

Managing Penetration Testing Data with Kvasir

Toorcon 15 (San Diego)

@grutz






BACKGROUND

\$ whois grutz

Corporate penetration tester for ~15 years

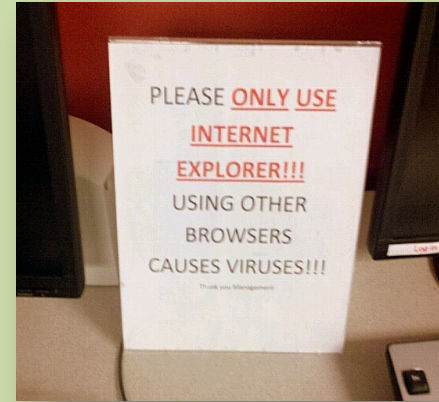
~10 years internal with Federal Reserve and Pacific Gas & Electric

5 years consulting to customers for 

Developed Squirtle, the NTLM Attack tool

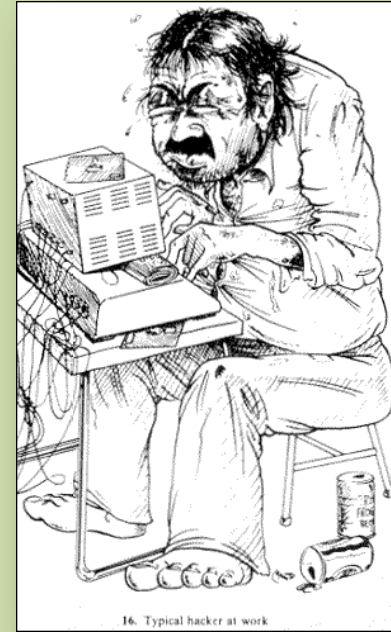
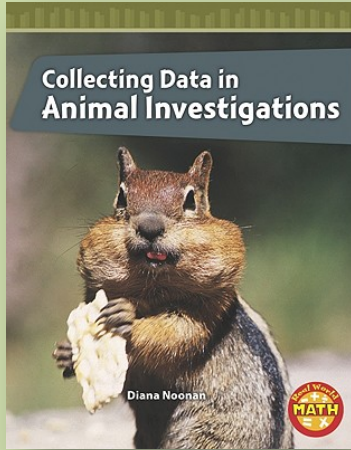
Smashed up some Huawei/H3C/HP gear





DEFINING THE PROBLEM

Testing is all about collecting data...

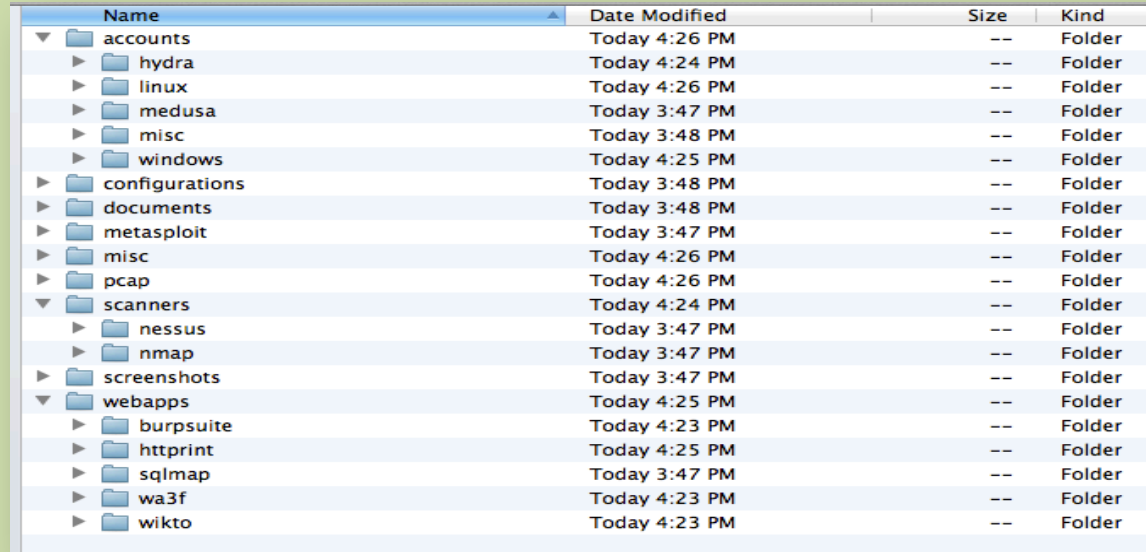


As pentesters we collect a TON of data...



