

فهرست مطالب

عنوان	صفحه
۱-مقدمه.....	۱
۱-۱-انواع حملات.....	۱
۱-۱-۱ حملات رد سرویس.....	۲
۱-۱-۲ حملاتی که به منظور بدست آوردن اطلاعات صورت می گیرد.....	۴
۱-۱-۳ حملاتی که سرویسدهی شبکه را دچار مشکل می کند.....	۵
۲-۱ امنیت پروتکلها.....	۵
۱-۲-۱ پیچیدگی سرویس.....	۶
۱-۲-۲ سوء استفاده از سرویس.....	۶
۱-۲-۳ اطلاعات ارائه شده توسط سرویس.....	۶
۱-۲-۴ میزان دیالوگ یا سرویسگر.....	۷
۱-۲-۵ قابلیت پیکربندی سرویس.....	۷
۱-۲-۶ انواع مکانیزم احراز هویت توسط سرویس.....	۷
۲ فایروالهای packet-filter.....	۱۰
۲-۱ فایروالهای stateless.....	۱۰
۲-۱-۱ کنترل بسته ها براساس پروتکل.....	۱۰
۲-۱-۲ کنترل بسته ها براساس آدرس ip.....	۱۱
۲-۱-۳ کنترل بسته ها برآساس پورت های tcp/udp.....	۱۱
۲-۱-۴ کنترل بسته ها از روی سایر اطلاعات موجود در سرآیند.....	۱۲
۲-۱-۵ مشکلات فیلترهای استاندارد.....	۱۳
۲-۱-۶ کنترل بسته ها توسط سیستم عامل.....	۱۴
۲-۲ سیستم های statefull.....	۱۴
۲-۳ مشکلات فیلترها.....	۱۵
۳ NAT.....	۱۶
۳-۱ انواع ترجمه آدرس در NAT.....	۱۸
۳-۱-۱ ترجمه پویا.....	۱۸
۳-۱-۲ ترجمه ایستا.....	۱۹
۳-۱-۳ توزیع بار.....	۱۹
۳-۱-۴ افزونگی (REDUNDANCEY).....	۱۹

۲۰ NAT مشکلات ۳-۲
۲۲ ۴ پراکسی
۲۳ ۴-۱ عملکرد های امنیتی پراکسی
۲۳ ۴-۱-۱ پنهان کردن اطلاعات سرویسگیر ها
۲۳ ۴-۱-۲ بستن یک سری URL
۲۴ ۴-۱-۳ کنترل محتوبات بسته ها
۲۴ ۴-۱-۴ اطمینان از سالم بودن بسته ها
۲۴ ۴-۱-۵ کنترل روی دسترسی ها
۲۵ ۴-۲ تاثیر پراکسی در سرعت
۲۵ ۴-۲-۱ CACH کردن
۲۵ ۴-۲-۲ توزیع بار
۲۵ ۴-۳ مشکلات پراکسی
۲۷ ۵ سیستم های تهاجم یاب
۲۸ ۵-۱ سیستم های تهاجم یاب براساس بازرسی
۲۹ ۵-۲ سیستم های تهاجم یاب طعمه
۳۰ ۶ IP FILTER
۳۱ ۶-۱ نصب IP FILTER بر روی SOLARIS
۳۱ ۶-۲ پیاده سازی یک فیلتر با استفاده از IP FILTER
۳۷ ۷ SNORT
۳۸ ۷-۱ SNIFFER
۳۸ ۷-۲ PACKET LOGGER
۳۹ ۷-۳ مود تهاجم یاب شبکه
۴۰ ۷-۴ فیلترهای BPF
۴۲ ۷-۵ فایل پیکربندی SNORT
۴۳ ۷-۵-۱ PREPROCESSOR ها
۴۴ ۷-۵-۲ قوانین تهاجم
۴۴ ۷-۵-۳ ماجول های خروجی
۴۷ ۸ SAINT
۴۸ ۸-۱ فایل پیکربندی
۵۳ ۸-۲ خط فرمان

۵۷	۸-۳ فرمت بانک اطلاعاتی
۵۷	۸-۳-۱ بانک اطلاعاتی FACTS
۵۸	۸-۳-۲ بانک اطلاعاتی ALL-HOSTS
۵۹	۸-۳-۳ بانک اطلاعاتی TODO
۵۹	۸-۳-۴ بانک اطلاعاتی CVE
۵۹	۸-۴ آنالیز خروجی
۶۲	ضمیمه ۱: ویروس ها، حمله و دفاع
۸۶	ضمیمه ۲: امنیت در شبکه های بی سیم
۹۹	ضمیمه ۳: پیکربندی IIS با رعایت مسائل امنیتی
۱۲۵	منابع