

12.1 Honeybot



★ HoneyBOT - Log_20171004.bin

File View Reports Help

Ports Remotes

Date	Time	Remote IP	Remote Port	Local IP	Local Port	Pr
10/4/2017	8:46:01 PM	169.254.102.21	64373	169.254.102.21	0	T
10/4/2017	8:46:02 PM	169.254.102.21	64375	169.254.102.21	0	T

Command Prompt

```
TCP port 69 (unknown service): LISTENING
TCP port 70 (gopher service): LISTENING
TCP port 71 (unknown service): LISTENING
TCP port 72 (unknown service): LISTENING
TCP port 73 (unknown service): LISTENING
TCP port 74 (unknown service): LISTENING
TCP port 75 (unknown service): LISTENING
TCP port 76 (unknown service): LISTENING
TCP port 77 (unknown service): LISTENING
TCP port 78 (unknown service): LISTENING
TCP port 79 (finger service): LISTENING
TCP port 80 (http service): LISTENING

D:\Users\knewman1\security>time
The current time is: 20:46:11.53
Enter the new time:

D:\Users\knewman1\security>
```

Date	Time	Remote IP	Remote Port	Local IP	Local Port	Pr
10/4/2017	8:46:04 PM	169.254.102.21	64414	169.254.102.21	0	T
10/4/2017	8:46:04 PM	169.254.102.21	64415	169.254.102.21	0	T

69 records | 1345 sockets

8:46 PM 10/4/2017

★ HoneyBOT - Log_20171004.bin

File View Reports Help



Ports	Date	Time	Remote IP	Remote Port	Local IP	Local Port	Protocol	Bytes
Remotes	10/4/2017	8:46:01 PM	169.254.102.21	64372	169.254.102.21	0	TCP	0
	10/4/2017	8:46:01 PM	169.254.102.21	64373	169.254.102.21	0	TCP	0
	10/4/2017	8:46:02 PM	169.254.102.21	64375	169.254.102.21	0	TCP	0
	10/4/2017	8:46:02 PM	169.254.102.21	64376	169.254.102.21	0	TCP	0
	10/4/2017	8:46:02 PM	169.254.102.21	64377	169.254.102.21	0	TCP	0
	10/4/2017	8:46:02 PM	169.254.102.21	64378	169.254.102.21	0	TCP	0
	10/4/2017	8:46:02 PM	169.254.102.21	64379	169.254.102.21	0	TCP	0
	10/4/2017	8:46:02 PM	169.254.102.21	64380	169.254.102.21	0	TCP	0
	10/4/2017	8:46:02 PM	169.254.102.21	64381	169.254.102.21	0	TCP	0
	10/4/2017	8:46:02 PM	169.254.102.21	64382	169.254.102.21	0	TCP	0
	10/4/2017	8:46:02 PM	169.254.102.21	64383	169.254.102.21	0	TCP	0
	10/4/2017	8:46:02 PM	169.254.102.21	64384	169.254.102.21	0	TCP	0
	10/4/2017	8:46:02 PM	169.254.102.21	64385	169.254.102.21	0	TCP	0
	10/4/2017	8:46:02 PM	169.254.102.21	64386	169.254.102.21	0	TCP	0
	10/4/2017	8:46:02 PM	169.254.102.21	64387	169.254.102.21	0	TCP	0
	10/4/2017	8:46:02 PM	169.254.102.21	64388	169.254.102.21	0	TCP	0
	10/4/2017	8:46:02 PM	169.254.102.21	64389	169.254.102.21	0	TCP	0
	10/4/2017	8:46:03 PM	169.254.102.21	64390	169.254.102.21	0	TCP	0
	10/4/2017	8:46:03 PM	169.254.102.21	64391	169.254.102.21	0	TCP	0
	10/4/2017	8:46:03 PM	169.254.102.21	64392	169.254.102.21	0	TCP	0
	10/4/2017	8:46:03 PM	169.254.102.21	64393	169.254.102.21	0	TCP	0
	10/4/2017	8:46:03 PM	169.254.102.21	64396	169.254.102.21	0	TCP	0
	10/4/2017	8:46:03 PM	169.254.102.21	64397	169.254.102.21	0	TCP	0
	10/4/2017	8:46:03 PM	169.254.102.21	64398	169.254.102.21	0	TCP	0
	10/4/2017	8:46:03 PM	169.254.102.21	64399	169.254.102.21	0	TCP	0
	10/4/2017	8:46:03 PM	169.254.102.21	64400	169.254.102.21	0	TCP	0
	10/4/2017	8:46:03 PM	169.254.102.21	64401	169.254.102.21	0	TCP	0
	10/4/2017	8:46:03 PM	169.254.102.21	64402	169.254.102.21	0	TCP	0
	10/4/2017	8:46:03 PM	169.254.102.21	64403	169.254.102.21	0	TCP	0
	10/4/2017	8:46:03 PM	169.254.102.21	64404	169.254.102.21	0	TCP	0
	10/4/2017	8:46:03 PM	169.254.102.21	64405	169.254.102.21	0	TCP	0
	10/4/2017	8:46:03 PM	169.254.102.21	64406	169.254.102.21	0	TCP	0
	10/4/2017	8:46:04 PM	169.254.102.21	64407	169.254.102.21	0	TCP	0
	10/4/2017	8:46:04 PM	169.254.102.21	64408	169.254.102.21	0	TCP	0
	10/4/2017	8:46:04 PM	169.254.102.21	64409	169.254.102.21	0	TCP	0
	10/4/2017	8:46:04 PM	169.254.102.21	64410	169.254.102.21	0	TCP	0
	10/4/2017	8:46:04 PM	169.254.102.21	64411	169.254.102.21	0	TCP	0
	10/4/2017	8:46:04 PM	169.254.102.21	64412	169.254.102.21	0	TCP	0
	10/4/2017	8:46:04 PM	169.254.102.21	64413	169.254.102.21	0	TCP	0
	10/4/2017	8:46:04 PM	169.254.102.21	64414	169.254.102.21	0	TCP	0
	10/4/2017	8:46:04 PM	169.254.102.21	64415	169.254.102.21	0	TCP	0

