



Desk 211 Course Sheet

Malware Prevention and Endpoint Security Management

Description:

The 2-hour, self-paced online course covers management tools to protect desktop system integrity to mitigate threats such as viruses, spyware and malicious attacks. You will learn about common threats to desktops and some of the prominent desktop security tools. Key topics include firewalls, antivirus, antispyware, intrusion detection and prevention, and peripheral device management.

Prerequisite: Employment in an ITS capacity within the MnSCU system.

Location/Delivery Format: Online, Self-paced

<i>Topic</i>	<i>Outcomes</i>	<i>Method</i>	<i>Time</i>
Introduction	<ul style="list-style-type: none">• Introduce concepts and overview of antivirus, anti-spyware, firewall, intrusion prevention system and device control• Describe the need for endpoint security and the types of tools available	Presentation	
Commonly used tools	<ul style="list-style-type: none">• Symantec Endpoint Protection – AV, Anti-spyware, Firewall, IPS, Device Control	Presentation Demo #1	
	<ul style="list-style-type: none">• Windows Defender	Presentation Demo #2	
	<ul style="list-style-type: none">• Malwarebytes' Anti-Malware	Presentation Demo #3	
	<ul style="list-style-type: none">• SpyBot S&D	Presentation Demo #4	
	<ul style="list-style-type: none">• Clam AV	Presentation Demo #5	
	<ul style="list-style-type: none">• Pslist, filemon, portmon, process monitor, pstools, regmon	Presentation Demo #6	
	<ul style="list-style-type: none">• Silent runners	Presentation Demo #7	
	<ul style="list-style-type: none">• Windows FW	Presentation Demo #8	
	<ul style="list-style-type: none">• Morro – code name for upcoming MS AV and antimalware software.	Presentation Demo #9	
Assessment	<ul style="list-style-type: none">• Quiz on the key concepts related to endpoint security and key features of commonly used tools	Quiz	



Ncip 101 Course Sheet

Vulnerability Management & Reporting using nCircle

Description:

This 2-hour, self-paced online course introduces you to the nCircle IP360 vulnerability management tool. You will learn how to configure and manage IP360. The course will introduce vulnerability management concepts, administering IP360, and how to generate vulnerability reports on assets.

Prerequisite: Employment in an ITS capacity within the MnSCU system and have permission to use IP360 at your institution.

Location/Delivery Format: Online, Self-paced

Topic	Outcomes	Method	Time
Introduction	Introduce nCircle IP360 background, technology, architecture and terminology used within product documentation and this course. <ul style="list-style-type: none">• Scanning – Authenticated or not• Assets and Vulnerability v. Risk v. Threat v. Exploit• Reporting, Mitigation, and Remediation	Presentation	
Assessment		Quiz	5 mins
Networks	Configuring networks and network groups	Presentation	
Scanning	<ul style="list-style-type: none">• Configuring, scheduling and customizing scans• Scan-on-demand• Scan History	Presentation	
Set up a network and a scan	Video, demo/test system, or user's own login in production	Demo	
Assessment		Quiz	5 mins
Reports	The three primary reporting types in IP360 <ul style="list-style-type: none">• Differential• Time-frame• Distinct Audit Vulnerability Scores and Asset Values	Presentation	
Review a distinct audit report		Demo	
Reporting Filters	Reporting filters and illustration of usage	Presentation & Demo	
Focus Interface	Searching with the Focus Interface vs. Reporting	Presentation & Demo	
Respond & Administer	Notifications via the Respond interface Personal Options and Resetting Passwords	Presentation	
Support & Administrivia	Support resources available to users.	Presentation	
Assessment		Quiz	5 mins



NETW 211 Course Sheet

Hardening Network Devices

Description:

The 2-hour, self-paced course covers hardening procedures for network devices. You will learn general network device hardening principles. You will also learn how to harden Cisco routers and switches.

Recommended Prerequisites or previous knowledge: NETW 101, NETW 111, Employment in an ITS capacity within the MnSCU system.

Location/Delivery Format: Online, Self-paced

Topic	Outcomes	Method	Time
Intro to Hardening	<ul style="list-style-type: none">• Why harden, what do we mean by “hardening,”	Presentation	10 min
General principles	<ul style="list-style-type: none">• General principles of hardening—remove unnecessary services, keep software up to date, limit access to the device, etc. (SSH & AAA review)	Presentation	10 min
Quiz 1			
Common Unnecessary Services	<ul style="list-style-type: none">• Description of unnecessary services that are often on network devices but not needed	Presentation	10 min
Configuring Cisco devices to remove unnecessary services	<ul style="list-style-type: none">• How to configure Cisco devices to remove the services just discussed	Presentation & Demo	15 min
Quiz 2			
Hardening with ACLs	<ul style="list-style-type: none">• Using ACLs to limit access to a network device, w/ Cisco configuration	Presentation & Demo	15 min
Quiz 3	<ul style="list-style-type: none">•		
Configuration Management	<ul style="list-style-type: none">• SVN/CVS Config Management• Documentation and Commenting	Presentation & Example	20 min
Quiz 4			
Auditing and Testing	<ul style="list-style-type: none">• Example of auditing and testing – using example tools – i.e. Red Seal, RAT - Auditing	Presentation and Demo	20 min
Quiz 5			



