

و امنیت شبکه

پودمان 4

به هر فعالیتی که منجر به محافظت از شبکه امنیت شبکه شامل روش هایی است که : برای محافظت از شبکه های رایانه ای در مقار مهاجم یا نفوذگر	امنیت شبکه شبکه شود امنیت شبکه می گویند .
به هر فعالیتی که منجر به محافظت از شبکه امنیت شبکه شامل روش هایی است که : برای محافظت از شبکه های رایانه ای در مقار مهاجم یا نفوذگر	شبکه شود امنیت شبکه می گویند .
امنیت شبکه شامل روش هایی است که : برای محافظت از شبکه های رایانه ای در مقار مهاجم یا نفوذگر	
برای محافظت از شبکه های رایانه ای در مقار مهاجم یا نفوذگر	۵ :
مهاجم یا نفوذگر	در مقابل دسترسی های غیر مجاز و سوء استفاده در شبکه استفاده می شود.
به هر شخص یا عنصری در شبکه که حمله ا	حمله ای علیه سیستم انجام دهد ، مهاجم یا نفوذگر می گویند.
*حملات از یک آسیب پذیری برای رسیدن به	یدن به نتایج مورد نظر استفاده می کنند.
«هک: نفوذ بدون اجازه به سیستم های رایانه	ل رایانه ای رایانه ای
*هکر : به افرادی که هک می کنند هکر گفت	کر گفته می شود.
انواع مهاجم (هکر ها):	
۱ – کراکر (هکر های کلاه سیاه): کراکر ها	براکر ها افرادی هستند به صورت <mark>غیر قانونی</mark> به حریم شبکه سازمان و کاربران وارد شده و اطلاعات آنها را به سرقت می برند .
۲-هکر (قانونمند- هکر های کلاه سفید)	سفید): این افراد به صورت <mark>قانونی</mark> اقدام به تست نفوذ روی شبکه می کنند و هدف آنها بالا بردن امنیت یک سازمان است
۳-هکر-واکر (کلاه خاکستری) هدف هک	ف هکرهای کلاه خاکستری استفاده از اطلاعات سایر کامپیوترها به هر مقصودی است ولی صدمهای به کامپیوتر وارد نمی کند. نام
دیگر این گروه Whacker میباشد هدف ا	هدف اصلی واکر استفاده از اطلاعات سایر کامپیوترها به مقصود مختلف میباشد .
تست آسیب پذیری	
این کار توسط کارشناس تست نفوذ و أسیب پ	سیب پذیری انجام می شود. (ETHICAL HACKING) کارشناسان تست نفوذ همان هکر ها ی قانونمند هستند .
هکرها مراحلی را که کراکر ها برای نفوذ به س	وذ به سیستم انجام می دهند طی کرده و نتایج کار خود را در قالب گزارشی از آسیب های موجود در آن سیستم یا شبکه به مدیران
أن سازمان تحويل مي دهند.	
فازهایی که یک هکر انجام می دهد:	دهد:
فاز ۱ :جمع أورى اطلاعات oot printing	Foot p فاز ۲ :پویش Scanning
فاز ۳ :ایجاد و حفظ دسترسی (حمله)	فاز ۴ :پاک کردن رد پاها
فاز ۱ :جمع آوری اطلاعات printing	Foot prin
در این فاز ؛ هکر قانونمند با استفاه از ابزارهای	زارهای متعدد تا جایی که امکان دارد در در مورد سازمان مورد هدف اطلاعات کسب می کند.
ابزارهای آنلاینی برای این کار وجود دارد از ج	د از جمله :(Google Hacking-Whois-Arin-Ripe)
جمع آوری اطلاعات به دو روش انجام می گیر	می گیرد:
شناسایی غیرفعال : به صورت نامحسوه	محسوس اقدام به جمع آوري اطلاعات مي كنند ؛ بنابراين شناسايي آنها مشكل است .
شناسایی فعال: به کاوش شبکه برای ک ^ن	رای کشف رایانه های افراد و آدرس IP و منابع شبکه می پردازد.(ممکن است شناسایی شود)
اطلاعاتی از جمله : محدوده آدرس IP های	ا های هدف ؛ نام دامنه ؛ اطلاعات کار کنان سازمان ؛ شماره تما <i>س</i> و
یکی از تکنیک های رایج در زمینه جمع آور	مع آوری اطلاعات استفادہ از موتور جستجوی گوگل است Google Hacking
کارگاه ۱ جمع آوری	آوری اطلاعات از تارنما Foot printing
اگر ش	اگر شخصی یک دامنه برای تارنمای خود ثبت کرده باشد ؛ مشخصات آن فرد در یک بانک اطلاعاتی جامع ثبت می شود .(نام و
نام خ	نام خانوادگی – شماره تلفن و تاریخ ثبت و انقضا و)
اطلاع از مشخصات فردی شخصی که و هر	و هر كاربر اينترنت قادر به مشاهده اطلاعات مدير يا صاحب تارنما است .
مالکیت تارنما را دارد جهن	جهت مشاهده این اطلاعات :
در مر	در مرورگر http://www.whois.com را اجرا می کنیم .در کادر جستجوی نشانی تارنما آدرس مورد نظر را وارد کنید . و
روى	روی دکمه whois کلیک کنید تا مشخصات صاحب دامنه ؛ نشانی رایانامه و نمایش داده شود .
اطلاع ازسرویس دهنده تارنما با است	با استفاده از دستور nslookup می توان به آدرس IP سرویس دهنده دسترسی پیدا کرد.
برای	برای اطلاع از نام سرور و IP آن از این دستور استفاده می شود.
مسیر رسیدن به ادرس IP هدف استفاد	استفاده از دستور Traceert

C:\Users\Hana>nslookup chap.sch.ir Sonvon: TK2E10 AEEC70	تفاوت Ping و nslookup در چیست؟
استفاده می شود. Address: 192.168.1.1	از دستور nslookup برای اطلاع از نام دامنه –نام و IP سرورآن
می گیریم . با اجرای این می گیریم . با اجرای این این این این این این این این این ا	برای بدست آوردن IP یک سایت از URL سایت مورد نظر Ping
را بررسی می کند. ۲۰۰۲ Address: 37.228.138.195	دستور چندین بسته (Packet) ارتباط شبکه ای بین چندین نقطه
C:\Users\Hana>ping chap.sch.ir	
Pinging chap.sch.ir [37.228.138.195] with 32 bytes of data: Reply from 37.228.138.195: bytes=32 time=25ms TTL=52 Reply from 37.228.138.195: bytes=32 time=62ms TTL=52 Reply from 37.228.138.195: bytes=32 time=58ms TTL=52 Reply from 37.228.138.195: bytes=32 time=51ms TTL=52	
Ping statistics for 37.228.138.195:	
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 25ms, Maximum = 62ms, Average = 49ms	
C:\Users\Hana>	
ا هذف و ادرس مسيرياب	با استفادہ از دستور tracert می توان مسیر رسیدن به ادرس P
over a maximum of 30 hops:	های میانی را پیدا کرد.
ہ اجازہ عبور بستہ ہا ی 1 <1 ms 2 ms 3 ms TK2510_0FFC7A [192.168.1.1]	از مشکلات این دستور امکان وجود فایروال در میانه راه و عد
3 * * * Request timed out.	tracert است .
4 58 ms 35 ms 37 ms 10,222.99.87	
6 * * * Request Limed out.	
7 * * * Request timed out.	
8 54 ms 38 ms 48 ms 10.221.57.30	
9 53 ms 58 ms 30 ms 10.221.59.2	
10 30 ms 34 ms 43 ms 10.221.119.1	
12 26 ms 41 ms 48 ms 10.241.0.61	
13 * * * Request timed out.	
14 57 ms 38 ms 38 ms 37.228.138.195.pol.ir [37.228.138.195] 15 42 ms 28 ms 48 ms 37.228.138.195.pol.ir [37.228.138.195]	
Trace complete.	
C:\Users\Hana>	
	فاز ۲ :پویش Scanning

