بسمه تعالی

با عرض سلام و روز به خیر خدمت تمامی دانشجویان محترم؛

همانطور که مستحضر هستید با توجه به شرایط پیش آمده در کشور و به دلیل ایجاد بحران آلودگی به بیماری کرونا، تصمیم بر آن شد که دانشگاه‌های کل کشور تا رفع این مشکل و تا اطلاع ثانوی، تعطیل باشند. با توجه به این مهم، طی جلسات مهمی که تیم محترم ارزیاب و تصمیم گیرنده دانشگاه فنی و حرفه‌ای و همچنین دانشکده شمسی‌پور برگزار کردند تصمیم گرفته شد تا هر استاد، مفاهیم و مطالب مرتبط به هر درس خود را در قالب مستندات مشخصی در اختیار دانشجویان محترم قرار دهد.

طی این تصمیم و ابلاغ آن به همه اساتید محترم، بنده هم به تبعیت از این دستور، متن مشخصی که قرار بود در کلاس **"آشنایی با مبانی امنیت شبکه و اطلاعات"** به صورت شفاهی در اختیار شما دانشجویان قرار گیرد را در قالب تنظیم **سه جلسه** کلاسی، آماده نمودم و در اختیار شما قرار می‌دهم. امید است دانشجویان محترم با مطالعه صفحات مربوط به هر جلسه، انشاالله خود را برای سال آینده و حضور مستمر و قدرتمند در جلسات کلاس آماده کنند.

در پایان لازم به ذکر است کانال ارتباطی کلاس و همچنین آدرس پست الکترونیکی بنده به شرح زیر می‌باشند. لطفا دانشجویان محترم در این کانال تلگرامی حتما عضو شوند و مطالب ارسال شده در آن را پیگیری کنند:

Telegram: @MySSP
E-Mail: MehdiAhmadi@tvu.ac.ir

با آرزوی ریشه‌کن شدن بحران کرونا در کشور و سلامتی تمامی دانشجویان و خانواده های محترم آنها

با تشکر ویژه از جناب دکتر سپهرزاده گرامی و ارجمند

مهدی احمدی
۹۸/۱۲/۱۱

جلسه اول

Network ۱-۱-۱

به گروهی از دستگاه‌ها و کامپیوترهایی که از طریق کانال‌های ارتباطی به یکدیگر متصل می‌شوند و در ادامه می‌توانند به تبادل اطلاعات با یکدیگر بپردازند Network گفته می‌شود.

در یک دید مشخص شبکه‌های کامپیوتری مجموعه‌ای از کامپیوترها و دستگاه‌های مستقل متصل به هم هستند و در ادامه از طریق یک کانال ارتباطی مشخص می‌توانند اطلاعات را با هم تبادل کنند.

مستقل‌بودن هر کامپیوتر به این معنا است که هر کدام از این ماشین‌ها دربردارنده واحدهای کنترلی و پردازشی مجزا از هم هستند. کانال ارتباطی موجود میان کامپیوترهای قرار گرفته در سطح شبکه نیز همیشه می‌بایست به شیوه‌ای ایمن تعریف شده باشد تا در آینده از هرگونه اقدام تخریب‌گرایانه یک فرد نفوذگر جلوگیری به عمل آید.

گفتنی است معمولا افرادی که از آن‌ها با نام "هکر" یا "نفوذگر" یاد می‌شود همواره علاقه دارند تا به بررسی و جست‌وجو بر روی سطح شبکه موجود بپردازند و در ادامه با کسب اطلاعات مختلف به یک کامپیوتر آسیب‌پذیر به شیوه‌ای غیرمجاز متصل شوند.

در ادامه این افراد می‌توانند به آسانی و به صورت غیرقانونی به اطلاعات حساس و مهم موجود در کامپیوتری که به آن نفوذ شده است و از آن با نام "سیستم قربانی" یاد می‌شود دسترسی داشته باشند.

شبکه‌های کامپیوتری را از چند دید می‌توان تقسیم‌بندی نمود در این بخش، شبکه‌ها را از دو دید مشخص زیر بررسی می‌کنم:

۱- اندازه

۲- نوع اتصال

۱-۱-۱-۱ اندازه

در یک نگاه کلی "اندازه" به عنوان یکی از تقسیم‌بندی‌های مشخص شبکه‌های کامپیوتری محسوب می‌شود و بر اساس آن، شبکه‌های کامپیوتری را به چند دسته زیر طبقه‌بندی می‌نمایند:

1- PAN
2- LAN
3- MAN
4- WAN

PAN ۱-۱-۱-۱-۱

به شبکه کامپیوتری که هنگام برقراری ارتباط میان دستگاه‌های اطراف یک شخص ایجاد می‌شود اصطلاحا یک شبکه PAN[1] یا "شبکه شخصی" می‌گویند.

از دستگاه‌هایی که در اطراف یک شخص می‌باشند به عنوان نمونه می‌توان به Mobile، Laptop و PDA که قابلیت برقراری ارتباط را دارند اشاره نمود.

معمولا از این شبکه‌های کامپیوتری در جهت اتصال وسایل شخصی چند نفر به یکدیگر استفاده می‌شود و در واقع می‌توان با ایجاد یک شبکه PAN، امکان ارتباط دستگاه‌های اطراف یک فرد را پیاده‌سازی کرد.

[1] Personal Area Network

جلسه اول

LAN ۲-۱-۱-۱-۱

به شبکه کامپیوتری ایجاد شده در یک محدوده جغرافیایی کوچک همانند یک خانه، یک شرکت یا مجموعه‌ای از ساختمان‌های نزدیک به هم اصطلاحا یک شبکه LAN[1] یا "شبکه محلی" می‌گویند.
در یک دید مشخص زمانی که یک سازمان یا یک شرکت نیاز به ایجاد یک شبکه مشخص در محدوده خود دارد می‌تواند به آسانی با ایجاد یک شبکه محلی به این مهم دست پیدا کند.
معمولا در شبکه‌هایی که با نام LAN شناخته می‌شوند سرعت دسترسی به کامپیوترهای موجود در سطح شبکه بالا است و هزینه انتقال بسته‌های اطلاعاتی نسبت به دیگر نوع‌های شبکه کمتر می‌باشد.

MAN ۳-۱-۱-۱-۱

به شبکه‌های کامپیوتری ایجاد شده در محدوده یک شهر بزرگ اصطلاحا یک شبکه MAN[2] یا "شبکه کلان شهری" گفته می‌شود. در این نوع از شبکه‌ها از زیرساخت‌های بی‌سیم یا اتصالات فیبر نوری در جهت ایجاد ارتباط میان کامپیوترهای مختلف استفاده می‌شود.
در یک دید مشخص یک شبکه MAN برای ناحیه جغرافیایی بزرگتر از یک LAN در نظر گرفته شده است و معمولا از چند بلوک ساختمانی تا کل یک شهر را می‌تواند پوشش دهد.

WAN ۴-۱-۱-۱-۱

به شبکه‌های کامپیوتری که ناحیه جغرافیایی زیادی را پوشش می‌دهند اصطلاحا یک شبکه WAN[3] یا "شبکه گسترده" می‌گویند. در یک دید مشخص معمولا این نوع از شبکه‌های کامپیوتری در جهت اتصال شبکه‌های LAN و دیگر شبکه‌های موجود استفاده می‌شوند.
با توجه به این مهم کاربران موجود در یک نقطه مشخص می‌توانند توسط پیاده‌سازی شبکه‌های WAN با افراد راه‌دور[4] ارتباط برقرار کنند و در ادامه نیازهای خود را توسط شبکه برآورده سازند.

۲ نوع اتصال ۱-۱-۱-۲

در یک نگاه کلی "نوع اتصال" نیز به عنوان یکی دیگر از تقسیم‌بندی‌های مشخص شبکه‌های کامپیوتری محسوب می‌شود و بر اساس آن، شبکه‌های کامپیوتری را به چند دسته مشخص زیر طبقه‌بندی می‌نمایند:

1- Intranet
2- Extranet
3- Internet

Intranet ۱-۲-۱-۱-۱

به شبکه داخلی ایجاد شده در یک سازمان یا یک شرکت که از پروتکل‌های مرتبط به اینترنت همانند پروتکل‌های HTTP، IP و TCP در جهت ساماندهی و پیاده‌سازی شبکه استفاده شده است یک شبکه Intranet می‌گویند.

---

[1] Local Area Network
[2] Metropolitan Area Network
[3] Wide Area Network
[4] Remote

در یک دید مشخص یک شبکه مبتنی بر Intranet یک شبکه کامپیوتری کوچک است که بر حسب دلایل مشخصی در سطح یک سازمان یا یک شرکت ایجاد می‌شود و در ادامه آماده استفاده از جانب کارمندان آن سازمان یا شرکت می‌شود.
معمولا این نوع شبکه به اینترنت متصل نیست و از آن در جهت اتصال بخش‌ها و شرکت‌های مختلف یک سازمان به یکدیگر استفاده می‌شود.
در یک نگاه کلی هدف از ایجاد شبکه‌های کامپیوتری مبتنی بر Intranet در داخل سازمان‌ها و شرکت‌ها به اشتراک گذاشتن منابع و برقراری ارتباط آسان میان شرکت‌های وابسته به هم یک سازمان می‌باشد.
در واقع یک شبکه Intranet را می‌توان یک شبکه خصوصی که یک سازمان بر آن نظارت دارد دانست و با توجه به این مهم تمامی اطلاعات مورد استفاده آن سازمان در Serverهای شخصی و حفاظت‌شده همان سازمان نگهداری می‌گردند.

Extranet ۲-۲-۱-۱-۱

یک شبکه مبتنی بر Extranet یک شبکه کامپیوتری است که این امکان را به کاربران موجود در شبکه Intranet اهدا می‌کند تا این افراد بتوانند به صورت کنترل‌شده به منابع خارج از شبکه نیز دسترسی داشته باشند.
در واقع این نوع از شبکه‌های کامپیوتری یک شبکه شخصی هستند که با استفاده از پروتکل اینترنت و اتصال‌های شبکه امکان به‌کارگیری منابع درون شبکه‌ای را برای کاربران بیرون از سازمان فراهم می‌نمایند.
به دیگر سخن یک شبکه Extranet یک شبکه Intranet است که به صورت کاملا خصوصی مدیریت می‌شود و این امکان را فراهم‌سازی می‌کند تا در نقاط ایمن به شبکه‌های فراسازمانی نیز دسترسی داشت.
در یک نگاه کلی یک شبکه Extranet یک شبکه Intranet است که در داخل یک شبکه عمومی همانند شبکه گسترده اینترنت قرار دارد و در ادامه دسترسی عموم مردم به آن محدود شده است.
معمولا از این شبکه تعبیه شده در دنیای کامپیوتر در جهت انتقال حجم زیاد داده‌ها، به اشتراک‌گذاری خصوصی منابع یک سازمان برای شرکای تجاری و همکاری میان شرکت‌های مختلف با هم استفاده می‌شود.