63 records | 1345 sockets

★ HoneyBOT - Log_20171004.bin

File View Reports Help



Ports	Date	Time	Remote IP	Remote Port	Local IP	Local Port	Protocol	Bytes
Remotes	10/4/2017	8:49:56 PM	0.0.0.0	68	169.254.102.21	67	UDP	300
	10/4/2017	8:50:12 PM	0.0.0.0	68	169.254.102.21	67	UDP	300
	10/4/2017	8:50:39 PM	169.254.102.21	64483	169.254.102.21	21	TCP	144
	10/4/2017	8:50:40 PM	169.254.102.21	64484	169.254.102.21	21	TCP	144
	10/4/2017	8:50:44 PM	0.0.0.0	68	169.254.102.21	67	UDP	300
	10/4/2017	8:50:48 PM	0.0.0.0	68	169.254.102.21	67	UDP	300
	10/4/2017	8:50:56 PM	0.0.0.0	68	169.254.102.21	67	UDP	300
	10/4/2017	8:51:13 PM	0.0.0.0	68	169.254.102.21	67	UDP	300
	10/4/2017	8:51:27 PM	169.254.102.21	64500	169.254.102.21	21	TCP	134
	10/4/2017	8:51:28 PM	169.254.102.21	64501	169.254.102.21	21	TCP	134
	10/4/2017	8:51:29 PM	169.254.102.21	64502	169.254.102.21	21	TCP	134
	10/4/2017	8:51:56 PM	169.254.102.21	64511	169.254.102.21	21	TCP	134
	10/4/2017	8:51:57 PM	169.254.102.21	64512	169.254.102.21	21	TCP	134

★ Packet Log (ftp)

Connection Details:

Date: 10/4/2017
Time: 8:51:27 PM
Millisecond: 726
Time Zone: -5:00
Source IP: 169.254.102.21
Source Port: 64500
Server IP: 169.254.102.21
Server Port: 21 (ftp)
Protocol: TCP

Bytes Sent: 108
Bytes Received: 26

Packet History

Time	Direction	Bytes	Data
8:51:27 PM	RX	0	SYN
8:51:27 PM	TX	41	220 PUBLIC08 FTP Service (Version 5.0).
8:51:27 PM	RX	13	USER Kiauna
8:51:27 PM	TX	35	331 Password required for Kiauna.
8:51:27 PM	RX	13	PASS Newman
8:51:28 PM	TX	32	530 User Kiauna cannot log in.
8:51:28 PM	RX	0	FIN

Packet Data:

View as ☒ text☐ hex

<< < > >>

Advanced IP Scanner

File Actions Settings View Help



169.254.102.21

Example: 192.168.0.1-100, 192.168.0.200

Results

Favorites

Status	Name	IP	Manufacturer	MAC address
>	CYBERUG-61.ad.maryville.edu	169.254.102.21		02:00:4C:4F:50

1 alive, 0 dead, 0 unknown

HoneyBOT - Log_20171009.bin

File View Reports Help

Ports Remotes

Date	Time	Remote IP	Remote Port	Local IP	Local Port	Protocol	Bytes
10/9/2017	2:28:36 PM	169.254.102.21	14521	169.254.102.21	0	TCP	0
10/9/2017	2:28:36 PM	169.254.102.21	14523	169.254.102.21	0	TCP	0
10/9/2017	2:28:36 PM	169.254.102.21	14525	169.254.102.21	0	TCP	0
10/9/2017	2:28:37 PM	169.254.102.21	14528	169.254.102.21	0	TCP	0
10/9/2017	2:28:37 PM	169.254.102.21	14530	169.254.102.21	0	TCP	0
10/9/2017	2:28:37 PM	169.254.102.21	14532	169.254.102.21	0	TCP	0
10/9/2017	2:28:38 PM	169.254.102.21	14535	169.254.102.21	0	TCP	0
10/9/2017	2:28:38 PM	169.254.102.21	14537	169.254.102.21	558	TCP	0
10/9/2017	2:28:38 PM	169.254.102.21	14539	169.254.102.21	0	TCP	0
10/9/2017	2:28:39 PM	169.254.102.21	14541	169.254.102.21	0	TCP	0
10/9/2017	2:28:39 PM	169.254.102.21	14543	169.254.102.21	0	TCP	0
10/9/2017	2:28:39 PM	169.254.102.21	14545	169.254.102.21	0	TCP	0
10/9/2017	2:28:40 PM	169.254.102.21	14547	169.254.102.21	0	TCP	0
10/9/2017	2:28:40 PM	169.254.102.21	14549	169.254.102.21	0	TCP	0
10/9/2017	2:28:40 PM	169.254.102.21	14551	169.254.102.21	0	TCP	0
10/9/2017	2:28:41 PM	169.254.102.21	14553	169.254.102.21	0	TCP	0
10/9/2017	2:28:41 PM	169.254.102.21	14555	169.254.102.21	0	TCP	0
10/9/2017	2:28:41 PM	169.254.102.21	14557	169.254.102.21	0	TCP	0
10/9/2017	2:28:42 PM	169.254.102.21	14559	169.254.102.21	0	TCP	0
10/9/2017	2:28:42 PM	169.254.102.21	14561	169.254.102.21	0	TCP	0
10/9/2017	2:28:42 PM	169.254.102.21	14563	169.254.102.21	0	TCP	0
10/9/2017	2:28:43 PM	169.254.102.21	14566	169.254.102.21	0	TCP	0
10/9/2017	2:28:43 PM	169.254.102.21	14568	169.254.102.21	0	TCP	0
10/9/2017	2:28:43 PM	169.254.102.21	14570	169.254.102.21	0	TCP	0
10/9/2017	2:28:44 PM	169.254.102.21	14572	169.254.102.21	0	TCP	0
10/9/2017	2:28:44 PM	169.254.102.21	14575	169.254.102.21	0	TCP	0
10/9/2017	2:29:01 PM	0.0.0.0	68	169.254.102.21	67	UDP	300
10/9/2017	2:29:06 PM	0.0.0.0	68	169.254.102.21	67	UDP	300
10/9/2017	2:29:13 PM	0.0.0.0	68	169.254.102.21	67	UDP	300
10/9/2017	2:29:29 PM	0.0.0.0	68	169.254.102.21	67	UDP	300

3970 records | 1345 sockets

Nessus Scans Settings

KiaunaNewman / 169.254.102.21

Configure Audit Trail Launch Export

Vulnerabilities 58

Filter Search Vulnerabilities 58 Vulnerabilities

Sev	Name	Family	Count
CRITICAL	DameWare Mini Remote Control Pre-Authentication Remote Overflow	Windows	1
CRITICAL	Kuang2 the Virus Detection	Backdoors	1
CRITICAL	Microsoft Windows 2000 Unsupported Installation Detection	Windows	1
HIGH	FakeBO NetBus Handling Code Remote Overflow	Gain a shell remotely	1
HIGH	MySQL < 3.23.59 / 4.0.21 Multiple Vulnerabilities	Databases	1
HIGH	NetBus 1.x Software Detection	Backdoors	1
MEDIUM	Check Point Firewall-1 Identification	Firewalls	3
MEDIUM	SSL Certificate Cannot Be Trusted	General	2
MEDIUM	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Mid...	Windows	1

