Net sec

Technology, Internet

1. Name at least five applications and tools pre-loaded on the TargetWindows01 server desktop, and identify whether that application starts as a service on the system or must be run manually. WINDOWS APPLICATION LOADEDSTARTS AS SERVICE Y/N 1. tftpd32 Starts as a service 2. FileZilla Server Interface- The interface does not start as a service and must be ran manually 3. Wireshark – Does not start as a service and must be ran manually 4. Nessus Server Manager – Does not start as a service and must be ran manually 5. NetWitness Investigator – Does not start as a service and must be ran manually 2.

What was the allocated source IP host address for the TargetWindows01 server, TargetUbuntu01 server, and the IP default gateway router? TagetWindows01 Server- Source IP = 172. 30. 0. 8 TargetUbuntu01 Server – Source IP = 172. 30. 0. 4 TargetUbuntu02 Server – Source IP = 172. 30. 0. 9 The Default Gateway IP is = 172. 30. 0. 1 3. Did the targeted IP hosts respond to the ICMP echo-request packet with an ICMP echo-reply packet when you initiated the “ ping” command at your DOS prompt? If yes, how many ICMP echo-request packets were sent back to the IP source? Yes, the targeted IP host responded back with 4 echo-replies. 4.

If you ping the TargetWindows01 server and the UbuntuTarget01 server, which fields in the ICMP echo-request/echo-replies vary? The fields that vary is the Time To Live (TTL) fields. For the TargetUbuntu01 it's 64 and the TargetWindows01 is 128. 5. What is the command line syntax for running an “ Intense Scan” with Zenmap on a target subnet of 172. 30. 0. 0/24? The syntax for an Intense Scan in Zenmap is as followed: nmap -T4 -A -v -PE -PS22, 25, 80 -PA21, 23, 80, 3389 172. 30. 0. 0/24 6. Name at least five

different scans that may be performed from the Zenmap GUI. Document under what circumstances you would choose to run those particular scans.

Intense Scan-Provides a very detailed information about ports and protocols, Operating Systems, and Mac Addresses Internse Scan, all TCP ports – Provide intense scan on all tcp ports 1-65535. Ping Scan-Provide basic information about availability and MAC addresses Quick Scan- Provides a fast scan limiting the number of TCP ports scanned only the top 100 most common TCP ports Regular Scan-This is the default scan by issuing TCP SYN scans for the most common 1000 TCP ports using pings for host detection. 7. How many different tests (i. e. , scripts) did your " Intense Scan" definition perform?

List them all after reviewing the scan report. The Intense Scan initiated 36 Scripts. The scripts can be found at http://nmap. org/nsedoc/ 8. Describe what each of these tests or scripts performs within the Zenmap GUI (Nmap) scan report. Below are each of the 36 scripts and a description of each, derived from http://nmap. org/nsedoc/. acarsd-info Retrieves information from a listening acarsd daemon. Acarsd decodes ACARS (AircraftCommunicationAddressing and Reporting System) data in real time. The information retrieved by this script includes the daemon version, API version, administrator e-mail address and listening frequency. ddress-info Shows extra information about IPv6 addresses, such as embedded MAC or IPv4 addresses when available. afp-brute Performs password guessing against Apple Filing Protocol (AFP). afp-ls Attempts to get useful information about files from AFP volumes. The output is intended to resemble the output of ls. afp-path-vuln Detects the Mac OS X AFP directory traversal

vulnerability, CVE-2010-0533. afp-serverinfo Shows AFP server information. This information includes the server's hostname, IPv4 and IPv6 addresses, and hardware type (for example Macmini or MacBookPro). fp-showmount Shows AFP shares and ACLs. ajp-auth Retrieves the authentication scheme and realm of an AJP service (Apache JServ Protocol) that requires authentication. ajp-brute Performs brute force passwords auditing against the Apache JServ protocol. The Apache JServ Protocol is commonly used by web servers to communicate with back-end Java application server containers. ajp-headers Performs a HEAD or GET request against either the root directory or any optional directory of an Apache JServ Protocol server and returns the server response headers. ajp-methods

Discovers which options are supported by the AJP (Apache JServ Protocol) server by sending an OPTIONS request and lists potentially risky methods. ajp-request Requests a URI over the Apache JServ Protocol and displays the result (or stores it in a file). Different AJP methods such as; GET, HEAD, TRACE, PUT or DELETE may be used. amqp-info Gathers information (a list of all server properties) from an AMQP (advanced message queuing protocol) server. asn-query Maps IP addresses to autonomous system (AS) numbers. auth-owners Attempts to find the owner of an open TCP port by querying an auth daemon which must also be open on the target system.

The auth service, also known as identd, normally runs on port 113. auth-spoof Checks for an identd (auth) server which is spoofing its replies. backorifice-brute Performs brute force password auditing against the BackOrifice service. The backorifice-brute. ports script argument is mandatory (it specifies ports to run the script against). backorifice-info

Connects to a BackOrifice service and gathers information about the host and the BackOrifice service itself. banner A simple banner grabber which connects to an open TCP port and prints out anything sent by the listening service within five seconds. bitcoin-getaddr

Queries a Bitcoin server for a list of known Bitcoin nodes bitcoin-info Extracts version and node information from a Bitcoin server bitcoinrpc-info Obtains information from a Bitcoin server by calling getinfo on its JSON-RPC interface. bittorrent-discovery Discovers bittorrent peers sharing a file based on a user-supplied torrent file or magnet link. Peers implement the Bittorrent protocol and share the torrent, whereas the nodes (only shown if the include-nodes NSE argument is given) implement the DHT protocol and are used to track the peers. The sets of peers and nodes are not the same, but they usually intersect. bjnp-discover

Retrieves printer or scanner information from a remote device supporting the BJNP protocol. The protocol is known to be supported by network based Canon devices. broadcast-ataoe-discover Discovers servers supporting the ATA over Ethernet protocol. ATA over Ethernet is an ethernet protocol developed by the Brantley Coile Company and allows for simple, high-performance access to SATA drives over Ethernet. broadcast-avahi-dos Attempts to discover hosts in the local network using the DNS Service Discovery protocol and sends a NULL UDP packet to each host to test if it is vulnerable to the Avahi NULL UDP packet denial of service (CVE-2011-1002). roadcast-bjnp-discover Attempts to discover Canon devices (Printers/Scanners) supporting the BJNP protocol by sending BJNP Discover requests to the network broadcast address for both ports associated with the

protocol. broadcast-db2-discover Attempts to discover DB2 servers on the network by sending a broadcast request to port 523/udp. broadcast-dhcp-discover Sends a DHCP request to the broadcast address (255. 255. 255. 255) and reports the results. The script uses a static MAC address (DE: AD: CO: DE: CA: FE) while doing so in order to prevent scope exhaustion. broadcast-dhcp6-discover