So you sort them into directories...

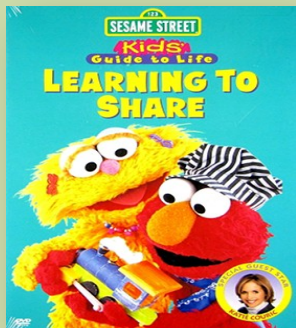
...which can be difficult to manage...



Name	Date Modified	Size	Kind
accounts	Today 4:26 PM	--	Folder
hydra	Today 4:24 PM	--	Folder
linux	Today 4:26 PM	--	Folder
medusa	Today 3:47 PM	--	Folder
misc	Today 3:48 PM	--	Folder
windows	Today 4:25 PM	--	Folder
configurations	Today 3:48 PM	--	Folder
documents	Today 3:48 PM	--	Folder
metasploit	Today 3:47 PM	--	Folder
misc	Today 4:26 PM	--	Folder
pcap	Today 4:26 PM	--	Folder
scanners	Today 4:24 PM	--	Folder
nessus	Today 3:47 PM	--	Folder
nmap	Today 3:47 PM	--	Folder
screenshots	Today 3:47 PM	--	Folder
webapps	Today 4:25 PM	--	Folder
burpsuite	Today 4:23 PM	--	Folder
httpprint	Today 4:25 PM	--	Folder
sqlmap	Today 3:47 PM	--	Folder
wa3f	Today 4:23 PM	--	Folder
wikto	Today 4:23 PM	--	Folder

Sharing data across your team

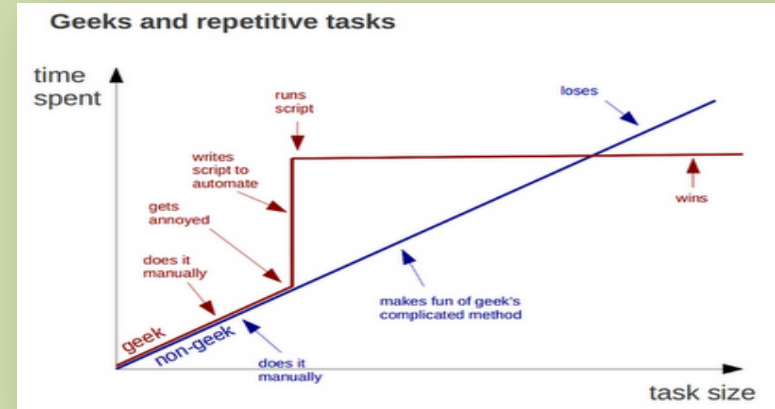
...can have its challenges



Did you get everything you need?

Great! Now write a report, monkey!





CURRENT OPTIONS?

Currently...

- Metasploit Pro, Cobalt Strike, STRATEGIC, CORE, etc
- Nexpose, Nessus, QualysGuard, Saint, Fortigate, etc
- ThreadFix, Archer, RiskIO, Secunia VIM, etc
- Issue / Bug tracking tools (and their wikis)
 - TRAC, Redmine, Bugzilla, etc
- Wikis!
- Spreadsheets!
- Roll your own!

Issues with these tools

- Not designed to manage PT data
 - You have to conform your data to the tool
 - *Vulnerability Management != Penetration Test Data!*
- Requires enhancements / add-ons
 - Develop your own add-ons
 - Maintain support and training
- Changes are difficult to implement
 - No access to source code for when things break
 - High complexity, vendor demands, delays
- “In the cloud” or “vendor hosted” solutions
- Spreadsheets??? Really?!?!