Internet ۳-۲-۱-۱-۱

شبکه Internet یک شبکه جهانی ایجاد شده در سراسر دنیا می‌باشد و دربردارنده میلیون‌ها کامپیوتر متصل به هم است و این امکان را فراهم‌سازی می‌نماید تا بتوان توسط آن، حجم زیادی از داده‌ها و اطلاعات را میان کامپیوترهای موجود در سراسر جهان مبادله کرد.
واژه Internet از دو واژه Inter که مخفف Interconnected است و به معنای "به هم پیوسته" می‌باشد و Net که مخفف Networks است و به معنای "شبکه‌ها" می‌باشد تشکیل شده است.
با توجه به این مهم، Interconnected Networks که از آن با نام Internet یاد می‌شود به معنای "شبکه‌های به هم پیوسته" در دسترس کاربران در اقصی نقاط جهان می‌باشد[۱].
معمولا از این شبکه گسترده در جهت ارسال و دریافت داده‌ها و اطلاعات موجود در کامپیوترهای مختلف که ممکن است در سراسر جهان قرار گرفته شده باشند می‌توان استفاده کرد.

[۱] گفتنی است از آن با مفهوم "شبکه شبکه‌ها" نام برده می‌شود

جلسه اول

Client ۱-۱-۲

به نرم‌افزار یا سخت‌افزار موجود در سطح شبکه که منتظر دریافت خدمت از جانب نرم‌افزار یا سخت‌افزارهای راه‌دور[۱] است اصطلاحا Client می‌گویند.

با توجه به تعریف ذکرشده در بالا، مفهوم Client موجود در دنیای کامپیوتر را می‌توان از دو دید نرم‌افزاری و سخت‌افزاری مورد بررسی قرار داد.

در یک دید مشخص ممکن است در سطح شبکه تعریف شده از جانب یک شرکت یا یک سازمان و یا در شبکه گسترده اینترنت، کامپیوترها و برنامه‌هایی که به عنوان Server نقش خدمت‌گذار را بر عهده دارند موجود باشند.

در مقابل آن‌ها نیز برنامه‌هایی تحت نام Client مشغول فعالیت می‌باشند و به واسطه نوع فعالیت تعریف شده برای آن‌ها خدمتی را از Server طلب می‌نمایند.

در واقع برنامه‌هایی که تحت نام Client در دنیای کامپیوتر ایجاد می‌شوند همیشه به دنبال دریافت پاسخی از جانب برنامه‌های Server هستند.

این نوع از برنامه‌ها معمولا دستورهایی را جهت اجرا از طریق شبکه به برنامه‌های Server ارسال می‌کنند و در ادامه از برنامه Server می‌خواهند تا به درستی فرمان دریافت‌شده از جانب برنامه Client را بررسی نماید و پاسخ مناسبی به آن ارایه کند.

Server ۱-۲-۱-۱

به نرم‌افزار یا سخت‌افزار موجود در سطح شبکه که وظیفه ارایه خدمت به برنامه‌های درخواست‌کننده را بر عهده دارد اصطلاحا Server می‌گویند.

با توجه به تعریف ذکرشده در بالا مفهوم Server موجود در دنیای کامپیوتر را نیز می‌توان از دو دید نرم‌افزاری و سخت‌افزاری مورد بررسی قرار داد.

در یک دید مشخص همان‌گونه که اشاره شد برنامه‌هایی به نام Client وجود دارند و معمولا این برنامه‌ها در جهت کسب اطلاعات از یک کامپیوتر راه‌دور و یا انجام یک خدمت از پیش تعریف شده بر روی آن سیستم، فرمانی را به برنامه Server ارسال می‌نمایند.

در ادامه برنامه Server وظیفه دارد تا دستورهای دریافت‌شده از جانب برنامه Client را بررسی کند و پاسخ درستی به کامپیوتر درخواست‌کننده ارایه نماید.

ممکن است در برخی از موارد بیش از یک کامپیوتر Client وجود داشته باشند اما معمولا یک برنامه Server به تمامی درخواست‌های این کامپیوترها ارایه سرویس می‌نماید.

Port ۱-۱-۳

کامپیوترها دارای مجموعه‌ای درگاه به نام Port هستند و از آن‌ها در جهت اتصال دستگاه‌های خارجی و همچنین برنامه‌ها به کامپیوترها استفاده می‌شود.

در یک نگاه کلی Portهای قابل استفاده در سیستم‌های کامپیوتری را به دو دسته پورت‌های نرم‌افزاری و سخت‌افزاری تقسیم‌بندی می‌کنند. از پورت‌های نرم‌افزاری در جهت اتصال برنامه‌های Client به یک برنامه Server

[۱] که به آن Server می‌گویند

موجود در سیستم راه‌دور استفاده می‌نمایند. در مقابل از پورت‌های سخت‌افزاری در جهت اتصال دستگاه‌های سخت‌افزاری همچون حافظه‌های USB، Mouse، Keyboard، Printer و دیگر وسایل می‌توان استفاده کرد. پورت‌های سخت‌افزاری موجود در کامپیوترها را نیز به دو گروه پورت‌های سریال و پورت‌های موازی تقسیم‌بندی می‌نمایند.

معمولا هکرها در جهت نفوذ به سیستم‌های کامپیوتری و سپس صدمه‌زدن به آن‌ها از پورت‌های نرم‌افزاری استفاده می‌کنند و در واقع با ایجاد یک اتصال مشخص از روی کامپیوتر خود به سیستم قربانی به آسانی می‌توانند فعالیت‌های مورد نیاز خود را در آن کامپیوتر پوشش دهند.

در یک نگاه کلی پورت‌های نرم‌افزاری از عدد مشخص ۱ تا ۶۵۵۳۵ در دسترس افراد نفوذگر می‌باشند و در واقع این افراد می‌توانند با اتصال به یکی از این پورت‌های باز شده موجود در سیستم قربانی به آن کامپیوتر دسترسی پیدا کنند.

به عنوان نمونه در شکل مشخص زیر برخی از پورت‌های مهم و کاربردی موجود در سطح شبکه و کامپیوتر نمایش داده شده است[1]:

TCP/UDP Port Numbers

7	Echo	554	RTSP	2745	Bagle.H	6891-6901	Windows Live
19	Chargen	546-547	DHCPv6	2967	Symantec AV	6970	Quicktime
20-21	FTP	560	rmonitor	3050	Interbase DB	7212	GhostSurf
22	SSH/SCP	563	NNTP over SSL	3074	XBOX Live	7648-7649	CU-SeeMe
23	Telnet	587	SMTP	3124	HTTP Proxy	8000	Internet Radio
25	SMTP	591	FileMaker	3127	MyDoom	8080	HTTP Proxy
42	WINS Replication	593	Microsoft DCOM	3128	HTTP Proxy	8086-8087	Kaspersky AV
43	WHOIS	631	Internet Printing	3222	GLBP	8118	Privoxy
49	TACACS	636	LDAP over SSL	3260	iSCSI Target	8200	VMware Server
53	DNS	639	MS DP(PIM)	3306	MySQL	8500	Adobe ColdFusion
67-68	DHCP/BOOTP	646	LDP(MPLS)	3389	Terminal Server	8767	TeamSpeak
69	TFTP	691	MS Exchange	3689	iTunes	8866	Bagle.B
70	Gopher	860	iSCSI	3690	Subversion	9100	HP JetDirect
79	Finger	873	rsync	3724	World of Warcraft	9101-9103	Bacula
80	HTTP	902	VMware Server	3784-3785	Ventrilo	9119	MXit
88	Kerberos	989-990	FTP over SSL	4333	mSQL	9800	WebDAV
102	MS Exchange	993	IMAP4 over SSL	4444	Blaster	9898	Dabber
110	POP3	995	POP3 over SSL	4664	Google Desktop	9988	Rbot/Spybot
113	Ident	1025	Microsoft RPC	4672	eMule	9999	Urchin
119	NNTP(Usenet)	1026-1029	Windows Messenger	4899	Radmin	10000	Webmin
123	NTP	1080	SOCKS Proxy	5000	UPnP	10000	BackupExec
135	Microsoft RPC	1080	MyDoom	5001	Singlebox	10113-10116	NetIQ
137-139	NetBIOS	1194	OpenVPN	5001	iperf	11371	OpenPGP
143	IMAP4	1214	Kazaa	5004-5005	RTP	12035-12036	Second Life
161-162	SNMP	1241	Nessus	5050	Yahoo! Messenger	12345	NetBus
177	XDMCP	1311	Dell OpenManage	5060	SIP	13720-13721	NetBackup
179	BGP	1337	WASTE	5190	AIM/ICQ	14567	Battlefield
201	AppleTalk	1433-1434	Microsoft SQL	5222-5223	XMPP/Jabber	15118	Dipnet/Oddbob
264	BGMP	1512	WINS	5432	PostgreSQL	19226	AdminSecure
318	TSP	1589	Cisco VQP	5500	VNC Server	19638	Ensim
381-383	HP Openview	1701	L2TP	5554	Sasser	20000	Usermin
389	LDAP	1723	MS PPTP	5631-5632	pcAnywhere	24800	Synergy
411-412	Direct Connect	1725	Steam	5800	VNC over HTTP	25999	Xfire
443	HTTP over SSL	1741	CiscoWorks 2000	5900	VNC Server	27015	Half-Life
445	Microsoft DS	1755	MS Media Server	6000-6001	X11	27374	Sub7
464	Kerberos	1812-1813	RADIUS	6112	Battle.net	28960	Call of Duty
465	SMTP over SSL	1863	MSN	6129	DameWare	31337	Back Orifice
497	Retrospect	1985	Cisco HSRP	6257	WinMX	33434	traceroute
500	ISAKMP	2000	Cisco SCCP	6346-6347	Gnutella		
512	rexec	2002	Cisco ACS	6500	GameSpy Arcade		
513	rlogin	2049	NFS	6566	SANE		
514	syslog	2082-2083	cPanel	6588	AnalogX		
515	LPD/LPR	2100	Oracle XDB	6665-6669	IRC		
520	RIP	2222	DirectAdmin	6679	IRC over SSL		
521	RIPng(IPv6)	2302	Halo	6699	Napster		
540	UUCP	2483-2484	Oracel DB	6881-6999	BitTorrent		

[1] گفتنی است در شکل نمایش داده شده شماره پورت‌هایی که با رنگ تیره مشخص شده‌اند بیانگر پورت‌های استفاده‌شده از جانب بدافزارها می‌باشند

جلسه اول

IP ۱-۳-۱-۱

در یک نگاه کلی IP[1] که از آن به نام "آدرس پروتکل اینترنت" نیز یاد می‌شود بیانگر عدد مشخصی است که به هر یک از دستگاه‌ها و کامپیوترهای متصل به شبکه اعطا شده است و در واقع به کمک آن می‌توان یک کامپیوتر را به صورت یکتا در سطح اینترنت یا شبکه محلی پیدا کرد.