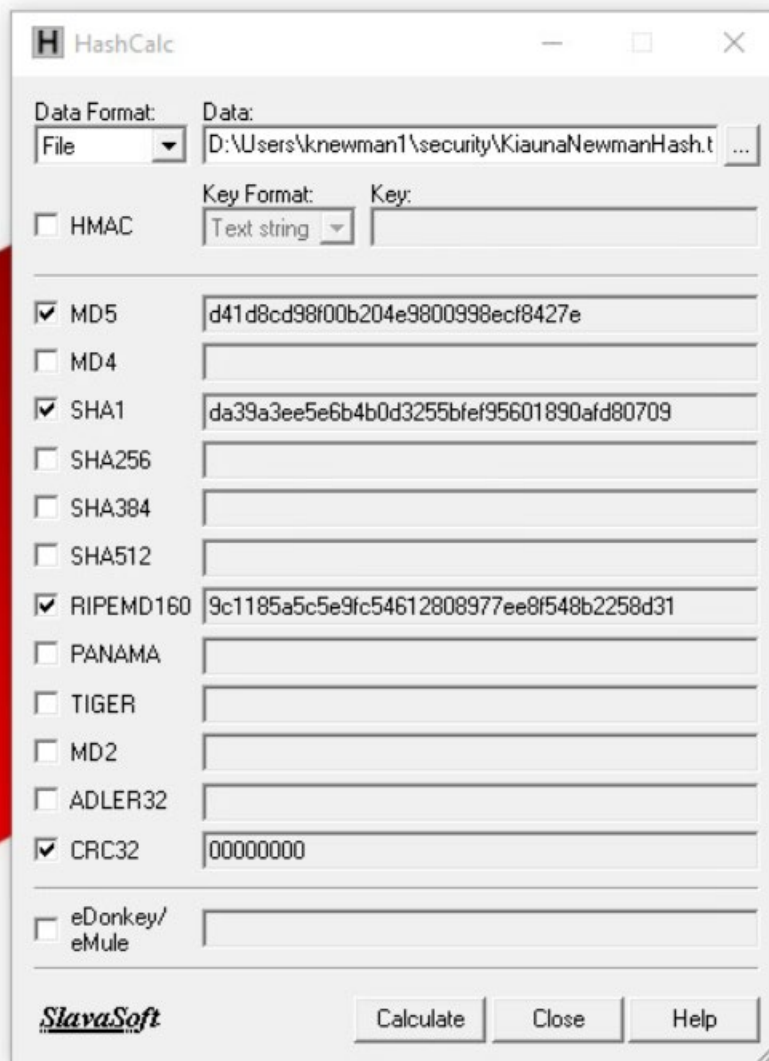
Host Details

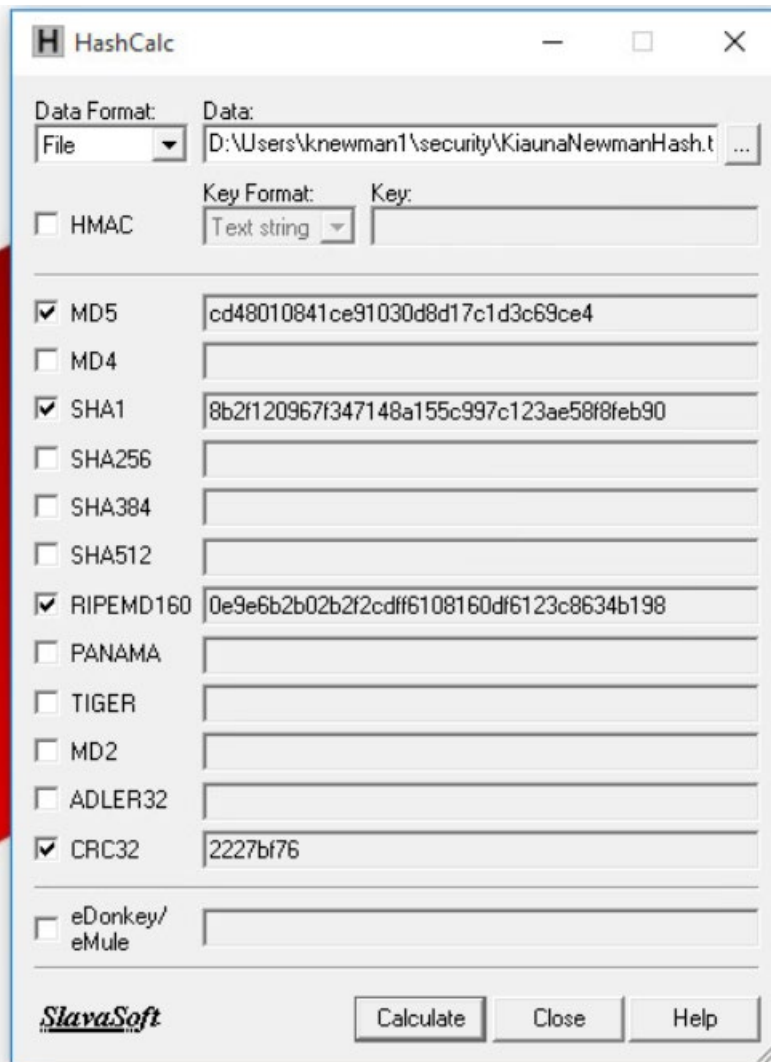
IP: 169.254.102.21
DNS: CYBERUG-61.ad.maryville.edu
MAC: 02:00:4c:4f:4f:50
OS: Microsoft Windows 2000 Server
Start: Today at 1:50 PM
End: Today at 2:28 PM
Elapsed: 38 minutes
KB: Download

Vulnerabilities

Donut chart showing vulnerability distribution: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue).