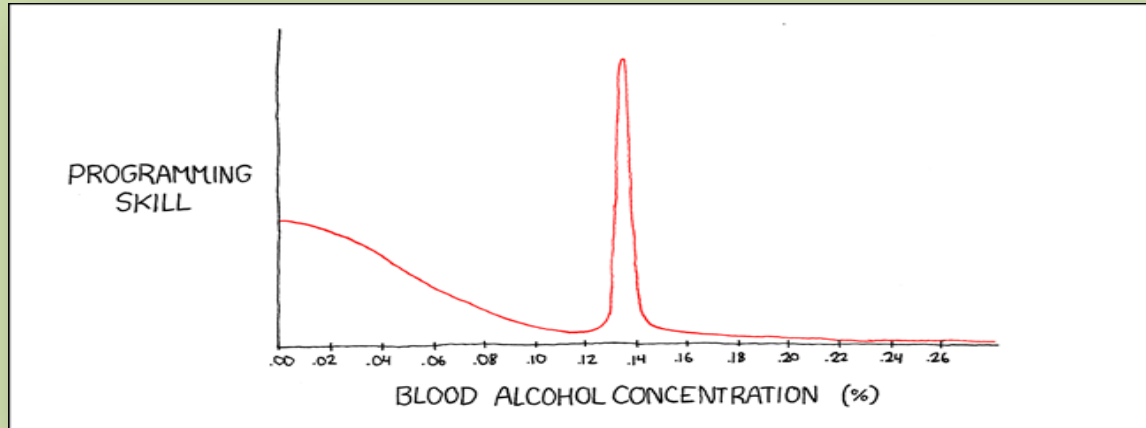
ENTER KVASIR

0118 999 881 999 119 725 3



ACHTUNG!

I am an ADHD coder. Large bits of Kvasir were thought of after working at a customer's site and developed with little sleep and lots of caffeine and/or alcohol. I am also not a really good UI coder.



Kvasir's Cisco Pedigree

- Recognized long ago that managing disparate data is essential to effective testing results
- Began from our acquisition of “The Wheel Group” back in 1999
- Multiple iterations:
 - AttackAll, AutoSPA, Halo/Banshee, AutoSPAng
- Close source / proprietary



Design Philosophy

- Take disparate data and cram it into a (mostly) consistent relational database format.
- Focus on **PENETRATION TEST** tools and data
- Be quick
- Be adaptable
- Try not to get in the way of the hacking
- No cross-contamination of customer data

Benefits to using Kvasir

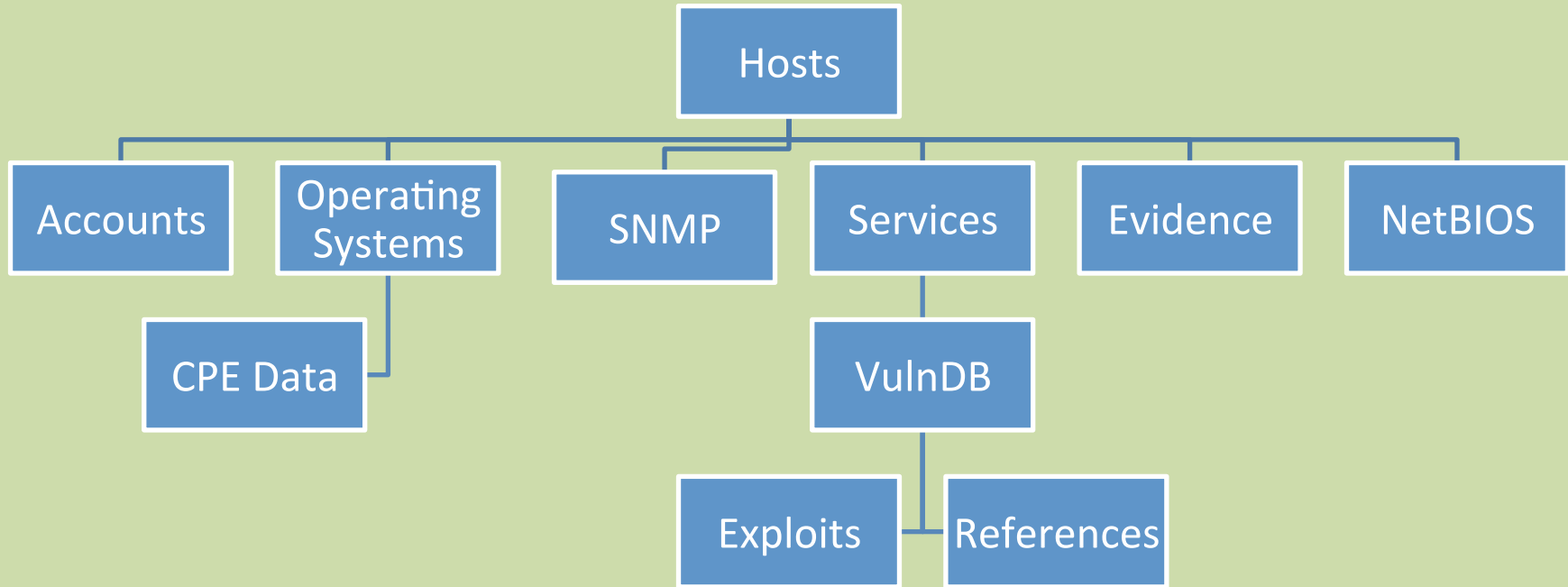
- Alcohol infused coding practices
- Designed by and for Penetration Testers
- **OPEN SOURCE! FREE!!!**
- Data access through web2py shell == awesome!

```
In [34]: fh.seek(0)

In [35]: for z in fh.readlines():
         (ip, port) = z.split(':')
         port = int(port)
         host_rec = db.t_hosts.insert(f_ip4=ip, f_engineer=1, f_asset_group='vnc')
         db.commit()
         svc_rec = db.t_services.insert(f_hosts_id=host_rec, f_proto='tcp', f_number=port, f_name='vnc')
         db.commit()
         ....:
```