تعریف درگاه : یک آدرس مجازی برای برنامه های مبتنی بر شبکه است و یک عدد بین ۱ تا ۶۵۵۳۵ برای هر برنامه اختصاص داده می شود . به عنوان مثال :

کاربرد (سرویس)	شماره درگاه
برای استاندارد HTTP در وب است (انتقال ابر متن)	٨٠
اپلیکیشن ارتباط با مسیریاب میکروتیک(winbox)	۸۱۹۲
دسترسی راه دورtelnet	۲۳
اتصالات امنssh	77
درگاه رمزنگاری شده https(پروتکل امن انتقال متن)	۴۴۳
سرویس دهنده DNS(نام دامنه)	۵۳
FTP	۲۱

با استفاده از اطلاعات بدست آمده از مرحله قبل برای پیداکردن نقاط ضعف شبکه استفاده می کند .

زمانی که یک دستگاه از طریق شبکه به دستگاهی دیگر متصل می گردد، یک پورت TCP یا UDP بین ۰ تا ۶۵۵۳۵ به آن اختصاص داده می شود.

پویش درگاه : (Port Scanning)یکی از روشهایی است که نفوذگران برای تشخیص سرویسهای راهاندازی شده در یک میزبان هدف (host target) استفاده میکنند.

نکته : یکی از نقاط آسیب پذیر در سیستم های رایانه ای ؛ درگاه های باز ونداشتن نظارت روی آن ها است . اگر درگاهی باز باشد هکر می تواند از طریق این درگاه به کل سیستم نفوذ کرده و آن را مختل کند . بنابراین باید از بسته بودن درگاه هایی که استفاده نمی شود اطمینان حاصل کرد.

اسکن پورت : فرایندی است که طی آن تمام پورتهای یک آدرس IP بررسی میشود تا پورتهای باز یا بستهی آن به دست بیاید. یک نرمافزار اسکن پورت از پورت صفر شروع کرده و تا پورت ۶۵۵۳۵ را مورد بررسی قرار میدهد. برای انجام این کار تنها کافی است که این نرمافزار به هر یک از پورتها یک درخواست فرستاده و منتظر

. که آيا پورت	صد نیز یک پاسخ ارسال کرده و به نرمافزار میگوید	، انجام میدهد. سرور مق	حالت، نرمافزار این کار را تک به تک برای هر پورت	یک پاسخ بماند. در سادهترین
				باز است یا خیر.
			تمام درگاه ها را اسکن می کند؟	سوال : آيا روش پويش درگاه
ىكن است كە	اگر در سر راه ؛ فایروال شبکه وجود داشته باشد مم	معرض دید شبکه باشد.	شی برای پیدا کردن پورتهای قابل دسترسی یا در	اسكن پورت فقط مي تواند رو
			نباط أن را قطع كند.	جلوی درخواست را بگیرد و ار
			پویش درگاه سیستم هدف	کارگاہ ۲
	ے شود)	ں باز باز مشخص م _ح	ِیش درگاه ها Net Tools می باشد .(در گاه های	یکی از ابزارهای جامع برای پر
داده می شود.	پس از وارد نمودن IP هدف در گاه های باز نمایش د	Netv را اجرا نموده و	Start گزینه vork Tools> Port scanner	پس از اجرای برنامه از منوی :
	م .	127.0.0 قرار می دھی	ای باز سیستم خود ؛ آدرس IP سیستم هدف را 1.1	نکته ۱: برای اطلاع از درگاه ه
	م ·	nets استفادہ می نمایی	ل اطلاع از درگاه های باز سیستم خود از دستور tat	نکته۲: در محیط CMD برای
_			پویش أدرس IP های فعال شبکه هدف	کارگاہ ۳
Ping Tester - Profest Main Run Switch	ssional 9.52 [License to: DRAWW ALIEN] Edit Tools Help	- 🗆 X	که برای مدیریت شبکه کاربرد دارد .	Ping Tester ابزاری است
1. Target Host 192.168.0.1	Add S 2. Parameters Image: Constraint of the second secon	3. Task Plan Scheduling Schedule Manually O Schedule	IP هدف را وارد نموده و پویش می کنیم .	پس از اجرای نرم افزار آدرس
4.2.2.4 www.google.com www.yahoo.com IP_Group_01	Add G Send Buffer Size: 32 Bytes ▲ A Add R Time Dut: 700 Milliseconds ▼ Edit Total Test Qty: Continually ▼	Ping O Tracent O Scan AutoEmail Notification	رتی که IP فعال باشد نمایش داده می شود.	پس از چند ثانیه مکث در صو
94.130.69.113	met_0255) v Delete Repeat Per IP: 1 v	Open 😨 🥑 🥭 🔤 DOS	Trace مے، توانیم به مسیر رسیدن به آدرس IP	نکته : با استفاده از دکمه ert
No. IP 1. 94.130.69.113	Ping Host Name MAC Address TTL 200 ms mm4 aix-cloud de 48		میانی دسترسی پیدا کنیم .	هدف و آدرس مسیریاب های
		ок		
		Total: 1 <u>View</u> Active: 1 View		
		Inactive: 0 View		
		Add to new group: Add G		
			Acunet	پویش آسیب پذیری با ابزار x
acune	etix			
			iv 1.11 · 1	
	Scan Add Target Delete	می بسد.	ر زمینه پویس و نسف اسیب پدیری تاریک ابرار ۸۲. Creat new Tars بالمدامه کن	ا: دندی از برنامه های تاربردی د ا: دندی Target کندند
🚳 Dashboard	No Targets created yet. Create new Target			ار هوی ۲۵۱۶۹۲ کرید یا
Add Targe	et		وارد می نماییم . ×	سپس آدرس تارنمای هدف را
			(w	(مثلا تارنمای ww.125.ir
Address			ئلیک می کنیم .	روی دکمه Add Target ۲
http://www	w.125.ir			
		<u> </u>	الله مذهبه گندند Scan الانتخاب می کن	I Target and
Choose Scann	ning Options	I:: ·<	اللي صفحة ترينة Scart مي تعليم.	سپس در منوی ۲۵۱۶۹۲ از ب دخه Benort از ب
Scan Type	Full Scan	ی طبیم تا	ل را داداند. گردی زماند.	موارد دارای آسب را گذارش
Report	None	•	چری سید. In قرار می دهیم که گذارش گری (فوری) انجام ش	تورو درای اسیب را ترارس Schedule را دهی Schedule
Schedule	Standard Reports			
benedate	Affected Items Developer			
	Executive Summary			
	Quick	_		
	Compliance Reports			