Sends a DHCPv6 request (Solicit) to the DHCPv6 multicast address, parses the response, then extracts and prints the address along with any options returned by the server. broadcast-dns-service-discovery Attempts to discover hosts' services using the DNS Service Discovery protocol. It sends a multicast DNS-SD query and collects all the responses. broadcast-dropbox-listener Listens for the LAN sync information broadcasts that the Dropbox. com client broadcasts every 20 seconds, then prints all the discovered client IP addresses, port numbers, version numbers, display names, and more. broadcast-eigrp-discovery

Performs network discovery and routing information gathering through Cisco's Enhanced Interior Gateway Routing Protocol (EIGRP). broadcast-igmp-discovery Discovers targets that have IGMP Multicast memberships and grabs interesting information. broadcast-listener Sniffs the network for incoming broadcast communication and attempts to decode the received packets. It supports protocols like CDP, HSRP, Spotify, DropBox, DHCP, ARP and a few more. See packetdecoders. lua for more information. broadcast-ms-sql-discover Discovers Microsoft SQL servers in the same broadcast domain. broadcast-netbios-master-browser

Attempts to discover master browsers and the domains they manage. broadcast-networker-discover Discovers EMC Networker backup software servers on a LAN by sending a network broadcast query. broadcast-novell-locate Attempts to use the Service Location Protocol to discover Novell NetWare Core Protocol (NCP) servers. broadcast-pc-anywhere Sends a special broadcast probe to discover PC-Anywhere hosts running on a LAN. broadcast-pc-duo Discovers PC-DUO remote control hosts and gateways running on a LAN by sending a special broadcast UDP probe. broadcast-pim-discovery Discovers routers that are running PIM (Protocol Independent Multicast). roadcast-ping Sends broadcast pings on a selected interface using raw ethernet packets and outputs the responding hosts' IP and MAC addresses or (if requested) adds them as targets. Root privileges on UNIX are required to run this script since it uses raw sockets. Most operating systems don't respond to broadcast-ping probes, but they can be configured to do so. broadcast-pppoe-discover Discovers PPPoE (Point-to-Point Protocol over Ethernet) servers using the PPPoE Discovery protocol (PPPoED). PPPoE is an ethernet based protocol so the script has to know what ethernet interface to use for discovery.

If no interface is specified, requests are sent out on all available interfaces. broadcast-rip-discover Discovers hosts and routing information from devices running RIPv2 on the LAN. It does so by sending a RIPv2 Request command and collects the responses from all devices responding to the request. broadcast-ripng-discover Discovers hosts and routing information from devices running RIPng on the LAN by sending a broadcast RIPng Request command and collecting any responses. broadcast-sybase-asa-discover

Discovers Sybase Anywhere servers on the LAN by sending broadcast discovery messages. broadcast-tellstick-discover

Discovers Telldus Technologies TellStickNet devices on the LAN. The Telldus TellStick is used to wirelessly control electric devices such as lights, dimmers and electric outlets. For more information: http://www. telldus. com/ broadcast-upnp-info Attempts to extract system information from the UPnP service by sending a multicast query, then collecting, parsing, and displaying all responses. broadcast-versant-locate Discovers Versant object databases using the broadcast srvloc protocol. broadcast-wake-on-lan Wakes a remote system up from sleep by sending a Wake-On-Lan packet. broadcast-wpad-discover

Retrieves a list of proxy servers on a LAN using the Web Proxy Autodiscovery Protocol (WPAD). It implements both the DHCP and DNS methods of doing so and starts by querying DHCP to get the address. DHCP discovery requires nmap to be running in privileged mode and will be skipped when this is not the case. DNS discovery relies on the script being able to resolve the local domain either through a script argument or by attempting to reverse resolve the local IP. broadcast-wsdd-discover Uses a multicast query to discover devices supporting the Web Services Dynamic Discovery (WS-Discovery) protocol.

It also attempts to locate any published Windows Communication Framework (WCF) web services (. NET 4. 0 or later). broadcast-xdmcp-discover Discovers servers running the X Display Manager Control Protocol (XDMCP) by sending a XDMCP broadcast request to the LAN. Display managers allowing access are marked using the keyword Willing in the result. cassandra-brute

Performs brute force password auditing against the Cassandra database. cassandra-info Attempts to get basic info and server status from a Cassandra database. cccam-version Detects the CCcam service (software for sharing subscription TV among multiple receivers). itrix-brute-xml Attempts to guess valid credentials for the Citrix PN Web Agent XML Service. The XML service authenticates against the local Windows server or the Active Directory. citrix-enum-apps Extracts a list of published applications from the ICA Browser service. citrix-enum-apps-xml Extracts a list of applications, ACLs, and settings from the Citrix XML service. citrix-enum-servers Extracts a list of Citrix servers from the ICA Browser service. citrix-enum-servers-xml Extracts the name of the server farm and member servers from Citrix XML service. couchdb-databases Gets database tables from a CouchDB database. ouchdb-stats Gets database statistics from a CouchDB database. creds-summary Lists all discovered credentials (e. g. from brute force and default password checking scripts) at end of scan. cups-info Lists printers managed by the CUPS printing service. cups-queue-info Lists currently queued print jobs of the remote CUPS service grouped by printer. cvs-brute Performs brute force password auditing against CVS pserver authentication. cvs-brute-repository Attempts to guess the name of the CVS repositories hosted on the remote server. With knowledge of the correct repository name, usernames and passwords can be guessed. aap-get-library Retrieves a list ofmusicfrom a DAAP server. The list includes artist names and album and song titles. daytime Retrieves the day and time from the Daytime service. db2-das-info Connects to the IBM DB2 Administration Server (DAS) on TCP or UDP port 523 and exports the server profile. No authentication is required for this

request. db2-discover Attempts to discover DB2 servers on the network by querying open ibm-db2 UDP ports (normally port 523). dhcp-discover Sends a DHCPINFORM request to a host on UDP port 67 to obtain all the local configuration parameters without allocating a new address. ict-info Connects to a dictionary server using the DICT protocol, runs the SHOW SERVER command, and displays the result. The DICT protocol is defined in RFC 2229 and is a protocol which allows a client to query a dictionary server for definitions from a set of natural language dictionary databases. distcc-cve2004-2687 Detects and exploits a remote code execution vulnerability in the distributed compiler daemon distcc. The vulnerability was disclosed in 2002, but is still present in modern implementation due to poor configuration of the service. dns-blacklist

Checks target IP addresses against multiple DNS anti-spam and open proxy blacklists and returns a list of services for which an IP has been flagged. Checks may be limited by service category (eg: SPAM, PROXY) or to a specific service name. dns-brute Attempts to enumerate DNS hostnames by brute force guessing of common subdomains. dns-cache-snoop Performs DNS cache snooping against a DNS server. dns-check-zone Checks DNS zone configuration against best practices, including RFC 1912. The configuration checks are divided into categories which each have a number of different tests. dns-client-subnet-scan