Serv221 Course Sheet

Intrusion Detection, Prevention, and File Integrity Monitoring

Description:

The 2-hour, self-paced online course introduces intrusion detection, intrusion prevention and file integrity monitoring. You will learn about network- and host-based tools most commonly used to monitor system integrity and detect & prevent intrusions. The course will introduce many tools and software packages available to implement IDS and IPS at your institution. You will learn specifically about Snort and Cisco-based IDS/IPS implementations. You will also learn more about specific host-based software: a file integrity monitoring program called Tripwire and an intrusion detection package called OSSEC.

Prerequisite: Employment in an ITS capacity within the MnSCU system.

Location/Delivery Format: Online, Self-paced

Topic	Outcomes	Method	Time
Introduction	<ul style="list-style-type: none">• Introduce concepts and overview of intrusion detection, intrusion prevention and file integrity monitoring• Describe the benefits of IDS/IPS and file integrity monitoring	Presentation	
Intrusion Detection / Prevention	<ul style="list-style-type: none">• Snort	Presentation & Demo #1	
	<ul style="list-style-type: none">• Cisco NIDS/NIPS, HIDS, ASA/PIX, IOS switching and routing	Presentation & Demo #2	
	<ul style="list-style-type: none">• Endian Firewall	Presentation & Demo #3	
	<ul style="list-style-type: none">• Samhain HIDS	Presentation & Demo #4	
	<ul style="list-style-type: none">• Osiris HIDS	Presentation & Demo #5	
	<ul style="list-style-type: none">• Tripwire HIDS	Presentation & Demo #6	
	<ul style="list-style-type: none">• Aide HIDS	Presentation & Demo #7	
	<ul style="list-style-type: none">• OSSEC HIDS	Presentation & Demo #8	
	<ul style="list-style-type: none">• Bro NIDS	Presentation & Demo #9	
	<ul style="list-style-type: none">• Untangle NIDS	Presentation & Demo #10	
File integrity monitoring	<ul style="list-style-type: none">• Tripwire	Presentation & Demo #11	
Assessment	Quiz on the key concepts related to IDS/IPS, file integrity monitoring, and key features of commonly used tools	Quiz	



Serv321 Course Sheet

Advanced Server Management via Scripting and Directory Services

Description:

The 3-hour, self-paced online course introduces advanced system management techniques using scripting facilities and other technologies. You will learn about scripting tools, languages, and freely available third-party utilities commonly used to manage Windows, UNIX & LINUX operating systems. The course will introduce shells including PowerShell and BASH. You will learn about: creating basic scripts to manage files, processes and permissions; using scripting languages like Perl, Python and VBScript; and languages built into each shell. You will also learn about version control and system management.

Prerequisite: Employment in an ITS capacity within the MnSCU system.

Location/Delivery Format: Online, Self-paced

Topic	Outcomes	Method	Time
Introduction	<ul style="list-style-type: none"> Goals Concepts What can done with scripts and version control tools - advantages 	Presentation	
Windows scripting and management	PowerShell , Cmd , Group Policy, WMI, VBScript, WinRM , Cygwin, Sys Internals, Python/PERL	Presentation	
PowerShell & Cmd.exe	PowerShell, PowerShell ISE, Common Utilities	Presentation	
Demo #1 Cmd & PowerShell	Example scripts & Windows operations using PowerShell	Demo	
Quiz #1		Quiz	
Active Directory	Managing Servers with Group Policy Objects, Active Directory, and WScript	Presentation	
Demo #2 WScript		Demo	
Quiz #2		Quiz	
UNIX & LINUX	Solaris, OS X, Ubuntu – BASH, system utilities, Common Utilities sed awk cut paste basename dirname find test ("[" head tail logger ps (-o) comm	Presentation	
Demo #3 UNIX & LINUX tools	Example scripts & LINUX operations using BASH	Demo	
Quiz #3		Quiz	
Version Control and system management	Revision control, deployments, standards, auditing, and backups; Expect , Puppet , MultiSSH ,	Presentation	
Demo #4 Version control and system management tools		Demo	
Quiz #4		Quiz	