<http://web2py.com/books/default/chapter/29/06/the-database-abstraction-layer>

High-level Database Design

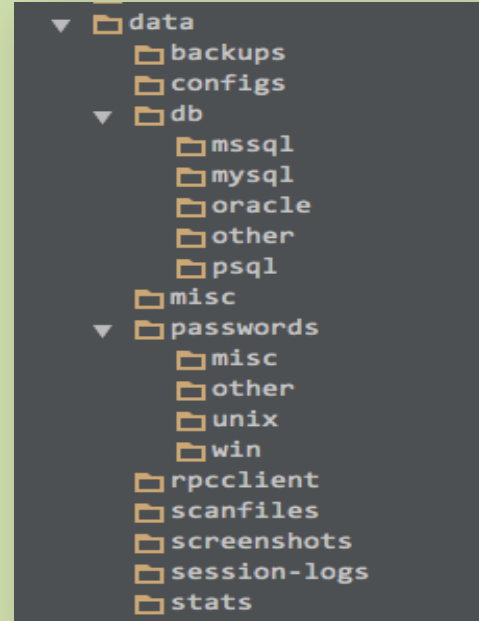


Data Directory Structure

All script output is stored under “data”

Local to the web server

Session-logs/ contain ‘script’ file output from launched terminals



Supported Host/Vulnerability Scanners

Right Now

Nexpose

Nmap

Nessus

Metasploit (hosts only)

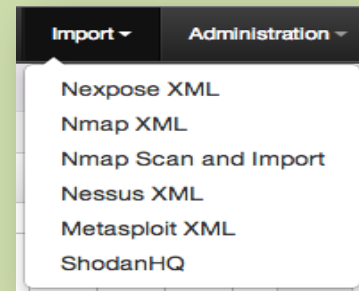
ShodanHQ

Horizon

QualysGuard

Metasploit Pro (Webscan)

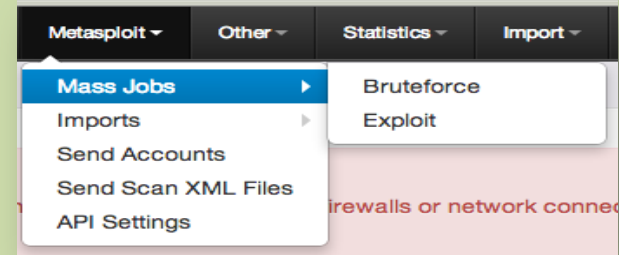
BurpSuite Pro (Report XML)

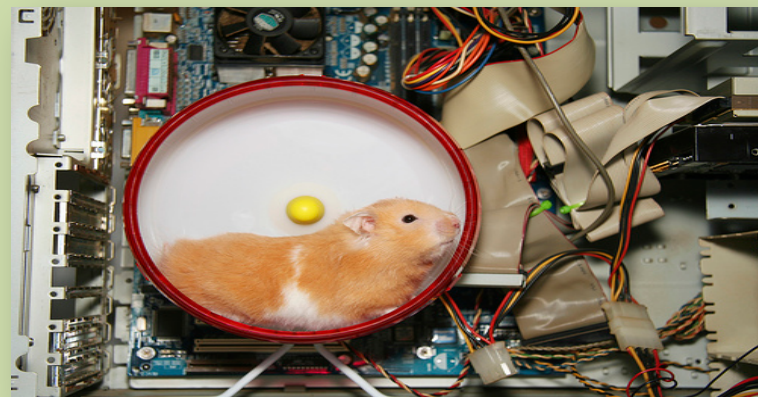


Others?