این پروتکل در شبکه‌های مبتنی بر TCP/IP استفاده می‌شود و همواره زمانی که قرار است پیامی از یک کامپیوتر به کامپیوتر مقصد ارسال گردد این پیام با آدرس IP هر دو کامپیوتر همراه خواهد بود.

در ادامه در سطح شبکه، کامپیوترهایی به عنوان مسیریاب وظیفه دارند تا پیام را از کامپیوتر مبدا و با توجه به IP آن دریافت کنند و سپس آن را به IP که مشخص کننده کامپیوتر مقصد می‌باشد تحویل دهند.

آدرس‌های IP مورد استفاده در کامپیوتر به دو نسخه زیر تقسیم‌بندی می‌گردند و هر کدام به روش‌های متفاوتی ارایه می‌شوند:

۱- نسخه ۴ بیتی
۲- نسخه ۶ بیتی

Protocol ۲-۳-۱-۱

در یک نگاه کلی قوانینی که در جهت تبادل اطلاعات میان دو دستگاه موجود در سطح شبکه وجود دارند به نام Protocol شناخته می‌شوند.

در یک دید مشخص تمامی کامپیوترها برای آنکه بتوانند با یکدیگر ارتباط برقرار کنند و در ادامه اطلاعاتی را به هم ارسال نمایند نیاز به یک زبان مشترک دارند، این زبان مشترک "پروتکل" نام دارد.

در واقع پروتکل‌ها مجموعه استانداردی از قوانین و توافق‌ها هستند و تعیین می‌کنند که چگونه کامپیوترهای درون یک شبکه با هم ارتباط برقرار کنند، داده‌ها را جهت انتقال قالب‌بندی نمایند، در هنگام نقل و انتقال داده‌ها مکانیزم چک کردن خطاها را بررسی کنند، در صورت وجود خطا آن‌ها را تصحیح نمایند و همچنین داده‌ها را پیش از ارسال از کامپیوتر مبداء به سمت ماشین مقصد فشرده سازی کنند.

گفتنی است برخی از پروتکل‌های مهم و موجود در دنیای کامپیوتر که از آن‌ها می‌توان در سطح شبکه استفاده نمود عبارتند از:

۱- FTP: پروتکل انتقال فایل‌ها در اینترنت
۲- SMTP: پروتکل انتقالات پست الکترونیکی
۳- TCP: پروتکل کنترل انتقالات جهت ضمانت تحویل داده‌های پی‌درپی

پشته پروتکل ۱-۲-۳-۱-۱

به مجموعه چند پروتکل مستقل موجود در سطح شبکه که با همکاری یکدیگر، امکان استفاده از شبکه‌های کامپیوتری فراهم‌سازی می‌شود اصطلاحا "پشته پروتکل" می‌گویند.

در واقع یک پشته پروتکل پشته‌ای از مجموعه‌ای پروتکل است که با یکدیگر فعالیت می‌کنند و امکان انجام یک عملیات ویژه را برای نرم‌افزار یا سخت‌افزار فراهم می‌نماید.

[1] Internet Protocol

جلسه اول

گفتنی است به عنوان نمونه TCP/IP مثالی از یک پشته پروتکل می‌باشد و از دو پروتکل مستقل TCP و IP تشکیل شده است.

RFC ۲-۲-۳-۱-۱

به مستنداتی که پروتکل‌ها در داخل آن‌ها تعریف می‌شوند و در ادامه در دسترس قرار می‌گیرند تا در سطح شبکه استفاده شوند RFC[1] می‌گویند.
در یک نگاه کلی RFC به معنای "درخواست برای توضیح" می‌باشد و در واقع شامل یکسری استاندارد است که بر حسب آن‌ها قواعد پروتکل‌ها و ریز قواعد یک پروتکل مشخص می‌گردند.
با توجه به این مهم هر پروتکل[2]، RFC مخصوص به خود را دارد و در ادامه با تعاریفی که در آن مشخص می‌شوند امکان استفاده از هر پروتکل فراهم می‌شود.
در یک دید مشخص RFCها به عنوان مراجع بسیار بزرگی در دنیای کامپیوتر و شبکه محسوب می‌شوند و هر کدام از آن‌ها درباره موضوعی ویژه نوشته شده‌اند و شماره مربوط به خود را دارند.

گفتنی است به عنوان نمونه RFC 768 مربوط به پروتکل UDP و RFC 793 مربوط به پروتکل TCP می‌باشند و در واقع در آن‌ها مجموعه استانداردهای این پروتکل‌ها در جهت استفاده در شبکه تعریف شده‌اند.

این مراجع معمولا به صورت فایل‌های متنی بسیار بزرگ به تشریح پروتکل‌های مختلف می‌پردازند و منتشر می‌گردند و در ادامه مورد استفاده قرار می‌گیرند.
برخی از سایت‌ها در جهت ارایه RFCها فعالیت می‌کنند و توسط استفاده از آن‌ها می‌توان اطلاعات مفید و مناسبی درباره هر RFC کسب کرد.
این سایت‌ها همانند کتابخانه‌های گسترده، مراجع مشخصی به تعاریف هر RFC دارند و در جهت کسب اطلاعات درباره هر RFC نیاز می‌باشد تا شماره آن RFC یا نام پروتکل را در سایت مورد استفاده وارد کنید.

گفتنی است به عنوان نمونه در سایت مشخص زیر که به عنوان مرجع تمامی RFCها ایجاد شده است می‌توانید با دانستن شماره یک RFC یا ذکر نام یک پروتکل، تمامی استانداردهای تعریف یک پروتکل را مشاهده کنید:
http://www.ietf.org/rfc.html

[1] Request For Comment

[۲] مانند پروتکل‌های HTTP و HTML

جلسه دوم

Policy ۳-۳-۱-۱

در یک نگاه کلی Policy که از آن با نام "سیاست‌نامه" نیز یاد می‌شود قاعده و قانونی است که مشخص می‌کند چگونه می‌توان با تهدیدهای پیش‌آمده مقابله کرد.
در واقع روش، ابزار و مراحل تغییر روش کار در جهت کاهش تهدیدها و پاک‌کردن تهدیدها با نام Policy در دسترس کارشناسان فعال در حوزه امنیت شبکه و اطلاعات قرار دارند.
در یک دید مشخص همیشه تهدیدهای سازمانی مهم هستند لذا همواره Policy های سازمانی نیز با اهمیت خواهند بود و می‌بایست به آن‌ها از منظر ایجاد امنیت هرچه بیشتر در یک سازمان نگاه کرد.

Socket ۴-۳-۱-۱

همان‌گونه به آن اشاره شد در کامپیوترها درگاه‌های مشخصی به نام Port تعریف شده‌اند و برنامه‌نویسان و کاربران می‌توانند از آن‌ها در صورت نیاز استفاده کنند.
Portها هم به صورت سخت‌افزاری و هم به صورت نرم‌افزاری در دسترس می‌باشند و به کمک آن‌ها این امکان فراهم‌سازی خواهد شد تا بتوان با یک کامپیوتر به شیوه‌های مشخص ارتباط برقرار نمود.
در یک نگاه کلی Portهای نرم‌افزاری امکانی را برای برنامه‌نویسان آماده‌سازی می‌کنند تا این افراد بتوانند از طریق برنامه‌نویسی و به واسطه به‌کارگیری آدرس IP، به سیستم‌های راه‌دور متصل شوند و نیازهای خود را برآورده سازند.
در صورتی که این مهم از جانب یک هکر انجام شود او می‌تواند بدون اطلاع کاربر اصلی کامپیوتر به آن سیستم نفوذ نماید و در ادامه اطلاعات مهم و حساس موجود در آن را به نفع خود سرقت کند.

گفتنی است به عنوان نمونه این امکان برای یک فرد هکر وجود دارد تا به واسطه نگارش یک بدافزار به یک سیستم قربانی نفوذ نماید و در ادامه Portهای مشخصی را بر روی آن کامپیوتر در جهت استفاده‌های آتی خود باز کند.

معمولا برخی از برنامه‌های مخربی که در دنیای کامپیوتر مشغول فعالیت می‌باشند با داشتن آدرس IP یک ماشین راه‌دور و باز کردن یک Port مشخص بر روی آن چگونگی نفوذ یک مهاجم را پیاده‌سازی می‌کنند.
به ترکیب آدرس IP و Port باز شده بر روی کامپیوتر یک Socket می‌گوییم و در ادامه می‌توان توسط آن از سیستم دیگری به آن کامپیوتر متصل شد.
در واقع با استفاده از آدرس IP یک کامپیوتر که از آن با نام "آدرس پروتکل اینترنت" نیز یاد می‌شود می‌توان یک کامپیوتر مشخص را بر روی شبکه موجود پیدا کرد و در ادامه می‌توان از طریق Port باز شده بر روی آن کامپیوتر به صورت مجاز یا غیرمجاز از آن سیستم استفاده نمود.