Generate Report	ی نماییم سپس روی دکمه	یکی از امکانات این ابزارگزارش گیری از پویش است .برای این کار تب Report را انتخاب ه Now Poport را کارک سرکنی مین بر Report این کار تب Now Poport را انتخاب ه
Tomplate	و در کادر بار سده درینه	New Report را طیک می دنیم . درینه All vullerabilities را اسخاب می نماییم . Affected Items
Choose		و در نفایت روی دکمه Generate Report کلیک نموده و نوع گذارش را تعیین می کنیم
choose		
Standard Reports		
Affected Items		
Developer		
		فاز ۳ :ایجاد و حفظ دسترسی (حمله)
		هکر پس از شناسایی نقاط آسیب پذیر ؛ حمله خود را آغاز می کند.
ستفاده می کنند.	برای این کار از Backdoor ا	«پس از دسترسی به سیستم هدف ؛ باید برای اجرای حملات بعدی ؛ دسترسی خود را حفظ کرم اینداد است
	و کنترل امنیتی فراهم می کند.	تعریف Backdoor: نقاطی در برنامه است که امکان دستیابی به یک سیستم را بدون بررسی (در در ماریک استان می اندار می اندار می استان می استان می استان می استان می استان می استان می از می ا
	ند.	(ضعف برنامه – ارسال یک بدافزار در قالب رایانامه) می تواند به ایجاد Backdoor کمک ک می میگار با می بیاند کرد. ایر آن با متر با می می تواند به ایجاد می می از می می ایند از می می از می ک
		یعنی یک درگاه برای خود باز گرده و از آن طریق وارد سیستم گاربر می شود.
	حملات DDOS	حملات (Denial of service)
با چندین هزار سیستم شروع به ارسال	در این حالت هکر از چندین و ی	در حملات :Dos هدف هکر ایجاد اختلال و یا قطع سرویس دهی سرور به کاربران است
ر چنین حالتی Crash می کند.	همزمان ترافیک می کند . سرور د	(هکر شروع به ارسال ترافیک با حجم بالا به سمت سرور می کند و به قدری سرور را درگیر
ه ۲۰۱۸ مورد حمله DDOS قرار گرفت	مثال : تارنمای GitHub در فوریا	جواب دادن به این ترافیک می کند که سرور توان پاسخ دادن به کاربران مجاز را نداشته باشد.
ت. این روش یکی از خطرناک ترین راه	مله عدم پذیرش سرویس DoS اس	یکی از قویترین شیوه های هکرها برای آسیب رساندن به شرکت ها و سازمان ها، استفاده از ح
ذیرش سرویس در سال های اخیر نقش	ون و ابزارهای رایگان، حمله عدم پ	های حمله است که می تواند باعث قطع شدن سرویس بشود . به دلیل وجود روش های گوناگ
بزارها و شیوه های حمله، می توانند این ا	ِارها را گرفت اما هکرها با توسعه اب ِ	پر رنگتری پیدا کرده است . هرچند که با تنظیم صحیح قایروال می شود جلوی خیلی از این اب است به ما
		محدودیت ها رو دور برند. مداله عدم مذبر شد بر مد DoS
اير کرد: مغر د خواست های در کرد	المل كردن سيمس الدرهرفي ا	حمله عدم پدیرس سرویس ۲۰۰ جمله DOS تلاش است دار جامگیه از دست. از کاردان به سیمس با سمر مرد زمانت
پر فردن کیک درخواست کای شرور با	مطيل فردن شرويس. اين تفلك ب	حسب فاقاط ماسی است برای جنو میری از مسترسی فاربرای به سرویس یا شرور و در مهایت درخواست های تقلبه انجام می شود.
	ہرویس را مشغول می نماید.	حر جر می ای ای ای ای جراحی کر است. عموما دو گونه حمله DoS داریم، یکی که به از کار افتادن سرور منتج می شود و دیگری که ب
		حمله عدم یذیرش سرویس توزیع شدهDDoS
	له DDoSگفته می شود.	در صورتیکه کامپیوترهای زیادی در حمله DoS به یک هدف مشارکت داشته باشند،به آن حم
دمله اصلي انجام مي شود . كامپيوترهاي	له DoS از طريق أن كامپيتورها، <	سناریوی انجام این حمله : ابتدا تعداد زیادی کامپیوتر (آلوده می نماید) با نصب و اجرای ابزار حم
انی نتواند با بلاک کردن IP جلوی حمله	ند. این شیوه باعث می شود که قربا	آلوده شده تحت فرمان هکر (شبکه زامبی) معمولا به هزاران کامپیوتر و حتی صدها هزار می رس
ن تر خواهد بود.)	ىبكە زامبى بزرگتر باشە، حمله موفق	را بگیرد. (هکرها معمولا با پخش کردن تروجان این شبکه زامبی را به دست می آورند هرچه ن
		کارگاه ۴ شبیه سازی حمله DDOS در کارگاه رایانه
Low Orbit Ion Cannon When harpoons, air strikes and nukes fails v. 1.0.7.0 Select your target 	2. Ready?	برای حملهDOS ابزارهای زیادی وجود دارد برای حمله به سرور و سر ریز 💉 💼
Low Orbit Ion Cannon	Lock on IMMA CHARG	کردن درخواست های ارسالی همچنین برای کنترل شبکه زامبی از ابزار LOIC ا
Selected target		(Low Orbit Ion Cano))استفاده می شود .
37.	228.138.195	با این ابزار یک کاربر به راحتی می تواند علیه سرورهای کوچک حمله DOS اسا حسین ابزار یک کاربر به راحتی می تواند علیه سرورهای کوچک حمله DOS
3. Affack options	: TCP / UDP message	انجام دهد . (با ارسال درخواست های UCP ، UDF و ITT به قربانی) . در این باذنا دی کاف ایت آدی آی بیس ای کن ایس ا ID
9001 / 80 TCP - 1500	A cat is fine too. Desudesudesu	این نرم افرار همر کافی است ادرس ای پی سرور وارد کند. ۲۲۱ و یا ۲۰ سرور رو ما د کند میدید. با انتخاب بابامتهای ممام ممام اقدام به DoS کند را فشده
Port Method Threads	<≃ faster Speed slower =	وارد کنید و شپس با انتخاب پرامترسای مسین اندام به 200 عید. با عشرین دکمه IMMA CHARGIN MAH LAZER و بس از جند ثانیه، سایت از
Praetox.com	Requesting Downloading Downloaded Requested	دسترس خارج مي شود.
		,