Performs a domain lookup using the edns-client-subnet option which allows clients to specify the subnet that queries supposedly originate from. The script uses this option to supply a number of geographically distributed locations in an attempt to enumerate as many different address records as

possible. The script also supports requests using a given subnet. dns-fuzz Launches a DNS fuzzing attack against DNS servers. dns-ip6-arpa-scan Performs a quick reverse DNS lookup of an IPv6 network using a technique which analyzes DNS server response codes to dramatically reduce the number of queries needed to enumerate large networks. ns-nsec-enum Enumerates DNS names using the DNSSEC NSEC-walking technique. dns-nsec3-enum Tries to enumerate domain names from the DNS server that supports DNSSEC NSEC3 records. dns-nsid Retrieves information from a DNS nameserver by requesting its nameserver ID (nsid) and asking for its id. server and version. bind values. This script performs the same queries as the following two dig commands: - dig CH TXT bind. version @target - dig +nsid CH TXT id. server @target dns-random-srcport Checks a DNS server for the predictable-port recursion vulnerability.

Predictable source ports can make a DNS server vulnerable to cache poisoning attacks (see CVE-2008-1447). dns-random-txid Checks a DNS server for the predictable-TXID DNS recursion vulnerability. Predictable TXID values can make a DNS server vulnerable to cache poisoning attacks (see CVE-2008-1447). dns-recursion Checks if a DNS server allows queries for third-party names. It is expected that recursion will be enabled on your own internal nameservers. dns-service-discovery Attempts to discover target hosts' services using the DNS Service Discovery protocol. dns-srv-enum Enumerates various common service (SRV) records for a given domain name.

The service records contain the hostname, port and priority of servers for a given service. The following services are enumerated by the script: - Active

Directory Global Catalog - Exchange Autodiscovery - Kerberos KDC Service - Kerberos Passwd Change Service - LDAP Servers - SIP Servers - XMPP S2S - XMPP C2S dns-update Attempts to perform a dynamic DNS update without authentication. dns-zeustracker Checks if the target IP range is part of a Zeus botnet by querying ZTDNS @ abuse. ch. Please review the following information before you start to scan: https://zeustracker. abuse. ch/ztdns. php dns-zone-transfer

Requests a zone transfer (AXFR) from a DNS server. domcon-brute Performs brute force password auditing against the Lotus Domino Console. domcon-cmd Runs a console command on the Lotus Domino Console using the given authentication credentials (see also: domcon-brute) domino-enum-users Attempts to discover valid IBM Lotus Domino users and download their ID files by exploiting the CVE-2006-5835 vulnerability. dpap-brute Performs brute force password auditing against an iPhoto Library. drda-brute Performs password guessing against databases supporting the IBM DB2 protocol such as Informix, DB2 and Derby drda-info

Attempts to extract information from database servers supporting the DRDA protocol. The script sends a DRDA EXCSAT (exchange server attributes) command packet and parses the response. duplicates Attempts to discover multihomed systems by analysing and comparing information collected by other scripts. The information analyzed currently includes, SSL certificates, SSH host keys, MAC addresses, and Netbios server names. eap-info Enumerates the authentication methods offered by an EAP (Extensible Authentication Protocol) authenticator for a given identity or for the anonymous identity if no argument is passed. pmd-info Connects to Erlang

Port Mapper Daemon (epmd) and retrieves a list of nodes with their respective port numbers. eppc-enum-processes Attempts to enumerate process info over the Apple Remote Event protocol. When accessing an application over the Apple Remote Event protocol the service responds with the uid and pid of the application, if it is running, prior to requesting authentication. finger Attempts to retrieve a list of usernames using the finger service. firewalk Tries to discover firewall rules using an IP TTL expiration technique known as firewalking. firewall-bypass

Detects a vulnerability in netfilter and other firewalls that use helpers to dynamically open ports for protocols such as ftp and sip. flume-master-info Retrieves information from Flume master HTTP pages. ftp-anon Checks if an FTP server allows anonymous logins. ftp-bounce Checks to see if an FTP server allows port scanning using the FTP bounce method. ftp-brute Performs brute force password auditing against FTP servers. ftp-libopie Checks if an FTPd is prone to CVE-2010-1938 (OPIE off-by-one stack overflow), a vulnerability discovered by Maksymilian Arciemowicz and Adam " pi3" Zabrocki. See the advisory at http://nmap. rg/r/fbsd-sa-opie. Be advised that, if launched against a vulnerable host, this script will crash the FTPd. ftp-proftpd-backdoor Tests for the presence of the ProFTPD 1. 3. 3c backdoor reported as OSVDB-ID 69562. This script attempts to exploit the backdoor using the innocuous id command by default, but that can be changed with the ftp-proftpd-backdoor. cmd script argument. ftp-vsftpd-backdoor Tests for the presence of the vsFTPd 2. 3. 4 backdoor reported on 2011-07-04 (CVE-2011-2523). This script attempts to exploit the backdoor using the innocuous id command by default, but that can be changed with the exploit. md or ftp-

vsftpd-backdoor. cmd script arguments. ftp-vuln-cve2010-4221 Checks for a stack-based buffer overflow in the ProFTPD server, version between 1. 3. 2rc3 and 1. 3. 3b. By sending a large number of TELNET_IAC escape sequence, the proftpd process miscalculates the buffer length, and a remote attacker will be able to corrupt the stack and execute arbitrary code within the context of the proftpd process (CVE-2010-4221). Authentication is not required to exploit this vulnerability. ganglia-info Retrieves system information (OS version, available memory, etc. from a listening Ganglia Monitoring Daemon or Ganglia Meta Daemon. giop-info Queries a CORBA naming server for a list of objects. gkrellm-info Queries a GKRellM service for monitoring information. A single round of collection is made, showing a snapshot of information at the time of the request. gopher-ls Lists files and directories at the root of a gopher service. gpsd-info Retrieves GPS time, coordinates and speed from the GPSD network daemon. hadoop-datanode-info Discovers information such as log directories from an Apache Hadoop DataNode HTTP status page. hadoop-jobtracker-info

Retrieves information from an Apache Hadoop JobTracker HTTP status page. hadoop-namenode-info Retrieves information from an Apache Hadoop NameNode HTTP status page. hadoop-secondary-namenode-info Retrieves information from an Apache Hadoop secondary NameNode HTTP status page. hadoop-tasktracker-info Retrieves information from an Apache Hadoop TaskTracker HTTP status page. hbase-master-info Retrieves information from an Apache HBase (Hadoop database) master HTTP status page. hbase-region-info Retrieves information from an Apache HBase (Hadoop database) region server HTTP status page. hddtemp-info

