1. Record Nr. UNINA9910465787003321

Autore	Salmon Arthur
Titolo	Applied network security : master the art of detecting and averting advanced network security attacks and techniques / / Arthur Salmon, Warun Levesque, Michael McLafferty
Pubbl/distr/stampa	Birmingham, England ; ; Mumbai, [India] : , : Packt, , 2017 ©2017
ISBN	1-78646-968-5
Edizione	[1st edition]
Descrizione fisica	1 online resource (320 pages) : illustrations
Disciplina	005.8
Soggetti	Computer networks - Security measures Business enterprises - Computer networks - Security measures Electronic books.
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Cover -- Copyright -- Credits -- About the Authors -- About the Reviewer -- www.PacktPub.com -- Customer Feedback -- Table of Contents -- Preface -- Chapter 1: Introduction to Network Security -- Murphy's law -- Hackers (and their types) defined -- Hacker tools -- The hacking process -- Ethical hacking issues -- Current technologies -- Recent events and statistics of network attacks -- Our defense -- Security for individuals versus companies -- Wi-Fi vulnerabilities -- Knowns and unknowns -- False positives -- Mitigation against threats -- Building an assessment -- Summary -- References -- Chapter 2: Sniffing the Network -- What is network sniffing? -- Why network sniffing is important -- Scan a single IP -- Scan a host -- Scan a range of IPs -- Scan a subnet -- Nmap port selection -- Scan a single port -- Scan a range of ports -- Scan 100 most common ports (fast) -- Scan all 65535 ports -- Nmap port scan types -- Scan using TCP SYN scan (default) -- Scan using TCP connect -- Service and OS detection -- Detect OS and services -- Standard service detection -- More aggressive service detection -- Lighter banner-grabbing detection -- Nmap output formats -- Save default output to file -- Save in all formats -- Scan using a specific NSE script -- Scan with a set of scripts -- Lab 1-a scan to search for DDoS reflection UDP services -- Using

Wireshark filters -- Wireshark filter cheat sheet -- Lab 2 -- Sparta -- Brute-force passwords -- Lab 3-scanning -- Scanning a subnet -- Spoofing and decoy scans -- Evading firewalls -- Gathering version info -- UDP scan -- The reason switch -- Using a list -- Output to a file -- Commands -- Starting the listener -- Countermeasures -- Summary -- Chapter 3: How to Crack Wi-Fi Passwords -- Why should we crack our own Wi-Fi? -- What's the right way to do it? -- The method -- The requirements -- What is packet injection?.
Wi-Fi cracking tools -- The steps -- The Transmission Control Protocol (TCP) handshake -- The password lists -- How to make a strong password -- The short version (a cheat-sheet for the aircrack-ng suite) -- Summary -- Chapter 4: Creating a RAT Using Msfvenom -- Remote Access Trojans -- Ways to disguise your RAT though Metasploit -- PDF-embedded RAT -- MS Word-embedded RAT -- Android RAT -- Your defence -- Summary -- References -- Chapter 5: Veil Framework -- Veil-Evasion -- Veil-Pillage -- How do hackers hide their attack? -- Intrusion with a PDF -- The scenario -- Veil-PowerTools -- What is antivirus protection? -- What are some vulnerabilities in antivirus protection? -- Evasion and antivirus signatures -- Summary -- References -- Chapter 6: Social Engineering Toolkit and Browser Exploitation -- Social engineering -- What are web injections? -- How SQL injections work -- Cross site scripting (XSS) attacks -- Preventative measures against XSS attacks -- How to reduce your chances of being attacked -- Browser exploitation with BeEF -- Browser hijacking -- BeEF with BetterCap -- BeEF with man-in-the-middle framework (MITMF) -- BeEF with SET -- Summary -- Chapter 7: Advanced Network Attacks -- What is an MITM attack? -- Related types of attacks -- Examples of MITM -- Tools for MITM attacks -- Installing MITMF using Kali Linux -- Summary -- Chapter 8: Passing and Cracking the Hash -- What is a hash? -- Authentication protocols -- Cryptographic hash functions -- How do hackers obtain the hash? -- What tools are used to get the hash? -- How are hashes cracked? -- How do pass the hash attacks impact businesses? -- What defences are there against hash password attacks? -- Summary -- References -- Links to download tools -- Chapter 9: SQL Injection -- What is SQL and how does it work? -- SQL command examples -- SQL injection.
Examples of SQL injection attacks -- Ways to defend against SQL injection attacks -- Attack vectors for web applications -- Bypassing authentication -- Bypass blocked and filtered websites -- Finding vulnerabilities from a targeted sites -- Extracting data with SQLmap -- Hunting for web app vulnerabilities with Open Web Application Security Project (OWASP) ZAP -- Summary -- Chapter 10: Scapy -- Scapy -- Creating our first packet -- Sending and receiving -- Layering -- Viewing the packet -- Handling files -- The TCP three way handshake -- SYN scan -- A DNS query -- Malformed packets -- Ping of death -- Teardrop attack (aka Nestea) -- ARP cache poisoning -- ARP poisoning commands -- ACK scan -- TCP port scanning -- VLAN hopping -- Wireless sniffing -- OS fingerprinting ISN -- Sniffing -- Passive OS detection -- Summary -- Chapter 11: Web Application Exploits -- Web application exploits -- What tools are used for web application penetration testing? -- What is Autopwn? -- Using Autopwn2 -- What is BeEF and how to use it? -- Defenses against web application attacks -- Summary -- Chapter 12: Evil Twins and Spoofing -- What is an evil twin? -- What is address spoofing? -- What is DNS spoofing? -- What tools are used for setting up an evil twin? -- The dangers of public Wi-Fi and evil twins -- How to detect an evil twin? -- Summary -- Chapter 13: Injectable Devices -- A deeper look into USB -- A possible threat -- An evil USB -- How does the Rubber Ducky work? -- Disabling ports --