13.1 HashCALC





13.2 Process Monitor

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help


Time ...	Process Name	PID	Operation	Path	Result	Detail
6:57:4...	SearchIndexer...	4628	FileSystemControlC:		SUCCESS	Control: FSCTL_R...
6:57:4...	SearchIndexer...	4628	FileSystemControlC:		SUCCESS	Control: FSCTL_R...
6:57:4...	VMBlastS.exe	2100	TCP Receive	CYBERUG-61.ad.maryville.edu:22443->...	SUCCESS	Length: 49, sequ...
6:57:4...	VMBlastW.exe	6392	TCP Receive	CYBERUG-61.ad.maryville.edu:18403->...	SUCCESS	Length: 10, sequ...
6:57:4...	VMBlastS.exe	2100	TCP Send	CYBERUG-61.ad.maryville.edu:18416->...	SUCCESS	Length: 10, starti...
6:57:4...	VMBlastS.exe	2100	TCP Receive	CYBERUG-61.ad.maryville.edu:18416->...	SUCCESS	Length: 0, sequ...
6:57:4...	VMBlastS.exe	2100	TCP Receive	CYBERUG-61.ad.maryville.edu:18416->...	SUCCESS	Length: 4653, seq...
6:57:4...	VMBlastW.exe	6392	TCP Send	CYBERUG-61.ad.maryville.edu:18403->...	SUCCESS	Length: 4653, starti...
6:57:4...	VMBlastS.exe	6392	TCP Send	CYBERUG-61.ad.maryville.edu:22443->...	SUCCESS	Length: 4682, starti...
6:57:4...	VMBlastS.exe	2100	TCP Receive	CYBERUG-61.ad.maryville.edu:18416->...	SUCCESS	Length: 0, sequ...
6:57:4...	VMBlastS.exe	2100	TCP Receive	CYBERUG-61.ad.maryville.edu:18416->...	SUCCESS	Length: 2161, seq...
6:57:4...	VMBlastW.exe	6392	TCP Send	CYBERUG-61.ad.maryville.edu:18403->...	SUCCESS	Length: 2161, starti...
6:57:4...	VMBlastS.exe	2100	TCP Send	CYBERUG-61.ad.maryville.edu:22443->...	SUCCESS	Length: 2190, starti...
6:57:4...	VMBlastS.exe	2100	TCP Receive	CYBERUG-61.ad.maryville.edu:22443->...	SUCCESS	Length: 39, sequ...
6:57:4...	VMBlastW.exe	6392	TCP Receive	CYBERUG-61.ad.maryville.edu:18403->...	SUCCESS	Length: 6, sequ...
6:57:4...	VMBlastS.exe	2100	TCP Send	CYBERUG-61.ad.maryville.edu:18416->...	SUCCESS	Length: 6, startime...
6:57:4...	VMBlastS.exe	2100	TCP Receive	CYBERUG-61.ad.maryville.edu:22443->...	SUCCESS	Length: 39, sequ...
6:57:4...	VMBlastW.exe	6392	TCP Receive	CYBERUG-61.ad.maryville.edu:18403->...	SUCCESS	Length: 6, sequ...
6:57:4...	VMBlastS.exe	2100	TCP Send	CYBERUG-61.ad.maryville.edu:18416->...	SUCCESS	Length: 6, startime...
6:57:4...	VMBlastS.exe	2100	TCP Receive	CYBERUG-61.ad.maryville.edu:22443->...	SUCCESS	Length: 53, sequ...
6:57:4...	VMBlastW.exe	6392	TCP Receive	CYBERUG-61.ad.maryville.edu:18403->...	SUCCESS	Length: 14, sequ...
6:57:4...	VMBlastS.exe	2100	TCP Send	CYBERUG-61.ad.maryville.edu:18416->...	SUCCESS	Length: 14, startim...
6:57:4...	VMBlastS.exe	2100	TCP Receive	CYBERUG-61.ad.maryville.edu:18416->...	SUCCESS	Length: 10, sequ...
6:57:4...	VMBlastW.exe	6392	TCP Send	CYBERUG-61.ad.maryville.edu:18403->...	SUCCESS	Length: 10, startim...
6:57:4...	Explorer.EXE	456	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
6:57:4...	Explorer.EXE	456	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
6:57:4...	Explorer.EXE	456	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
6:57:4...	Explorer.EXE	456	RegOpenKey	HKCU\Software\Classes\CLSID\{56AD...}	NAME NOT FOUND	Desired Access: R...
6:57:4...	Explorer.EXE	456	RegOpenKey	HKCR\CLSID\{56AD4C5D-B908-4F85-...	NAME NOT FOUND	Desired Access: R...
6:57:4...	Explorer.EXE	456	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
6:57:4...	Explorer.EXE	456	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
6:57:4...	Explorer.EXE	456	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
6:57:4...	Explorer.EXE	456	RegOpenKey	HKCU\Software\Classes\CLSID\{56AD...}	NAME NOT FOUND	Desired Access: R...
6:57:4...	Explorer.EXE	456	RegOpenKey	HKCR\CLSID\{56AD4C5D-B908-4F85-...	NAME NOT FOUND	Desired Access: R...
6:57:4...	Explorer.EXE	456	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
6:57:4...	Explorer.EXE	456	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
6:57:4...	Explorer.EXE	456	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
6:57:4...	Explorer.EXE	456	RegOpenKey	HKCU\Software\Classes\Applications\...	NAME NOT FOUND	Desired Access: R...
6:57:4...	Explorer.EXE	456	RegOpenKey	HKCR\Applications\Procmon64.exe	NAME NOT FOUND	Desired Access: R...

Showing 14,775 of 126,583 events (11%)

Backed by virtual memory

Process Monitor - Sysinternals: www.sysinternals.com

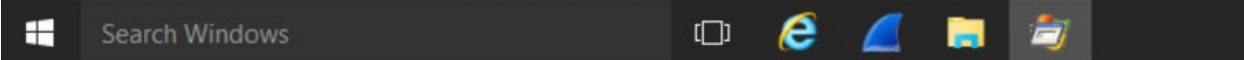
File Edit Event Filter Tools Options Help