گفتنی است با توجه به رشد روزافزون بدافزارها در دنیای کامپیوتر و با توجه به اهمیت حفظ امنیت شبکه و اطلاعات می‌بایست همیشه Portهای غیرقابل استفاده خود را در کامپیوتر اصطلاحا ببندید. در ادامه نیز می‌بایست با بررسی Portهای باز شده غیر ایمن آن‌ها را به درستی بررسی نمود و در صورت عدم نیاز، آن‌ها را ببندید و به این واسطه از فعالیت برنامه‌های مخرب جلوگیری نمایید.

SSL ۱-۴-۳-۱-۱

در یک نگاه کلی پروتکل SSL[۱] به معنای "لایه سوکت امن" می‌باشد و برای نخستین‌بار این پروتکل در سال ۱۹۹۶ میلادی توسط شرکت Netscape[۲] طراحی و پیاده‌سازی شد و در ادامه در جهت انتقال داده‌ها به صورت امن مورد استفاده قرار گرفت.

این پروتکل به صورت استاندارد مفهوم امنیت را بر پایه رمزنگاری داده‌های رد و بدل شده میان ماشین‌های Client و Server و به کمک به‌کارگیری کلیدهای رمزنگاری‌شده فراهم‌سازی می‌نماید.

در یک دید مشخص امنیت فراهم‌سازی شده توسط این پروتکل به صورت دو طرفه می‌باشد و با به‌کارگیری فرایند رمزنگاری و رمزگشایی داده‌ها در هر دو طرف Client و Server، امکان تامین امنیت هرچه بیشتر آماده‌سازی خواهد شد.

گفتنی است در وب‌سایت‌هایی که در آن‌ها پروتکل امن SSL در جهت رمزنگاری داده‌ها و اطلاعات، پیاده‌سازی شده است از پروتکل ایمن HTTPS[۳] به جای به کار بردن HTTP استفاده می‌شود.

در مدل TCP/IP پروتکل SSL در پایین‌تر از لایه کاربرد[۴] و در بالاتر از لایه انتقال[۵] قرار گرفته است و می‌توان از آن در جهت امن‌کردن پروتکل‌های غیر ایمن لایه کاربردی همانند HTTP، LDAP[۶] و IMAP[۷] استفاده نمود.

در یک نگاه کلی شرکتی که صلاحیت صدور و اعطای گواهی‌های دیجیتال SSL را دارد برای ماشین‌های Client و Server گواهی‌های امنیتی صادر می‌نماید و این امکان را در ادامه فراهم‌سازی می‌کند تا انتقال داده‌ها و اطلاعات در سطح امنیتی افزوده در بستر اینترنت انجام گیرند.

شرکت‌های بسیاری اقدام به ارایه سرویس‌های پروتکل امن SSL نموده‌اند که از آن دست می‌توان به Entrust، Digicert و Symantec اشاره نمود.

Network Communication ۱-۱-۴

در سطح شبکه برای آنکه یک فرستنده بتواند اطلاعاتی را به یک گیرنده ارسال کند می‌بایست با آن، اصطلاحا ارتباط برقرار نماید. در واقع با استفاده از ایجاد یک ارتباط مشخص میان کامپیوتر فرستنده و کامپیوتر گیرنده این امکان در ادامه فراهم‌سازی خواهد شد تا این دو کامپیوتر بتوانند اطلاعاتی را از طریق شبکه به یکدیگر ارسال کنند.

در حوزه امنیت شبکه و اطلاعات ایجاد یک ارتباط صحیح و ایمن بسیار مورد توجه قرار می‌گیرد و به واسطه انجام این مهم می‌توان به ارتباط ایجاد شده اعتماد کرد و اطلاعات مهم را در دسترس عموم قرار داد.

در صورتی که یک فرد نفوذگر توسط روش‌های مختلف بتواند به یک سیستم قربانی متصل گردد به آسانی می‌تواند بدافزارهایی را بر روی آن کامپیوتر نصب نماید و در ادامه از آن‌ها در جهت آسیب‌رساندن به سیستم قربانی سوءاستفاده کند.

---

[1] Secure Socket Layer

[۲] "نت اسکیپ" یک شرکت کامپیوتری آمریکایی است که در سال ۱۹۹۴ میلادی راه‌اندازی شد و در زمینه ارایه مجموعه نرم‌افزارهای اینترنتی، مرورگر وب، پورتال‌های وب و خدمات اینترنتی فعالیت می‌نماید

[3] Hypertext Transfer Protocol Secure

[۴] لایه چهارم

[۵] لایه سوم

[۶] Lightweight Directory Access Protocol: قراردادی در شبکه‌های کامپیوتری است و در لایه کاربرد مورد استفاده قرار می‌گیرد و از آن برای ارتباط با سرویس دایرکتوری بهره‌برداری می‌شود

[۷] Internet Message Access Protocol: به عنوان یکی از پروتکل‌های مهم در جهت نقل و انتقالات چند رسانه‌ای در سطح وب محسوب می‌شود. به عنوان نمونه سرویس‌های Email و سایت‌هایی که امکان نمایش Online فایل‌های صوتی و تصویری را فراهم‌سازی می‌کنند از این پروتکل استفاده می‌نمایند

همان‌گونه که اشاره شد پروتکل IP موجود در دنیای کامپیوتر دربردارنده دو نسخه ۴ و ۶ می‌باشد و در منابع کامپیوتری از آن‌ها با نام IPv4 و IPv6 یاد می‌شود.
در IP نسخه ۴، چگونگی ارتباط میان کامپیوترها به سه روش Unicast، Multicast و Broadcast و در IP نسخه ۶، این مهم توسط سه روش Unicast، Multicast و Anycast فراهم می‌باشد.

Unicast ۱-۴-۱-۱

در این مدل برقراری ارتباط میان فرستنده و گیرنده، اطلاعات از یک کامپیوتر به یک کامپیوتر دیگر موجود در سطح شبکه ارسال می‌گردند. در واقع در این نوع برقراری ارتباط، تنها یک فرستنده و تنها یک گیرنده در شبکه وجود دارند و به این واسطه فرایند ایجاد ارتباط آماده‌سازی می‌شود.
به عنوان نمونه می‌توان به بازبینی یک سایت مشخص موجود در سطح شبکه اینترنت اشاره نمود. در این مثال، Webserver به عنوان فرستنده و کامپیوتری که آن سایت بر روی آن نمایش داده می‌شود به عنوان گیرنده محسوب می‌شوند.
همچنین بارگیری یک فایل مشخص از روی سرور FTP نیز به عنوان یک ارتباط Unicast محسوب می‌شود. در این مثال، سرور FTP به عنوان فرستنده و کامپیوتری که آن فایل بر روی آن بارگیری می‌شود به عنوان گیرنده محسوب می‌شوند.

گفتنی است در منابع کامپیوتری و در ساختار ارتباطات N به N اصطلاحا به ارتباطات Unicast، "ارتباطات یک به یک" می‌گویند.

Multicast ۲-۴-۱-۱

یکی دیگر از روش‌هایی که به واسطه آن می‌توان یک ارتباط را در سطح یک شبکه برقرار نمود روش Multicast می‌باشد. در این روش کامپیوترهای زیادی در سطح شبکه موجود هستند و می‌بایست تعدادی از این کامپیوترها در یک گروه مشخص دسته‌بندی شوند.
با توجه به این مهم یک فرستنده می‌تواند اطلاعاتی را به تمامی کامپیوترهای موجود در شبکه ارسال نماید و در ادامه تنها کامپیوترهایی که در یک گروه مشخص موجود هستند این اطلاعات را کسب می‌نمایند.
به دیگر سخن ممکن است در سطح شبکه تعداد زیادی کامپیوتر وجود داشته باشند و تنها بخشی از آن‌ها در یک دسته‌بندی مشخص قرار گرفته باشند.
در ادامه اگر یک فرستنده پیامی را به سطح شبکه ارسال نماید این پیام تنها توسط کامپیوترهای قرار گرفته در گروه تعریفی دریافت خواهد شد.
به عنوان نمونه می‌توان به تلویزیون های Online قابل دسترس در شبکه‌های کامپیوتری اشاره نمود. در واقع هر تلویزیون قابل دسترس از طریق شبکه می‌تواند از جانب چند گیرنده دریافت گردد و مشاهده شود.

گفتنی است در منابع کامپیوتری و در ساختار ارتباطات N به N اصطلاحا به ارتباطات مبتنی بر Multicast، "ارتباطات یک به چند" می‌گویند.

Broadcast ۳-۴-۱-۱

همان‌گونه که اشاره شد این روش برقراری ارتباط تنها در نسخه IPv4 قابل استفاده می‌باشد و در آن چگونگی ارتباط فرستنده با تمامی کامپیوترهای موجود در سطح شبکه فراهم می‌شود.
در واقع در این نوع ارتباط، یک کامپیوتر ارتباط خود را به صورت همزمان به تمامی کامپیوترهای در دسترس شبکه برقرار می‌نماید.
در یک نگاه کلی زمانی که از مفهوم Broadcast صحبت می‌شود منظور، تمامی کامپیوترهای موجود در شبکه می‌باشند و هیچ‌گونه استثناء در میان آن‌ها وجود ندارد.
در این حالت زمانی که یک کامپیوتر اطلاعاتی را در سطح شبکه ارسال می‌کند تمامی کامپیوترهایی که در آن شبکه موجود هستند این اطلاعات را دریافت خواهند کرد.
در ارتباطات مبتنی بر Broadcast، یک کامپیوتر یکبار اطلاعات مشخصی را در سطح شبکه ارسال می‌کند و در ادامه هر کامپیوتری که در آن شبکه فعال می‌باشد این اطلاعات را دریافت می‌نماید.

گفتنی است در منابع کامپیوتری و در ساختار ارتباطات N به N اصطلاحا به ارتباطات Broadcast، "ارتباطات یک به همه" می‌گویند.

Anycast ۴-۴-۱-۱

همان‌گونه که اشاره شد این روش برقراری ارتباط تنها در نسخه IPv6 قابل استفاده می‌باشد و در آن چگونگی ارتباط فرستنده با نزدیکترین کامپیوتر در دسترس فراهم می‌شود.
به عبارت دیگر در این روش نیز یک گروه از سرورهای کامپیوتری تعریف می‌گردند و در ادامه هر زمان یک کامپیوتر مبداء می‌خواهد اطلاعاتی را به کامپیوتر مقصد ارسال نماید این اتصال با نزدیکترین کامپیوتر موجود در گروه کامپیوترها برقرار می‌شود و در ادامه با استفاده از مسیریابی، اطلاعات ارسال‌شده به کامپیوتر مقصد تحویل داده خواهند شد.
در یک نگاه کلی با استفاده از روش Anycast یک آدرس IP از مسیرهای مختلفی در سطح شبکه قابل دستیابی می‌باشد و در ادامه بر اساس الگوریتم‌های مسیریابی قابل استفاده در شبکه، درباره این مهم که درخواست کاربر از کدام مسیر بهتر است برود تا به مقصد برسد تصمیم‌گیری می‌شود.