Reads hard disk information (such as brand, model, and sometimes temperature) from a listening hddtemp service. hostmap-bfk Discovers hostnames that resolve to the target's IP address by querying the online database at http://www. bfk. de/bfk_dnslogger. html. hostmap-robtex Discovers hostnames that resolve to the target's IP address by querying the online Robtex service at http://ip. robtex. com/. http-affiliate-id Grabs affiliate network IDs (e. g. GoogleAdSense or Analytics, Amazon Associates, etc.) from a web page. These can be used to identify pages with the same owner. http-apache-negotiation

Checks if the target http server has mod_negotiation enabled. This feature can be leveraged to find hidden resources and spider a web site using fewer requests. http-auth Retrieves the authentication scheme and realm of a web service that requires authentication. http-auth-finder Spiders a web site to find web pages requiring form-based or HTTP-based authentication. The results are returned in a table with each url and the detected method. http-awstatstotals-exec Exploits a remote code execution vulnerability in Awstats Totals 1. 0 up to 1. 14 and possibly other products based on it (CVE: 2008-3922). ttp-axis2-dir-traversal Exploits a directory traversal vulnerability in Apache Axis2 version 1. 4. 1 by sending a specially crafted request to the parameter xsd (OSVDB-59001). By default it will try to retrieve the configuration file of the Axis2 service '/conf/axis2. xml' using the path '/axis2/services/' to return the username and password of the admin account. http-backup-finder Spiders a website and attempts to identify backup copies of discovered files. It does so by requesting a number of different

combinations of the filename (eg. index. bak, index. html~, copy of index. html). http-barracuda-dir-traversal

Attempts to retrieve the configuration settings from a Barracuda Networks Spam & Virus Firewall device using the directory traversal vulnerability described at http://seclists. org/fulldisclosure/2010/Oct/119. http-brute Performs brute force password auditing against http basic authentication. http-cakephp-version Obtains the CakePHP version of a web application built with the CakePHP framework by fingerprinting default files shipped with the CakePHP framework. http-chrono Measures the time a website takes to deliver a web page and returns the maximum, minimum and average time it took to fetch a page. ttp-config-backup Checks for backups and swap files of common content management system and web server configuration files. http-cors Tests an http server for Cross-Origin Resource Sharing (CORS), a way for domains to explicitly opt in to having certain methods invoked by another domain. http-date Gets the date from HTTP-like services. Also prints how much the date differs from local time. Local time is the time the HTTP request was sent, so the difference includes at least the duration of one RTT. http-default-accounts Tests for access with default credentials used by a variety of web applications and devices. ttp-domino-enum-passwords Attempts to enumerate the hashed Domino Internet Passwords that are (by default) accessible by all authenticated users. This script can also download any Domino ID Files attached to the Person document. http-drupal-enum-users Enumerates Drupal users by exploiting a an information disclosure vulnerability in Views, Drupal's most popular module. http-drupal-modules Enumerates the installed Drupal modules by using a list of known modules.

http-email-harvest Spiders a web site and collects e-mail addresses. http-enum Enumerates directories used by popular web applications and servers. ttp-exif-spider Spiders a site's images looking for interesting exif data embedded in . jpg files. Displays the make and model of the camera, the date thephotowas taken, and the embedded geotag information. http-favicon Gets the favicon (" favorites icon") from a web page and matches it against a database of the icons of known web applications. If there is a match, the name of the application is printed; otherwise the MD5 hash of the icon data is printed. http-form-brute Performs brute force password auditing against http form-based authentication. http-form-fuzzer

Performs a simple form fuzzing against forms found on websites. Tries strings and numbers of increasing length and attempts to determine if the fuzzing was successful. http-frontpage-login Checks whether target machines are vulnerable to anonymous Frontpage login. http-generator Displays the contents of the " generator" meta tag of a web page (default: /) if there is one. http-git Checks for a Git repository found in a website's document root /. git/) and retrieves as much repo information as possible, including language/framework, remotes, last commit message, and repository description. http-gitweb-projects-enum

Retrieves a list of Git projects, owners and descriptions from a gitweb (web interface to the Git revision control system). http-google-malware Checks if hosts are on Google's blacklist of suspected malware and phishing servers. These lists are constantly updated and are part of Google's Safe Browsing service. http-grep Spiders a website and attempts to match all pages and urls against a given string. Matches are counted and grouped per url under

which they were discovered. http-headers Performs a HEAD request for the root folder ("/") of a web server and displays the HTTP headers returned. http-huawei-hg5xx-vuln

Detects Huawei modems models HG530x, HG520x, HG510x (and possibly others...) vulnerable to a remote credential and information disclosure vulnerability. It also extracts the PPPoE credentials and other interesting configuration values. http-icloud-findmyiphone Retrieves the locations of all " Find my iPhone" enabled iOS devices by querying the MobileMe web service (authentication required). http-icloud-sendmsg Sends a message to a iOS device through the Apple MobileMe web service. The device has to be registered with an Apple ID using the Find My Iphone application. http-iis-webdav-vuln Checks for a vulnerability in IIS 5. /6. 0 that allows arbitrary users to access secured WebDAV folders by searching for a password-protected folder and attempting to access it. This vulnerability was patched in Microsoft Security Bulletin MS09-020, http://nmap. org/r/ms09-020. http-joomla-brute Performs brute force password auditing against Joomla web CMS installations. http-litespeed-sourcecode-download Exploits a null-byte poisoning vulnerability in Litespeed Web Servers 4. 0. x before 4. 0. 15 to retrieve the target script's source code by sending a HTTP request with a null byte followed by a . txt file extension (CVE-2010-2333). ttp-majordomo2-dir-traversal Exploits a directory traversal vulnerability existing in Majordomo2 to retrieve remote files. (CVE-2011-0049). http-malware-host Looks for signature of known server compromises. http-method-tamper Attempts to bypass password protected resources (HTTP 401 status) by performing HTTP verb tampering. If an array of paths to check is not set, it will crawl the web

server and perform the check against any password protected resource that it finds. http-methods Finds out what options are supported by an HTTP server by sending an OPTIONS request. Lists potentially risky methods.

Optionally tests each method individually to see if they are subject to e. g. IP address restrictions. http-open-proxy Checks if an HTTP proxy is open. http-open-redirect Spiders a website and attempts to identify open redirects. Open redirects are handlers which commonly take a URL as a parameter and responds with a http redirect (3XX) to the target. Risks of open redirects are described at http://cwe. mitre. org/data/definitions/601. html. http-passwd Checks if a web server is vulnerable to directory traversal by attempting to retrieve /etc/passwd or oot. ini. http-php-version Attempts to retrieve the PHP version from a web server.

PHP has a number of magic queries that return images or text that can vary with the PHP version. This script uses the following queries: /? = PHPE9568F36-D428-11d2-A769-00AA001ACF42: gets a GIF logo, which changes on April Fool's Day. /? = PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: gets an HTML credits page. http-phpself-xss Crawls a web server and attempts to find PHP files vulnerable to reflected cross site scripting via the variable $_SERVER[" PHP_SELF"]. http-proxy-brute Performs brute force password guessing against HTTP proxy servers. http-put Uploads a local file to a remote web server using the HTTP PUT method.