Time ...	Process Name	PID	Operation	Path	Result	Detail
6:57:4...	SearchIndexer....	4628	FileSystemControlC:		SUCCESS	Control: FSCTL_R...
6:57:4...	SearchIndexer....	4628	FileSystemControlC:		SUCCESS	Control: FSCTL_R...
6:57:4...	Exp...	456	CloseFile	D:\Users\knewman1\AppData\Local\T...	SUCCESS	CreationTime: 10/5...
6:57:4...	Microsoft Windows Search Indexer			C:\Windows\System32\winevt\Logs\S...	SUCCESS	Offset: 6,098,944, ...
6:57:4...	Microsoft Corporation			C:\Windows\System32\winevt\Logs\S...	SUCCESS	Offset: 6,116,952, ...
6:57:4...	C:\Windows\system32\SearchIndexer.exe					
6:57:4...	vmtoolsd.exe	4896	CreateFile	C:\ProgramData\VMware\VMware Tools	SUCCESS	Desired Access: R...
6:57:4...	vmtoolsd.exe	4896	QueryDirectory	C:\ProgramData\VMware\VMware Tool...	NO SUCH FILE	Filter: tools.conf
6:57:4...	vmtoolsd.exe	4896	CloseFile	C:\ProgramData\VMware\VMware Tools	SUCCESS	
6:57:4...	svchost.exe	888	CreateFile	\\ad.maryville.edu\SysVol\ad.maryville....	SUCCESS	Desired Access: G...
6:57:4...	svchost.exe	888	ReadFile	\\ad.maryville.edu\SysVol\ad.maryville....	SUCCESS	Offset: 0, Length: 5...
6:57:4...	svchost.exe	888	ReadFile	\\ad.maryville.edu\SysVol\ad.maryville....	SUCCESS	Offset: 0, Length: 5...
6:57:4...	svchost.exe	888	CloseFile	\\ad.maryville.edu\SysVol\ad.maryville....	SUCCESS	
6:57:4...	svchost.exe	888	CreateFile	\\ad.maryville.edu\SysVol\ad.maryville....	SUCCESS	Desired Access: G...
6:57:4...	Explorer.EXE	456	CloseFile	D:\Users\knewman1\AppData\Local\...	SUCCESS	
6:57:4...	Explorer.EXE	456	CloseFile	D:\Users\knewman1\AppData\Local\...	SUCCESS	
6:57:4...	Explorer.EXE	456	CloseFile	D:\Users\knewman1\AppData\Local\...	SUCCESS	
6:57:4...	Explorer.EXE	456	CloseFile	D:\Users\knewman1\AppData\Local\...	SUCCESS	
6:57:4...	svchost.exe	888	ReadFile	\\ad.maryville.edu\SysVol\ad.maryville....	SUCCESS	Offset: 0, Length: 6...
6:57:4...	svchost.exe	888	ReadFile	\\ad.maryville.edu\SysVol\ad.maryville....	SUCCESS	Offset: 0, Length: 6...
6:57:4...	svchost.exe	888	CloseFile	\\ad.maryville.edu\SysVol\ad.maryville....	SUCCESS	
6:57:4...	svchost.exe	888	CreateFile	\\ad.maryville.edu\sysvol\ad.maryville.e...	SUCCESS	Desired Access: G...
6:57:4...	svchost.exe	888	ReadFile	\\ad.maryville.edu\sysvol\ad.maryville.e...	SUCCESS	Offset: 0, Length: 2...
6:57:4...	svchost.exe	888	ReadFile	\\ad.maryville.edu\sysvol\ad.maryville.e...	SUCCESS	Offset: 0, Length: 2...
6:57:4...	svchost.exe	888	CloseFile	\\ad.maryville.edu\sysvol\ad.maryville.e...	SUCCESS	
6:57:4...	svchost.exe	888	CreateFile	\\ad.maryville.edu\SysVol\ad.maryville....	SUCCESS	Desired Access: G...
6:57:4...	svchost.exe	888	ReadFile	\\ad.maryville.edu\SysVol\ad.maryville....	SUCCESS	Offset: 0, Length: 6...
6:57:4...	svchost.exe	888	ReadFile	\\ad.maryville.edu\SysVol\ad.maryville....	SUCCESS	Offset: 0, Length: 6...
6:57:4...	svchost.exe	888	CloseFile	\\ad.maryville.edu\SysVol\ad.maryville....	SUCCESS	
6:57:4...	svchost.exe	888	CreateFile	\\ad.maryville.edu\SysVol\ad.maryville....	SUCCESS	Desired Access: G...
6:57:4...	svchost.exe	888	ReadFile	\\ad.maryville.edu\SysVol\ad.maryville....	SUCCESS	Offset: 0, Length: 2...
6:57:4...	svchost.exe	888	ReadFile	\\ad.maryville.edu\SysVol\ad.maryville....	SUCCESS	Offset: 0, Length: 2...
6:57:4...	svchost.exe	888	CloseFile	\\ad.maryville.edu\SysVol\ad.maryville....	SUCCESS	
6:57:4...	svchost.exe	888	CreateFile	C:\Windows\System32\GroupPolicy	SUCCESS	Desired Access: R...
6:57:4...	svchost.exe	888	QueryNetwork...	C:\Windows\System32\GroupPolicy	SUCCESS	CreationTime: 7/10...
6:57:4...	svchost.exe	888	CloseFile	C:\Windows\System32\GroupPolicy	SUCCESS	
6:57:4...	svchost.exe	888	CreateFile	C:\Windows\System32\GroupPolicy\gp...	SUCCESS	Desired Access: G...
6:57:4...	svchost.exe	888	LockFile	C:\Windows\System32\GroupPolicy\gp...	SUCCESS	Exclusive: False, O...
6:57:4...	svchost.exe	888	QueryStandardl...	C:\Windows\System32\GroupPolicy\gp...	SUCCESS	AllocationSize: 240...
6:57:4...	svchost.exe	888	ReadFile	C:\Windows\System32\GroupPolicy\gp...	SUCCESS	Offset: 0, Length: 2...

