متداولترین پورت های آسیب پذیر

امروزه شاهد حضور مقتدرانه سیستم های عامل در تمامی عرصه های پردازش اطلاعات می باشیم .سیستم عامل، یکی از عناصر چهار گانه در یک سیستم کامپیوتری است که دارای نقشی حیاتی و تعیین کننده در رابطه با نحوه مدیریت منابع سخت افزاری و نرم افزاری است . پرداختن به مقوله امنیت سیستم های عامل ، همواره از بحث های مهم در رابطه با ایمن سازی اطلاعات در یک سیستم کامپیوتری بوده که امروزه با گسترش اینترنت ، اهمیت آن مضاعف شده است . بررسی و آنالیز امنیت در سیستم های عامل می بایست با ظرافت و در چارچوبی کاملا" علمی و با در نظر گرفتن تمامی واقعیت های موجود ، انجام تا از یک طرف تصمیم گیرندگان مسائل استراتژیک در یک سازمان قادر به انتخاب منطقی یک سیستم عامل باشند و از طرف دیگر امکان نگهداری و پشتیبانی آن با در نظر گرفتن مجموعه تهدیدات موجود و آتی ، بسرعت و بسادگی میسر گردد .

اکثر کرم ها و سایر حملات موفقیت آمیز در اینترنت ، بدلیل وجود نقاط آسیب پذیر در تعدادی اندک از سرویس های سیستم های عامل متداول است . مهاجمان ، با فرصت طلبی خاص خود از روش های متعددی بمنظور سوء استفاده از نقاط ضعف امنیتی شناخته شده ، استفاده نموده و در این راستا ابزارهای متنوع ، موثر و گسترده ای را به منظور نیل به اهداف خود ، بخدمت می گیرند . مهاجمان ، در این رهگذر متمرکز بر سازمان ها و موسساتی می گردند که هنوز مسائل موجود امنیتی (حفره ها و نقاط آسیب پذیر) خود را برطرف نکرده و بدون هیچگونه تبعیضی آنان را بعنوان هدف ، انتخاب می نمایند . مهاجمان بسادگی و بصورت مخرب ، کرم هائی نظیر : بلستر ، اسلامر و Code Red را در شبکه منتشر می نمایند. آگاهی از مهمترین نقاط آسیب پذیر در سیستم های عامل ، امری ضروری است . با شناسائی و آنالیز اینگونه نقاط آسیب پذیر توسط کارشناسان امنیت اطلاعات ، سازمان ها و موسسات قادر به استفاده از مستندات علمی تدوین شده بمنظور برخورد منطقی با مشکلات موجود و ایجاد یک لایه حفاظتی مناسب می باشند.

شناسائی متداولترین پورت هائی که تاکنون مهاجمان با استفاده از آنان حملات خود را سازماندهی نموده اند ، امری لازم و ضروری است . برخی از پورت ها بدفعات و بطور متناوب توسط مهاجمان و به منظور انجام یک تهاجم مورد استفاده قرار گرفته است . با بلاک نمودن اینگونه پورت ها ، حداقل امکانات لازم به منظور ایجاد یک محیط ایمن ایجاد خواهد شد . بهترین روشی که در این رابطه توصیه شده است ، بلاک نمودن تمامی پورت ها (غیرفعال نمودن تمامی ترافیک) و صدور مجوز جداگانه برای هر یک از پروتکل های مورد نیاز در یک سازمان و با توجه به شرایط موجود می باشد . حتی در صورتی که تمامی پورت ها بلاک شده باشند ، می بایست بطور مستمر آنان را به منظور تشخیص مزاحمت ها و سوء استفاده های احتمالی مانیتور نموده تا در صورت بروز مشکلات احتمالی سریعا" نسبت به رفع آنان اقدام گردد .

بخاطر داشته باشید که پورت های زیر را می بایست بر روی تمامی کامپیوترهای میزبان با لحاظ نمودن مسائل امنیتی پیکربندی نمود . غیر فعال نمودن پورت های زیر خلاء طراحی یک سیاست امنیتی را پر نخواهد کرد و می بایست در این رابطه تابع یک سیستم و سیاست امنیتی مناسب باشیم .

