Skill Set and Certifications

ari.edelkind@episec.com
New York, NY
917 968 6991

Ari Edelkind
July, 2004

Computer Skills

General experience ratings:

Some: *I have used this skill enough to feel comfortable doing so, and I am eager to learn more. I also have a significant theoretical understanding of the subject.*

Moderate: *I have an advanced theoretical understanding of this subject, and a significant technical unserstanding. I use this skill in practice, though I try to keep a book or other documentation handy while doing so.*

High: *I have an advanced understanding of this subject, both theoretical and technical. If the subject is an operating system, I have ported applications to it and spent time examining kernel internals. If desired, I can be expected to pass certification tests on this topic without studying.*

Note: *When sensible, all entries are given in alphabetical order.*

Operating Systems

AIX 5.2 ..... **Moderate**
BSDI (BSD/OS) 2.1 – 3.1 ..... **High**
DEC Digital Unix (OSF1) 3.0 ..... **Moderate**
DGUX 4.20 ..... **Moderate**
FreeBSD 2.1 – 5.2 ..... **High**
HP-UX 10.20, 11.23 ..... **Moderate**
IRIX 6.3 – 6.5.4 ..... **High**
Linux (multiple distributions), kernels 1.3 – 2.6 ..... **High**
NetBSD 1.4.3 – 1.5.2 ..... **High**
OpenBSD 2.1 – 2.9 ..... **High**
OpenStep 4.2 ..... **Some**
QNX 4.24, 6.1 ..... **Some**
Solaris (SunOS, SPARC) 2.3 – 8 ..... **High**

Other (possibly) relevant operating systems

Cisco IOS and Supervisor Software ..... **Moderate**
MacOS 7.5.1 – 9, X (10.3) ..... **High**
Windows 3.1, 95, 98, 2000, NT 4 ..... **High**

Programming

Assembly ..... **Moderate**
- i386, plus small amounts of SPARC and MIPS
- Used on DGUX, FreeBSD, Linux, NetBSD, OpenBSD
- Nasm and AT&T formats

C (ANSI and traditional) ..... **High**
- network sockets
- kernel programming
- pty/tty manipulation
- SVR4/BSD compatibility
- low-level data structure manipulation
- dynamic libraries, library call wrapping

HTML ..... **High**
JavaScript ..... **Moderate**
Perl 5 ..... **High**
PHP ..... **High**
Shell scripting ..... **High**
- sh, csh, ksh

SQL ..... **Moderate**
TCL ..... **Moderate**

Security

Auditing ..... **High**
- Code auditing (C, Perl, PHP, Shell scripts)
- Network and host auditing

chroot() ..... **High**
- functionality
- implementation
- breaking

Cryptography ..... **Moderate**
- Cryptographic theory ..... **High**
- Cryptographic libraries ..... **Moderate**
  (ssl, rsa, des, 3des, blowfish, md5, rijndael)
- Incorporation into programs ..... **Moderate**
- Cryptographic software (gnupg, pgp, kerberos, openssl)

Exploit creation (from scratch) ..... **Moderate**
- Debugging, process tracing, and library call wrapping to find exploitable problems in closed-source software
- Network sniffing and monitoring
- Use of Assembly, C, and Perl to write exploits for pedagogical demonstrations

Firewalls ..... **High**
- Firewall theory
- Firewall design
- Transparent firewalls (masquerading, NAT)

Host security ..... **High**
- Securing network services
- Setuid program evaluation and revocation
- Temporary (world-writable) directory issues
- Host-based filtering (ipf, netfilter, pf)
- DSO wrapping to enhance application security measures

Intrusion detection ..... **Moderate**
- IDS theory ..... **High**
- IDS circumvention theory ..... **Moderate**

Penetration testing ..... **Moderate**
Quotas (disk, memory, cpu) ..... **High**

General service setup/administration

Including, not limited to . . .

Backup services (amanda, burt, dump . . .) ..... **High**
FTP servers (ncftpd, proftpd, vsftpd, wu-ftpd . . .) ..... **High**
IMAP servers (courier, uw-imap) ..... **Moderate**
Inet services (inetd, xinetd, tcpserver) ..... **High**
Mail servers (sendmail, qmail) ..... **High**
Nameservers (bind, djbdns) ..... **High**
Network file systems (nfs, samba, netatalk) ..... **High**
Phone database servers ..... **Moderate**
POP3 servers (qpopper, popa3d, qmail-pop3d) ..... **High**
Printing services (lprng) ..... **High**
- BSD and SVR4 line printing services ..... **Moderate**

Shell services (ssh, openssh, telnet, evil r-commands) ..... **High**
Single sign-on (cryptocard) ..... **Moderate**
SQL servers (mysql, postgresql, sqlite) ..... **High**
User management services ..... **High**
- Centralized management (nis, nis+)
- Distributed management (custom scripts)

Web servers (apache, ncsa, publicfile) ..... **High**
- netscape enterprise ..... **Some**

Web server modules (php, mod_perl, mod_ssl) ..... **High**

Web-based services ..... **High**

- e-mail (imp, ilohamail)
- inventory system (custom)
- password management (custom)
- project tracking (keystone)

Certifications

It is this individual's opinion that certifications do not accurately portray one's knowledge; therefore, certifications are made available upon request.