Showing 1,523 of 126,583 events (1.2%) Backed by virtual memory

Search Windows

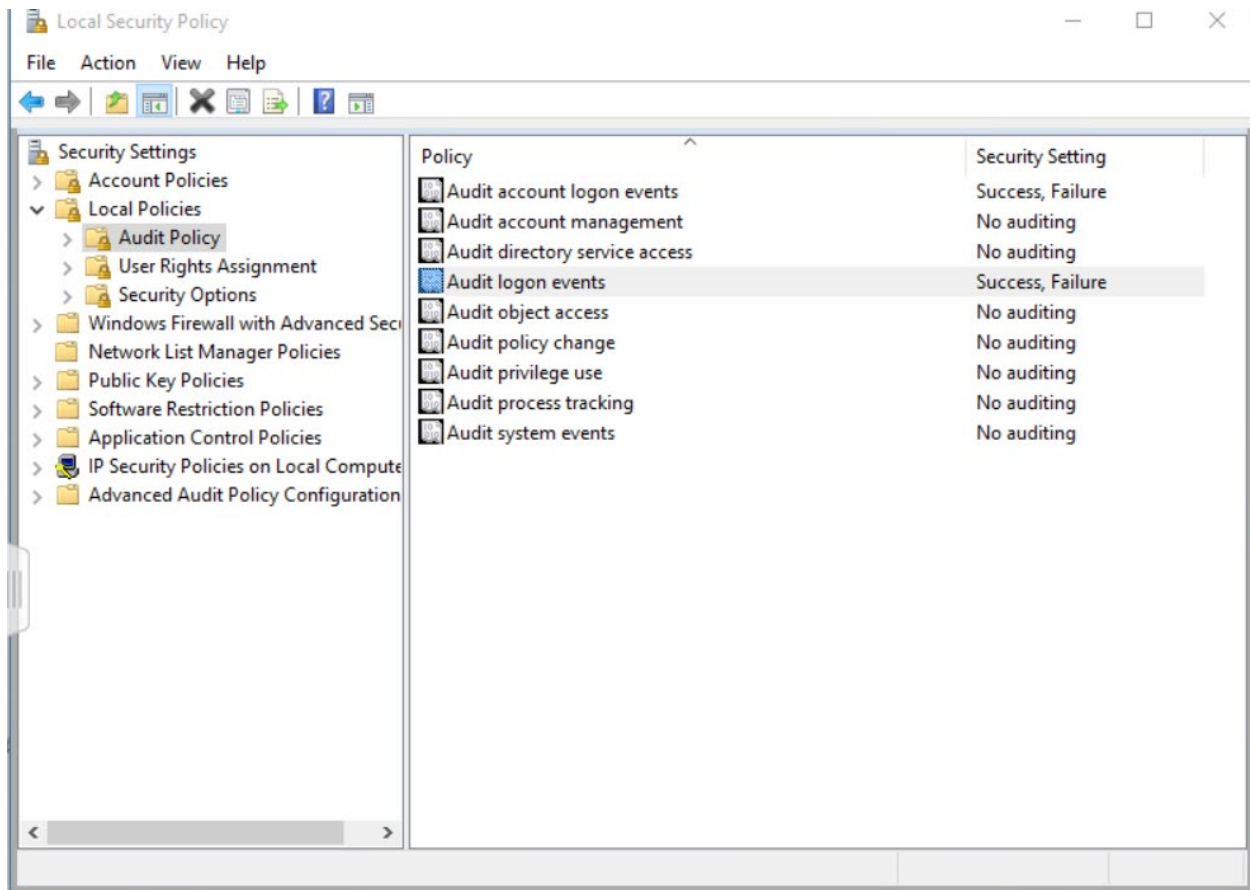


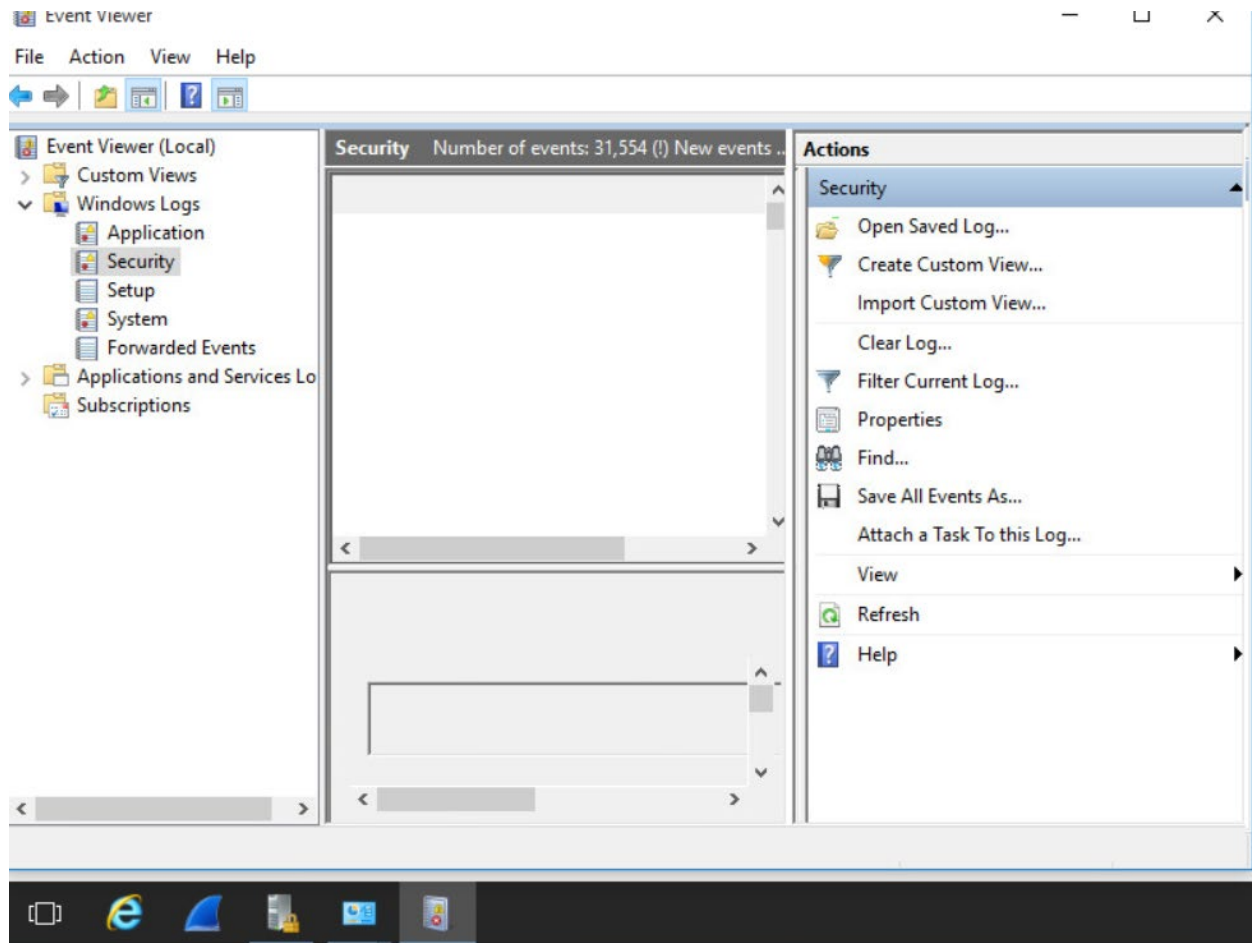
7:05:2...	IEXPLORE.EXE	6264	CreateFile	C:\Windows\SysWOW64\ole32.dll	SUCCESS	Desired Access: R...
7:05:2...	IEXPLORE.EXE	6264	QueryBasicInfor...	C:\Windows\SysWOW64\ole32.dll	SUCCESS	CreationTime: 5/17...
7:05:2...	IEXPLORE.EXE	6264	CloseFile	C:\Windows\SysWOW64\ole32.dll	SUCCESS	
7:05:2...	IEXPLORE.EXE	6264	CreateFile	C:\Windows\SysWOW64\winsta.dll	SUCCESS	Desired Access: R...
7:05:2...	IEXPLORE.EXE	6264	QueryBasicInfor...	C:\Windows\SysWOW64\winsta.dll	SUCCESS	CreationTime: 7/10...
7:05:2...	IEXPLORE.EXE	6264	CloseFile	C:\Windows\SysWOW64\winsta.dll	SUCCESS	
7:05:2...	IEXPLORE.EXE	6264	CreateFile	C:\Windows\SysWOW64\winsta.dll	SUCCESS	Desired Access: R...
7:05:2...	IEXPLORE.EXE	6264	CreateFileMapp...	C:\Windows\SysWOW64\winsta.dll	FILE LOCKED WI...	SyncType: SyncTy...
7:05:2...	IEXPLORE.EXE	6264	QueryStandardl...	C:\Windows\SysWOW64\winsta.dll	SUCCESS	AllocationSize: 262...
7:05:2...	IEXPLORE.EXE	6264	CreateFileMapp...	C:\Windows\SysWOW64\winsta.dll	SUCCESS	SyncType: SyncTy...
7:05:2...	IEXPLORE.EXE	6264	CloseFile	C:\Windows\SysWOW64\winsta.dll	SUCCESS	
7:05:2...	IEXPLORE.EXE	6264	CreateFile	C:\Windows\SysWOW64\winsta.dll	SUCCESS	Desired Access: R...
7:05:2...	IEXPLORE.EXE	6264	QueryBasicInfor...	C:\Windows\SysWOW64\winsta.dll	SUCCESS	CreationTime: 7/10...
7:05:2...	IEXPLORE.EXE	6264	CloseFile	C:\Windows\SysWOW64\winsta.dll	SUCCESS	
7:05:2...	IEXPLORE.EXE	6264	CreateFile	C:\Windows\SysWOW64\winsta.dll	SUCCESS	Desired Access: R...
7:05:2...	IEXPLORE.EXE	6264	CreateFileMapp...	C:\Windows\SysWOW64\winsta.dll	FILE LOCKED WI...	SyncType: SyncTy...
7:05:2...	IEXPLORE.EXE	6264	QueryStandardl...	C:\Windows\SysWOW64\winsta.dll	SUCCESS	AllocationSize: 262...
7:05:2...	IEXPLORE.EXE	6264	CreateFileMapp...	C:\Windows\SysWOW64\winsta.dll	SUCCESS	SyncType: SyncTy...
7:05:2...	IEXPLORE.EXE	6264	CloseFile	C:\Windows\SysWOW64\winsta.dll	SUCCESS	
7:05:2...	IEXPLORE.EXE	6264	CreateFile	C:\Windows\SysWOW64\winsta.dll	SUCCESS	Desired Access: R...
7:05:2...	IEXPLORE.EXE	6264	QueryBasicInfor...	C:\Windows\SysWOW64\winsta.dll	SUCCESS	CreationTime: 7/10...
7:05:2...	IEXPLORE.EXE	6264	CloseFile	C:\Windows\SysWOW64\winsta.dll	SUCCESS	
7:05:2...	IEXPLORE.EXE	6264	CreateFile	C:\Windows\SysWOW64\winsta.dll	SUCCESS	Desired Access: R...
7:05:2...	IEXPLORE.EXE	6264	CreateFileMapp...	C:\Windows\SysWOW64\winsta.dll	FILE LOCKED WI...	SyncType: SyncTy...
7:05:2...	IEXPLORE.EXE	6264	QueryStandardl...	C:\Windows\SysWOW64\winsta.dll	SUCCESS	AllocationSize: 262...
7:05:2...	IEXPLORE.EXE	6264	CreateFileMapp...	C:\Windows\SysWOW64\winsta.dll	SUCCESS	SyncType: SyncTy...
7:05:2...	IEXPLORE.EXE	6264	CloseFile	C:\Windows\SysWOW64\winsta.dll	SUCCESS	
7:05:2...	IEXPLORE.EXE	6264	CreateFile	C:\Windows\SysWOW64\winsta.dll	SUCCESS	Desired Access: R...
7:05:2...	IEXPLORE.EXE	6264	QueryBasicInfor...	C:\Windows\SysWOW64\winsta.dll	SUCCESS	CreationTime: 7/10...
7:05:2...	IEXPLORE.EXE	6264	CloseFile	C:\Windows\SysWOW64\winsta.dll	SUCCESS	
7:05:2...	IEXPLORE.EXE	6264	CreateFile	C:\Windows\SysWOW64\winsta.dll	SUCCESS	Desired Access: R...