	آدرس IP مبدا	آدرس IP مقصد	شماره درگاه میدا	شماره درگاه مقصد	نوع پروتکل	اینترفیس ورودی / خروجی	نوع اقدام	مدیر رول های مدنظر خود و اقدام لازم برای هر یک را در جدول
1	2,174,51,22	192,168,1,0/24			ICMP		DENY	فايروال مي نويسد .
	192,108,1,10	10,172,21,2			TOP		ALLOW	
	L					جرای شرط	المسلم المادن ا	
R			51.22		192,168.	اجرای شرط ۱	اجازه دادن ا	
	1	211	0		•			4
		1						
		/	10					
	2	192.16	0		CIESTI O			
di.	آدرس IP مبدا	آدرس IP مقصد	شماره درگاه میدا	شماره درگاه مقصد	نوع يروتكل	اینترفیس ورودی / خروجی	توع اقدام	زمانیکه بسته ای قصد عبور از فایروال Pack Filter را داشته
1	2,174,51,22	192,168,1,0/24	L	23	ICMP TCP		DENY -	باشد ؛ اطلاعات بسته با رول های جدول مقایسه شده و در صورت
								مطابقت با یکی از آنها ، مطابق نوع اقدام مشخص شده در آن رول
	L	1				اجرای شرط اماد شرط	المسلم الجازة ندادن	با بسته رفتار می شود.
<						יקניט שנש	949 999 -	ضعف این نوع فایروال : عدم تشخیص وضعیت جریان های
	192,168,1,0/	24				2.	.174.51.22	ترافیکی شبکه
							早_	
						- 0-=<		
)		10.172.21.2		
			ارد .	دول وضعیت د) خود یک جا	فظه Cache	فايروال در حا	Stateful Inspection Firewall : (فايروال حالت مند) : اين
					^ه می شود .	در نظر گرفت	به نام State	برای هر بسته علاوه بر آدرس IP درگاه و نوع پروتکل یک فیلد دیگر
						ىود.	استفادہ می ش	مثلا اگر بخواهیم بسته های TCP را مدیریت کنیم از این نوع فایروال
								ضعف این نوع فایروال : محدودیت در خواندن محتویات بسته
							ل گیرد.	Application Proxy Firewall : بین کلاینت و سرور قرار م
	ارسال کردہ و	نه را به مقصد	کند سپس بست	را بررسی می	محتوای آن	ريافت كرده و	وال بسته را د	زمانیکه کلاینت و سرور بخواهند برای هم بسته ارسال کنند ؛ ابتدا فایر
	خودش را به عنوان فرستنده بسته معرفي مي كند. با توجه به عملكرد اين فايروال بسته هايي كه داراي اطلاعات مخرب هستند فيلتر مي شوند .							
ċ	سرویس پراکسی یک سرویس میانجی است که هم می تواند به صورت نرم افزاری و هم به صورت سخت افزاری روی رایانه کاربر نصب شود و به صورت واسطه ای میان							
	کاربر و شبکه قرار بگیرد .							
				، شود .	رور نامیدہ می	: ؛ پراکسی س	رجی قرار گیرد	نکته : اگر روی یک رایانه مستقل نصب شود و بین شبکه داخلی و خار
را	، پاسخ ؛ نتيجه	رجی و برگشت	ن به شبکه خار	رسال درخواسن	ئسی پس از ار	ی کنند و پراک	سرور ارسال م	کاربران برای دسترسی به شبکه خارجی درخواست خود را به پراکسی و
		ند.	ِ أن استفاده ك	ران بلافاصله از	از سوی کارب	خواست مجدد	در صورت در-	برای کاربر ارسال کرده و در حافظه کش خود نیز نگهداری می کند تا
ز	یکیشن ها تمرک	یروال روی اپل	ل اینکه این فا	ل کند . به دلیل	ِ را بررسی می	مه های مجاز	گاه ؛ فقط برنا	• به جای بررسی ترافیک مجاز یا غیرمجاز از روی آدرس IP و در
							•	دارد به آن Application level Gateway گفته می شود
را	؛ اپليکيشن ها	نها قرار گرفته	ور ؛ در میان آ	ں دھندہ راہ د	رنده و سرویس	ن سرویس گی	اری ارتباط بیز	 این فایروال به صورت پراکسی نیز عمل می کند. و پیش از برقر
								مدیریت می کند.
								محاسن فايروال Application Proxy Firewall:
						نگویی در	، سرعت یاسخ	• فابروال توانابي Cache كردن اطلاعات است . به همين دليا
						//	₹ 20	شبکه بالا مررود.
							، ەد .	 آد، سی IP میدا نسته مخفی است و به همین دلیل امنیت بالا می
					(•====	: مظيفه	WAF(Web	نکته : فادوال های سویس وب (Application Firewall
			0			9 5		بورس بالم سروس و بالمعند المعند المعند الم

		فعال سازی فایروال سیستم عامل	کارگاه ۵
		م افزاری ؛ فایروال ویندوز است .	متدوال ترين فايروال نر
		ن فایروال از نوع Packet Filter است .	*روش فيلترينگ در اين
		ت رایانه شما را چندین برابر افزایش می دهد .	فعال بودن فايروال امنيه
Windows Defender Firewall		Windows Defender Firewall	۱–از کنترا بنا گزینه ا
← → · ↑ 🔗 · Control Par	el > All Control Panel Items > Windows Defender Firewall		با انتخاب کند ا
Control Panel Home	Help protect your PC with Windows Defender Firewall		
Allow an app or feature through Windows Defender	Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.		
Firewall	Update your Firewall settings		
Turn Windows Defender	Windows Defender Firewall is not using the recommended settings to protect your computer.		
Restore defaults	What are the recommended settings?		
Advanced settings Troublesheat my network	Private networks Connected	9	
Houbleshoot my network	Guest or public networks Not connected	<u></u>	
		را غيرفعال كنيد.	۲_فاد وال آنتی و دوس
porconal firowa	Il completely well is System Integration well	norsonal firowall	، فیرون محلی ویروس
personarmewa	درينه System integration و در آخر درينه in completely	س سده (کلید ۲۵) درینه personal mewall	وارد تنظيمات انتى ويروه
		و Ok می کنیم .	disabled را انتخاب
💣 Windows Defender Fi	irewall	ل کنید .	۳-فايروال ويندوز را فعا
← → ~ ↑ @ >	تخاب کرده سیس از کادر محاوره ای ظاهر شده فایروال Control Pa	Turn windows Defender Firewa را ان	گزينه all on or off
			ويندون افعال كنيد
Control Panel Home			ويندور را عنال عيد
Allow an app or featu	Ire		
through Windows De	fender		
Change potification s	rettings		
 Turn Windows Defen 	der		
Firewall on or off			
Restore defaults			
Customize setting	gs for each type of network	۲urn o کنید	۴–فایروال ویندوز را n
You can modify the fire	ewall settings for each type of network that you use.		
Private network setting	gs		
	Nindows Defender Firewall		
	all incoming connections, including those in the list of allowed apps		
Turn off)	Nindows Defender Firewall (not recommended)		
	mindows belefact interval (not recommended)		
Public network setting	Is Nindour Defender Firewall		
	all incoming connections, including those in the list of allowed apps		
✓ Notify	me when Windows Defender Firewall blocks a new app		
Turn off	Vindows Defender Firewall (not recommended)		
V	······································		
		و خروجی در فایروال	جریان های ورودی
() ·	رج از شبکه را ترافیک خروجی می گویند. 🚽 🔜	 جریان بسته های خروجی از رایانه به سمت خار 	utbound Traffic
لل غروجي الميكم مارجي	ب رامانه را ترافیک ورودی می گویند	ا :حان سته های ورودی از شبکه پیرونی به سم	Inbound Traffic
ېک ورودې			