گفتنی است در منابع کامپیوتری و در ساختار ارتباطات N به N اصطلاحا به ارتباطات Anycast، "ارتباطات یک به نزدیکترین" می‌گویند.

Connection ۱-۱-۵

زمانی که در سطح یک شبکه یک ماشین که از آن به عنوان مبداء یاد می‌شود قصد دارد تا داده‌ای را به ماشین دیگر موجود در سطح شبکه که از آن به نام ماشین مقصد یاد می‌شود ارسال کند یک مسیر مشخص میان آن‌ها برقرار می‌شود. در یک دید مشخص به این مسیر ایجاد شده در میان ماشین مبداء و ماشین مقصد "مسیر ارتباطی" می‌گوییم.

در یک نگاه کلی به دو طریق زیر این امکان برای ایجاد ارتباط میان دو کامپیوتر مبداء و کامپیوتر مقصد در سطح شبکه وجود دارد:

1- Connectionless Communication
2- Connection Oriented Communication

Connectionless Communication ۱-۵-۱-۱

در یک نگاه کلی "ارتباطات غیر اتصال گرا[۱]" نوعی ارتباط بدون ایجاد اتصال شبکه‌ای میان ماشین مبداء و ماشین مقصد محسوب می‌شود.
در واقع در این نوع ارتباط، زمانی که یک کامپیوتر قصد ارسال بسته ای را به ماشین مقصد دارد پس از تقسیم‌بندی بسته به واحدهای داده‌ای مجاز، هر واحد داده به صورت یکتا آدرس‌دهی می‌شود و بر اساس اطلاعات هر واحد، در ادامه مسیریابی صورت می‌گیرد.
در این نوع ایجاد ارتباط، بین دو نقطه مبداء و مقصد، یک پیام می‌تواند بدون هماهنگی قبلی از ماشین فرستنده به ماشین گیرنده ارسال شود و ممکن است داده‌ها به همان ترتیبی که ارسال شده‌اند در ماشین مقصد دریافت نگردند.

Connection Oriented Communication ۲-۵-۱-۱

در یک نگاه کلی "ارتباطات اتصال گرا[۲]" نوعی ارتباط شبکه‌ای در ارتباطات راه‌دور محسوب می‌گردند و به واسطه آن، در زمان ارسال داده‌ها از یک کامپیوتر مبداء به کامپیوتر مقصد در ابتدا ارتباط میان این دو کامپیوتر با هم برقرار می‌شود و در ادامه جریانی از داده‌ها به همان ترتیبی که فرستاده شده‌اند در ماشین مقصد دریافت می‌شوند.

Proxy Server ۱-۱-۷

در شبکه‌های کامپیوتری یک Proxy Server یک سیستم کامپیوتری یا یک نرم‌افزار است و به عنوان واسط، میان درخواست‌های کاربران و کامپیوترهای Client قرار می‌گیرد و از آن در جهت یافتن منابع از سایر Server ها استفاده می‌شود.
در یک دید مشخص یک کامپیوتر به یک Proxy Server متصل می‌شود و در ادامه یک منبع اطلاعاتی[۳] را از آن درخواست می‌نماید.
پس از انجام این مهم، Proxy Server منبع اطلاعاتی مورد نظر را در سطح شبکه به دست می‌آورد و آن را در ادامه در اختیار کامپیوتر درخواست‌کننده قرار می‌دهد.

گفتنی است در صورتی که این Proxy Server در یک کشور که دارای فعالیت فیلترینگ سایت‌ها نمی‌باشد قرار داشته باشد و با توجه به این مهم که درخواست کامپیوتر طلب‌کننده سرویس را با منابع خود پردازش می‌نماید آن درخواست بدون انجام فرایند فیلترینگ به میزبان درخواست‌کننده ارایه خواهد شد.

معمولا Proxy را چند کاربر به صورت همزمان مورد استفاده قرار می‌دهند و در یک دید مشخص، ارتباطات مبتنی بر Proxy را می‌توان به نوعی یک NAT[۱] دارنده قابلیت احراز هویت دانست.

[۱] همانند اتصالات مبتنی بر پروتکل UDP
[۲] همانند اتصالات مبتنی بر پروتکل TCP
[۳] به عنوان نمونه یک صفحه وب

مشهورترین Proxy، در زمینه وب می‌باشد و در واقع این Proxy تمامی ترافیک مربوط به پورت ۸۰ را دریافت می‌کند و مورد بررسی خود قرار می‌دهد و در ادامه اطلاعات را در اختیار کاربران می گذارد.
در یک نگاه کلی معمولا Proxy Serverها ارتباط خود با اینترنت را از طریق دو پروتکل مشخص HTTP و Socks انجام می‌دهند.
پروتکل HTTP در جهت تفسیرکردن ترافیک در سطح HTTP مورد استفاده قرار می‌گیرد و در واقع تنها می‌تواند ترافیک‌هایی که با //:HTTP و //:HTTPS مشخص شده‌اند را مدیریت کند لذا برای مرورگری وب در اینترنت بسیار مفید می‌باشد.
پروتکل Socks به هیچ‌وجه ترافیک درون شبکه را تفسیر نمی‌کند و این مهم باعث شده است تا این پروتکل از این نظر انعطاف کمتری از خود نشان دهد. در مقابل، پروتکل Socks از انواع ترافیک درون شبکه‌ای همانند HTTP، FTP و POP3 پشتیبانی می‌کند.

VPN ۱-۱-۸

یک VPN[۲] یک شبکه خصوصی مجازی‌سازی شده است و با استفاده از زیرساخت‌های ارتباطی عمومی[۳]، امکان برقراری ارتباطات امن میان دفاتر کاری راه‌دور[۴] را برای کاربران فراهم می‌کند.
با استفاده از یک ارتباط VPN می‌توان چند شبکه راه‌دور را به یکدیگر متصل کرد[۵] و در ادامه از آن‌ها در جهت مدیریت کسب و کار خود استفاده نمود.

گفتنی است امکان انجام این مهم از جانب VPN همانند آن است که به صورت فیزیکی و با استفاده از یک کابل مستقیم، این دفاتر کاری را با صرف هزینه بسیار پایین‌تر به یکدیگر متصل کرده باشید.

با توجه به وجود امکان اتصال ایمن دفاتر کاری راه‌دور به یکدیگر، کامپیوتر شما همانند کامپیوتری که به صورت فیزیکی در شبکه مقصد وجود دارد عمل می‌کند.
درخواست‌های اینترنتی که شما با برقراری ارتباط با این شبکه ارسال می‌نمایید در ابتدا می‌تواند به کامپیوتر مشخصی در سطح دنیا ارسال گردد و در ادامه با استفاده از کامپیوترهای میزبان موجود در سطح شبکه، درخواست شما به کامپیوتر مقصد موجود در راه‌دور تحویل داده خواهد شد.

گفتنی است در صورتی که در شبکه اینترنت کامپیوتر مقصد، مفهوم فیلترینگ سایت‌ها پیاده‌سازی نشده باشد با برقراری ارتباط VPN به آن شبکه، شما نیز دارای اینترنت بدون فیلترینگ خواهید بود.

---

[1] Network Address Translation
[2] Virtual Private Network
[۳] همانند شبکه گسترده اینترنت
[4] Remote Offices
[۵] به عنوان نمونه دفتر کاری خود در کشور عزیزمان ایران و دفاتر کاری خود در کشورهای دوردست

جلسه سوم

Cyber ۱-۲-۱

در یک نگاه کلی در دنیای کامپیوتر از واژه Cyber یا "سایبر" در مفاهیم مرتبط به کامپیوتر و امنیت شبکه و اطلاعات استفاده می‌شود.

در واقع Cyber به عنوان پیشوندی در ابتدای یک شخص، یک شیء و یک فضا قرار می‌گیرد و از آن در جهت توصیف آن استفاده می‌شود.

معمولا در دنیای کامپیوتر و امنیت شبکه و اطلاعات این واژه بسیار پر کاربرد است و از آن در جهت بررسی و معرفی فضای مجازی مبتنی بر شبکه گسترده اینترنت استفاده می‌شود.

Cyberspace ۱-۱-۲-۱

برای نخستین‌بار واژه Cyberspace یا "فضای سایبری" در سال ۱۹۸۴ میلادی توسط William Gibson نویسنده داستان‌های علمی - تخیلی در کتاب Neuromancer مورد استفاده قرار گرفت.

در منابع مختلف موجود در دنیای کامپیوتر تعاریف مشخصی برای این واژه ارایه شده است که از آن دست می‌توان به موارد زیر اشاره نمود:

۱- اصطلاحا به فضای مشخصی که دربردارنده تمامی مولفه‌های اطلاعات، ماشین و عوامل انسانی است فضای سایبری گفته می‌شود

۲- یک فضای سایبری از کاربران و مجموعه رفتارهای ناشی از نوع فعالیت آن‌ها در یک فضای وابسته به فناوری اطلاعات تشکیل شده است

۳- به مجموعه‌ای از ارتباطات برقرارشده توسط کامپیوترهای قابل دسترس از طریق شبکه گسترده اینترنت و بدون توجه به موقعیت مکانی آن‌ها در سطح دنیا، فضای سایبری گفته می‌شود

۴- به دامنه گسترده‌ای از اطلاعات شامل شبکه‌های وابسته مبتنی بر زیرساخت‌های فناوری اطلاعات همانند اینترنت، شبکه‌های ارتباطی و سیستم‌های کامپیوتری، فضای سایبری می‌گویند

Hack ۱-۲-۲

واژه هک به معنای استفاده از یک روش سریع و هوشمندانه به جهت نفوذ به یک سیستم کامپیوتری و کشف حقایق، اطلاعات و داده‌های موجود در آن می‌باشد.