Metasploit Pro API Integration

- Kvasir utilizes some MSF Pro-only API functions:
 - Bruteforce / Exploit
 - Import XML, PWDUMP, Screenshots
 - Sending Accounts / Scan data results
- TODO:
 - Sending exploits to Framework API
 - Direct MSF DB access (who uses 'pass' as a field name? MSF!)





THE KVASIR WORKFLOW

Installation and setup

<https://github.com/KvasirSecurity/Kvasir/wiki/Installation>

- Kvasir begins life as a completely blank slate
 - You must add users, CPE, Vulndata, Exploits, etc
 - Mostly automated through parts of the UI
- For multiple team members on a test:
 - One central person runs the SQL database
 - All team members have their own Kvasir instance and point to the SQL DB in settings.database_uri

Importing Support Data

- Vulnerability data can be:
 - Imported prior to engagement start
 - Imported as part of a Vulnerability Scan results
- Exploits XML data imported:
 - Nexpose's exploits.xml file
 - ImmunitySec CANVAS download / file
- CPE OS Data
 - Downloaded and parsed from MITRE

Populating Engagement Data

- Vulnerability Scanner Imports
 - Import direct from scanners or files
- Nmap Scanning Imports
 - Import XML output file (-oX)
 - Kick-off a scan and import the results
- Bruteforce/Account Tools
 - THC Hydra
 - Medusa
 - Metasploit creds.csv output
 - PW recovery tool output (John POT, user:password, etc)

Valkyries

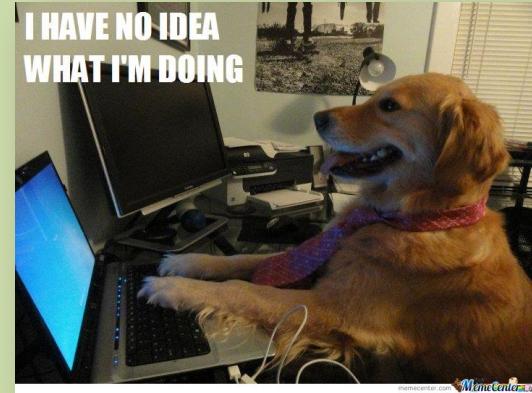
Tasks who results feed back to Kvasir
Not designed to replace Metasploit /
CANVAS / CORE, etc.

WebShot: Grab images of HTTP
instance using phantomjs

VNCShot: Grab images of open VNC
Servers using vncdotool



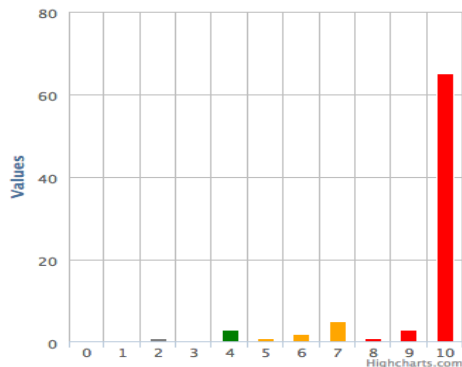
Others planned, just not completed



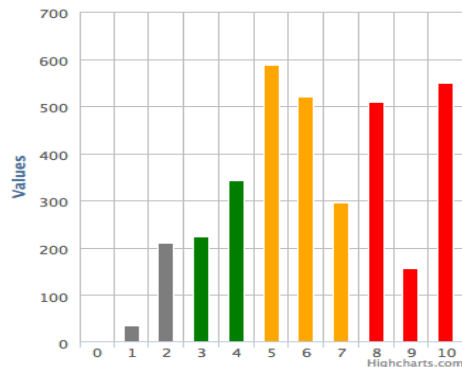
SCREENSHOTS!