You must specify the filename and URL path with NSE arguments. http-qnap-nas-info Attempts to retrieve the model, firmware version, and enabled services from a QNAP Network Attached Storage (NAS) device. http-rfi-spider Crawls webservers in search of RFI (remote file inclusion) vulnerabilities. It

tests every form field it finds and every parameter of a URL containing a query. http-robots. txt Checks for disallowed entries in /robots. txt on a web server. http-robtex-reverse-ip Obtains up to 100 forward DNS names for a target IP address by querying the Robtex service (http://www. robtex. com/ip/). http-robtex-shared-ns

Finds up to 100 domain names which use the same name server as the target by querying the Robtex service at http://www. robtex. com/dns/. http-sitemap-generator Spiders a web server and displays its directory structure along with number and types of files in each folder. Note that files listed as having an 'Other' extension are ones that have no extension or that are a root document. http-slowloris Tests a web server for vulnerability to the Slowloris DoS attack by launching a Slowloris attack. http-slowloris-check Tests a web server for vulnerability to the Slowloris DoS attack without actually launching a DoS attack. ttp-sql-injection Spiders an HTTP server looking for URLs containing queries vulnerable to an SQL injection attack. It also extracts forms from found websites and tries to identify fields that are vulnerable. http-title Shows the title of the default page of a web server. http-tplink-dir-traversal Exploits a directory traversal vulnerability existing in several TP-Link wireless routers. Attackers may exploit this vulnerability to read any of the configuration and password files remotely and without authentication. http-trace Sends an HTTP TRACE request and shows if the method TRACE is enabled.

If debug is enabled, it returns the header fields that were modified in the response. http-traceroute Exploits the Max-Forwards HTTP header to detect the presence of reverse proxies. http-unsafe-output-escaping Spiders a

website and attempts to identify output escaping problems where content is reflected back to the user. This script locates all parameters, ? x= foo&y= bar and checks if the values are reflected on the page. If they are indeed reflected, the script will try to insert ghz> hzx" zxc'xcv and check which (if any) characters were reflected back onto the page without proper html escaping.

This is an indication of potential XSS vulnerability. http-userdir-enum Attempts to enumerate valid usernames on web servers running with the mod_userdir module or similar enabled. http-vhosts Searches for web virtual hostnames by making a large number of HEAD requests against http servers using common hostnames. http-virustotal Checks whether a file has been determined as malware by Virustotal. Virustotal is a service that provides the capability to scan a file or check a checksum against a number of the major antivirus vendors.

The script uses the public API which requires a valid API key and has a limit on 4 queries per minute. A key can be acquired by registering as a user on the virustotal web page: http://www. virustotal. com http-vlcstreamer-ls Connects to a VLC Streamer helper service and lists directory contents. The VLC Streamer helper service is used by the iOS VLC Streamer application to enable streaming of multimedia content from the remote server to the device. http-vmware-path-vuln Checks for a path-traversal vulnerability in VMWare ESX, ESXi, and Server (CVE-2009-3733). http-vuln-cve2009-3960

Exploits cve-2009-3960 also known as Adobe XML External Entity Injection. http-vuln-cve2010-0738 Tests whether a JBoss target is vulnerable to jmx console authentication bypass (CVE-2010-0738). http-vuln-cve2010-2861

Executes a directory traversal attack against a ColdFusion server and tries to grab the password hash for the administrator user. It then uses the salt value (hidden in the web page) to create the SHA1 HMAC hash that the web server needs for authentication as admin. You can pass this value to the ColdFusion server as the admin without cracking the password hash. ttp-vuln-cve2011-3192 Detects a denial of service vulnerability in the way the Apache web server handles requests for multiple overlapping/simple ranges of a page. http-vuln-cve2011-3368 Tests for the CVE-2011-3368 (Reverse Proxy Bypass) vulnerability in Apache HTTP server's reverse proxy mode. The script will run 3 tests: o the loopback test, with 3 payloads to handle different rewrite rules o the internal hosts test. According to Contextis, we expect a delay before a server error. o The external website test. This does not mean that you can reach a LAN ip, but this is a relevant issue anyway. ttp-vuln-cve2012-1823 Detects PHP-CGI installations that are vulnerable to CVE-2012-1823, This critical vulnerability allows attackers to retrieve source code and execute code remotely. http-waf-detect Attempts to determine whether a web server is protected by an IPS (Intrusion Prevention System), IDS (Intrusion Detection System) or WAF (Web Application Firewall) by probing the web server with malicious payloads and detecting changes in the response code and body. http-waf-fingerprint Tries to detect the presence of a web application firewall and its type and version. http-wordpress-brute erforms brute force password auditing against Wordpress CMS/blog installations. http-wordpress-enum Enumerates usernames in Wordpress blog/CMS installations by exploiting an information disclosure vulnerability existing in versions 2. 6, 3. 1, 3. 1. 1, 3. 1. 3 and 3. 2-beta2 and possibly

others. http-wordpress-plugins Tries to obtain a list of installed WordPress plugins by brute force testing for known plugins. iax2-brute Performs brute force password auditing against the Asterisk IAX2 protocol. Guessing fails when a large number of attempts is made due to the maxcallnumber limit (default 2048).

In case your getting " ERROR: Too many retries, aborted ... " after a while, this is most likely what's happening. In order to avoid this problem try: - reducing the size of your dictionary - use the brute delay option to introduce a delay between guesses - split the guessing up in chunks and wait for a while between them iax2-version Detects the UDP IAX2 service. icap-info Tests a list of known ICAP service names and prints information about any it detects. The Internet Content Adaptation Protocol (ICAP) is used to extend transparent proxy servers and is generally used for content filtering and antivirus scanning. ke-version Get information from an IKE service. Tests the service with both Main and Aggressive Mode. Sends multiple transforms in a single request, so currently, only four packets are sent to the host. imap-brute Performs brute force password auditing against IMAP servers using either LOGIN, PLAIN, CRAM-MD5, DIGEST-MD5 or NTLM authentication. imap-capabilities Retrieves IMAP email server capabilities. informix-brute Performs brute force password auditing against IBM Informix Dynamic Server. informix-query Runs a query against IBM Informix Dynamic Server using the given authentication credentials (see also: informix-brute). nformix-tables Retrieves a list of tables and column definitions for each database on an Informix server. ip-forwarding Detects whether the remote device has ip forwarding or " Internet connection sharing" enabled, by sending an ICMP

echo request to a given target using the scanned host as default gateway. ip-geolocation-geobytes Tries to identify the physical location of an IP address using the Geobytes geolocation web service (http://www. geobytes. com/iplocator. htm). The limit of lookups using this service is 20 requests per hour. Once the limit is reached, an nmap. registry[" ip-geolocation-geobytes"]. blocked oolean is set so no further requests are made during a scan. ip-geolocation-geoplugin Tries to identify the physical location of an IP address using the Geoplugin geolocation web service (http://www. geoplugin. com/). There is no limit on lookups using this service. ip-geolocation-ipinfodb Tries to identify the physical location of an IP address using the IPInfoDB geolocation web service (http://ipinfodb. com/ip_location_api. php). ip-geolocation-maxmind Tries to identify the physical location of an IP address using a Geolocation Maxmind database file (available from http://www. maxmind. com/app/ip-location).