جدول زیر متداولترین پورت های آسیب پذیر را تاکنون توسط مهاجمان بکار گرفته شده است ، نشان می دهد :

Description	Protocol	Port	Name
small services	tcp/udp	20	Small services
file transfer	tcp	21	FTP
login service	tcp	22	SSH
login service	tcp	23	TELNET
mail	tcp	25	SMTP
time synchronization	tcp/udp	37	TIME
WINS replication	tcp/udp	42	WINS
naming services	udp	53	DNS
naming services	tcp	53	DNS zone transfers
host configuration	tcp/udp	67	DHCP server
host configuration	tcp/udp	68	DHCP client
miscellaneous	udp	69	TFTP
old WWW-like service	tcp	70	GOPHER
miscellaneous	tcp	79	FINGER
web	tcp	80	HTTP
web	tcp	81	alternate HTTP port
web (sometimes Kerberos)	tcp	88	alternate HTTP port
host configuration	tcp	98	LINUXCONF
mail	tcp	109	POP2
mail	tcp	110	POP3
RPC portmapper	tcp/udp	111	PORTMAP/RPCBIND
network news service	tcp	119	NNTP
time synchronization	udp	123	NTP
DCE-RPC endpoint mapper	tcp/udp	135	NetBIOS
NetBIOS name service	udp	137	NetBIOS
NetBIOS datagram service	udp	138	NetBIOS
file sharing & login service	tcp	139	NetBIOS/SAMBA
mail	tcp	143	IMAP

miscellaneous	tcp/udp	161	SNMP
miscellaneous	tcp/udp	162	SNMP
X display manager protocol	udp	177	XDMCP
miscellaneous	tcp	179	BGP
CheckPoint FireWall-1 mgmt	tcp	256	FW1-secureremote
CheckPoint FireWall-1 mgmt	tcp	264	FW1-secureremote
naming services	tcp/udp	389	LDAP
web	tcp	443	HTTPS
SMB over IP (Microsoft-DS)	tcp/udp	445	Windows 2000 NetBIOS
IPSEC Internet Key			
Exchange	udp	500	ISAKMP
} the three	tcp	512	REXEC
} Berkeley r-services	tcp	513	RLOGIN
} (used for remote login)	tcp	514	RSHELL
miscellaneous	udp	513	RWHO
miscellaneous	udp	514	SYSLOG
remote printing	tcp	515	LPD
miscellaneous	udp	517	TALK
routing protocol	udp	520	RIP
file transfer	tcp/udp	540	UUCP
HTTP DCE-RPC endpoint			
mapper	tcp	593	HTTP RPC-EPMAP
remote printing	tcp	631	IPP
LDAP over SSL	tcp	636	LDAP over SSL
remote administration	tcp	898	Sun Mgmt Console
remote administration	tcp	901	SAMBA-SWAT
} often allocated	tcp/udp	1025	Windows RPC programs
} by DCE-RPC portmapper		to	Windows RPC programs
} on Windows hosts	tcp/udp	1039	Windows RPC programs
miscellaneous	tcp	1080	SOCKS
database/groupware	tcp	1352	LotusNotes

database	tcp	1433	MS-SQL-S
database	udp	1434	MS-SQL-M
remote graphical display	tcp	1494	CITRIX
WINS replication	tcp/udp	1512	WINS replication
database	tcp	1521	ORACLE
NFS file sharing	tcp/udp	2049	NFS
Compaq remote administration	tcp	2301	COMPAQDIAG
Compaq remote administration	tcp	2381	COMPAQDIAG
collaborative file sharing	tcp	2401	CVS
web cache	tcp	3128	SQUID
Global catalog LDAP	tcp	3268	Global catalog LDAP
Global catalog LDAP SSL	tcp	3269	Global catalog LDAP SSL
database	tcp	3306	MYSQL
remote graphical display	tcp	3389	Microsoft Term. Svc.
NFS file sharing	tcp/udp	4045	LOCKD
remote administration	tcp	5987	Sun Mgmt Console
remote administration	tcp	5631	PCANYWHERE
remote administration	tcp/udp	5632	PCANYWHERE
remote administration	tcp	5800	VNC
remote administration	tcp	5900	VNC
X Windows server	tcp	6000-6255	X11
X Windows font service	tcp	7100	FONT-SERVICE
web	tcp	8000	alternate HTTP port
web	tcp	8001	alternate HTTP port
web	tcp	8002	alternate HTTP port
web	tcp	8080	alternate HTTP port
web	tcp	8081	alternate HTTP port
web	tcp	8888	alternate HTTP port

} often allocated	tcp/udp	32770	Unix RPC programs
} by RPC portmapper		to	Unix RPC programs
} on Solaris hosts	tcp/udp	32899	Unix RPC programs
Compaq remote administration	tcp	49400	COMPAQDIAG
Compaq remote administration	tcp	49401	COMPAQDIAG
Compaq remote administration	tcp	49401	COMPAQDIAG