I		
Pindows Defender Firewall wi	th Advanced Security	ا در فایروال ویندوز می توانیم جریان های ورودی و خروجی را مدیریت نماییم . برای این کار
File Action View Help		the 1Advanced Cetting a fill
		از كزينة Advanced Setting استفاده مي نماييم .
🔗 Windows Defender Firewall wit	Windows Defender Firewall with Advanced Security on Local Cor	nputer
Cuthound Rules		
Connection Security Rules	Windows Defender Firewall with Advanced Security provides netw	/ork securit
> 🖳 Monitoring		
	Overview	
	Domain Profile	
	Windows Defender Firewall is on.	
	Inbound connections that do not match a rule are blocked.	
	Outbound connections that do not match a rule are allowed.	
	Private Profile is Active	
	Windows Defender Firewall is off.	
	Public Profile	
	Windows Defender Firewall is off.	
	Windows Defender Firewall Properties	
المکه کنان رک	ويبذاوهم جانب ديگر دستيس به اينتيزي با	درماره أتشر (firewall) داخل بسست، عامل منزمز ابن امكان باره شما مردهر كه برمن نوب ، هنج
بىر ئە ئىيد، يەت	ه برانندی جانبی دیانر انسترسی به ایسراف (ا	ويواره الكل (۱۱۱ واحتی شيشگم خاص ويندور اين الكان را به شك ليکونك که بدون خصب کيږ
		لیست سفید درست کنید یا جلوی دسترسی به یک سری از پورتها و آی پی آدرس ها را بگیرید.
بهای گسترده و	خصوصی و عمومی خود فعال کنید. این انتخار	دیواره اتش شامل سه پروفایل مختلف است. که می توانید با دستورات مختلف ان ها را برای شبکه های
	بر بر ما بر ایر بر ا	بالآسم كبرا كالمتعاد والمتعاد والمتعاد والمراجع والمراجع والمراجع
	ندور ویستا به نمایش درآمده بودند.	خوب درون دیواره انش که با یک سیستم حفاطتی پیشرفته است تعبیه شدهاند که برای اولین بار در و
ب آبد داشته باشید.	حدقابا قبول باللتديدة واكنتدا يشترى بم	البهارين ترتبب بالستفاده ازاد دواره أتشر سيستم عامل مستواند ضرب امنيت خود ماشكهي خود بالدرج
0,0	عد عبن عبوتی بانار بردنا و اعتران بیستری (و	به این تربیب با استاده از عیواره اس سیستام عامل می توانید ختریب اسیت خود و سبت می خود را در
		برای این منظور بخش های مختلف دیواره آتش و چگونگی استفاده از آن را بررسی خواهیم کرد.
r		
		برای دسترسی به فایروال پیشرفته ویندوز گزینه Advanced settings را انتخاب کنید.
System and Securit	y • Windows Firewall • • • • Search Control Panel	
Control Panel Home	Help protect your computer with Windows Firewall	
Allow a program or feature	Windows Firewall can help prevent hackers or malicious software from	
through Windows Firewall	gaining access to your computer through the Internet or a network.	
Change notification settings A Turn Windows Firewall on or	How does a firewall help protect my computer?	
off	Long or work (private) peter Connected	
Restore defaults	Home or work (private) netw Connected	
Move Advanced settings	Networks at home or work where you know and trust the people and devices on the network	
	Windows Firewall states On	
	Incoming connections: Block all connections to programs	
	that are not on the list of allowed programs	
	Active home or work (private) hotwork 3	
Secula	networks: Notify me when Windows Firewall	
Action Center	blocks a new program	
Network and Sharing Center	Public networks Connected	
		ییکربندی پروفایل های شبکه
		فایروال ویندوز از سه پروفایل مختلف زیر استفاده می کند:
		Domain : زمانی که کامپیوتر شما به دامنهای متصل است.
	. :	Private : زمانی که کامپیوتر شما به شبکهای خصوصی مثلا «work» یا «nome» متصل اسد
		where Wi-Einters during the second
	با مستقيماً به أينترنت متصل است .	Public : رمانی که کامپیونر سما به یک سبکه عمومی مانند یک نقطه دستیابی FT-۱۷۷ متصل سده ی
	، خصوصی است یا عمومی.	نکته : ویندوز همیشه در هنگام اتصال از شما سؤال می کند که ایا این شبکهای که با آن متصل شدهاید
1		كبابت كركانت البندين فلبا التناديكير البرياق بالمراجع الم
، دامنه متصل	ن دارد یک لپناپ هنگامی که در محل کار به	ممکن است یک کامپیوتر از چندین پروقایل استفاده کند، این بستگی به موقعیت دارد. برای مثال، امکار
Wi-dy and	مقارا private من مان که در رک محل ع	است از پروفایا domain استفاده کند، هنگامی که در خانه به یک شبکه خصوصی متصل است از بر
بهوندی بات	روقيل ١٠٠٠٩ و (شکی عد در یک شکل ع	است از پروفایل ۱۳۵٬۱۰۰ استان عنا منافعی که در خونه به یاف سبوه خطوطی سطن از پر
		Fiمتصل است از یروفایل Public