This script supports queries using all Maxmind databases that are supported by their API including the commercial ones. ipidseq Classifies a host's IP ID sequence (test for susceptibility to idle scan). ipv6-node-info Obtains hostnames, IPv4 and IPv6 addresses through IPv6 Node Information Queries. ipv6-ra-flood Generates a flood of Router Advertisements (RA) with random source MAC addresses and IPv6 prefixes. Computers, which have stateless autoconfiguration enabled by default (every major OS), will start to compute IPv6 suffix and update their routing table to reflect the accepted announcement.

This will cause 100% CPU usage on Windows and platforms, preventing to process other application requests. irc-botnet-channels Checks an IRC server

for channels that are commonly used by malicious botnets. irc-brute Performs brute force password auditing against IRC (Internet Relay Chat) servers. irc-info Gathers information from an IRC server. irc-sasl-brute Performs brute force password auditing against IRC (Internet Relay Chat) servers supporting SASL authentication. irc-unrealircd-backdoor Checks if an IRC server is backdoored by running a time-based command (ping) and checking how long it takes to respond. scsi-brute Performs brute force password auditing against iSCSI targets. iscsi-info Collects and displays information from remote iSCSI targets. isns-info Lists portals and iSCSI nodes registered with the Internet Storage Name Service (iSNS). jdwp-exec Attempts to exploit java's remote debugging port. When remote debugging port is left open, it is possible to inject java bytecode and achieve remote code execution. This script abuses this to inject and execute a Java class file that executes the supplied shell command and returns its output. jdwp-info Attempts to exploit java's remote debugging port.

When remote debugging port is left open, it is possible to inject java bytecode and achieve remote code execution. This script injects and execute a Java class file that returns remote system information. jdwp-inject Attempts to exploit java's remote debugging port. When remote debugging port is left open, it is possible to inject java bytecode and achieve remote code execution. This script allows injection of arbitrary class files. jdwp-version Detects the Java Debug Wire Protocol. This protocol is used by Java programs to be debugged via the network.

It should not be open to the public Internet, as it does not provide any security against malicious attackers who can inject their own bytecode into

the debugged process. krb5-enum-users Discovers valid usernames by brute force querying likely usernames against a Kerberos service. When an invalid username is requested the server will responde using the Kerberos error code KRB5KDC_ERR_C_PRINCIPAL_UNKNOWN, allowing us to determine that the user name was invalid. Valid user names will illicit either the TGT in a AS-REP response or the error KRB5KDC_ERR_PREAUTH_REQUIRED, signaling that the user is required to perform pre authentication. dap-brute Attempts to brute-force LDAP authentication. By default it uses the built-in username and password lists. In order to use your own lists use the userdb and passdb script arguments. ldap-novell-getpass Universal Password enables advanced password policies, including extended characters in passwords, synchronization of passwords from eDirectory to other systems, and a single password for all access to eDirectory. ldap-rootdse Retrieves the LDAP root DSA-specific Entry (DSE) ldap-search Attempts to perform an LDAP search and returns all matches. lexmark-config Retrieves configuration information from a Lexmark S300-S400 printer. lmnr-resolve Resolves a hostname by using the LLMNR (Link-Local Multicast Name Resolution) protocol. lltd-discovery Uses the Microsoft LLTD protocol to discover hosts on a local network. maxdb-info Retrieves version and database information from a SAP Max DB database. mcafee-epo-agent Check if ePO agent is running on port 8081 or port identified as ePO Agent port. membase-brute Performs brute force password auditing against Couchbase Membase servers. membase-http-info Retrieves information (hostname, OS, uptime, etc.) from the CouchBase Web Administration port. The information retrieved by this script does not require any credentials. emcached-info Retrieves information

(including system architecture, process ID, and server time) from distributed memory object caching system memcached. metasploit-info Gathers info from the Metasploit rpc service. It requires a valid login pair. After authentication it tries to determine Metasploit version and deduce the OS type. Then it creates a new console and executes few commands to get additional info. References: * http://wiki. msgpack. org/display/MSGPACK/Format+specification * https://community. rapid7. com/docs/DOC-1516 Metasploit RPC API Guide metasploit-msgrpc-brute

Performs brute force username and password auditing against Metasploit msgrpc interface. metasploit-xmlrpc-brute Performs brute force password auditing against a Metasploit RPC server using the XMLRPC protocol. mmouse-brute Performs brute force password auditing against the RPA Tech Mobile Mouse servers. mmouse-exec Connects to an RPA Tech Mobile Mouse server, starts an application and sends a sequence of keys to it. Any application that the user has access to can be started and the key sequence is sent to the application after it has been started. modbus-discover Enumerates SCADA Modbus slave ids (sids) and collects their device information. ongodb-brute Performs brute force password auditing against the MongoDB database. mongodb-databases Attempts to get a list of tables from a MongoDB database. mongodb-info Attempts to get build info and server status from a MongoDB database. mrinfo Queries targets for multicast routing information. ms-sql-brute Performs password guessing against Microsoft SQL Server (ms-sql). Works best in conjunction with the broadcast-ms-sql-discover script. ms-sql-config Queries Microsoft SQL Server (ms-sql)

instances for a list of databases, linked servers, and configuration settings. ms-sql-dac

Queries the Microsoft SQL Browser service for the DAC (Dedicated Admin Connection) port of a given (or all) SQL Server instance. The DAC port is used to connect to the database instance when normal connection attempts fail, for example, when server is hanging, out of memory or in other bad states. In addition, the DAC port provides an admin with access to system objects otherwise not accessible over normal connections. ms-sql-dump-hashes Dumps the password hashes from an MS-SQL server in a format suitable for cracking by tools such as John-the-ripper. In order to do so the user needs to have the appropriate DB privileges. s-sql-empty-password Attempts to authenticate to Microsoft SQL Servers using an empty password for the sysadmin (sa) account. ms-sql-hasdbaccess Queries Microsoft SQL Server (ms-sql) instances for a list of databases a user has access to. ms-sql-info Attempts to determine configuration and version information for Microsoft SQL Server instances. ms-sql-query Runs a query against Microsoft SQL Server (ms-sql). ms-sql-tables Queries Microsoft SQL Server (ms-sql) for a list of tables per database. ms-sql-xp-cmdshell Attempts to run a command using the command shell of Microsoft SQL Server (ms-sql). msrpc-enum