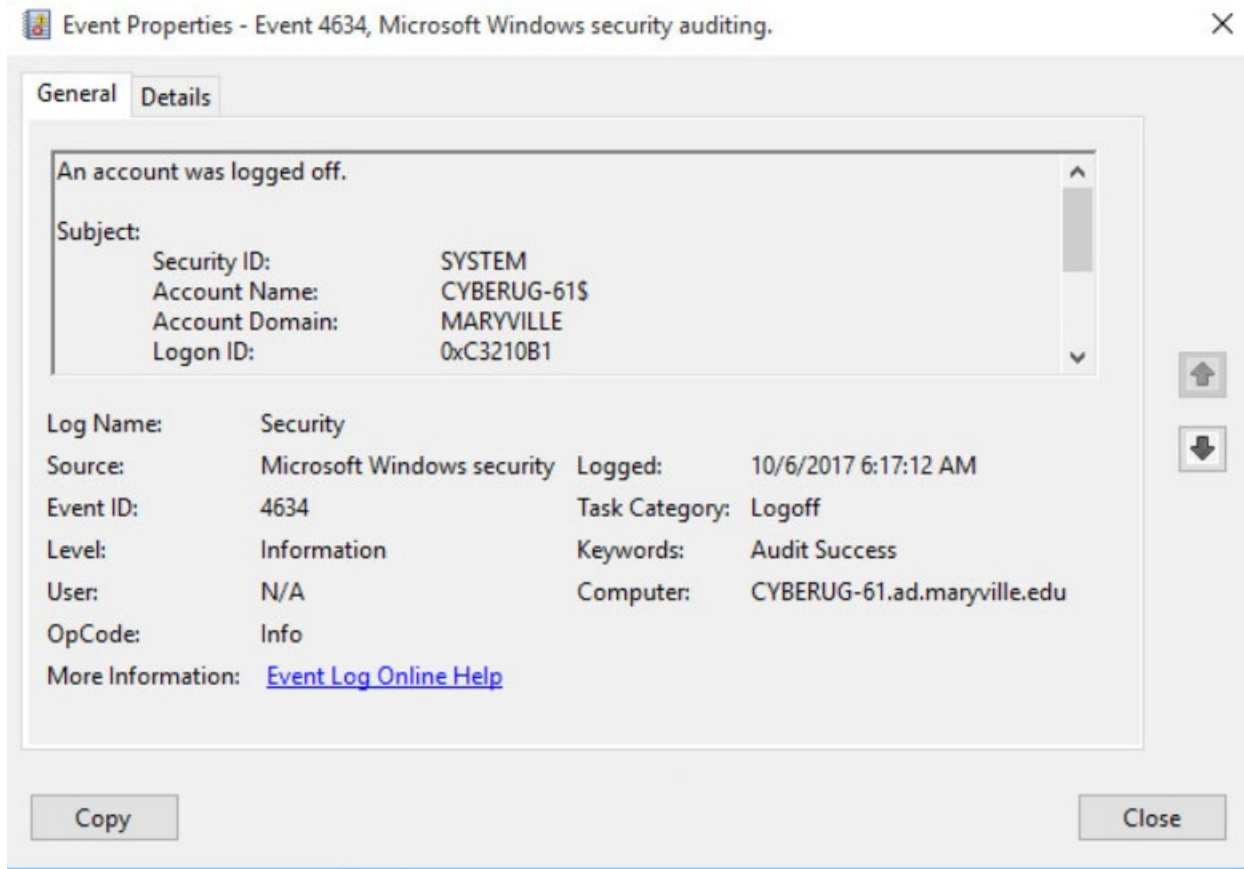
Showing 21,504 of 288,161 events (7.4%)

