LAMPIRAN A

SOURCE CODE REGISTRY WSUS

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate]

"ElevateNonAdmins"=dword:00000001

"WUServer"="http://wsus-server.maranatha.edu"

"WUStatusServer"="http://wsus-server.maranatha.edu"

"TargetGroupEnabled"=dword:00000001

"TargetGroup"="unjoindomain"

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU]

"NoAutoUpdate"=dword:00000000

"AUOptions"=dword:00000004

"ScheduledInstallDay"=dword:00000000

"ScheduledInstallTime"=dword:0000000c

"NoAUShutdownOption"=dword:00000000

"NoAUAsDefaultShutdownOption"=dword:00000000

"UseWUServer"=dword:00000001

"RescheduleWaitTimeEnabled"=dword:00000001

"RescheduleWaitTime"=dword:00000001

"NoAutoRebootWithLoggedOnUsers"=dword:00000001

"DetectionFrequencyEnabled"=dword:00000001

"DetectionFrequency"=dword:00000008

"AutoInstallMinorUpdates"=dword:00000001

"RebootWarningTimeoutEnabled"=dword:00000000

"RebootRelaunchTimeoutEnabled"=dword:00000001

"RebootRelaunchTimeout"=dword:0000001e

LAMPIRAN B

SNORT RULES

RULES ICMP

alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP ISS Pinger"; itype:8; content:"ISSPNGRQ"; depth:32; reference:arachnids,158; classtype:attempted-recon; sid:465; rev:4;)

alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP L3retriever Ping"; icode:0; itype:8; content:"ABCDEFGHIJKLMNOPQRSTUVWABCDEFGHI"; depth:32; reference:arachnids,311; classtype:attempted-recon; sid:466; rev:5;)

alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Nemesis v1.1 Echo"; dsize:20; icmp_id:0; icmp_seq:0; itype:8; content:"|00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00|"; reference:arachnids,449; classtype:attempted-recon; sid:467; rev:4;)

alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP PING NMAP"; dsize:0; itype:8; reference:arachnids,162; classtype:attempted-recon; sid:469; rev:4;)

alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP icmpenum v1.1.1"; dsize:0; icmp_id:666 ; icmp_seq:0; id:666; itype:8; reference:arachnids,450; classtype:attempted-recon; sid:471; rev:4;)

alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP redirect host"; icode:1; itype:5; reference:arachnids,135; reference:cve,1999-0265; classtype:bad-unknown; sid:472; rev:5;)

alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP redirect net"; icode:0; itype:5; reference:arachnids,199; reference:cve,1999-0265; classtype:bad-unknown; sid:473; rev:5;)

alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP superscan echo"; dsize:8; itype:8; content:"|00 00 00 00 00 00 00 00|"; classtype:attempted-recon; sid:474; rev:5;)

alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP traceroute ipopts"; ipopts:rr; itype:0; reference:arachnids,238; classtype:attempted-recon; sid:475; rev:4;)

alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP webtrends scanner"; icode:0; itype:8; content:"|00 00 00 00|EEEEEEEEEEEE"; reference:arachnids,307; classtype:attempted-recon; sid:476; rev:5;)

alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Source Quench"; icode:0; itype:4; classtype:bad-unknown; sid:477; rev:3;)

alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Broadscan Smurf Scanner"; dsize:4; icmp_id:0; icmp_seq:0; itype:8; classtype:attempted-recon; sid:478; rev:4;)

alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP PING speedera"; itype:8; content:"89|3A 3B|<=>?"; depth:100; classtype:misc-activity; sid:480; rev:6;)

alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP TJPingPro1.1Build 2 Windows"; itype:8; content:"TJPingPro by Jim"; depth:32; reference:arachnids,167; classtype:misc-activity; sid:481; rev:6;)

alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP PING WhatsupGold Windows"; itype:8; content:"WhatsUp - A Netw"; depth:32; reference:arachnids,168; classtype:misc-activity; sid:482; rev:6;)

alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP PING CyberKit 2.2 Windows"; itype:8; content:"|AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA|"; depth:32; reference:arachnids,154; classtype:misc-activity; sid:483; rev:6;)

alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP PING Sniffer Pro/NetXRay network scan"; itype:8; content:"Cinco Network, Inc."; depth:32; classtype:misc-activity; sid:484; rev:5;)

alert icmp any any -> any any (msg:"ICMP Destination Unreachable Communication Administratively Prohibited"; icode:13; itype:3; classtype:misc-activity; sid:485; rev:5;)

alert icmp any any -> any any (msg:"ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited"; icode:10; itype:3; classtype:misc-activity; sid:486; rev:5;)

alert icmp any any -> any any (msg:"ICMP Destination Unreachable Communication with Destination Network is Administratively Prohibited"; icode:9; itype:3; classtype:misc-activity; sid:487; rev:5;)

alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP digital island bandwidth query"; content:"mailto|3A|ops@digisle.com"; depth:22; classtype:misc-activity; sid:1813; rev:6;)

alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP PATH MTU denial of service"; itype:3; icode:4; byte_test:2,<,576,2; reference:bugtraq,13124; reference:cve,2004-1060; classtype:attempted-dos; sid:3626; rev:4;)