به دیگر سخن افراد مختلف با اهداف از پیش تعیین‌شده و در جهت دسترسی غیرمجاز و غیرقانونی به یک یا بیشتر از یک سیستم کامپیوتری رخنه می‌کنند و در ادامه به دور از اطلاع مالک اصلی سیستم قربانی اطلاعاتی که مورد نیاز دارند را از روی سیستم هک شده کسب می‌نمایند.

نخستین‌بار واژه هک در سال ۱۹۵۰ میلادی و در زمانی که هنوز کامپیوتر وجود نداشت توسط گردانندگان سیستم‌های رادیویی استفاده شد. در آن زمان این افراد در جهت ایجاد تغییر در سامانه‌های رادیویی و برای رسیدن به عملکرد بهتر از این واژه استفاده می‌کردند.

Hacker ۱-۲-۲-۱

همان‌گونه که اشاره شد نخستین بار واژه هک در سال ۱۹۵۰ میلادی و توسط گردانندگان سیستم‌های رادیویی استفاده گردید. با ابداع علم دیجیتال و خلق کامپیوترهای مختلف واژه هکر معنای جدیدی به خود گرفت و در واقع

جلسه سوم

به افرادی که در حوزه الکترونیک و کامپیوتر فعالیت داشتند و با دانش خود اقدام به ایجاد و تولید برنامه‌های مفید در جهت افزایش کارکرد سیستم‌ها داشتند یک هکر می گفتند.

در عصر حاضر معمولا واژه هکر به متخصصان فعال در حوزه امنیت کامپیوتر که توانایی نفوذ و کنترل سیستم‌های کامپیوتری را برای اهداف مختلف دارند گفته می‌شود.

اصطلاحا به فردی که توانایی شناسایی آسیب‌پذیری‌های موجود در یک سیستم کامپیوتری را دارد و در ادامه با به چالش‌کشیدن سطح امنیتی تعریف شده برای آن کامپیوتر به سیستم نفوذ می‌نماید یک هکر می‌گویند.

در واقع در یک دید مشخص ورود غیرمجاز به یک کامپیوتر و دسترسی به اطلاعات محرمانه موجود در یک کامپیوتر از ویژگی‌های یک هکر محسوب می‌شوند.

با توجه به پیشرفت‌هایی که در دنیای کامپیوتر و اینترنت صورت گرفته است زندگی روزمره ما نیز دست‌خوش تغییرات فراوانی گردیده است و در بسیاری از موارد، این تغییرات مثبت بوده است اما در مواردی هم شاهد اثرات منفی تکنولوژی‌های جدید بر روی روند زندگی خود بوده‌ایم.

افراد کلاهبردار نیز در کنار سایر افراد، از کامپیوتر و اینترنت بهره‌های سودجویانه زیادی می‌برند و در رسیدن به اهداف شوم خود از آن استفاده می‌کنند.

هکرها معمولا با اهداف مختلفی به اطلاعات شخصی و محرمانه افراد دسترسی پیدا می‌کنند و در ادامه از آن‌ها سوءاستفاده می‌نمایند.

در واقع این اطلاعات مربوط به حریم شخصی و خصوصی افراد می‌باشند و به یقین این افراد به هیچ‌وجه راضی به افشای آن‌ها به صورت غیرمجاز نیستند.

به عنوان نمونه این اطلاعات می‌توانند شامل رمزهای عبور، عکس‌های خانوادگی، اطلاعات بانکی، مشخصات و اطلاعات فردی و موارد از این دست باشند.

معمولا هدف از سرقت هویت افراد دیگر در جهت کسب اطلاعات حساس و شخصی و برای سوءاستفاده‌های مالی و در برخی موارد، انجام فعالیت‌های تخریب‌گرایانه است.

۱-۲-۲-۱-۱ انواع هکر

در یک نگاه کلی در دنیای کامپیوتر و در دنیای مربوط به امنیت شبکه‌های کامپیوتری، هکرها را به دسته‌های مختلفی تقسیم‌بندی می‌کنند:

۱- کلاه‌سفید
۲- کلاه‌سیاه
۳- کلاه‌خاکستری
۴- کلاه‌صورتی
۵- کلاه‌آبی
۶- نخبه

جلسه سوم

۱-۲-۲-۱-۱-۱ کلاه‌سفید

به هکرهایی که به سیستم‌های کامپیوتری مختلف نفوذ می‌کنند اما نیت و هدف آن‌ها بد نیست و در مقابل، خیرخواهانه است هکرهای کلاه‌سفید[1] می‌گویند.

در واقع این افراد پس از نفوذ به سیستم‌ها به بررسی امنیت سیستم‌ها می‌پردازند و پس از انجام این مهم گزارش کاملی را به مدیران امنیتی سایت‌ها و سازمان‌های مختلف ارایه می‌نمایند.

به دیگر سخن به هکرهایی که با استفاده از اطلاعات خود، حفره‌های امنیتی موجود در سیستم‌های کامپیوتری را کشف می‌کنند و در ادامه بدون آنکه فعالیت‌های خرابکارانه ای داشته باشند اقدام به رفع شکاف‌های امنیتی می‌نمایند هکرهای کلاه‌سفید می‌گویند.

معمولا هکرهای کلاه‌سفید علاوه بر یافتن شکاف‌های امنیتی و تلاش در پوشش حفره‌های امنیتی، از ورود هکرهای کلاه‌سیاه نیز به سیستم‌های کامپیوتری جلوگیری می‌کنند.

این افراد هم می‌توانند بدون اطلاع مدیران سازمان‌ها و ادارات مختلف فرایند نفوذ به سیستم‌ها را انجام دهند و در ادامه نقاط ضعف موجود در آن سیستم‌ها را بدون هیچ‌گونه چشم‌داشتی به آن‌ها گزارش دهند و هم می‌توانند با اطلاع کامل سازمان مشخصی اقدام به نفوذ به سیستم‌ها نمایند و در ادامه آسیب‌پذیری‌های مختلف موجود در آن سیستم‌ها را در جهت رفع، به سمع و نظر افراد کلیدی سازمان گزارش دهند.

معمولا این افراد با شرکت‌ها و سازمان‌های مختلف قرارداد می بندند و در ادامه با اطلاع مدیران ارشد، به بررسی و کشف نقاط ضعف سیستم‌ها می‌پردازند.

این مهم کمک می‌نماید تا اصطلاحا با یک فرایند هک اخلاقی، تمامی نقاط ضعف سیستم‌های موجود کشف گردند و در ادامه با ارایه پیشنهادهای سازنده، راه نفوذ افراد غیرمجاز در جهت دستبرد به اطلاعات مسدود شوند.

> گفتنی است اصطلاحا به این نوع از افراد، هکرهای خوب نیز گفته می‌شود. وجود این نوع از هکرها نه تنها برای سیستم‌های کامپیوتری یک سازمان مضر نیست بلکه با توجه به ارایه گزارش‌های امنیتی که ارایه می‌کنند شکاف‌های امنیتی موجود پوشیده خواهند شد و به این واسطه دیواره حفاظتی شبکه‌های تعریف شده برای آن سازمان بیش از پیش تحکیم می‌گردند.
>
> این گروه از هکرها در واقع دانشجویان و اساتیدی هستند که هدفشان تنها نشان‌دادن ضعف‌های امنیتی سیستم‌های کامپیوتری می‌باشد.

زیرمجموعه هکرهای کلاه‌سفید، Script Kiddieها قرار دارند و این اصطلاح را Marcus J. Ranum[2] برای توصیف هکرهای کلاه‌سفیدی که دقیقا نمی‌دانند در حال انجام چه کاری هستند ابداع نمود.

در واقع این اصطلاح برای هکرهای کلاه‌سفید تازه‌کار بی‌تجربه ای که می‌توانند به عنوان یک تهدید امنیتی به شمار آیند استفاده می‌شود.

این افراد با به کار بردن روش‌های ضعیف و استفاده کردن از Scriptهای از پیش نوشته‌شده می‌توانند یک ضعف امنیتی موجود در سطح شبکه را کشف نمایند.

---

[1] White Hat Hackers

[2] گفتنی است Marcus J. Ranum به عنوان یک متخصص و محقق در حوزه امنیت شبکه و کامپیوتر فعالیت دارد و نوآوری‌های مختلفی در زمینه طراحی و فعالیت دیواره آتشین داشته است

معمولا تفاوت این نوع از هکرها با هکرهای کلاه‌سفید در این است که هکرهای کلاه‌سفید دقیقا می‌دانند چه فعالیتی را انجام می‌دهند اما در مقابل، هکرهای Script Kiddy دقیقا از نتایج بالقوه و پنهانی کار خود بی‌خبر هستند.

۱-۲-۲-۱-۱-۲ کلاه‌سیاه

هکرهای کلاه‌سیاه[1] در مقابل هکرهای کلاه‌سفید قرار دارند و در جهت کسب سود شخصی یا نیت‌های سوءاستفاده از فرد قربانی اقدام به هک می‌نمایند.
این افراد معمولا سایت‌ها را تخریب می‌کنند، اطلاعات مختلف را از روی سیستم‌های کامپیوتری سرقت می‌نمایند و با توجه به وجود شکاف‌های امنیتی موجود در کامپیوترها کارهای مخرب و غیرقابل جبرانی را انجام می‌دهند.
به دیگر سخن به هکرهایی که با استفاده از اطلاعات خود، به سیستم‌های مختلف به صورت غیرقانونی نفوذ می‌نمایند و در ادامه به دزدی اطلاعات، تهدید، تخریب اطلاعات، جاسوسی و سوءاستفاده‌هایی از این دست می‌پردازند هکرهای کلاه‌سیاه می‌گویند.
همان‌گونه که اشاره شد نقطه مقابل هکرهای کلاه‌سیاه، هکرهای کلاه‌سفید هستند و در واقع با درایت و قدرت هکرهای خوب مجموعه فعالیت‌های هکرهای بد خنثی می‌شوند و به نوعی از فعالیت‌های مخرب آن‌ها در سطح سیستم‌های کامپیوتری جلوگیری به عمل می‌آید.

> گفتنی است به دلیل آنکه دسترسی این نوع از هکرها به سیستم‌های کامپیوتری غیرقانونی و غیرمجاز می‌باشد و در ادامه و با بررسی شکاف‌های امنیتی و کشف آسیب‌پذیری‌های مختلف اقدام به تخریب می‌کنند از نظر قوانین جرایم کامپیوتری مجرم شناخته می‌گردند و در صورت تایید پلیس فضای تبادل اطلاعات[2] مشمول جرایم مختلف خواهند شد.