Main Index

Top Host Severities



Vulnerabilities by Severity



Summary

Total Hosts	82
Confirmed Hosts	0
Unconfirmed Hosts	82
Accessed Hosts	0
Services/Vulnerabilities	
Total Services	1678
Total Vulnerabilities	3425
Hosts w/ Vulns	81 (98.78%)
Hosts w/ High Vulns (=> 8)	69 (84.15%)
Services w/ Vulns	723
Services w/ High Vulns (=> 8)	1213
Total Accounts	387
Compromised Accounts	37
Passwords	37
Joe Accounts	17

Top Vulnerabilities (8+)

[Show All](#)

[cisco-ios-ftp-multiple-vulns](#)
[cisco-ios-nhrp-bof](#)
[cisco-ios-obsolete-version](#)
[cisco-system-timers-bof](#)
[dns-bind-obsolete](#)
[http-cisco-0002](#)
[http-openssl-dtls-heap-bof](#)
[ipsec-weak-encryption-settings](#)
[oracle-cpu-january-2010-olap](#)
[oracle-missing-apr-2009-cpu](#)
[oracle-missing-july-2009-cpu](#)
[oracle-obsolete-version](#)
[rpc-cmsd-file-overwrite](#)
[sunpatch-119810](#)
[windows-hotfix-ms08-001](#)
[windows-hotfix-ms08-062](#)
[windows-hotfix-ms09-032](#)
[windows-hotfix-ms09-041](#)
[windows-hotfix-ms09-053](#)
[windows-hotfix-ms09-055](#)

Domains Discovered

[SPALAB](#)
[SANDBOX](#)
[SCO_DOMAIN](#)
[TARGETS](#)
[MYGROUP](#)

Host List

+ Add Host ✕ Delete Host ✎ Mark * Mass Actions ↻ Reload Filter: OFF/[All]

Show / hide columns Select Copy CSV Print

Show 50 entries Search:

C	IPv4	IPv6	Services	Vulns	Vuln Graph	Exploits	Hostname	NetBIOS	OS	Engineer	Asset Group
	10.89.172.36		5	6		7			Dell Remote Access Controller	test	tn
	10.89.172.40		8	11		23	WIN2KPROFSP4	WIN2KPROFSP4	Microsoft Windows 2000	test	tn
	10.89.172.41		6	2		6			Microsoft Windows Server 2008	test	tn
	10.89.172.79		36	31		19	sparc9-79		Sun Solaris 7 Sparc	test	tn
	10.89.172.44		32	12		2	VM-NW6SP5	VMNW6SP5	Novell NetWare 6.0.5 x86	test	nexpose
	10.89.172.50		17	56		106	WINXPSP0-50	WINXPSP0-50	Microsoft Windows XP	test	nexpose
	10.89.172.51		17	53		108	WINXPSP1-51	WINXPSP1-51	Microsoft Windows XP SP1	test	nexpose
	10.89.172.52		9	16		33	WINXPSP2-52	WINXPSP2-52	Microsoft Windows XP	test	nexpose
	10.89.172.53		26	49		87	WIN2KADV-53	WIN2KADV-53	Microsoft Windows 2000	test	nexpose
	10.89.172.55		14	17		42	WIN2008-STD	WIN2008-STD	Microsoft Windows Server 2008 Standard Edition	test	nexpose

Host Detail

Terminal launch – click or hot-key L

Flags are hot-keyed: C, D, F

Notes submit after enter

Hot-key: ^N

51
Tabs switch with hot-keys: a, s, v, e, o, t, m, b

10.89.172.51

Confirmed: Accessed: Follow Up:

Assigned to: test | Asset group: nexpose

Filter: OFF/[All]

Notes

Refresh New Win

No data available

Showing 0 to 0 of 0 entries

Hot-key: ^N

aa Services Vulnerabilities Evidence Operating System Accounts SNMP NetBIOS

51

Show 50 entries

Select all Deselect all Copy CSV

Search:

		Pwned	Port	Vuln ID	Sev	CVSS	Status	Exploits	Proof
	edit	<input type="checkbox"/>	tcp/80	http-iis-0061	10	7.5	vulnerable-exploited	Yes (5)	Running vulnerable HTTP service: Microsoft IIS 5.1.
	edit	<input type="checkbox"/>	tcp/80	windows-hotfix-ms09-061	10	7.1	potential	Yes (1)	Running vulnerable HTTP service: Microsoft IIS 5.1.
	edit	<input type="checkbox"/>	tcp/80	windows-hotfix-ms09-062	10	7.1	potential		Running vulnerable HTTP service: Microsoft IIS 5.1.