Queries an MSRPC endpoint mapper for a list of mapped services and displays the gathered information. mtrace Queries for the multicast path from a source to a destination host. murmur-version Detects the Murmur service (server for the Mumble voice communication client) version 1. 2. 0 and above. mysql-audit Audits MySQL database server security configuration against parts of the CIS MySQL v1. 0. 2 benchmark (the engine can be used

for other MySQL audits by creating appropriate audit files). mysql-brute Performs password guessing against MySQL. mysql-databases Attempts to list all databases on a MySQL server. mysql-dump-hashes

Dumps the password hashes from an MySQL server in a format suitable for cracking by tools such as John the Ripper. Appropriate DB privileges (root) are required. mysql-empty-password Checks for MySQL servers with an empty password for root or anonymous. mysql-enum Performs valid user enumeration against MySQL server. mysql-info Connects to a MySQL server and prints information such as the protocol and version numbers, thread ID, status, capabilities, and the password salt. mysql-query Runs a query against a MySQL database and returns the results as a table. mysql-users Attempts to list all users on a MySQL server. mysql-variables

Attempts to show all variables on a MySQL server. mysql-vuln-cve2012-2122 nat-pmp-info Get's the routers WAN IP using the NAT Port Mapping Protocol (NAT-PMP). The NAT-PMP protocol is supported by a broad range of routers including: - Apple AirPort Express - Apple AirPort Extreme - Apple Time Capsule - DD-WRT - OpenWrt v8. 09 or higher, with MiniUPnP daemon - pfSense v2. 0 - Tarifa (firmware) (Linksys WRT54G/GL/GS) - Tomato Firmware v1. 24 or higher. (Linksys WRT54G/GL/GS and many more) - Peplink Balance nat-pmp-mapport Maps a WAN port on the router to a local port on the client using the NAT Port Mapping Protocol (NAT-PMP).

It supports the following operations: o map - maps a new external port on the router to an internal port of the requesting IP o unmap - unmaps a previously mapped port for the requesting IP o unmapall - unmaps all previously mapped ports for the requesting IP nbstat Attempts to retrieve

the target's NetBIOS names and MAC address. ncp-enum-users Retrieves a list of all eDirectory users from the Novell NetWare Core Protocol (NCP) service. ncp-serverinfo Retrieves eDirectory server information (OS version, server name, mounts, etc.) from the Novell NetWare Core Protocol (NCP) service. ndmp-fs-info

Lists remote file systems by querying the remote device using the Network Data Management Protocol (ndmp). NDMP is a protocol intended to transport data between a NAS device and the backup device, removing the need for the data to pass through the backup server. The following products are known to support the protocol: Amanda Bacula CA Arcserve CommVault Simpana EMC Networker Hitachi Data Systems IBM Tivoli Quest Software Netvault Backup Symantec Netbackup Symantec Backup Exec ndmp-version Retrieves version information from the remote Network Data Management Protocol (ndmp) service.

NDMP is a protocol intended to transport data between a NAS device and the backup device, removing the need for the data to pass through the backup server. The following products are known to support the protocol: Amanda Bacula CA Arcserve CommVault Simpana EMC Networker Hitachi Data Systems IBM Tivoli Quest Software Netvault Backup Symantec Netbackup Symantec Backup Exec nessus-brute Performs brute force password auditing against a Nessus vulnerability scanning daemon using the NTP 1. 2 protocol. nessus-xmlrpc-brute Performs brute force password auditing against a Nessus vulnerability scanning daemon using the XMLRPC protocol. etbus-auth-bypass Checks if a NetBus server is vulnerable to an authentication bypass vulnerability which allows full access without knowing the password.

netbus-brute Performs brute force password auditing against the Netbus backdoor (" remote administration") service. netbus-info Opens a connection to a NetBus server and extracts information about the host and the NetBus service itself. netbus-version Extends version detection to detect NetBuster, a honeypot service that mimes NetBus. nexpose-brute Performs brute force password auditing against a Nexpose vulnerability scanner using the API 1. 1.

By default it only tries three guesses per username to avoid target account lockout. nfs-ls Attempts to get useful information about files from NFS exports. The output is intended to resemble the output of ls. nfs-showmount Shows NFS exports, like the showmount -e command. nfs-statfs Retrieves disk space statistics and information from a remote NFS share. The output is intended to resemble the output of df. nping-brute Performs brute force password auditing against an Nping Echo service. nrpe-enum Queries Nagios Remote Plugin Executor (NRPE) daemons to obtain information such as load averages, process counts, logged in user information, etc. tp-info Gets the time and configuration variables from an NTP server. We send two requests: a time request and a " read variables" (opcode 2) control message. Without verbosity, the script shows the time and the value of the version, processor, system, refid, and stratum variables. With verbosity, all variables are shown. ntp-monlist Obtains and prints an NTP server's monitor data. omp2-brute Performs brute force password auditing against the OpenVAS manager using OMPv2. omp2-enum-targets Attempts to retrieve the list of target systems and networks from an OpenVAS Manager server. openlookup-info

Parses and displays the banner information of an OpenLookup (network key-value store) server. openvas-otp-brute Performs brute force password auditing against a OpenVAS vulnerability scanner daemon using the OTP 1. 0 protocol. oracle-brute Performs brute force password auditing against Oracle servers. oracle-brute-stealth Exploits the CVE-2012-3137 vulnerability, a weakness in Oracle's O5LOGIN authentication scheme. The vulnerability exists in Oracle 11g R1/R2 and allows linking the session key to a password hash. When initiating an authentication attempt as a valid user the server will respond with a session key and salt.

Once received the script will disconnect the connection thereby not recording the login attempt. The session key and salt can then be used to brute force the users password. oracle-enum-users Attempts to enumerate valid Oracle user names against unpatched Oracle 11g servers (this bug was fixed in Oracle's October 2009 Critical Patch Update). oracle-sid-brute Guesses Oracle instance/SID names against the TNS-listener. ovs-agent-version Detects the version of an Oracle Virtual Server Agent by fingerprinting responses to an HTTP GET request and an XML-RPC method call. p2p-conficker Checks if a host is infected with Conficker.