7

Windows Firewall with Adva				
	nced Security	-	ی Windows Firewall Properties کلیک کنید	برای پیکربندی فایروال کافی است بر روی
		- <u>.</u>	م محمد المجانية عنه المحمد	
Windows Firewall w Wins	ows Firewall with Advanced Security on Local Computer Actions Windows	رص به	ت جدانانه در نظر ترقیه است. ویندور برای خانت پیس	فايروال ويندور براي هر پروفايل يک سربر
Monitoring	moone remained becausy provide names, even in the second of import Export	جی را بسته	ن و امد داده است. ولی شما م <i>ی</i> توانید تمامی ترافیک خرو	تمامی ترافیک خروجی و ورودی اجازه رفت
D	review Restor romain Profile	ِ يک ليست	د. این تنظیمات بسته به پروفایل هستند، شما میتوانید از	و برای هر ارتباط یک دستور خاص بنویسی
0	Vindows hrewal is on. View Inbound connections that do not match a rule are blocked. C there are strengthered and the strengthere are strengthered.	•		سفيد براي هو شبكه خاص استفاده كنيد.
P	rivate Profile is Active			
0	Windows Firewall is on. Inbound connections that do not match a rule are blocked.			
P	Outbound connections that do not match a rule are allowed. ublic Profile is Active			
6	Windows Firewall is on. Inbound connections that do not match a rule are blocked.			
0	Outbound connections that do not match a rule are allowed. Windows Fraval properties			
<	, · · · ·			
Windows Firewall with	Advanced Security on Local Computer Pr	ت نخواهيد کاد و	د کنید، شما هیچ پیغامی مینی بر پلو که شدن برنامه دریاف	اگ شما ارتباطات outbound را مسدود
Domain Profile Privat	e Profile Public Profile IPsec Settings			
Specify behavior fo domain.	r when a computer is connected to its corporate		دسترسی تحواهد داشت.	برنامه بدون هیچ سر و صدایی به هیچ چیز
State	state: On (recommended)			
inbou	ind connections: Block (default) -			
Outbo	Allow (default)			
Prote	cted network connections: Customize			
Settings	settings that control Windows			
Firewall I	behavior.			
troublest	coging settings for Customize			
Learn more about the	ese settings			
2	OK Cancel Apply			
		(ایجاد یک دستور (Rule	
Windows Firewall with				
	n Advanced Security		ر از دو گزینه «Inbound Rules» یا	برای ایجاد یک دستور یا قانون جدید، یکے
File Action View	n Advanced Security Help		، از دو گزینه «Inbound Rules» یا تهنده ماانتخاب کند بری محالیت	برای ایجاد یک دستور یا قانون جدید، یکی «Outbound Bules» از در در در
File Action View	n Advanced Security Help I III Outbound Rules	Actions	، از دو گزینه «Inbound Rules» یا بتهبندیها انتخاب کنید و سپس Create Rule را	برای ایجاد یک دستور یا قانون جدید، یکی «Outbound Rules»را از درون دس
File Action View	Advanced Security Help Outbound Rules Name Group FanchCache Content Retrieval (HTTP-O BranchCache	Actions Outbound Rules	، از دو گزینه «Inbound Rules» یا بتهبندیها انتخاب کنید و سپس Create Rule را	برای ایجاد یک دستور یا قانون جدید، یکی «Outbound Rules»را از درون دس بزنید .
File Action View File Action View Windows Firewall w Inbound Rules Connection Sect Monitoring	Advanced Security Help U Dutbound Rules Name Group TanchCache Content Retrieval (HTTP-O, BranchCache BranchCache Hosted Cache Client (HTT, BranchCache BranchCache Hosted Cache Server(HTTP, BranchCache	Actions Outbound Rules New Rule fr. Filter by Profile	، از دو گزینه «Inbound Rules» یا تهبندیها انتخاب کنید و سپس Create Rule را	برای ایجاد یک دستور یا قانون جدید، یکی «Outbound Rules»را از درون دس بزنید .
File Action View	Advanced Security Help Totbound Rules Outbound Rules BranchCache Content Retrieval (HTTP-O BranchCache BranchCache Hosted Cache Client (HTT BranchCache BranchCache Posted Cache Server(HTP BranchCache Cannet to a Network Principetor (CP-Polu) Connet to a	Actions Outbound Rules New Rule In Filter by Profile Filter by State	، از دو گزینه «Inbound Rules» یا تهبندیها انتخاب کنید و سپس Create Rule را	برای ایجاد یک دستور یا قانون جدید، یکی «Outbound Rules»را از درون دس بزنید .
File Action View	Advanced Security Help	Actions Outbound Rules New Rule(h) Filter by Profile Filter by State Filter by State Filter by State	، از دو گزینه «Inbound Rules» یا تهبندیها انتخاب کنید و سپس Create Rule را	برای ایجاد یک دستور یا قانون جدید، یکی «Outbound Rules»را از درون دس بزنید .
File Action View	Advanced Security Help Cutbound Rules Outbound Rules BranchCache Content Retrieval (HTTP-O BranchCache Hosted Cache Client (HTT BranchCache BranchCache Hosted Cache Server(HTTP BranchCache Connect to a Network Projector (TCP-Out) Connect to a Connect to a Network Projector (WSD Ex Connect to a Connect to a Network Projector (WS	Actions Outbound Rules View Rule(h) Filter by Profile Filter by State Filter by Group Grefresh Filter by Filter b	، از دو گزینه «Inbound Rules» یا تهبندیها انتخاب کنید و سپس Create Rule را	برای ایجاد یک دستور یا قانون جدید، یکی «Outbound Rules»را از درون دس بزنید .
File Action View	A Advanced Security Help P P Cutbound Rules Name BranchCache Content Retrieval (HTTP-O BranchCache BranchCache Hosted Cache Client (HTT BranchCache Hosted Cache Client (HTT BranchCache Hosted Cache Server(HTTP-U BranchCache Per Discovery (WSD-Out) Connect to a Network Projector (TCP-Out) Connect to a Network Projector (TCP-Out) Connect to a Network Projector (WSD Ev Connect to a Netw	Actions Outbound Rules New Rule In Filter by Profile Filter by State Filter by Group Filter by Group G Refresh Export List Help Help	، از دو گزینه «Inbound Rules» یا تهبندیها انتخاب کنید و سپس Create Rule را	برای ایجاد یک دستور یا قانون جدید، یکی «Outbound Rules»را از درون دس بزنید .
File Action View	Advanced Security Help	Actions Outbound Rules New Rule (h) Filter by Profile Filter by State Filter by Group View Refresh Export List Help	، از دو گزینه «Inbound Rules» یا تهبندیها انتخاب کنید و سپس Create Rule را	برای ایجاد یک دستور یا قانون جدید، یکی «Outbound Rules»را از درون دس بزنید .
File Action View	Advanced Security Help Cutbound Rules Name Group GranchCache Content Retrieval (HTTP-O BranchCache BranchCache Hosted Cache Server(HTTP BranchCache Hosted Cache Server(HTTP BranchCache Peor Discovery (WSD-Out) Connect to a Network Projector (TCP-Out) Connect to a Network Projector (TCP-Out) Connect to a Network Projector (WSD Ev Connect to a Network	Actions Outbound Rules New Rule	، از دو گزینه «Inbound Rules» یا تهبندیها انتخاب کنید و سپس Create Rule را	برای ایجاد یک دستور یا قانون جدید، یکی «Outbound Rules»را از درون دس بزنید .
File Action View	Advanced Security Help Control of the security Help Control of the security Control of the security Control of the security Control of the security of the sec	Actions Outbound Rules Filter by Profile Filter by State Filter by Group Filte	، از دو گزینه «Inbound Rules» یا تهبندیها انتخاب کنید و سپس Create Rule را	برای ایجاد یک دستور یا قانون جدید، یکی «Outbound Rules»را از درون دس بزنید .
File Action View	Advanced Security Help	Actions Outbound Rules New Rule (h) Filter by Profile Filter by Group Filter by Group Carefresh Export List Help	، از دو گزینه «Inbound Rules» یا تهبندیها انتخاب کنید و سپس Create Rule را	برای ایجاد یک دستور یا قانون جدید، یکی «Outbound Rules»را از درون دس بزنید .
File Action View	Advanced Security Help Cutoound Rules Name Group GranchCache Content Retrieval (HTTP-O., BranchCache Content Retrieval (HTTP-O., BranchCache Hosted Cache Server(HTTP,.) BranchCache Hosted Cache Server(HTTP,.) BranchCache Peer Discovery (WSD-Out) Connect to a Network Projector (TCP-Out) Connect to a Network Projector (TCP-Out) Connect to a Network Projector (WSD Ev., Core Networking - Group Policy (LSASS-,, Core Networking - Group Policy (LSASS-,, Core Networking - Broup Policy (LSASS	Actions Outboand Rules New Rule Filter by Profile Filter by Strate Filter by Strate Filter by Strate Filter by Strate Filter by Strate Filter by Strate Filter by Strate Help	، از دو گزینه «Inbound Rules» یا تهبندیها انتخاب کنید و سپس Create Rule را	برای ایجاد یک دستور یا قانون جدید، یکی «Outbound Rules»را از درون دس بزنید .