A KeyGrabber? -- What the glitch? -- Summary -- Chapter 14: The Internet of Things -- What is the Internet of Things? -- IOT vulnerabilities and cyber security -- IOT and botnets -- Summary -- Sources -- Chapter 15: Detection Systems -- IDS -- IPS -- Host based -- Network-based -- Physical -- Summary of differences -- Why? -- Who and when?.
Security Information and Event Management (SIEM) -- Splunk -- Alert status -- IDS versus IPS -- Snort as an IPS -- How? -- Lab 1-installing Snort and creating ICMP rules lab -- Lab 2-create the following snort.conf and icmp.rules files -- Rule options -- Lab 3-execute Snort -- Show log alert -- Alert explanation -- Lab 4-execute Snort as Daemon -- Summary -- Chapter 16: Advance Wireless Security Lab Using the Wi-Fi Pineapple Nano/Tetra -- The history of Wi-Fi - the WLAN standard -- Wireless vulnerability -- The Wi-Fi Pineapple -- For penetration testing -- Lab 1-how to set up -- Getting connected -- Performing a scan -- Getting connected, managing your network, and broadcasting Wi-Fi -- Reporting data -- Logging data with Pineapple -- Reporting data -- Enabling the landing page -- Summary -- Chapter 17: Offensive Security and Threat Hunting -- What is offensive security? -- What tools are used for offensive security? -- SET browser exploit lab -- Threat hunting platforms -- Using the Pineapple for offensive security -- Lab 1-setting up an Evil Portal on the Pineapple -- Summary -- Index.

Sommario/riassunto

Master the art of detecting and averting advanced network security attacks and techniques About This Book Deep dive into the advanced network security attacks and techniques by leveraging tools such as Kali Linux 2, MetaSploit, Nmap, and Wireshark Become an expert in cracking WiFi passwords, penetrating anti-virus networks, sniffing the network, and USB hacks This step-by-step guide shows you how to confidently and quickly detect vulnerabilities for your network before the hacker does Who This Book Is For This book is for network security professionals, cyber security professionals, and Pentesters who are well versed with fundamentals of network security and now want to master it. So whether you're a cyber security professional, hobbyist, business manager, or student aspiring to becoming an ethical hacker or just want to learn more about the cyber security aspect of the IT industry, then this book is definitely for you. What You Will Learn Use SET to clone webpages including the login page Understand the concept of Wi-Fi cracking and use PCAP file to obtain passwords Attack using a USB as payload injector Familiarize yourself with the process of trojan attacks Use Shodan to identify honeypots, rogue access points, vulnerable webcams, and other exploits found in the database Explore various tools for wireless penetration testing and auditing Create an evil twin to intercept network traffic Identify human patterns in networks attacks In Detail Computer networks are increasing at an exponential rate and the most challenging factor organisations are currently facing is network security. Breaching a network is not considered an ingenious effort anymore, so it is very important to gain expertise in securing your network. The book begins by showing you how to identify malicious network behaviour and improve your wireless security. We will teach you what network sniffing is, the various tools associated with it, and how to scan for vulnerable wireless networks. Then we'll show you how attackers hide the payloads and bypass the victim's antivirus. Furthermore, we'll teach you how to spoof IP / MAC address and perform an SQL injection attack and prevent it on your website. We will create an evil twin and demonstrate how to intercept network traffic. Later, you will get familiar with Shodan and Intrusion Detection and will explore the features and tools associated with it.

Toward the end, we cover tools such as Yardstick, Ubertooth, Wifi Pineapple, and A...