Services

	edit	10.89.172.36	tcp	80	open	0		HTTP	RAC_ONE_HTTP 1.0
	edit	10.89.172.36	tcp	443	open	4	Yes (1)	HTTPS	RMC Webserver 2.0
	edit	10.89.172.36	tcp	554	open	0		RTSP	
	edit	10.89.172.40 :: WIN2KPROFSP4	info	0	info	8	Yes (19)		

Exploits:	Name	Title	Source	Rank
	MS Windows CanonicalizePathName() Remote Exploit (MS06-040)	2223	exploitdb	Expert
	MS Windows NetplisRemote() Remote Overflow Exploit (MS06-040)	2162	exploitdb	Expert
	MS Windows NetplisRemote() Remote Overflow Exploit (MS06-040) (2k3)	2355	exploitdb	Expert
	Microsoft Server Service NetpwPathCanonicalize Overflow	16367	exploitdb	Expert
	Microsoft Server Service NetpwPathCanonicalize Overflow	exploit/windows/smb/ms06_040_netapi	metasploit	Intermediate
	MS Windows Server Service Code Execution Exploit (MS08-067)	7104	exploitdb	Expert
	MS Windows Server Service Code Execution Exploit (MS08-067) (2k/2k3)	7132	exploitdb	Expert
	MS Windows Server Service Code Execution PoC (MS08-067)	6824	exploitdb	Expert
	Microsoft Server Service Relative Path Stack Corruption	16362	exploitdb	Expert
	Microsoft Server Service Relative Path Stack Corruption	exploit/windows/smb/ms08_067_netapi	metasploit	Novice
	Windows Server Service Underflow (MS08-067)	ms08_067	canvas	Unknown
	MS Windows Mailslot Ring0 Memory Corruption Exploit (MS06-035)	2057	exploitdb	Expert
	Microsoft SRV.SYS Mailslot Write Corruption	auxiliary/dos/windows/smb/ms06_035_mailslot	metasploit	Intermediate
	MS Windows 2K/XP TCP Connection Reset Remote Attack Tool	276	exploitdb	Expert
	Multiple Vendor TCP Sequence Number Approximation Vulnerability (1)	24030	exploitdb	Expert
	Multiple Vendor TCP Sequence Number Approximation Vulnerability (2)	24031	exploitdb	Expert
	Multiple Vendor TCP Sequence Number Approximation Vulnerability (3)	24032	exploitdb	Expert
	Multiple Vendor TCP Sequence Number Approximation Vulnerability (4)	24033	exploitdb	Expert
	TCP Connection Reset Remote Exploit	291	exploitdb	Expert

Vulnerabilities:	dcerpc-ms-netapi-netpathcanonicalize-dos :: windows-hotfix-ms08-067 :: cifs-nt-0002 :: windows-hotfix-ms06-035 :: cifs-acct-password-never-expires :: cifs-acct-password-never-expires :: tcp-seq-num-approximation :: cifs-nt-0001
------------------	---

Accounts

+ Add ✕ Delete ↻ Reload 🗑️ Compromise/Uncompromise 📄 Import File ✍️ Paste File 👤 Show PWDUMP Filter: OFF/[All]

Show / hide columns Select Copy CSV Print

Show entries Search:

Host	Port	Username	Fullname	Domain	Password	Hash 1 Type	Hash 1	Hash 2 Type	Hash 2	UID	GID	Level	Active	Source	Message
10.89.172.203 :: WIN2K3-203	info/0	db2admin			db2admin							ADMIN	true	cifs-db2-default-login	
10.89.172.148 :: URANUS	tcp/1433	sa			sa							ADMIN	true	tds-default-account-sa-sa	
10.89.172.157 :: VENUS	tcp/21	ftp			ftp							ADMIN	true	ftp-generic-0001	
10.89.172.201 :: rh62-oracle	tcp/21	anonymous			joe@							ADMIN	true	ftp-generic-0002	
10.89.172.195 :: WIN2K-195	tcp/21	anonymous			joe@							ADMIN	true	ftp-generic-0002	
10.89.172.151 :: MERCURY	tcp/21	ftp			ftp							ADMIN	true	ftp-generic-0001	
10.89.172.131	tcp/23				cisco							ADMIN	true	telnet-cisco-default-password-cisco	