معمولا هکرهای کلاه‌سیاه از کم‌اطلاعی کاربران مختلف سوءاستفاده می‌کنند و به این واسطه دست به اعمال نفوذ بر روی سیستم‌های کامپیوتری می زنند.
به عنوان نمونه در صورتی که یک کاربر، کلمه‌های عبور ساده‌ای انتخاب کرده باشد راه نفوذ یک هکر کلاه‌سیاه را به سادگی بازگشایی می‌کند.
با بررسی شکاف‌های امنیتی و با کشف آسیب‌پذیری‌های مختلف، مسیر نفوذ هکرهای کلاه‌سیاه هموارتر خواهد شد اما با این وجود و با ایجاد پلیس فتا و ارایه راهکارهای غنی و مفید، فعالیت این نوع از هکرها با مشکلات زیادی روبرو شده است و در واقع این افراد با بررسی‌های کارشناسانه این سازمان و با صرف هزینه زمانی اندک دستگیر می‌گردند و به جرایم مشخصی محکوم می‌شوند.

> گفتنی است در دنیای کامپیوتر به این مدل از هکرها اصطلاحا Cracker نیز گفته می‌شود. در واقع این افراد به عنوان خرابکارانه‌ترین نوع هکرهای موجود شناخته می‌شوند و با فعالیت‌های خود تلاش در تخریب سابقه و اطلاعات یک سازمان مهم دارند.

[1] Black Hat Hackers

[2] فتا

جلسه سوم

۱-۲-۲-۱-۱-۳ کلاه‌خاکستری

هکرهای کلاه‌خاکستری[1] از تلفیق دو هکر کلاه‌سفید و کلاه‌سیاه به دست می آیند. به دیگر سخن فعالیت یک هکر کلاه‌خاکستری بین دو هکر کلاه‌سفید و کلاه‌سیاه تعریف شده است.

این افراد معمولا در جهت کسب اطلاعات موجود در یک سیستم کامپیوتری به آن نفوذ می‌کنند و به بازبینی و بررسی آن می‌پردازند ولی در خلال انجام این مهم هیچ‌گونه صدمه‌ای به آن کامپیوتر نمی‌رسانند و اطلاعات موجود در آن را تخریب نمی‌کنند.

به دیگر سخن هکرهای کلاه‌خاکستری به عنوان تفریح و بیشتر به جهت سرگرمی، فعالیت‌های مبتنی بر هک را در سیستم‌های کامپیوتری مختلف انجام می‌دهند.

این نوع از هکرها در زمان فعالیت‌های انجام گرفته از جانب خود، اطلاعات موجود را سرقت می‌کنند و معمولا هیچ‌گونه صدمه‌ای به کامپیوترهای هدف وارد نمی‌نمایند.

با توجه به این مهم تفاوت هکرهای کلاه‌خاکستری و هکرهای کلاه‌سیاه در نوع رفتار آن‌ها در سیستم‌های کامپیوتری می‌باشد. به عبارت دیگر، همان‌گونه که اشاره شد هکرهای کلاه‌سیاه پس از نفوذ به کامپیوترهای هدف، اطلاعات موجود در آن‌ها را سرقت می‌کنند و ممکن است این اطلاعات را در سیستم قربانی تخریب نمایند و یا اعمال مخرب دیگری را در آن کامپیوترها انجام دهند اما در مقابل، هدف اصلی هکرهای کلاه‌خاکستری نفوذ به سیستم‌ها و سپس سرقت اطلاعات بدون آنکه هیچ‌گونه صدمه‌ای به سیستم قربانی وارد نمایند است.

گفتنی است در دنیای کامپیوتر به این مدل از هکرها اصطلاحا Whacker نیز گفته می‌شود. در واقع هدف اصلی این نوع از هکرها دسترسی غیرمجاز به کامپیوترها و صرفا در جهت کسب اطلاعات به شیوه‌ای غیرقانونی از روی سیستم‌های مختلف است.

معمولا این نوع از هکرها در سطح اینترنت به گشت و گذار می‌پردازند و امنیت سایت‌های مختلف را بررسی می‌کنند و در ادامه شکاف‌های امنیتی موجود در آن‌ها را کشف می‌نمایند و به دسترسی اطلاعات درون آن‌ها می‌پردازند.

معمولا هدف بیشتر این افراد کسب اطلاعات هرچه بیشتر درباره یک سازمان و آموزش هرچه بیشتر خودشان می‌باشد و در واقع با هدف کنجکاوی به بررسی میزان آسیب‌پذیری سایت‌های مختلف اعمال نفوذ می‌کنند.

گفتنی است با اینکه هدف هکرهای کلاه‌خاکستری صرفا بررسی شکاف‌های امنیتی موجود در سایت‌های مختلف است و این مهم با تعریف هکرهای کلاه‌سفید یکسان است اما با این وجود ممکن است در زمان‌هایی این نوع از هکرها از روی کنجکاوی بیشتر یا مسایل دیگر، اقدام به تخریب داده‌ها یا سرقت اطلاعات از روی سیستم‌های قربانی کنند.

با توجه به این مهم در این زمان هکرهای کلاه‌خاکستری در دسته‌بندی هکرهای کلاه‌سیاه قرار خواهند گرفت و به نوعی به عنوان مجرم تلقی می‌شوند.

در برخی از موارد هکرهای کلاه‌خاکستری به شیوه‌ای کاملا مخفیانه به بازبینی مشکلات امنیتی سایت‌ها می‌پردازند و پس از رویت شکاف‌های امنیتی، کار خود را به پایان می‌رسانند اما در برخی از موارد نیز ممکن است به صورت

[1] Whacker Hat Hackers

مخفیانه به سیستم‌های کامپیوتری نفوذ نمایند و پس از کشف شکاف‌های امنیتی، پیشنهاد همکاری در جهت رفع مشکلات بازبینی‌شده را به مدیران امنیتی سیستم‌ها ارایه کنند.

۱-۲-۲-۱-۱-۴ کلاه‌صورتی

هکرهای کلاه‌صورتی[1] دانش کاملی در زمینه برنامه‌نویسی ندارند و تنها با بهره‌گیری از برنامه‌ها و نرم‌افزارهای از پیش نوشته‌شده توسط دیگر برنامه‌نویسان حرفه‌ای اقدام به هک سیستم‌ها می‌نمایند.
به دیگر سخن این افراد ممکن است دانش برنامه‌نویسی مشخصی داشته باشند اما میزان آگاهی آن‌ها به حدی نیست که خود، اقدام به برنامه‌نویسی و هک سیستم‌های کامپیوتری بنمایند بلکه با کمک برنامه‌نویسان زبده دیگر و از طریق نرم‌افزارهایی که در جهت بررسی شکاف‌های امنیتی خلق شده‌اند تلاش در شناسایی میزان آسیب‌پذیری کامپیوترها و سپس نفوذ به آن‌ها دارند.

گفتنی است در دنیای کامپیوتر به این مدل از هکرها اصطلاحا Booter نیز گفته می‌شود. در واقع هدف اصلی این نوع از هکرها دسترسی غیرمجاز به کامپیوترها توسط نرم‌افزارهای از پیش نوشته‌شده و صرفا در جهت خودنمایی هرچه بیشتر است.

به عبارت دیگر معمولا افرادی که توسط خرید برنامه‌های هک نوشته‌شده از جانب دیگران و با دانش و آگاهی کم اقدام به فرایند هک در سیستم‌های کامپیوتری می‌نمایند در گروه هکرهای کلاه‌صورتی قرار می‌گیرند. هدف اصلی این نوع از هکرها نیز معمولا در جهت انتقام و خودنمایی بیشتر در مقابل دیگر افراد در ارتباط با آن‌ها می‌باشد.

۱-۲-۲-۱-۱-۵ کلاه‌آبی

یک هکر کلاه‌آبی[2] فردی است که در خارج از یک شرکت و با هماهنگی مدیران ارشد امنیتی آن شرکت، به دنبال باگ‌های امنیتی احتمالی موجود در سیستم‌های کامپیوتری می‌شود و در ادامه گزارش یافته‌های خود را به شرکت ارایه می‌کند.
در واقع معمولا شرکت‌ها و سازمان‌های مختلف، برنامه‌ها و سیستم‌های تحت حمایت خود را برای مدت معینی به این دسته از هکرها می سپارند و این افراد در ادامه تلاش می‌نمایند تا با بررسی دقیق نرم‌افزارها و سیستم‌های کامپیوتری سپرده‌شده به خود، تمامی باگ‌ها و حفره‌های امنیتی احتمالی را کشف نمایند و لیست آن‌ها را در جهت رفع به مدیران ارشد امنیتی ارایه کنند.

گفتنی است در دنیای کامپیوتر به این مدل از هکرها اصطلاحا هکرهای امنیتی نیز گفته می‌شود. در واقع هدف اصلی این نوع از هکرها بررسی موشکافه تمامی سیستم‌های کامپیوتری وابسته به یک سازمان یا یک شرکت و ارایه گزارشات امنیتی مهم است.

[1] Pink Hat Hackers
[2] Blue Hat Hacker

جلسه سوم

۱-۲-۲-۱-۱-۶ نخبه

در یک نگاه کلی یک هکر نخبه[1] در میان هکرهای دیگر موجود در دنیای کامپیوتر دارای مرتبه، رتبه و جایگاه ویژه‌ای است. این نوع از هکرها معمولا با بررسی‌های دقیقی که بر روی سیستم‌های کامپیوتری انجام می‌دهند مشکلات و شکاف‌های امنیتی که تا به امروز ناشناخته بوده‌اند را کشف می‌کنند و در ادامه در صورت امکان، راه‌حل‌های سازنده ای را طی ارایه گزارشات مکفی بیان می‌نمایند.
معمولا هکرهای نخبه آسیب‌پذیری‌های موجود در سیستم‌های‌عامل و نرم‌افزارها را طی بررسی‌های مختلف و جامع کشف می‌کنند و سپس تمامی آسیب‌پذیری‌های رویت‌شده را به شرکت‌های تابعه ارایه می‌کنند.
پس از انجام این مهم این شرکت‌ها، شکاف‌های امنیتی ذکرشده را بررسی می‌کنند و در ادامه Patchها و Updateهای مختلفی را جهت استفاده کاربران نشر می‌دهند.