C or higher, based on Conficker's peer to peer communication. path-mtu Performs simple Path MTU Discovery to target hosts. pcanywhere-brute Performs brute force password auditing against the pcAnywhere remote access protocol. pgsql-brute Performs password guessing against PostgreSQL. pjl-ready-message Retrieves or sets the ready message on printers that support the Printer Job Language. This includes most PostScript printers that listen on port 9100. Without an argument, displays the current

ready message. With the pjl_ready_message script argument, displays the old ready message and changes it to the message given. op3-brute Tries to log into a POP3 account by guessing usernames and passwords. pop3-capabilities Retrieves POP3 email server capabilities. pptp-version Attempts to extract system information from the point-to-point tunneling protocol (PPTP) service. qscan Repeatedly probe open and/or closed ports on a host to obtain a series of round-trip time values for each port. These values are used to group collections of ports which are statistically different from other groups. Ports being in different groups (or " families") may be due to network mechanisms such as port forwarding to machines behind a NAT. quake3-info

Extracts information from a Quake3 game server and other games which use the same protocol. quake3-master-getservers Queries Quake3-style master servers for game servers (many games other than Quake 3 use this same protocol). rdp-enum-encryption Determines which Security layer and Encryption level is supported by the RDP service. It does so by cycling through all existing protocols and ciphers. When run in debug mode, the script also returns the protocols and ciphers that fail and any errors that were reported. rdp-vuln-ms12-020 Checks if a machine is vulnerable to MS12-020 RDP vulnerability. realvnc-auth-bypass

Checks if a VNC server is vulnerable to the RealVNC authentication bypass (CVE-2006-2369). redis-brute Performs brute force passwords auditing against a Redis key-value store. redis-info Retrieves information (such as version number and architecture) from a Redis key-value store. resolveall Resolves hostnames and adds every address (IPv4 or IPv6, depending on Nmap mode) to Nmap's target list. This differs from Nmap's normal host

resolution process, which only scans the first address (A or AAAA record) returned for each host name. reverse-index Creates a reverse index at the end of scan output showing which hosts run a particular service.

This is in addition to Nmap's normal output listing the services on each host. rexec-brute Performs brute force password auditing against the classic UNIX rexec (remote exec) service. riak-http-info Retrieves information (such as node name and architecture) from a Basho Riak distributed database using the HTTP protocol. rlogin-brute Performs brute force password auditing against the classic UNIX rlogin (remote login) service. This script must be run in privileged mode on UNIX because it must bind to a low source port number. rmi-dumpregistry Connects to a remote RMI registry and attempts to dump all of its objects. mi-vuln-classloader Tests whether Java rmiregistry allows class loading. The default configuration of rmiregistry allows loading classes from remote URLs, which can lead to remote code execution. The vendor (Oracle/Sun) classifies this as a design feature. rpc-grind Fingerprints the target RPC port to extract the target service, RPC number and version. rpcap-brute Performs brute force password auditing against the WinPcap Remote Capture Daemon (rpcap). rpcap-info Connects to the rpcap service (provides remote sniffing capabilities through WinPcap) and retrieves interface information.

The service can either be setup to require authentication or not and also supports IP restrictions. rpcinfo Connects to portmapper and fetches a list of all registered programs. It then prints out a table including (for each program) the RPC program number, supported version numbers, port number and protocol, and program name. rsync-brute Performs brute force

password auditing against the rsync remote file syncing protocol. rsync-list-modules Lists modules available for rsync (remote file sync) synchronization. rtsp-methods Determines which methods are supported by the RTSP (real time streaming protocol) server. tsp-url-brute Attempts to enumerate RTSP media URLS by testing for common paths on devices such as surveillance IP cameras. samba-vuln-cve-2012-1182 Checks if target machines are vulnerable to the Samba heap overflow vulnerability CVE-2012-1182. servicetags Attempts to extract system information (OS, hardware, etc.) from the Sun Service Tags service agent (UDP port 6481). sip-brute Performs brute force password auditing against Session Initiation Protocol (SIP - http://en. wikipedia. org/wiki/Session_Initiation_Protocol) accounts. This protocol is most commonly associated with VoIP sessions. ip-call-spoof Spoofs a call to a SIP phone and detects the action taken by the target (busy, declined, hung up, etc.) sip-enum-users Enumerates a SIP server's valid extensions (users). sip-methods Enumerates a SIP Server's allowed methods (INVITE, OPTIONS, SUBSCRIBE, etc.) skypev2-version Detects the Skype version 2 service. smb-brute Attempts to guess username/password combinations over SMB, storing discovered combinations for use in other scripts. Every attempt will be made to get a valid list of users and to verify each username before actually using them.

When a username is discovered, besides being printed, it is also saved in the Nmap registry so other Nmap scripts can use it. That means that if you're going to run smb-brute. nse, you should run other smb scripts you want. This checks passwords in a case-insensitive way, determining case after a password is found, for Windows versions before Vista. smb-check-vulns

Checks for vulnerabilities: MS08-067, a Windows RPC vulnerability Conficker, an infection by the Conficker worm Unnamed regsvc DoS, a denial-of-service vulnerability I accidentally found in Windows 2000 SMBv2 exploit (CVE-2009-3103, Microsoft Security Advisory 75497) MS06-025, a Windows Ras RPC service vulnerability MS07-029, a Windows Dns Server RPC service vulnerability smb-enum-domains Attempts to enumerate domains on a system, along with their policies. This generally requires credentials, except against Windows 2000. In addition to the actual domain, the " Builtin" domain is generally displayed. Windows returns this in the list of domains, but its policies don't appear to be used anywhere. smb-enum-groups Obtains a list of groups from the remote Windows system, as well as a list of the group's users. This works similarly to enum. exe with the /G switch. smb-enum-processes

Pulls a list of processes from the remote server over SMB. This will determine all running processes, their process IDs, and their parent processes. It is done by querying the remote registry service, which is disabled by default on Vista; on all other Windows versions, it requires Administrator privileges. smb-enum-sessions Enumerates the users logged into a system either locally or through an SMB share. The local users can be logged on either physically on the machine, or through a terminal services session. Connections to a SMB share are, for example, people connected to fileshares or making RPC calls.

Nmap's connection will also show up, and is generally identified by the one that connected " 0 seconds ago". smb-enum-shares Attempts to list shares using the srvsvc. NetShareEnumAll MSRPC function and retrieve more

information about them using srvsvc. NetShareGetInfo. If access to those functions is denied, a list of common share names are checked. smb-enum-users Attempts to enumerate the users on a remote Windows system, with as much information as possible, through two different techniques (both over MSRPC, which uses port 445 or 139; see smb. lua). The goal of this script is to iscover all user accounts that exist on a remote system. This can be helpful for administration, by seeing who has an account on a server, or for penetration testing or network footprinting, by determining which accounts exist on a system. smb-flood Exhausts a remote SMB server's connection limit by by opening as many connections as we can. Most implementations of SMB have a hard global limit of 11 connections for user accounts and 10 connections for anonymous. Once that limit is reached, further connections are denied. This script exploits that limit by taking up all the connections and holding them. smb-ls

Attempts to retrieve useful information about files shared on SMB volumes. The output is intended to resemble the output of the UNIX ls command. smb-mbenum Queries information managed by the Windows Master Browser. smb-os-discovery Attempts to determine the operating system, computer name, domain, workgroup, and current time over the SMB protocol (ports 445 or 139). This is done by starting a session with the anonymous account (or with a proper user account, if one is given; it likely doesn't make a difference); in response to a session starting, the server will send back all this information. smb-print-text