session Hijacking	Understands and can exploit session hijacking vulnerabilities.	Yes
G18	PT008.29	Cross Site Request Forgery	Understands and can exploit CSRF vulnerabilities. Understands the role of sessions in CSRF attacks.	Yes

ID	Skill ID	Skill	Details	Assault Course
G19	PT008.31	Web Cryptography	Understands how cryptography can be used to protect data in transit and data at rest, both on the server and client side. Understands the concepts of TLS and can determine whether a TLS-enabled web server has been configured in compliance with best practice (i.e. it supports recommended ciphers and key lengths). Identification and exploitation of Encoded values (e.g. Base64). Identification and exploitation of Cryptographic values (e.g. MD5 hashes).	Yes
G20	PT008.35	Parameter Manipulation	Understands parameter manipulation techniques, particularly the use of client- side proxies.	Yes
G21	PT008.36	Directory Traversal	Understands and can identify directory traversal vulnerabilities within applications.	Yes
G22	PT008.37	File Uploads	Understands and can identify common vulnerabilities with file upload capabilities within applications. Understands the role of MIME types in relation to file upload features. Can generate malicious payloads in a variety of common file formats.	Yes
G23	PT008.39	Web Application Logic Flaws	Can assess and exploit vulnerabilities within the functional logic, function access control and business logic of an application.	Yes

Appendix H - Databases (PT009)

ID	Skill ID	Skill	Details	Assault Course
H1	PT009.01	SQL Relational Databases	Can use SQL to interact with relational databases and extract information, e.g. SQLite, PostgreSQL. Understands common connection and authentication methods to connect to SQL databases. Can recognise common database connection string formats, e.g. JDBC, ODBC. Understands and can demonstrate the remote exploitation of common SQL databases. Understands and can demonstrate how access can be gained to a database through the use of default accounts credentials and insecure passwords. Can identify and extract useful information stored within a database (e.g. user account names and passwords, recovering passwords where possible).	Yes
H2	PT009.02	Microsoft SQL Server	Understands and can demonstrate the remote exploitation of Microsoft SQL Server. Understands and can demonstrate how access can be gained to a Microsoft SQL server through the use of default accounts credentials and insecure passwords. Can identify and extract useful information stored within a database (e.g. user account names and passwords, recovering passwords where possible). Following the compromise of Microsoft SQL server, can execute system commands, escalate privileges, read/write from/to the file system, and/or gain further access to a host.	Yes

ID	Skill ID	Skill	Details	Assault Course
H3	PT009.03	Oracle RDBMS	Understands and can demonstrate the remote exploitation of an Oracle RDBMS instance. Understands the security attributes of the Oracle TNS Listener service. Understands and can demonstrate how access can be gained to an Oracle RDBMS through the use of default accounts credentials and insecure passwords. Can identify and extract useful information stored within a database (e.g. user account names and passwords, recovering passwords where possible). Can demonstrate how the software version and patch status can be obtained from an Oracle database. Following the compromise of an Oracle database, can execute system commands, escalate privileges, read/write from/to the file system, and/or gain further access to a host.	Yes
H4	PT009.04	MySQL	Understands and can demonstrate the remote exploitation of an MySQL database. Understands and can demonstrate how access can be gained to an MySQL database through the use of default accounts credentials and insecure passwords. Can identify and extract useful information stored within a database (e.g. user account names and passwords, recovering passwords where possible). Can demonstrate how the software version and patch status can obtained from an MySQL database. Following the compromise of an MySQL database, can execute system commands, escalate privileges, read/write from/to the file system, and/or gain further access to a host.	Yes

ID	Skill ID	Skill	Details	Assault Course
H5	PT009.05	PostgreSQL	Understands and can demonstrate the remote exploitation of a PostgreSQL database. Understands and can demonstrate how access can be gained to a PostgreSQL database through the use of default accounts credentials and insecure passwords. Can identify and extract useful information stored within a database (e.g. user account names and passwords, recovering passwords where possible). Can demonstrate how the software version and patch status can be obtained from an PostgreSQL database. Following the compromise of a PostgreSQL database server can execute system commands, escalate privileges, read/write from/to the file system and/or gain further access to a host.	Yes