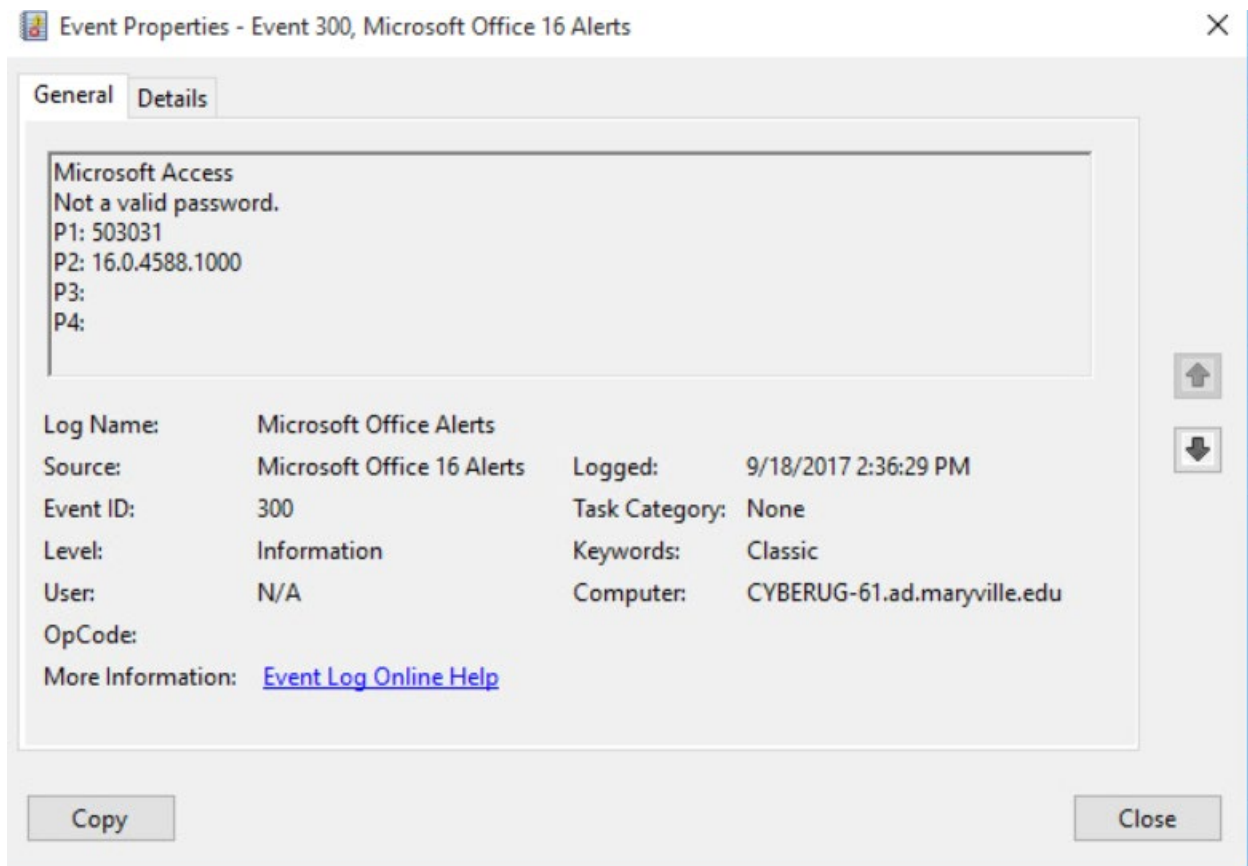
Backed by virtual memory

13.4 Windows Event Viewer

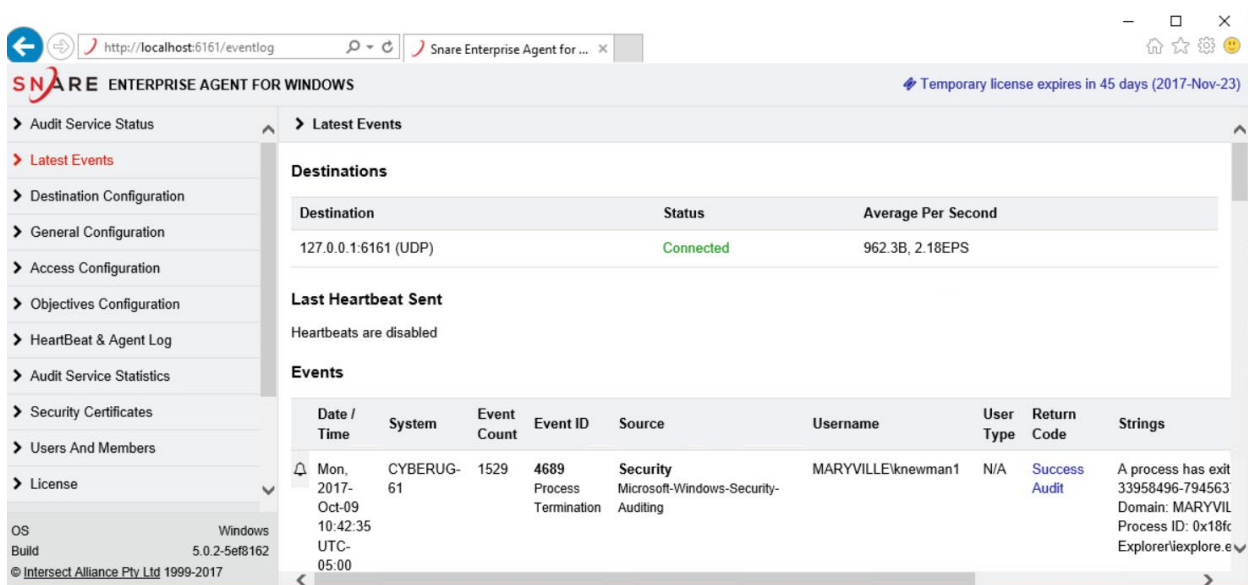








13.5 Snare



Microsoft Windows [Version 10.0.10586.176]
(c) 2015 Microsoft Corporation
D:\Users\knewman1>

Snare Enterprise Agent for Windows

Temporary license expires in 45 days (2017-Nov-23)

Latest Events

Destinations

Destination	Status	Average Per Second
127.0.0.1:6161 (UDP)	Connected	690.6B, 1.71EPS

Last Heartbeat Sent

Heartbeats are disabled

Events

Date / Time	System	Event Count	Event ID	Source	Username	User Type	Return Code	Strings
Mon, 2017-Oct-09 10:44:13 UTC	CYBERUG-61	1769	8004	Microsoft-Windows-GroupPolicy/Operational	NT AUTHORITY\SYSTEM	N/A	Information	Completed manual MARYVILLE\CYBE

OS: Windows
Build: 5.0.2-5efb162
© Intersect Alliance Pty Ltd 1999-2017