گفتنی است در دنیای کامپیوتر به این مدل از هکرها اصطلاحا Elite نیز گفته می‌شود. در واقع هدف اصلی این نوع از هکرها بررسی موشکافه سیستم‌عامل‌ها، نرم‌افزارها و تمامی سیستم‌های کامپیوتری است و به این طریق حفره‌های امنیتی کشف‌نشده را در جهت رفع مشکل گزارش می‌نمایند.

Phreaking ۲-۲-۲-۱

واژه Phreaking از دو واژه Phone و Freak که به ترتیب در زبان شیرین فارسی به معنای "تلفن" و "غیرمعمول و دمدمی‌مزاج" می‌باشند تشکیل شده است.
Phreaking اصطلاحا به فعالیت‌هایی همانند مطالعه، آزمایش و جست‌وجو در سیستم‌های مخابراتی اشاره دارد و در واقع فرایند بررسی این نوع از سیستم‌ها را بیان می‌کند.

Phreaker ۱-۲-۲-۲-۱

در علم کامپیوتر به هکرهایی که بر روی خطوط تلفن و سیستم‌های مخابراتی فعالیت می‌کنند و تلاش دارند به این واسطه به یک سازمان نفوذ کنند Phreaker گفته می‌شود.
به دیگر سخن به فردی که تلاش می‌کند به صورت غیرقانونی و غیرمجاز به شبکه‌های تلفن و سیستم‌های ارتباطات ایمن راه‌دور نفوذ نماید Phreaker می‌گویند.
در گذشته بیشتر سیستم‌ها آنالوگ بودند و با توجه به این مهم شرکت‌های مخابراتی از سیستم‌هایی که بر روی آن‌ها تماس برقرار می‌نمودند استفاده می‌کردند.
در آن زمان جهت ایجاد ارتباط میان بخش‌های مختلف، از فرکانس‌های فراوان استفاده می‌شد و این فرکانس‌ها همانند سوییچ‌های مخابراتی فعالیت می‌کردند و Phreaker ها با استفاده از زبان‌های برنامه‌نویسی مختلف می‌توانستند اطلاعات مبادله شده از طریق این فرکانس‌ها را بررسی نمایند.
Phreaker ها پس از بررسی فرکانس‌های موجود، کدهای در حال مبادله را کشف می‌کردند و با انجام این مهم به آسانی می‌توانستند کنترل و مدیریت شبکه‌های مخابراتی را در دست بگیرند.

[1] Elite Hacker

Dark Web ۱-۲-۳

به وب‌سایت‌هایی که در دسترس عموم مردم قرار ندارند و از آن‌ها بیشتر در جهت تامین اهداف غیرمجاز و غیرقانونی استفاده می‌شود Dark Web می‌گویند.

در این سایت‌ها اطلاعات زیادی در جهت استفاده هکرها، تروریست‌ها و افراد سودجو قرار گرفته است و این افراد می‌توانند برای اهداف غیرقانونی خود از این اطلاعات سوءاستفاده نمایند.

این اطلاعات به صورت Online در اختیار افراد سودجو قرار دارند و برای آنکه تنها از طریق این افراد مورد استفاده قرار گیرند با کلمات‌عبور مشخصی رمزنگاری شده‌اند.

معمولا تمامی فعالیت‌هایی که توسط افراد نفوذگر به کمک سایت‌های موجود در Dark Web انجام می‌گیرند غیرقابل ردیابی و شناسایی هستند.

این وب‌سایت‌ها همان‌گونه که اشاره شد در دسترس عموم مردم قرار ندارند و تنها افراد سودجو به کمک IPهای مخفی موجود در Server می‌توانند به آن‌ها دسترسی داشته باشند.

معمولا افرادی که در حوزه های مواد مخدر، ارز تقلبی، استخدام هکر، مدارک جعلی، اسلحه و مهمات، قتل و فروش اعضای بدن انسان فعالیت دارند از سایت‌های موجود در Dark Web استفاده می‌کنند.

سایت‌هایی که در طبقه‌بندی Dark Web قرار می‌گیرند معمولا اطلاعات ردگیری مشخصی در موتورهای جست‌وجو ندارند و با توجه به این مهم اگر آن‌ها را در سطح اینترنت جست‌وجو نمایید ممکن است این اقدام شما با شکست روبرو شود.

گفتنی است علت نام‌گذاری این نوع از وب‌سایت‌ها به نام Dark Web به دلیل مدیریت فعالیت‌های پنهان و ناشناخته به کمک آن‌ها می‌باشد.

TOR ۱-۳-۲-۱

در یک نگاه کلی TOR[1] سامانه‌ای است که هویت کاربران را در سطح شبکه گسترده اینترنت مخفی نگه می‌دارد و ردگیری افرادی که به شنود داده‌ها می‌پردازند را تا حد بسیار زیادی کاهش می‌دهد.

این شنودها می‌توانند شامل تمامی فعالیت‌های کاربران مانند سایت‌های بازدیدشده، فایل‌های بارگذاری یا بارگیری‌شده، پیام‌هایی که از طریق نرم‌افزارهای پیام‌رسان ارسال و دریافت شده‌اند و کلا هرگونه ارتباطی که در سطح اینترنت اتفاق افتاده اند باشند.

در یک دید مشخص، TOR یک سرویس است و کمک می‌کند تا زمانی که یک فرد از اینترنت استفاده می‌نماید به صورت ناشناس بماند و ردگیری او در زمان فعالیت مشکل گردد و از دو بخش مشخص زیر تشکیل شده است:

۱- نرم‌افزاری که از اینترنت Download می‌شود و اجازه مخفی‌سازی را فراهم‌سازی می‌کند

۲- شبکه‌ای از کامپیوترهای گوناگون که این نرم‌افزار بارگیری‌شده می‌تواند بر روی آن فعالیت کند

در این شبکه، هر دستگاه یک لایه رمز برای خواندن دستورها و رمزگشایی دستورها دارد و به واسطه آن می‌تواند پیام‌ها را به دستگاه بعدی پس از خود ارسال کند و در ادامه این مهم در دستگاه‌های دیگر نیز تکرار می‌شود.

[1] The Onion Router

انجام این کار باعث می‌شود تا هیچ‌کدام از سیستم‌هایی که در داخل این شبکه قرار دارند نتوانند از محتویات پیام‌های رد و بدل شده اطلاعاتی کسب نمایند و این مهم با پنهان‌سازی افزوده در سطح شبکه مورد استفاده مدیریت می‌شود.

گفتنی است سامانه TOR نمونه‌ای از یک Dark Web می‌باشد و معمولا از آن در جهت معاملات غیرقانونی اسلحه و مهمات از جانب گروهک‌های تروریستی استفاده می‌شود.

Dark Net ۲-۳-۲-۱

به مجموعه‌ای از ارتباطات که به شکلی عمیق و گسترده در بخش‌هایی از شبکه موجود هستند و معمولا برای افراد عادی غیرقابل دسترس می‌باشند یا ناشناخته هستند Dark Net گفته می‌شود.
افرادی که از Dark Netها استفاده می‌کنند معمولا به شبکه‌های محلی و داخلی در جهت رد و بدل کردن اطلاعات و پیام‌های خود وابسته هستند.
به عنوان نمونه فرض کنید یک فرد هکر بتواند به اینترنت همسایه خود دسترسی غیرمجاز پیدا کند و در ادامه اطلاعاتی را در جهت ارسال به مقصد بر روی شبکه او منتقل نماید.
در ادامه نیز با ردگیری همسایه‌های دیگر در دسترس، به آن‌ها هم به شیوه‌ای غیرقانونی نفوذ کند و به این واسطه اطلاعات مشخصی را به مقصد هدایت نماید.
از این مهم به نام Dark Net یاد می‌شود و به واسطه آن، ردگیری پیام‌ها و اطلاعات از جانب افرادی که به دنبال امنیت هستند با دشواری زیاد روبرو خواهد بود.
از این محیط ممکن است برای انجام امور مختلف و به صورت غیرقانونی استفاده شود و در واقع هدف بیشتر افراد از بهره‌گیری Dark Netها سوءاستفاده کردن و فرار از کشف و بازجویی است.

گفتنی است معمولا افراد سودجو از Dark Netها در کنار Dark Webها استفاده می‌نمایند و به این واسطه فعالیت‌های مورد نیاز خود را به شیوه‌ای غیرمجاز و غیرقانونی انجام می‌دهند.

Deep Web ۳-۳-۲-۱

به بخشی از محتویات صفحات وب که به دلیل دور ماندن از دید موتورهای جست‌وجو توسط کاربران یافت نمی‌گردند Deep Web می‌گویند.
با توجه به رشد شبکه‌ها و ایجاد سایت‌های مختلف در دنیای کامپیوتر، هر وب‌سایت از صفحات زیادی تشکیل شده است و معمولا موتورهای جست‌وجو از یافتن و جست‌وجوی تمامی صفحات باز می مانند.
در واقع با خلق صفحات اینترنتی مختلف و تغییر وب‌سایت‌های گوناگون، امکان پیگیری تمامی صفحات توسط موتورهای جست‌وجو به شکست می‌انجامد.
برخی از صفحات نیز به صورت پویا در داخل پایگاه‌های داده‌ای قرار دارند و در زمان بارگذاری سایت‌ها به شیوه‌ای پویا به کاربران نمایش داده می‌شوند.
این نوع از صفحات، بخش عظیمی از شبکه اینترنت را تشکیل داده اند و تنها توسط افرادی که دارای نام کاربری و رمز عبور صحیح می‌باشند در دسترس هستند.
با توجه به این مهم این مدل از صفحات اینترنتی از دسترس موتورهای جست‌وجو خارج هستند و امکان پیگیری آن‌ها معمولا ضعیف است.

جلسه سوم

به طور کلی اینترنت را به دو دسته Surface Web و Deep Web تقسیم‌بندی می‌کنند و در واقع به بخشی از وب که توسط موتورهای جست‌وجو اندیس‌گذاری شده‌اند Surface Web و به بخشی از وب که توسط موتورهای جست‌وجو به صورت استاندارد اندیس‌گذاری نشده‌اند Deep Web می‌گویند.

گفتنی است در برخی از منابع از Deep Web به نام Dark Web یاد می‌شود در صورتی که این دو مهم با هم فرق می‌کنند و در دو دسته‌بندی مختلف قرار دارند.

موفق باشید