File Action View	Advanced Security Help Totheward Security Help Totheward Security Outbound Rules Outbound Rules FranchCache Content Retrieval (HTTP-O., BranchCache Hosted Cache Client (HTT.,, BranchCache Hosted Cache Server(HTTP., Connect to a Network Projector (TCP-Out) Connect to a Network Projector (TCP-Out) Connect to a Network Projector (WSD Ew., Connect to a Network Projector (WSD Ew., Connect to a Connect to Connect to a Network Core Networking - Dynamic Host Config., Core Networking - Grup Policy (IAPP-Out) Core Networking - Interferourg Mana., Core Networking - Interfero Mana Connect Network Core Networking - Interfero Mana Connect Network Core Networking - Interfero Mana Mana Connect Network Core Networking - Interfero Mana Mana Mana Mana Mana Mana Mana Man	Actions Outbound Rules New Rule In Filter by Profile Filter by Group View Refresh Export List Help	، از دو گزینه «Inbound Rules» یا تهبندیها انتخاب کنید و سپس Create Rule را	برای ایجاد یک دستور یا قانون جدید، یکی «Outbound Rules»را از درون دس بزنید .
File Action View	Advanced Security Help Tothound Rules Name BranchCache Content Retrieval (HTTP-O BranchCache Hosted Cache Client (HTT BranchCache Hosted Cache Server(HTTP BranchCache Hosted Cache Server(HTTP BranchCache Hosted Cache Server(HTTP BranchCache Hosted Cache Server(HTTP Connect to a Network Projector (TCP-Out) Connect to a Network Projector (WSD Ev Connect to a Connect to a Connect to a Connect to a Network Projector (WSD Ev Connect to a Network Projector (WSD Ev Connect to a Network Projector (WSD Ev Connect to a Network Core Networking - Dynamic Host Config Core Network Core Networking - Group Policy (LSASS Core Network Core Networking - IPHTTB (TCP-Out) Core Network	Actions Outbound Rules Term Profile Filter by State Filter b	، از دو گزینه «Inbound Rules» یا ته بندی ها انتخاب کنید و سپس Create Rule را اندین ۴ نوع وختاف از دستورات را دارد:	برای ایجاد یک دستور یا قانون جدید، یکی «Outbound Rules»را از درون دس بزنید .
File Action View	Advanced Security Help Cutbound Rules Outbound Rules FranchCache Content Retrieval (HTTP-O., BranchCache BranchCache Hosted Cache Client (HTTP-, BranchCache Hosted Cache Server(HTTP-, BranchCache Hosted Cache Server(HTTP-, BranchCache Hosted Cache Server(HTTP-, BranchCache Hosted Cache Server(HTP-, Connect to a Network Projector (TCP-Out) Connect to a Network Projector (TCP-Out) Connect to a Network Projector (TCP-Out) Connect to a Network Projector (WSD Ew., Connect to a Connect to a Network Projector (WSD Ew., Connect to a Network Projector (WSD Ew., Connect to a Connect to a Network Projector (WSD Ew., Connect to a Network Projector (WSD Com, Core Networking - Dynamic Host Config., Core Networking - Group Policy (NP-Out) Core Networking - Group Policy (NP-Out) Core Networking - IPHTTPS (TCP-Out)	Actions Outbound Rules New Rule (h) Filter by Profile Filter by State Filter by Group Filter by Group Refresh Export List Help	ل از دو گزینه «Inbound Rules» یا ته بندی ها انتخاب کنید و سپس Create Rule را تاب بین ۴ نوع مختلف از دستورات را دارید:	برای ایجاد یک دستور یا قانون جدید، یکی «Outbound Rules»را از درون دس بزنید . د پنجره جدید شما توانایی انتخ Program
File Action View	Advanced Security Help Tothound Rules Outbound Rules StanchCache Content Retrieval (HTTP-G), BranchCache Hosted Cache Server(HTTP,, BranchCache Hosted Cache Server(HTTP,, BranchCache Peor Discover) (WSD-Out) Connect to a Network Projector (TCP-Out) Connect to a Network Projector (TCP-Out) Connect to a Network Projector (WSD Ev., Connect to a Network Projector (WSD-CL, Core Networking - Dynamic Host Config., Core Networking - Group Policy (ISASS,, Core Networking - Group Policy (ISASS,, Core Networking - Group Policy (ICP-C), Core Networking - Broup Policy (ICP-C), Core Networking - IPHTTPS (TCP-Out) Core Network Core Networking - IPHTTPS (TCP-Out) Core Network Core Networking - IPHTTPS (TCP-Out) Core Network Core Network Projector (WSD Ev., Core Network Core Network Brojector (WSD-C), Core Network Core Network Brojector (Brojec), Core Network Core Network Brojec), Co	Actions Outbound Rules New Rule In Filter by Profile Filter by Group Filter by Group Refresh Export List Help	ل از دو گزینه «Inbound Rules» یا ته بندی ها انتخاب کنید و سپس Create Rule را بین ۴ نوع مختلف از دستورات را دارید: مسدود کردن یا اجازه دادن به یک برنامه. تغیب ات در دسترسی به یورتها و پروتکل ها	برای ایجاد یک دستور یا قانون جدید، یکی «Outbound Rules»را از درون دس بزنید . بزنید . در پنجره جدید شما توانایی انتخ Program Port
File Action View	Advanced Security Help Cutbound Rules Name Group GranchCache Content Retrieval (HTTP-O., BranchCache Hosted Cache Gient (HTT., BranchCache Hosted Cache Server(HTTP., BranchCache Peor Discovy (WSD-Out) GranchtCache Peor Discovy (WSD-Out) Connect to a Network Projector (TCP-Out) Connect to a Network Projector (WSD Ev., Connect to a Connect to a Network Projector (WSD Ev., Connect to a Network Projector (WSD Ev., Connect to a Connect to a Network Projector (WSD Ev., Connect to a Connect to a Network Projector (WSD Ev., Core Networking - Group Policy (ICP-O., Core Network R Core Networking - Internet Group Mana., Core Network ev., Core Networking - Internet Group Mana., Core Network ev., Core Networking - Internet Group Mana., Core Network ev., Core Networking - Internet Group Mana., Core Network ev., Core	Actions Outbound Rules New Rule Filter by Profile Filter by Strate Filter by Strate Filter by Strate Filter by Strate Filter by Strate Help Outbound Help	ل از دو گزینه «Inbound Rules» یا ته بندی ها انتخاب کنید و سپس Create Rule را عاب بین ۴ نوع مختلف از دستورات را دارید: مسدود کردن یا اجازه دادن به یک برنامه. تغییرات در دسترسی به پورتها و پروتکل ها استفاده از دستورات از پیش نوشته شده	برای ایجاد یک دستور یا قانون جدید، یکی «Outbound Rules»را از درون دس بزنید . بزنید . در پنجره جدید شما توانایی انتخ Program Port Predefined
File Action View	Advanced Security Help	Actions Outbound Rules New Rule (ه.) Fitter by Profile Fitter by Group Fitter by Group Fitter by Group Refresh Export List Help	ل از دو گزینه «Inbound Rules» یا ته بندی ها انتخاب کنید و سپس Create Rule را عاب بین ۴ نوع مختلف از دستورات را دارید: مسدود کردن یا اجازه دادن به یک برنامه. تغییرات در دسترسی به پورت ها و پروتکل ها استفاده از دستورات از پیش نوشته شده مخامط از سه حالت قیل بعنی مسدود کردن یا اجازه	برای ایجاد یک دستور یا قانون جدید، یکی «Outbound Rules»را از درون دس بزنید . بنید . برنید مجدید شما توانایی انتخ Program Port Predefined Custom
File Action View Image: State of the	Advanced Security Help Provide a strain of the strain	Actions Outbound Rules New Rule In Filter by Profile Filter by State Filter by Group Filter by Grou	ل از دو گزینه «Inbound Rules» یا ته بندی ها انتخاب کنید و سپس Create Rule را تاب بین ۴ نوع مختلف از دستورات را دارید: مسدود کردن یا اجازه دادن به یک برنامه. تغییرات در دسترسی به پورت ها و پروتکل ها استفاده از دستورات از پیش نوشته شده مخلوطی از سه حالت قبل یعنی مسدود کردن یا اجازه	برای ایجاد یک دستور یا قانون جدید، یکی «Outbound Rules»را از درون دس بزنید . د پنجره جدید شما توانایی انتخ Program Port Predefined Custom