Windows Domain Memberships

Select a domain:

Show / hide columns Copy CSV Excel PDF Print

Show entries Search:

Host	Domain	Type	Lockout Duration	Shares
10.89.172.142 :: VENUS	WORKGROUP	Workstation	1440	None
10.89.172.143 :: WIN2K3-SP2-VM	WORKGROUP	Workstation	1440	None
10.89.172.148 :: URANUS	WORKGROUP	Workstation	1440	None

Username	Password	Level	Hashes	Source	Port
ftp	ftp	ADMIN	None:None	ftp-generic-0001	tcp/21 (FTP)
anonymous	joe@	ADMIN	None:None	ftp-generic-0002	tcp/21 (FTP)
sa	sa	ADMIN	None:None	tds-default-account-sa-sa	tcp/1433 (TDS)

10.89.172.151 :: MERCURY	WORKGROUP	Workstation	1440	None
10.89.172.152 :: EARTH	WORKGROUP	Workstation	1440	None
10.89.172.153 :: MARS	WORKGROUP	Workstation	1440	None

Evidence (Screenshots, Docs, etc)


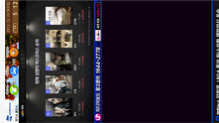


localhost:8000/kvasir/evidence/list

KVASIR Home All Hosts Host Data Tasks Metasploit Other Statistics Import Administration Welcome test

+ Add ✕ Delete ↻ Reload

Select all Deselect all Copy CSV Print

Show 50 entries Search: vnc

	Host	Type	Text	Evidence	File Size
edit	112.148.175.116	Screenshot	VNC Screenshot - 112.148.175.116:5900		1613337b
edit	112.148.54.90	Screenshot	VNC Screenshot - 112.148.54.90:5900		1690017b
edit	112.148.9.154	Screenshot	VNC Screenshot - 112.148.9.154:5900		1575521b
edit	112.149.31.115	Screenshot	VNC Screenshot - 112.149.31.115:5900		2566461b

Password Statistics

[Hashes](#) | [Top Passwords](#) | [Password Stats](#) | [Password Lengths](#) | [Docbook/SPARX Tables](#)

Copy | CSV | Excel | PDF | Print

Show entries Search:

Password	Count
ftp	13
joe@	13
cisco	4
	2
db2admin	1
DBSNMP	1
sa	1
TIGER	1

Vulnerability Statistics

Filter: OFF/[All]

Show 50 entries

Select all Deselect all Copy CSV Print

Search:

Vulnerability ID	Status	Count	Severity	CVSS Score
windows-hotfix-ms08-067	potential	53	10	10.0
kerberos-svc-auth-gss-buffer-overflow	potential	43	10	10.0
windows-hotfix-ms09-048	potential	28	10	7.1
telnet-generic-0006	vulnerable-exploited	22	10	10.0
rpc-rwalld-syslog-format-string-bof	potential	21	10	7.5
rpc-cmsd-0001	potential	21	10	10.0
smtp-sendmail-signal-memory-corruption	potential	21	10	7.6
smtp-sendmail-header-parsing-bof	vulnerable-version	20	10	10.0
smtp-sendmail-header-parsing-bof2	vulnerable-version	20	10	10.0
nfs-statd-suse-string-parsing-vuln	potential	18	10	10.0
rpc-cmsd-file-overwrite	potential	18	10	9.3
nfs-statd-0003	potential	18	10	10.0
xdmcp-dtlogin-double-free	potential	17	10	10.0
windows-hotfix-ms09-061	potential	15	10	7.1
windows-hotfix-ms09-062	potential	15	10	7.1



ON THE HORIZON

Lots to still do...

- Consistent vulnerability database (VulnDB?) that maps to vendor tags (QID, NessusID, Nexpose ID)
- Additional vulnerability scanner support
- Metasploit to release their new MDM structure
- Maltego Integration
- Probably an overhaul of the user interface
- Whatever is in TODO.md that I thought of while sleepless on a 10hr flight back home

<http://github.com/KvasirSecurity/Kvasir>



THANK YOU!