گزارش گیری از رخداد های فایروال:

کارگاہ ۶

- بررسی درستی رول های اضافه شده و عیب یابی رول هایی که دچار مشکل شده اند.
 - بررسی اینکه آیا فایروال باعث اختلال در نرم افزاری شده است یا خیر؟
 - بررسی درگاه هایی که بسته شده اند و بسته هایی که حذف شده اند .
- بررسی اینکه درون شبکه یک آدرس IP و یا گروهی از آدرس IP در تلاش هستند به فایروال و یا قسمت های مهم دیگر دسترسی پیدا کنند یا خیر ؟

فعال سازی گزارش گیری فایروال ویندوز

Advanced settings را انتخاب نموده و در بخش راست صفحه گزینه Properties را انتخاب می کنیم.

فايروال سخت افزاري

MAC Filtering

Packet Filtering

Stateful Filtering

دستگاه های UTM

ساز و کارهای دفاعی و محافظتی در سطوح شبکه :

دسترسی کاربران به شبکه را بر اساس مک آدرس آنها اعتبار سنجی می کند.

با استفاده از سازو کار IDSو IP بر اساس آدرس IP تصمیم می گیرد بسته از شبکه رد شود یا خیر در سطح اپلیکیشن انجام می شود . یکی از قویترین انواع فیلترینگ است

ا مسلح بهت بیشن ادام می شود و یا یی از طریفرین اوع میشرید و اسلم یکی از قدرتمند ترین تجهیزات فعال در شبکه هستند که انواع فیلترینگ را انجام می دهند و علاوه بر آن سرویس

هایی مانند Anti-spam-AntiVirus-IDPS-IPsec/VPN

عملیات فیلترینگ در فایروال ؛ دردو قسمت انجام می شود :

۱–در لبه ورودی و هنگام ورود بسته به فایروال

۲-در لبه خروجی و قبل از خروج بسته ها

سرویس فایروال یکی از مهمترین سرویس های روی مسیریاب میکروتیک است که امکاناتی از قبیل :

- ✓ فیلترینگ از نوع stateful
 - 🗸 فيلترينگ اپليكيشن
- فیلترینگ بر اساس آدرس IP و درگاه و اندازه و محتوای بسته

در فایروال میکروتیک (همانند فایروال ویندوز) دو نوع ترافیک ورودی و خروجی وجود دارد که به هر یک از این نوع ترافیک ها یک زنجیر ترافیک یا Chain گفته می شود .

ترافیک از سمت یک سرویس گیرنده یا شبکه می آید و به خود فایروال ختم می شود	Input Chain
حالتی است که مبدا ترافیک فایروال است و به سمت یک سرویس گیرنده یا شبکه بیرونی ختم می شود	Output Chain
ک حالت دیگر وجود دارد که در فایروال ویندوز وجود ندارد که به آن Forward chain گفته می شود	*در فايروال ميكروتيك يك
یک شبکه یا سرویس گیرنده ارسال می شود و از درون فایروال عبور می کند و به مقصد خود می رسد.	حالتی است که ترافیک از

جایگاه فایروال در شبکه



مسدود کردن دسترسی از طریق Winbox به میکروتیک

در فایروال میکروتیک تنظیماتی انجام می دهیم که سرویس گیرنده های شبکه خارجی نتوانند از طریق Winbox با مسیریاب میکروتیک ارتباط برقرار کنند .

۱- پس از ورود به محیط Winbox از منوی IP گزینه Firewall و یک رول جدید ایجاد می کنیم .

۲- سربرگ General را انتخاب می کنیم سپس گزینه Input را اتتخاب می کنیم .

۳- مقدار گزینه Dst-Asress را برای آن تعیین کنید . بهتر است برابر با مقدار اینترفیس اتصال به اینترنت باشد .

۴- پروتکل مقصد را برابر با مقدار tcp و پورت آن را برابر با مقدار ۸۲۹۱

۵-سربرگ Action مقدار عبارت Drop را انتخاب می کنیم .

۶– اتصال به میکروتیک با IP مورد نظر قطع می شود .

کارگاه ۷

۲- در انتهای رول مقدار Packet تعداد بسته های ارسال شده از سمت خارج شبکه به سمت میکروتیک برابر با یک مقداری غیر از صفر خواهد بود .

کارگاه ۸ مسدود کردن دسترسی به Winbox از طریق مک آدرس

برای مسدود سازی دسترسی به میکروتیک از طریق مک آدرس با استفاده از منوی Tolls گزینه Mac server می توان دسترسی به میکروتیک را محدود نمود .

پس از این کار اتصال به میکروتیک حتی از طریق IP مدیر نیز مسدود می شود .

توصیه می شود که این کار انجام نشود.

New NAT Rule		با استفاده از IP>Firewall تب Extra از بخش Time برای کلابنت ها می توانیم
General Advanced Extra Action Statistics	ОК	
-▼- Connection Limit	Cancel	محدوديت زمانى ايجاد نماييم.
-▼- Limit		
-▼- Dst. Limit	Apply	
- - Nth	Disable	
-▼- Time		
-▼- Src. Address Type	Comment	
-▼- Dst. Address Type	Сору	
	Remove	
-▼- IP Fragment	Reset Counters	
	Reset All Counters	
- - Nth		
-▲- Time		در قسمت Time ساعت و در قسمت Days روزهای هفته مشخص می شود.
Time: 00:00:00 -	1d 00:00:00	
Days: 🗸 sat 🖌 fri 🖌 thu 🗸 w	red 🗸 tue 🗸 mon 🖌 sun	

کارگاه ۹ مسدود سازی دستور Ping (هم از شبکه داخلی و هم از شبکه خارجی) جهت مسدود سازی دستور Ping (هم از شبکه داخلی و هم از شبکه خارجی) نکته : با این کار هکرها دچار سردرگمی می شوند . ۱-با استفاده از Pirewall و یک فایروال برای آن می نویسیم . ۲-از آنجا که مقصد ترافیک میکروتیک می باشد رول از نوع input انتخاب می شود . ۳-برای اینکه کسی نتواند میکروتیک را ping کند در قسمت آدرس مبدا و مقصد را خالی می گذاریم . ۴-دستور ping با پروتکل ICMP کار می کند . ۵-در تب Action گزینه reject را انتخاب می کنیم با این کار هکر ها دچار سردرگمی می شوند.